# When Technology Meets Humanity

## Fostering peace, equality, and prosperity in the digital era

White Paper and Policy Toolkit

Jovan Kurbalija

*Draft Version (9 December 2021)*

DiPLO

# Impressum

I want to thank everyone who contributed to shaping arguments through discussions and advice, including some who are not named. Special thanks go to Sorina Teleanu, Katarina Andjelkovic, and Natasa Perucica for their support and background research.

Talks with the Vatican COVID-19 Commission's New Technology for Peace and Integral Development Working Group, headed by Alessio Percorario with help of Melinda Davis, Gabriele Verga, and Francesco Silvestri, were particularly valuable and inspirational.

Dorijan Najdovski, Virgina Paque, Mary Murphy, Su Sonia Herring, and others were kind enough to offer suggestions and make editorial comments.

Jovan Kurbalija

Vatican City,
9 December 2021

**About** **6**

**Introduction** **8**
How can you use this white paper and toolkit? 11

**TEN digital technologies** **12**
Internet platforms and applications 12
Data technology 12
Artificial intelligence 13
Virtual and augmented reality 14
Blockchain 14
Biotechnology 14
The internet of things 14
Quantum computing 15
3D printing 15
5G 15

**TEN Core values for the digital era** **16**
Human life and embodiment 16
Human dignity 17
Human well-being and prosperity 17
Human agency and creativity 18
Protection of natural habitat 18
Solidarity and common good 19
Peace and nonviolence 20
Diversity 20
Equality and justice 20
Trust 21

**TEN approaches for digital governance** **22**
Interdisciplinarity and policy coherence 22
Precautionary principle 22
Responsibility and the ‘polluter pays’ principle 23
Time-context approach 23
Transparency 23
Subsidiarity 23
Inclusion 24
By design approach to digital policy 25
Policy trade-offs 25
Evidence and factfulness 26

**TEN types of legal and policy instruments** **26**
Hard law: National and international legal rules 27
Soft law: Declarations, resolutions, recommendations, guidelines, and compacts 27
Standards and certification mechanisms 28
Self-regulation: Business policies and terms of reference 28
Sustainable development goals 29
Impact assessments and due diligence instruments 30

Oversight instruments 31
National, regional, and global strategies 31
Regulatory sandboxes and policy prototyping 32
Dispute resolution and mediation 32

**TEN clusters of policy topics** **34**
Critical infrastructure 34
Security and safety 35
Human rights and digital identity 38
Development 41
Environment and the ecosystem 44
nomy and labour 47
Education, culture, and science 53
Humanitarian assistance 55
Health and social well-being 56
Content policy and media 57

Conclusion **59**

**Reference list** **60**

# About

*We have to accept that technological products are not neutral, for they create a framework which ends up conditioning lifestyles and shaping social possibilities along the lines dictated by the interests of certain powerful groups. Decisions which may seem purely instrumental are in reality decisions about the kind of society we want to build.*

Pope Francis, Laudato Si

*The choices we make — or fail to make — today could result in further breakdown and a future of perpetual crises, or a breakthrough to a better, more sustainable, peaceful future for our people and planet.*

UN Secretary General Antonio Gueterres, Our Common Agenda

Inspired by these words, this white paper is about the digital choices we make today to build a better world tomorrow.

Some of our choices in the digital world are part of our daily routine, ranging from a simple 'like' on a post to comments on social media. Others are more serious, such as reporting inappropriate content online. Many may have far-reaching consequences: a programmer imprinting their own bias on an artificial intelligence (AI) algorithm, a corporation prioritising profit over human dignity, a government adopting new laws. And some decisions on fast-evolving fields such as bio-engineering may impact the very essence that defines us as human beings.

Given the amplifying power of digital technology, the choices we make now – no matter how big or small – will be of consequence in the future. In equal measure, inaction on critical digital issues is also a choice.

This urgency calls for conversation to establish a new 'social contract' of a sort, one that would outline what it is that we expect from technology, and what interactions between humans and machines should look like in the future. This debate must transcend cultural, generational, religious, social, and national boundaries, and collect inputs from different fields of the societal landscape; from security to human rights, from e-commerce to overcoming digital divides, from cultural diversity to AI ethics, to name a few.

This white paper and proposed toolkit are inspired by the need for new social contracts from local communities to global institutions, as suggested by the UN Secretary-General in *Our Common Agenda*. They should contribute to the conversation when it comes to decision-making related to the development, use, and governance of digital technology while anchoring such decisions in the pursuit of sustainable technological growth.

This is how the proposed toolkit approaches this challenge: It lists 10 major **technologies** that are grounded into 10 **core values** and should be implemented through 10 **approaches** and **instruments** to 10 clusters of **policy topics**.

Through this toolkit, we aim in particular to help decision-makers in their work to both realise the potential of digital technologies, and to contain the numerous associated risks, while upholding core human values. It is inspired by a strong belief that cooperation – rather than rivalry – can maximise the potential of digital growth and minimise its negative consequences.

In Chapter 1, we outline the ten technologies that we focus on, ranging from AI and data to blockchain and 5G. In Chapter 2, we analyse ten core values that these technologies should support, including human life and dignity, justice, and peace. These values are implemented through

ten approaches – discussed in Chapter 3 – which could be considered a 'cognitive set of tools' that help us apply the aforementioned values to real life. In Chapter 4, we discuss ten types of legal and policy mechanisms that are used to govern digital technologies, including national and international laws, standards, and business practices. In Chapter 5, we outline ten clusters of policy topics, including technical infrastructure, human rights, and the environment.

Finally, this paper provides concrete recommendations for policy actions to support the digital transition. These recommendations are highlighted in orange text.

While the responsibility for this text is on the author, it builds on the diversity of views of the members of the COVID-19 Commission, who come from different backgrounds, including government, business, civil society, academia, and the technical community, as well as insights from community consultations worldwide.

# Introduction

**Every so often, technology cha(lle)nges humanity.** Technology-induced shifts in human history can be traced back to our ancestors' taming fire; starting to write; beginning to use the wheel; and, more recently, inventing the printing press, the telegraph, and the internet. Often described as new epochs, paradigm changes, or industrial revolutions, these shifts trigger fundamental changes and challenge us to venture into the unknown.[1] **As humanity steps away from its comfort zone, certainty ends, opportunity begins, and risks increase.**

**Today, we are once again at a turning point.** The multifarious, complex, and often profound impacts of tech developments are felt at all levels, from matters of war and peace to lifestyle, work, individual well-being, and ultimately our existence itself.

**The rapid acceleration in technologies such as AI and robotics is fundamentally reshaping our notions of human rights, freedoms, and human agency**. Technology is revolutionising education, improving medical care, and advancing agricultural production, among numerous impacts of society. The COVID-19 pandemic vividly displays the critical relevance of digital infrastructure for modern society.
**While new digital technologies unlock great potential for our society, they simultaneously trigger new risks and socio-economic divides** (World Bank, 2016)**.** As new industries emerge, older ones are scrambling to maintain their digital relevance. Jobs are disappearing in fading industries. Social security and support systems are under pressure. From the militarisation of cyberspace to competition for AI dominance, a new geostrategic race is in the making.

**The internet amplifies existing problems and risks.** Criminal activity existed well before the advent of technology. Yet, criminal acts have become much more dangerous through the exploitation of vulnerabilities in our interdependent networks and services. Disinformation (also known as fake news) is as old as humanity. Yet, social media platforms broadcast such content faster and more pervasively than ever thought imaginable, undermining trust in public information and science, and inflicting a great cost on our society.

**Like all new technologies, digital technology creates winners and losers.** Never before in history have companies had such economic, cognitive[2] and social power.[3] Big tech companies are becoming more powerful than many countries (see: comparisons). Apple's current market capitalisation (US$2.71 trillion) is higher than the total 2019 GDP (US$2.33 trillion) of the entire African continent and is close to the GDPs of the UK (US$2.81 trillion), France (US$2.79 trillion), and India (US$2.69 trillion).

In the span of just a few decades, China's Shenzhen evolved from a small fishing village into a vibrant global technology hub. San Francisco's Bay Area has become the centre of economic dynamism in the USA and home to the world's largest concentration of investment and innovation. Nearly one-third of the world's billionaires made their fortunes in the tech sector (Martin and Loudenback, 2017). However, many have not been as fortunate, considering individuals, social groups, and countries lost as a result of digitalisation.The tech transition has led to a "lost generation" of people who are too old to adopt new technology, and too young for retirement. The widening gap between the winners and losers of digital technology is tearing apart the social fabric and triggering new conflicts and instabilities worldwide.

At this turning point, **humanity is not prepared to respond to digital change,** or even to properly digest, analyse, and fully understand its implications. The digital future is being shaped in an ad hoc manner, often unilaterally by tech sector actors while countries and citizens largely remain on the sidelines. Thus, the need for an informed, inclusive, and impactful societal response to tech developments is of the utmost urgency.

[1] The impact of the ensuing Fourth Industrial Revolution, or Industry 4.0, bears little resemblance to previous industrial breakthroughs (water and steam power, electricity, and computerisation), as it created ruptures in almost every industry and altered entire systems of production and governance. Furthermore, its velocity has no historical precedent (Schwab, 2016).

[2] Cognitive power is the ability of tech platforms to grasp and in some cases manipulate our emotions and intentions.
[3] Only East India Trade Company (17th Century) had a partially comparable corporate power (without the cognitive power of modern tech companies).

While technology is complicated, society is complex. For example, chess is a complicated game with a finite number of combinations, while soccer is a complex game with an infinite number of interactions among players.

Over centuries, humanity has developed heuristic ways to deal with the limited predictability of complex societal systems by, for example, carefully listening to and observing social dynamics and reacting via a gradual evolution of society as a whole.

Digital technology could be deployed more smoothly if it relies more on societal wisdom when dealing with complex rather than complicated challenges.

**Today's policy decisions are not only about us. They will also fundamentally impact future generations**. Their rights should be protected, as suggested by the UN Secretary-General in his recent report *Our Common Agenda*. Our generation should pass to the next a richer heritage than we received from previous generations. Future generations need to be able to make decisions that are informed by their time and interests. It is a public good to ensure that our shared heritage remains available for future generations. This includes preventing the privatisation of our common knowledge through AI-driven codifications made by tech companies. While it is difficult to grasp and predict future AI and digital developments, we must nonetheless prepare to deal with them. The first step will be to empower individuals and institutions to understand the impacts of technology on society and to make the policy choices ahead of us.

**Our choices are not made in a void.** They are shaped by institutional, political, social, and cultural dynamics. Companies are motivated by the bottom line, their imperative to turn a profit. Governments are guided by the public interest to preserve law and order and maintain healthy market, political, and social systems. Civil society strives to protect the interests and rights of individuals and communities through awareness and advocacy.

Against this backdrop, this white paper provides an overall framework for addressing the following questions:

- How do we **implement the core values of humanity** in the decision-making processes undertaken by tech and governance leaders, programmers, and others involved in shaping our digital future?
- **How do we simplify and strengthen the existing digital governance landscape,** which is currently composed of more than 1,000 mechanisms that deal with technical standards and the operation of telecom infrastructure, internet domains, and hardware and software developments?
- How do we **overcome institutional, professional,** and **national silos** in digital governance?
- How do we **apply online existing offline rules** on human rights,[4] security,[5] taxation,[6] health, trade, and other public policy issues?
- How do we make **policy choices and trade-offs** between different interests as well as current and future considerations?

[4] *The same rights that people have offline must also be protected online* in Resolution 'The Right to Privacy in the Digital Age, Sixty-eighth session, UN Doc A/68/456/Add.2 (18 December 2013).

[5] *'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment*' in UNGGE, *Government Group of Experts on Developments in the field of information and telecommunications in the context of international security: Note by the Secretary-General,* Sixty-eighth session, UN Doc A/68/98 (24 June 2013, reissued for technical reasons on 30 July 2013).

[6] The Ottawa Taxation Principles: neutrality, efficiency, certainty and simplicity, effectiveness and fairness, and flexibility. (in OECD, 2003).

- How do we ensure that **emerging technology narrows the digital gap**, rather than widen or create new ones?
- How do we ensure **digital dividends are enjoyed by all?**
- How do we make **digital policy more inclusive and protect the interests of missing actors, including future generations?**

**Who are the actors in digital cooperation?**
While human-centred and balanced digital development is a shared responsibility of humanity, each actor also has specific responsibilities. Citizens, countries, companies, religious communities, academic institutions, and civil society should act in their specific areas of interest and expertise as well. One attempt to outline specific roles and responsibilities of major actors in digital policy is provided by paragraph 49 of the *WSIS Declaration of Principles*:[17]

- States: 'policy authority for internet-related public policy issues' (including international aspects)
- Private sector: 'development of the internet, both in the technical and economic fields'
- Civil society: 'important role on internet matters, especially at the community level'
- Intergovernmental organisations: 'the coordination of internet-related public policy issues'
- International organisations: 'development of internet-related technical standards and relevant policies'

Churches and religious communities are increasingly involved in discussions on the impacts of digitalisation and AI on society. Their focus areas are the regulation of lethal autonomous weapon systems (LAWS), the future of work, and humanitarian assistance. For example, Pax Christi, a Catholic peace movement, leads the Campaign to Stop Killer Robots.

# How can you use this white paper and toolkit?

In the online version, you can dive deeper layer-by-layer from the white paper to the policy toolkit and additional resources (Figure 1.)


Figure 1. Layered structure of white paper and policy toolkit

Particularly useful aspects of the toolkit are links across digital technologies, core values, operating principles, policy mechanisms, and policy clusters. Throughout the toolkit, recommendations are indicated in orange.

# TEN digital technologies

This toolkit addresses ten main digital technologies, which can be understood as **electronic tools, systems, devices, and resources that generate, store, or process data for various purposes**.

Most of these technologies are intertwined through combined use: data underpins AI, while internet platforms and applications facilitate most digital technologies.

The societal and policy impacts of these technologies can be followed throughout this document via their interplay with the core values of society, their operating principles and instruments, and relevant digital policy topics.

## Internet platforms and applications

Internet platforms and applications shape most of our daily digital experiences from social media networks to email, websites, and e-commerce platforms. They are also the space where some of society's predominant policy challenges happen, including data breaches, attacks on privacy, and the spreading of misinformation and hate speech.

As explained in more detail in the digital infrastructure section, the internet operates using a few main protocols. The transport control protocol/internet protocol (TCP/IP) connects different networks and ensures the flow of data. HyperText Markup Language (HTML) facilitates the management and display of information on websites, social media networks, and e-commerce platforms, among others.

The debate is ongoing about whether and how the internet architecture, which has been around for almost 50 years, should be updated to meet technical challenges.

## Data technology

Data technologies manage the storage and use of data. Data has come into sharper public focus due to its relevance for personal freedom and agency, economic activities, and political life. Countries have started considering data as a national asset. The flow and storage of data have fast become a geopolitical issue.

Data governance has therefore climbed political agendas worldwide. The regulation of data technologies is shaped by policies and laws on security, privacy, data localisation, standardisation, and interoperability. The question of jurisdiction over data is becoming particularly important as authorities worldwide request access to data held on cloud servers beyond their national jurisdiction. Increasingly, countries are pushing for data localisation (i.e. requiring domestic and foreign companies to store data of residents within national borders), especially when it comes to sensitive data.

As the majority of data is stored on servers in the cloud, data technology is often discussed in the context of **cloud computing**. Cloud computing consists of server farms that facilitate most of the internet's activities, ranging from e-commerce to social media platforms. Given its relevance to digital activities and society, cloud computing is considered part of the critical information infrastructure. It is directly impacted by policy processes related to security, privacy, data localisation, standardisation, and interoperability.

### Data as a digital public good

Data can have various legal statuses. It can be a public good by being both non-excludable (anyone can access it) and non-rivalrous (access by one person does not diminish its value to others). The following table shows various types of data, and their potential for becoming digital public good.

| | Rivalrous | Non-rivalrous |
|---|---|---|
| **Excludable** | Since the introduction of the EU General Data Protection Regulation (GDPR) and other data protection regulations worldwide, **personal data and their monetisation by tech companies** have become the focus of many policy debates. The bulk of the surrounding policy debate is on the use, protection, and management of personal data. | **Community and club data** is gaining increasing visibility. For example, what are the rights of citizens and public authorities of cities generated by public services such as transportation? Would it be considered public data in general or public community data (accessible to citizens/institutions of a particular community). |
| **Non-excludable** | **Open data – commercial use:** Data is accessed openly, but it can be packed as a commercial service. It may become rivalrous on the market as part of a product or application. For example, meteorological data is accessed freely but once it is used in commercial apps, it can become rivalrous. | **Open data – public use:** Data generated by publicly supported projects (CERN – scientific data, meteorological data, etc.) |

## Artificial intelligence

AI refers to a combination of data and algorithms to perform certain tasks or replicate certain specific behaviours that normally require human intelligence, such as visual perception, speech recognition, and decision-making. AI is an umbrella concept that includes machine learning, neural networks, speech processing, and robotics. The common element across different types of AI are algorithms, i.e. computer codes carrying the necessary instructions to process data into information, knowledge, and creative insights.

AI is used in internet services, such as search engines, social media platforms, e-commerce, manufacturing, transportation, agriculture, healthcare, and many other areas. AI is a multifaceted phenomenon with significant potential for good. However, it can also pose risks to human rights and safety, as well as labour market disruptions and other societal issues.

For example, AI can make the internet of things (IoT) and devices ranging from driverless cars to home appliances smarter. In the field of security, AI empowers LAWS; this carries enormous consequences for the conduct of war and for humanitarian law. In law, AI automates court proceedings in many countries. In human rights, AI may impact humans' right to free choice in social, economic, and political life. In the economy, AI facilitates new business models and furthers the automation of labour. It is also used for price monitoring, as well as price fixing, which has triggered competition rulings in a few countries. And in the health field, AI-enabled systems are being used for health diagnosis and treatment, as well as new drug developments.

## Virtual and augmented reality

Virtual reality (VR) is a set of applications and tools that simulate the physical environment through digitally generated images, sounds, and even touch and smell. Augmented reality (AR) enables users to view the real-world environment with augmented (added) elements generated by digital devices (e.g. smartphones).

Major investments by big tech companies – like Facebook's Metaverse – are likely to make AR and VR ubiquitous and highly immersive. The shift between the real and the virtual will be seamless. It will alter our perception of reality with numerous impacts on personal identity, law, and overall societal organisation.[7]

## Blockchain

Blockchain is built around a decentralised record of transactions in the form of a ledger, copies of which are distributed among users (or nodes). Through distributed technology and cryptography for the verification of transactions, blockchain relays trust from a single central authority to the entire community involved, replacing traditional structures. Transactions are validated by all nodes simultaneously, and the transactions are protected against tampering and revision. The more digital eyes around it, the lower the chance of fraud. Cryptography provides a highly reliable automated system of validating transactions, instead of relying on humans.

Cryptocurrencies, such as Bitcoin and Ethereum, are the best-known applications of blockchain technologies. Blockchain has also been applied to facilitating free and fair elections, documenting supply chain performance for increased efficiency, and facilitating transparent property transactions.

Blockchain has potential applications and impacts for security, in the context of the growing demand for verifiable and reliable information; law, in support of preserving legal evidence; the economy, via its potential to develop reliable and inclusive financial mechanisms; government, in helping reduce administrative burdens, and health, with its potential to more effectively handle protected data. In these fields and many others, we are only just starting to witness the full potential of blockchain applications.

## Biotechnology

Biotechnology is built around the convergence between digital technologies and biology. It covers many cross-cutting issues including the use of AI and big data to discover new drugs; **3D printing** that can, produce **cultured meat** in labs; **gene editing,** which is the insertion, deletion, modification, or replacement of DNA in the genome of a living organism, that has the potential to correct genetic defects to fight certain medical syndromes; and **brain-machine interfaces** (also called **brain-computer interfaces),** which allow direct communication between the human brain and external devices with a mix of potentials for almost treatment of health problems and major risks from the possibility of hacking human characteristics and actions someday (CBINSIGHTS, 2021).

Biotechnology can be supported by nano devices on a very small scale, such as atoms and molecules. In addition to applications in medicine for, for example, the delivery of drugs to specific cells or organs, nanotechnology is used in the hardware industry to develop smaller and smarter sensors and more compact microprocessors. In environmental protection, it finds applications in detecting impurities in water and cleaning pollutants and other uses that might help control climate change.

## The internet of things

The IoT offers a new generation of internet-connected devices and has the potential to make significant impacts in environmental monitoring, agriculture, and disaster recovery, among others. IoT applications include consumer electronics (internet-connected smart devices and automated or connected home appliances),

[7] The potential impact of VR/AR on society can be seen in the way that online games affect children and youth.

vehicles (including self-driving cars), municipal infrastructure (smart cities and smart houses, which connect in wide systems), and medical devices (which allow medical professionals and patients to monitor health issues).

Other sectors that use IoT technology include energy, infrastructure, agriculture, and manufacturing. IoT devices and systems are often empowered by sensors that collect a lot of data, which triggers many questions on data ownership and protection.

The main issues related to IoT are security (which looks at the vulnerability of smart devices, and the need for security by design and default practices); infrastructure (including standards and protocols); privacy issues (including access to, misuse of, and the protection of data); and issues related to emerging technologies (such as drones, driverless cars, and voice-activated digital assistants).

## Quantum computing

Quantum technology shifts from storing and processing information in binary 0 and 1 states to quantum bits (qubits) that can represent 0 and 1 at the same time, reducing the time needed to process a data set. To illustrate, in 2020 a team of Chinese researchers announced the development of a quantum computer that took minutes to complete a calculation that would have taken a supercomputer 2 billion years (Gong et al., 2021). Today's computing systems, although having significantly improved decade after decade, can only solve problems up to a certain size and complexity. Larger and more complex issues require advanced capabilities, and quantum computing promises to offer them.

The potential for quantum computing is often seen in the following fields: secure communication via secure cryptographic key exchange with major application in health, military, financial and other areas of major concerns for the security of data exchanges; powerful computing that can bring on the new level AI and other technologies that require processing power; and measuring and censoring that can increase the precision of high relevance in medical research and treatment, such as neutral surgery.

While it remains to be seen if and how all of this potential will be realised, quantum computing is attracting a lot of research support from governments and venture capital investment.

## 3D printing

3D printing enables the fabrication of objects from objects we use every day, such as household items, to medical prosthetics and implants, and even entire houses. 3D printing opens new economic possibilities for automated manufacturing with far-reaching consequences on the labour market. It also poses new security risks, such as the possibility to print weapons.

As a relatively new technological field, 3D printing lacks globally adopted standards that can facilitate the interoperability of various 3D printing systems and platforms. Legally speaking, 3D printing opens new issues related to intellectual property rights in the chain from designing to printing 3D objects, and the regulation of trade that involves only electronic transactions as it is the consumer who prints the physical goods.

## 5G

5G, the fifth-generation mobile network, provides more bandwidth and faster transfer of data. Compared to previous generations of mobile networks, 5G comes with significant improvements in speed, latency, and bandwidth, enabling the real-time remote control of automated processes and the greater optimisation of network traffic.

5G is likely to unlock the potential of the IoT, AI, and other advanced technologies described in this section. For example, it can support a massive sensor network with thousands of simultaneous connections, which prior generations of mobile networks could not come close to hosting.

# TEN Core values for the digital era

> *A better world is possible thanks to technological progress, if this is accompanied by an ethic inspired by a vision of the common good, an ethic of freedom, responsibility and fraternity, capable of fostering the full development of people in relation to others and to the whole of creation.*
>
> Pope Francis[8]

**Digital technology is not an end in itself.** It should serve the core values of humanity. Thus, there should be moral continuity even in the face of new and disruptive technologies. 'Thou shall not kill' and 'Thou shalt not steal' do not become obsolete simply because new technologies for killing and stealing have been invented, such as cyberattacks on hospitals and health care centres during the pandemic.[9]

This moral continuity is built around core values that are intrinsic to humans. As Kant argued in defining human dignity, these core values are 'given' to us without transactional importance: 'What has a price can be replaced by something else as its equivalent; what on the other hand is raised above all price and therefore admits of no equivalent has a dignity' (Kant, 1998, pp. 42–43)

**Values are interdependent, reinforcing, and sometimes conflicting.** They should not be viewed in isolation. In some cases, a delicate balance needs to be established between, for instance, the encryption of private communications and access to such communications by authorities to prevent serious crime, carry out investigations, and fight terrorism.

**Values are global in aspiration and local in application.** They can be interpreted and applied differently across distinct communities and cultures. For instance, a study conducted by the Massachusetts Institute of Technology, known as the 'Moral Machine' (Awad et al., 2018, pp. 59–64), showed contrasting applications of the same value. Around 2.3 million respondents from over 100 countries were asked to choose between saving the life of an elderly person, that of an adult, or that of a child, in 13 life-or-death scenarios related to autonomous vehicles. Although the preservation of human life was identified as a shared value among all survey respondents, respondents from Eastern cultures chose to save the elderly person, and respondents from Western cultures chose to save the child (Huang, 2018).

The list of ten core values starts with four values related to individual humans (human life, dignity, well-being and prosperity, agency and creativity) via the protection of our natural habitat to five values that shape life with others from family via local communities to national states and the global community.

## Human life and embodiment

The protection of human life is a cornerstone value that is codified in religious texts, political declarations, and legal regulation. The centrality of human life is reiterated in regulations and policy documents for the digital space. For example, the United Nations Educational, Scientific and Cultural Organization (UNESCO, 2021) *Recommendation on the ethics of artificial intelligence* in paragraph 36 stresses that 'life and death decisions' should not be ceded to AI systems. The German Ethics Commission's *Automated and Connected Driving Report* goes further by stating that 'human life enjoys top priority' (BMVI, 2017, p. 33) over animal welfare and property.

---

[8] Address by His Holiness Pope Francis to the participants in the seminar 'The common good in the digital age', organised by the Dicastery for promoting integral human development (DPIHD) and the Pontifical Council for Culture (PCC), September 2019. Available at https://www.vatican.va/content/francesco/en/speeches/2019/september/documents/papa-francesco_2019097_eradigitale.html.

[9] Input by Dr. Maryanna Cusimano Love.

So far, the main risk for human lives from the use of digital technologies comes in the form of legal autonomous weapons systems (LAWS), often referred to as 'killer robots'. It has been reiterated in various documents that decisions on life and death, mainly related to the use of LAWS, should rest with humans.

The question of **human embodiment** came into sharper focus with advances in bio and digital technologies, such as brain-machine interfaces and neural technologies. Science fiction is becoming a technological reality. Fast developments in digital, biological, and nano technologies will accelerate the merger of the human body and machines often described as transhumanism. For example, back in 2016, Sebastian Thrun from Google announced the arrival of 'super human' (Kharpal, 2018): 'Through artificial intelligence, it will be possible for us to continuously move beyond the natural biological borders of our senses and capabilities. We will remember everything, we will know everybody, we will create things which now seem to us completely impossible or even unthinkable'.

VR and AR, or the metaverse as described by Facebook, will change our experience of the physical space in which we live. With more immersion in VR, our bodily experience won't be any more central to our identity. This shift towards the metaverse will open a new set of questions: How can one be present simultaneously in various physical and virtual spaces? What will be our real identity?

These new developments in AI, biotechnology, and the metaverse have accelerated debates on digital and human embodiment among thinkers dealing with ethics, theology, and anthropology.[10]

## Human dignity

Human dignity relates to the recognition of the intrinsic and equal worth of each individual human being. Fundamental to this dignity is human agency and the realisation of the individual, creative, and professional potential of each person. The protection of human dignity underpins many human rights, from privacy to freedom of expression and a wide range of socio-economic human rights.

Human dignity, like other values, can be strengthened or endangered by digital developments. On the positive side, we can point to the empowering potential of digital developments, especially for marginalised groups and communities whose identities and voices were not heard in the pre-digital world. On the negative side, human dignity is often one of the first targets in hate speech and communication. As numerous studies show, digital communication tends to polarise and focus debates on who said something instead of what was actually said. Intrusion on human privacy and intimacy is also more commonplace in our increasingly connected world and represents an infringement of human dignity.

In the field of AI governance, human dignity features even more prominently. For example, UNESCO's *Recommendation on the ethics of artificial intelligence* (UNESCO, 2021) indicates that 'The inviolable and inherent dignity of every human constitutes the foundation for the universal, indivisible, inalienable, interdependent and interrelated system of human rights and fundamental freedoms.'

## Human well-being and prosperity

Throughout history, the betterment of human well-being has been a result of technological and scientific progress. Maslow's hierarchy of needs can help us understand the effects of digitalisation on human well-being and prosperity (Figure 2).

[10] Erin Green argues that meaningful dealing with AI should be anchored in understanding that our 'embodied experience shapes all reasoning, both theological and technological' (Green, 2020).
Sallie McFague puts embodiment in the centre for dealing with technological developments (McFague, 1993).

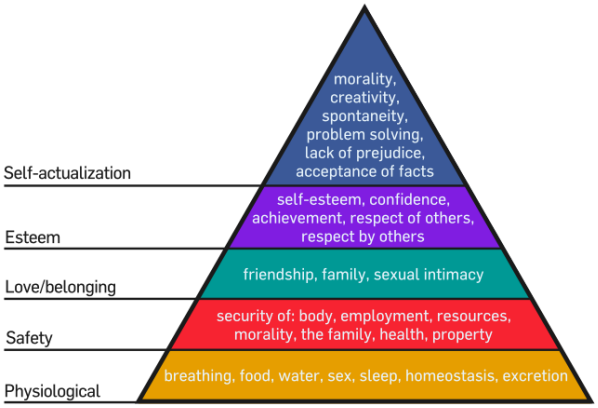


Figure 2. Maslow's hierarchy of needs.
Source: Wikimedia Commons

In the ongoing COVID-19 crisis, digitalisation has become a vital tool in meeting human needs, from the bottom to the top of Maslow's pyramid. Digital services have become a key component of *food supply,* particularly in urban areas. One step up in the pyramid, security in many cases has become synonymous with cybersecurity, reflecting our dependence on digital networks.

Online communication between friends and family has facilitated a sense of *belonging* as Zoom, Facebook, Instagram, and other digital platforms have provided new ways for us to stay connected. It is yet to be seen whether we will fully shift back to pre-pandemic norms, or whether we will engage in some sort of hybrid model for social interaction.

Further, it is becoming more common to use social media presence (including the number of followers and likes) to measure *esteem* and *prestige*. Influencers are often the most respected in online spaces.

*Self-actualization*, holding the top of Maslow's pyramid, is made possible via the many new opportunities the internet affords for personal and creative fulfilment.

## Human agency and creativity

Free will, the cornerstone of human agency and creativity, underpins our daily life in many ways. One is our freedom to make choices that are related to our private life, our economic consumption habits, politics, and so on. The ability to choose is essential for human dignity, well-being, and societal progress. For a long time, the internet has been a great enabler of choice by helping people overcome geographical, social, gender, and other limitations.[11]
However, commercialisation, the power of tech companies, and AI-driven social platforms bring the risk that technology may constrain our choices. By relying on digital assistance, we may lose our capacity to think critically and make choices. One example is our orientation in space. Our reliance on global positioning systems (GPS) to move around overcomes our need to read maps or other orientation techniques developed over centuries. This risk is recognised by the UNESCO Recommendation that calls for assessments of the 'sociological and psychological effects of AI-based recommendations on humans in their decision-making autonomy' (UNESCO, 2021).

Fast and widespread digitalisation also opens the question of whether individuals can choose to opt-out of life in a techno-driven society.

Human agency is also expressed in the search for meaning, which is different from calculations even if they are performed by powerful machines. Machines can find patterns and even explain our meaning, but they cannot generate meaning in understanding societies and complex phenomena.

Creativity is another expression of human agency in the fields of science, technology, arts, and culture. Behind innovation in technology is the creativity of engineers and entrepreneurs. In addition to personal talents and free will, creative artefacts also emerge through interaction with others on personal, social, and institutional levels.[12]

## Protection of natural habitat

Our survival depends on our natural habitat – our air, water, and earth. Harmony between humans and nature is critical for healthy lives and long-term prosperity. However, we have put a lot of strain on our environment with dire

[11] Switzerland proposed the concept of digital self-determination as a way for citizens to be empowered on all matters related to their personal data.
[12] For more on human creativity and theology consult *Homo Theurgos* by Romilo Knežević.

consequences and a significant risk to the future of humanity.

This has prompted political dialogue and international action, with increasing efforts on issues like biodiversity, climate change, and overall environmental protection.

The impact of technological progress on nature is an important facet of these policy processes. Discussions increasingly focus on digitalisation, which is the most dynamic aspect of technological progress. At this point, digital growth has had conflicting effects on the environment and natural ecosystems.

Positively, digital technologies can support monitoring and mitigation efforts by analysing large quantities of data, modelling future developments, and identifying environmental issues and possible solutions. Big data and AI systems can monitor climate change, ocean pollution, and overfishing, among many others.

Negatively, digitalisation has also become one of the more significant contributors to pollution, climate change, and overall environmental degradation. Digital platforms, for example, are major consumers of energy. Data servers consume 2% of global electricity consumption and are forecasted to increase their share to 8% by 2030. In 2019, bitcoin mining consumed 64.15 TWh of electricity, which exceeded the energy demand of entire countries like Chile, Switzerland, New Zealand, and Bangladesh.

Beyond the energy required for the operation of our digital world, digitalisation has environmental costs throughout the lifecycle of all digitally enabled products. The rapid consumption of digital devices, such as mobile phones and computers, has a significant effect, particularly driven by fast device turnover. Their production is a big undertaking that requires energy and large amounts of raw materials. This device turnover is also the primary force behind the generation of e-waste, which totals over 50 million tonnes worldwide per year. Only about 20% of this waste is recycled – perhaps this is best exemplified by a recent estimate that up to 7% of the world's gold is trapped in our e-waste (Wainwright, 2021).

Going forward, we must ensure that we lean into the positive impacts of digitalisation rather than exacerbate the negative. For example, the use of renewable energy in the operation of digital infrastructure and products, as well as developing more sustainable products, minimising e-waste, and improving recycling efforts. Many trade-offs will have to be made from government, producer, and consumer perspectives.

## Solidarity and common good

As social beings, we are defined by our interactions with others through our social, spiritual, political, and other relations. Solidarity underpins these relations from local communities to nation states and ultimately, humanity as a whole.

Solidarity takes on a new form and relevance in our relations with others on social media platforms, online games, VR, and other online mediated platforms. Empathy and emotions are nurtured in different ways in terms of both form and depth. We are experiencing an unprecedented rupture to the traditional – physically driven – social and emotional bonding that humans have developed since time immemorial. It remains to be seen if future generations will develop new types of online or hybrid social bonding and solidarity or whether they will return to traditional forms of physical encounters in families, local communities, and working spaces. The ways we engage with others and develop emotional and social links will shape the social fabric of tomorrow with far-reaching consequences for family life, law, and other aspects of society.

C**ommon good**s are tangible aspects of solidarity in society. **Digital common goods (digital commons)** have been in focus in discussions around software, data, and AI. The open source movement places common goods at its foundation. Currently, there are discussions and initiatives to consider data and AI as common goods that could be used to achieve sustainable development, reduce inequalities, and advance social peace.

## Peace and nonviolence

Ensuring peace and preventing violence are two of the core values of humanity and pillars of the international system. The protection of peace is codified as the core value of the United Nations Charter and many other international conventions and treaties.

Peace is more than just the absence of violence and conflict. It requires a holistic approach to human development that also addresses the roots of the conflict; such an approach would lead not only to greater stability but also to reducing social inequality. Digital technology has a mixed record on fostering sustainable peace. On one hand, it has increased inclusion and access to information to levels never thought possible. On the other hand, especially in the social media era, digitalisation has contributed to widening fractures and polarisation in society through the spread of misinformation (Catholic Relief Services, n.d.) and hate speech. Often, online tensions and conflicts are a prelude to physical violence, attacks on vulnerable communities, and ultimately civil wars.

In international relations, digital technologies can aid peace processes by providing technologies that enhance transparency, accountability, healing, and social cohesion. Among specific uses of technologies for the promotion of peace, we can include digital systems for verifying arms control agreements and drones for collecting information to address refugee flows.

## Diversity

Diversity starts with our uniqueness compared to other human beings. It continues with our age, sex, race, culture, religion, profession, and other aspects of our individual identity. Diversity is about our local communities, regions, and nations. Respect for diversity, while building on our common values and desires, is key in building a prosperous, inclusive, and harmonious society.

As diversity nurtures innovation and creativity, it has helped spur many digital developments. From the early days, the internet has been an important enabler of diversity through the inclusion of a wide range of individuals and cultures. Lately, however, tech platforms have facilitated the creation of echo chambers among groups, entrenching like-minded individuals in spaces where they are not exposed to diversity in individuals, language, and communication style.

From a platform for diversity and democracy, the internet turned into a challenge for both. The future of digitalisation and our society depends on at least protecting diversity, and at best, nurturing it. In particular, it will be a challenge for emerging digital developments like AI platforms, which may sacrifice diversity as they aim to achieve economic optimisation.

## Equality and justice

A harmonious society is built on equality and justice.[13] With its inherent tendency to concentrate data and economic power, digital technology contributes towards inequalities in modern society. Digital growth does not 'lift all boats equally'; it leaves many communities behind. Digitalisation, together with globalisation and economic policies, is considered the key contributor to inequalities in modern societies (Milanović, 2018).
Digitalisation has many aspects that create inequalities, starting with unequal access to networks and devices (e.g. because of lack of infrastructure, financial barriers), to gaps in digital skills and on to gender inequalities as, for example, men still dominate the engineering and the computer industries. Digital divides are also triggered along generational divides and language barriers.

Feelings of injustice are common for those who have not adapted sufficiently fast to digitally driven transformations of the economy. Similar to the industrial revolution of the 19th century, there is a lost generation of digitalisation whose skills and professions have decreased their relevance in today's digital economy. Loss of a job, a profession, a vocation has caused a loss of self-esteem among

[13] Just Net Coalition puts justice in the centre of digital governance debate; See: Digital Justice Manifesto – A Call to Own our Digital Future (https://justnetcoalition.org/digital-justice-manifesto)

many with a huge impact on the social and political life of societies around the world.

Only recently has society begun to address the issues associated with this tech-induced 'lost generation' , such as special retraining programmes and early retirement. Future generations will adapt more easily to the new types of fluid job markets, as they become better prepared for less certainty and constant change.

Given its importance for preserving the social fabric and stability, equality and justice should be taken into consideration when designing future digital and AI technologies.

## Trust

Trust is the social glue which binds people, communities, countries together. Trust helps to increase the well-being, success, and stability of societies by reducing friction and making it easier to cooperate. Trust builds social capital, the networks that are built upon solid relationships and which enable smooth societal functioning.

According to landmark research by Robert Putnam, the basis for the economic success of cities in Renaissance Italy was the high level of social capital provided via trust (Putnam et al., 1993). Many of our online routines are built on trust, just like offline. Trust is important in technology, and also in the industry that supplies the services or products. We also need to trust the government that should protect our rights online as does offline. Trust improves predictability in digital developments, and facilitates growth.

Trust in technology, government, and tech companies is built through transparency about digital actors' roles and responsibilities, inclusion in the development of digital policy, oversight (e.g. over actions that may have implications for rights and freedoms), and confidence-building measures between countries and digital communities. Blockchain is considered one of the technological solutions for increasing trust and confidence in the digital realm.

# TEN approaches for digital governance

The ten approaches make **core values more operational and closer to policy reality**. These approaches could be also considered as a set of cognitive tools for framing policy issues and their impact on society.

## Interdisciplinarity and policy coherence

While digital technology has a cross-cutting impact on all segments of society, **digital policy is conducted in silos**. For example, data governance is addressed from **technological** (standardisation), **legal** (jurisdiction), **economic** (free flow of data), **human rights** (privacy), and **security** (data protection) perspectives (Figure 3). These perspectives are covered by different organisations, instruments, and procedures.[14]

The use of an interdisciplinary approach should, at least, create awareness about various policy aspects and, at most, ensure policy coherence in countries, businesses, and international organisations that participate in digital governance.


Figure 3. Data governance (DiploFoundation, 2017)

## Precautionary principle

**Do not act when in doubt and risks are high** is the gist of the precautionary principle. A more elaborate policy definition was provided in the 1992 Rio Declaration on Environment and Development: ''Where there are threats of serious or irreversible damage to the environment, lack of full scientific certainty should not be used as a reason for postponing cost-effective measures to prevent environmental degradation'(UNCED, 1992).

Analogous to the environment, digitalisation poses many uncertainties and disproportionally high risks. The only flaw in the analogy between environmental- and digital activities lies in their predominant effect: environment on nature and digitalisation on society.

The precautionary principle should address a wide range of risks including structural changes and the capacity of society to sustain the impact of digitalisation in terms of, for example, changes in

[14] One recent example is the way ICANN dealt with the introduction of the GDPR and privacy rules. For a long time, civil society warned ICANN – without much impact – about the privacy aspect of its WHOIS database, which gave public access to information on people who register web domains (registrants). When the GDPR requested that data on EU registrants be made private, ICANN was completely caught unprepared for the new regulation that brought into question the core function of the organisation. A coordination mechanism and an institutional culture to 'other' professional views would have helped ICANN better prepare for the new GDPR.

the labour market and education. The application of the precautionary principle will be particularly relevant in the field of AI.

## Responsibility and the 'polluter pays' principle

Responsibility assigned to natural and legal entities is the core principle of any legal system that should not be changed in the digital realm. Certain human responsibilities cannot be delegated to machine or AI systems.

Responsible entities should also bear the cost if their activities cause damage analogous to the polluter pays principle in international environmental law.[15] **Those responsible should pay for the prevention, elimination, and mitigation of negative consequences.**

In the digital realm, externalities of digital products are not assumed by those who produce or benefit from them commercially. For example, the cost of damage caused by faulty software is often covered by individual users or society as a whole. Analogous to car manufacturers who are responsible for the technical faults of cars they produce, **tech companies should bear proportional and fair responsibility for the failures and negative impacts of their services and products.** Applying the polluter pays principle to digital products would contribute to distributive justice and sustainable digital growth.

## Time-context approach

Time-context plays an important role in developing and using digital technology. **Digital policy should follow the complete lifecycle of development for digital tools and services**. For example, in the case of AI, it is essential to apply all policy requirements from the initial design till the deployment of AI applications, products, and systems.

The time-context approach is important for **intergenerational justice** which is defined by the Brundtland Commission Report (1987) as a 'development that meets the needs of the present generation without compromising the ability of future generations to meet their own needs and choose their lifestyle'. The realisation of this call for rights of future generations will depend very much on AI and the direction of future digital developments.

## Transparency

Transparency contributes to awareness, trust, and sustainable developments in the digital realm. It has various interrelated aspects. In the digital service economy, users would be fully informed if there is transparency about data flows including how user data is monetised and the cost structure of a product. This type of transparency can strengthen the sovereignty of consumers in the field of digital consumption.

Regarding security, timely disclosure of data breaches and cybersecurity failures would increase user trust. Procedural transparency is important in the work of all bodies that make decisions impacting digital and AI developments. Open data requirements operationalise the principle of transparency in dealing with governments and other actors.

**AI has increased demands for more transparency, auditability, and explainability of algorithms and applications given their potentially profound impact on society**. They aim to open the 'black box' of many AI developments and, in particular, deep learning. These principles are included in some way in many national AI strategies and white papers to make algorithms and AI applications transparent and understood by users. Transparency, auditability, and explainability could address the risk of bias and discrimination, as well as the malicious use and manipulation of AI systems.

## Subsidiarity

Subsidiarity ensures that policy decisions are made as close as possible to those affected by policy decisions. Subsidiarity could prevent abuses by

[15] Principle 16 of UNCED (1992).

higher-level authorities as well as support for local authorities and intermediate organisations. It also contributes to administrative and policy decentralisation.

Subsidiarity is endangered in the digital realm due to the centralisation of policymaking, especially in the hands of the major tech platforms. Policies and rules developed in a centralised way do not reflect the reality on the ground, as the same digital technologies often have a very different impact on local communities worldwide. The subsidiarity principle should be supported by a 'policy elevator' that should move policy issues both ways (up and down) among local, national, regional, and global levels.

## Inclusion

Inclusion is essential for laying the foundation for sustainable and enabling technological growth. Weak participation of underrepresented actors, including indigenous communities, youth, elderly, and people with disabilities, often stems from social exclusion, lack of empowerment, and discrimination. Inclusion must be cross-cutting affecting various aspects of economic, political, cultural, and social life.

**Access inclusion is** about affordable access to digital networks and services. It provides technical facilities for all other inclusions. **Policy inclusion** enables the participation of citizens, communities, companies, and countries in digital policy processes at the local, national, regional, and global levels. **Data inclusion** is facilitated through access to data commons and open data. **Business inclusion** is about participation in digital-driven business activities, access to the labour market, and entrepreneurial opportunities.

**Financial inclusion** facilitates access to affordable, useful, and trusted financial and banking services through the use of traditional and innovative approaches, such as Mpesa in Kenya. **Gender inclusion** involves women and girls in education, business, and other activities online. **Geographical inclusion** broadens the benefits from digital growth beyond major tech centres to island states, rural communities, and remote areas. **Legal inclusion** is about access facilitating the right to justice and legal redress for online activities. **Knowledge inclusion** is access to knowledge and production of local content contributing to cultural, academic, and research diversity. For increasing the knowledge gap on the global level ( Figure 4).

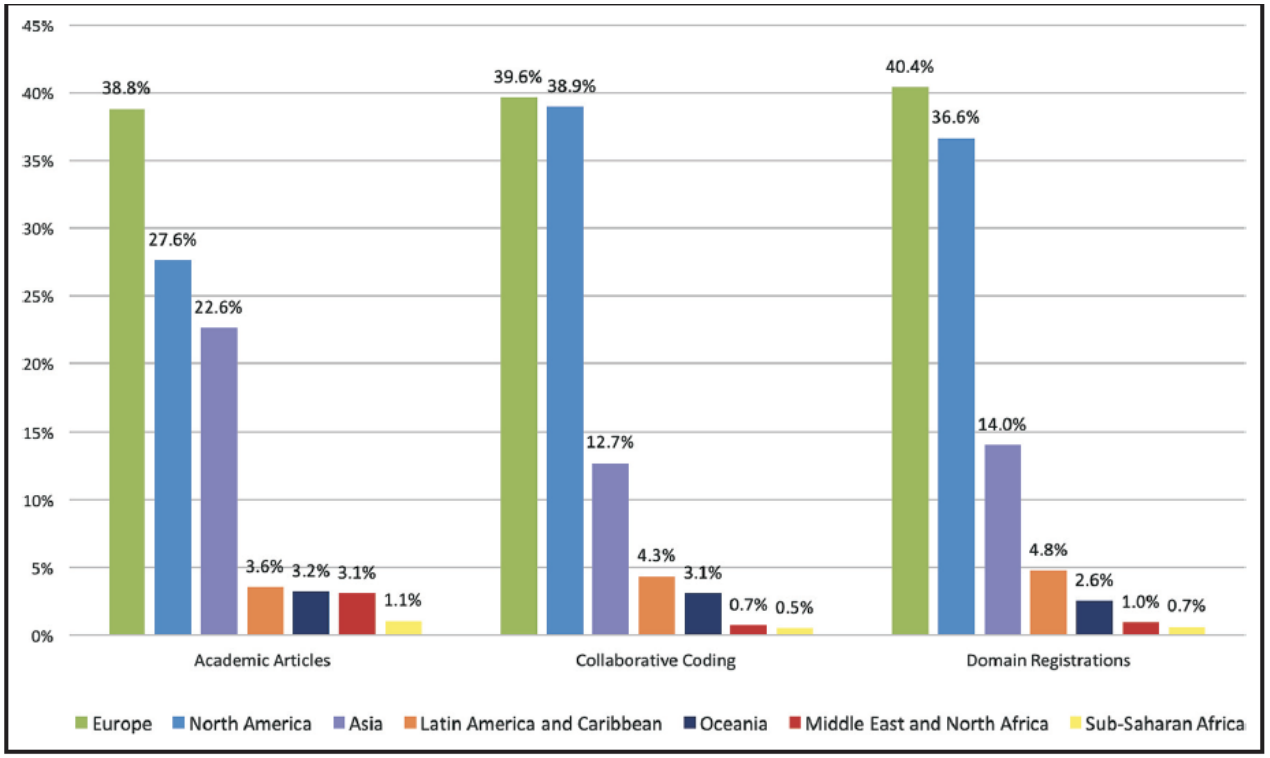


Figure 4. Regional patterns of content creation and domain registrations (Ojanperä et al., 2017).

Language inclusion provides content and services in local languages. Youth inclusion prepares young people to use digital tools for educational, labour, and creative purposes. Elderly inclusion enables the elderly to live autonomous and dignified lives by using digital networks and tools. Disability inclusion supports the active participation of people with disabilities in economic and social life via the use of digital tools.

## By design approach to digital policy

There is always a drive to implement core values via the design of technology. Blockchain is often mentioned as a way to promote trust through the technological design of the distributed ledger. The encryption by default approach integrated into social media apps, or the World Wide Web Consortium (W3C) Do Not Track standard, which prevents tracking while browsing the internet, are good examples. Increasingly, debate on AI governance focuses on the impact of the design of algorithms and the way applications impact social reality from biases to LAWS.

However, 'by design' approaches require considerable caution since they can create counter-intentional effects. For example, ToR was designed to provide anonymity to people s at risk (e.g. journalists or human rights activists in dictatorial regimes). However, ToR is being used as the key technological platform of the DarkWeb, which often hosts criminal and illegal activities.

## Policy trade-offs

Achieving a win-win solution is the holy grail of public policy. But, the reality is that we often end up with a zero-sum solution in which some gain and others lose. Trade-offs are complex in digital technology as it has multiple features and impacts cutting across different technological, economic, and policy areas. According to Edward Wenk (1986), 'The most demanding skill in engineering design may ... be the acute weighing of tradeoffs' (p. 53). Digital governance often requires delicate trade-offs:

- Freedom of expression vs. protection of public order. The well-known debate between Article 19 (freedom of expression) and Article 27 (protection of the public order) of the Universal Declaration of Human Rights has been extended to the

internet. It is very often discussed in the context of content control and censorship on the internet.

- Cybersecurity vs privacy. Like security in real life, cybersecurity may endanger some human rights, such as the right to privacy. The balance between cybersecurity and privacy is in constant flux, depending on the overall global political situation. After 9/11, with the securitisation of the global agenda, the balance shifted towards cybersecurity. Snowden turned it back to privacy. Currently, this balance is in delicate flux.
- Intellectual property protection of authors' rights vs fair use of materials. This is another 'real' law dilemma that has taken a new perspective in the online world.

Trade-offs are much more than the 'calculation' of interests, which can identify a 'middle ground'. Trade-offs are part of the political and cultural context and overall political dynamics.

## Evidence and factfulness

Although the internet is made up of engineering artefacts, it does not provide enough data on the impact of digital developments on society. For example, it is hard to get an exact estimate of the cost of cyberattacks, the economic impact digital developments will have on the economy, or how many jobs will be lost due to automation. The lack of evidence and data can lead to misinterpretation or manipulation. Digital decisions are often based on very few facts, especially regarding the impact of digital developments on society and the economy.  Data is missing in particular in small and developing nations. Open data and open science projects should be encouraged and supported to collect data on digitalisation's impact on society.

# TEN types of legal and policy instruments

Values are formally implemented via legal and policy instruments, which range from hard law (legislation, treaties) and soft law (declaration, guidelines) to oversight instruments.

There are more than 1,000 policy instruments worldwide that can be categorised into ten types of groups. A detailed survey of policy instruments is available at Digital Watch and on this interactive map.

The rule that ***offline* rules and norms apply *online*** is widely accepted in human rights,[16] security,[17] taxation,[18] and other policy fields. In some cases, such as the protection of human life, offline rules can apply directly online. But, in many other situations, they have to be adjusted according to the amplifying impact of the internet. For example, rules about misinformation exist in the offline world, but the speed at which fake news circulates in the online space requires new ways to apply existing rules. Privacy rules have existed for decades; however, their application in the digital realm requires new solutions.

This challenge is becoming even more prominent as we enter a new phase of applying a wide set of international treaties and national laws on health, trade, culture, and other traditional policy areas to digital developments. Do we need to adopt new *digital* or *cyber* treaties? Should we amend existing treaties and laws in the segment of their implementation by, for example, adopting a new optional protocol on the Vienna Convention on Diplomatic Relations to regulate diplomatic immunities online? Or, should we just gradually develop rules through court decisions, as the Court of Justice of the EU (CJEU) paved the way for the right to be forgotten to be introduced into the legal system, leading to its later codification in the GDPR.

Yet, in some fields such as AI, new norms and rules may be needed for normative lacunas without any rules and customs. The development of AI rules – a field where there are inherently many unknowns – requires innovative approaches, such as policy sandboxes, which allows the development and implementation of new norms while receiving constant feedback on the impact of these new norms as they are applied. [19]

Since there is no one-size-fits-all approach, the adjustment of existing policy instruments to our changing digital reality needs to be handled with the utmost care to both preserve the rule of law in society and enable creative and innovative digital growth.

## Hard law: National and international legal rules

The core functions of law remain as relevant in the digital age as they were thousands of years ago when our distant predecessors created legal rules to manage their community life. In essence, the law regulates the rights and responsibilities of and between individuals, and the entities they establish (from companies to national governments).

In the digital age, new laws are being adopted by nations worldwide for fast-emerging developments such as cybersecurity, AI, and data protection. Jurisprudence (previous court decisions) is particularly important in the digital realm for two main reasons. First, as most internet developments have been happening in the USA, the legal rules

[16] *'The same rights that people have offline must also be protected online'* in the resolution 'The Right to Privacy in the Digital Age, Sixty-eighth session, UN Doc A/68/456/Add.2 (18 December 2013).

[17] *'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment*'.

[18] The Ottawa taxation principles are neutrality, efficiency, certainty and simplicity, effectiveness and fairness, and flexibility (OECD, 2003).

[19] This approach was developed by the World Bank and 4IRC. In Singapore, theTechnology Office of the Prime Minister developed mechanisms that enable continuity, dialogue, feedback loops, and agility in decision-making, particularly in relation to experimentation or piloting of new technologies.

have been shaped by US precedent law, where most rules are set by court decisions. Second, a jurisprudence approach is often the only way to deal with new types of legal problems triggered by digital developments. For example, even in the EU legal tradition, where legislation is more important than precedents, most early rules were adopted by the court, including the landmark judgements of the CJEU on the right to be forgotten, the status of Uber drivers, and data protection and the Safe Harbour and Privacy Shield agreements between the USA and the EU.

On the international level, most digital relations are managed by the rules of international private law (conflict law in the Anglo-Saxon tradition), which deals with contracts, torts, and commercial responsibilities. International public law, which regulates relations between countries, is currently in a transition phase when it comes to digitalisation. So far, there are not many treaties and conventions dealing exclusively with digital issues. One of the first instruments was the Council of Europe Convention on Cybercrime adopted in 2001.[20] . There are also conventions and treaties that deal with telecommunication infrastructure, such as the International Telecommunication Regulations (ITRs) of ITU.[21]

Apart from these specific legal instruments, the main challenge is to harmonise a wide set of existing conventions and treaties on the environment, human rights, trade, and humanitarian issues to deal with the specificities of the digital realm.[22] **We need a comprehensive review of existing conventions and treaties to discern whether they apply to digital issues in their existing forms, or whether they need amendments involving digital protocols.**

## Soft law: Declarations, resolutions, recommendations, guidelines, and compacts

Soft law instruments include declarations, resolutions, recommendations, guidelines, and compacts. They are not legally binding like treaties and conventions, but rather codify the *global will* as they are, typically, adopted by a majority of countries after prolonged negotiations. Ultimately, they could become customary law if countries follow the practices outlined in them.

In the digital realm, the main soft law instruments are the documents developed in the context of the World Summit on Information Society (WSIS), including the *Declaration of Principles*, the *Geneva Plan of Action*, and the T*unis Agenda for the Information Society*. In cybersecurity, soft law instruments are United National General Assembly (UNGA) resolutions adapting the reports developed by the UN Government Group of Experts and Open-ended Working Group (UN GGE). A forthcoming major development will be the *UN Digital Compact* as the UN Secretary-General calls for its adoption in 2023. Soft law instruments have a few advantages compared to treaties for dealing with digital topics. First, they are less demanding from a legislative perspective as they do not require formal ratification by national parliaments. Second, they are flexible enough to facilitate the testing of new approaches and adjust to rapid developments in the digital field. Third, soft law can facilitate easier involvement of civil society, business, and academia in the development and use of digital technologies.

## Standards and certification mechanisms

Our digital reality is made possible by the standards guiding the manufacture and use of digital devices and services, from our mobile phones to social media platforms and video-conferencing services. Standards deal with

[20] Following the Russian initiative, the UN will start negotiations for the new cybercrime convention. It remains to be seen how two conventions – the existing 2001 convention and the new one – will coexist in the global regulatory space for cybercrime.

[21] It is not well-known that global telecommunications are run by 2 different sets of ITRs, with 55 countries following the ITRs from 1988, and 89 countries legally bound by the amended set of ITRs from 2012. Fortunately, there are only minor differences between the two sets of rules, and this legal duality does not affect the normal functioning of digital networks.

[22] Another source of international law - International customary law - has limited applicability since recent digital developments cannot provide sufficient elements for supporting general practice (consuetudo) as proof of existing customary rules.

hardware, software, and digital networks, fostering interoperability, quality of service, and safety. Thus, they have high importance for innovation, economic growth, safety, and the sustainability of the digital space. Increasingly, human rights and the public interest are entering the focus of digital standards, especially those dealing with data, AI, and biotechnology.

As policy implementation instruments, standards are increasingly used to address topics where countries cannot agree on international conventions.

The global standardisation landscape is very complex, consisting of a diverse set of organisations, working methods, and procedures, with two main groups of actors:

- Formal standards-development organisations (SDOs): ITU (for telecommunication standards), the International Organisation for Standardisation (ISO; for business and security standards), and the International Electrotechnical Commission (IEC; for electronic device standards).
- Quasi-formal organisations: the Internet Engineering Task Force (IETF; for internet standards), the Institute of Electrical and Electronics Engineers (IEEE), and the Wi-Fi Alliance (for Wi-Fi standards), and W3C (for web standards).

**Certification instruments** monitor the implementation of digital standards by confirming that organisations observe specific standards. Usually, national certification bodies operate certification schemes and can issue certificates to manufacturers confirming that their products/services meet certain standards. Sometimes certification instruments are essential for companies to demonstrate compliance with certain regulations. At the EU level, for instance, some regulations refer to standards to be followed as a way to demonstrate compliance with the rules.

## Self-regulation: Business policies and terms of reference

In the US Congress, there is bipartisan support for the reform of Section 230 of the *Communications Decency Act*, which provides liability immunity for online platforms regarding third-party content. This reform would make companies like Facebook and Google liable for content made available on their platforms, as is the case with traditional publishers. Such a legislative change would have far-reaching consequences worldwide, considering that the majority of large online platforms are US-based.

## Sustainable development goals

The sustainable development goals (SDGs) relate to all parts of this toolkit, from the values they promote to the operating principles they abide by, their uses as instruments and, ultimately, the ways they address policy topic areas.

As instruments, the SDGs have two principal uses in the digital realm: providing an interdisciplinary approach to digital policy and establishing guardrails for AI developments.

The interdisciplinary approach to digital policy is one of the serious challenges for synchronising digital policy to the transversal impact of digital concepts on society. In the current language, the SDGs can help break down policy silos.

The SDGs and their targets can be understood as a network, as illustrated (Figure 5) in the links between SDG 10 (inequality) and other SDG goals and targets (for more information see the section on inequalities).

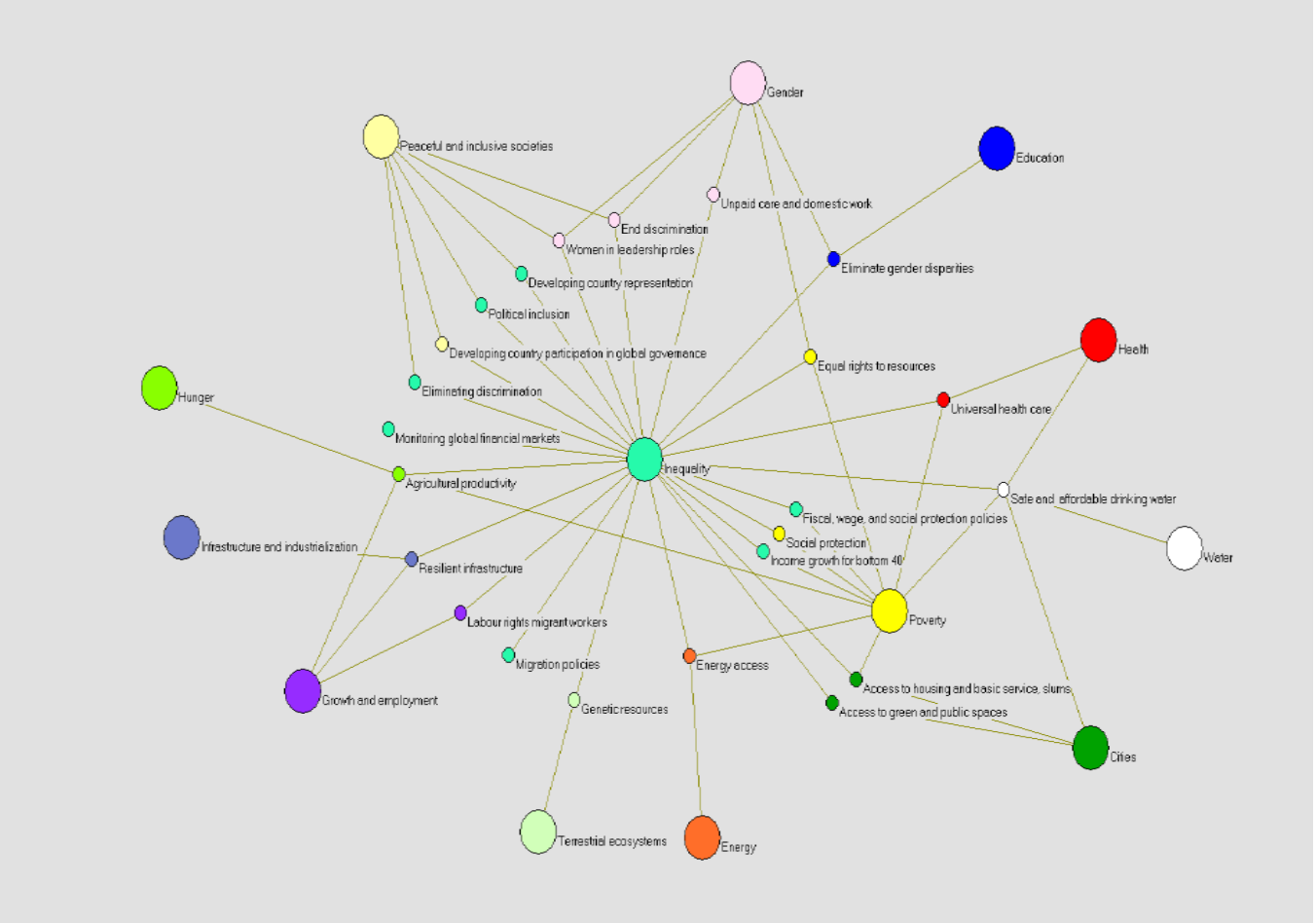


Figure 5. Links between different SDG 10 and other SDG policy goals

The SDGs can also serve as **guardrails for the development of AI**. If AI developers follow the SDGs, their algorithms will support the core values of humanity holistically. In addition to ethics, which is currently in the focus of AI debates, their algorithms would also increase inclusion in economic and social life, reduce inequalities, and support marginalised communities. Since each aspect of AI development is covered by 17 SDGs and 169 targets, the global tech and governance community should start using them as available, practical, and measurable guardrails for the development and monitoring of AI applications.

### Agenda 2030 and digital technology

There are no dedicated SDGs for digital technology in the *Agenda 2030 for Sustainable Development.* The way Agenda 2030 addresses digital developments is an example of a technology-neutral approach where rules and policies are more related to values and society than to specific technologies. This makes Agenda 2030 applicable to any current and future digital development from AI to biotechnology.

In addition, a handful of targets explicitly mention digital technologies: access to the internet (9c), scholarships for education in ICT (4b), the use of ICT to promote empowerment of women (5b), and technology and science (17.8). We could, nonetheless, refer to digital technologies as an invisible *SDG 18*, given the omnipresence of ICT in everyday life and its cross-cutting nature. The overall SDG setting is further developed in the Report of the UN High-level Panel on Digital Cooperation (UN HLP DC), and, based on the report, the UN Secretary-General's *Roadmap for Digital Cooperation*. The report reiterated that digital cooperation is key to achieving both the SDGs and more broadly, the 'future we want' (UN HLP DC, 2019).

The SDGs and related targets epitomise the core internet values and principles and steer the development and use of digital technologies. Huawei's *Accelerating SDGs through ICT* report presents a high correlation between ICT development and progress on the SDGs. For example, the report shows that SDG 3 (good health and well-being) and

SDG 4 (quality education) have the highest positive correlation with ICT, with 70% and 72%, respectively, indicating that more ICT maturity should lead to more progress on sustainable development (Huawei, 2019). An improved ICT infrastructure and affordable digital access can improve access to healthcare and medicines, while for certain remote communities they are the only way of accessing education.

## Impact assessments and due diligence instruments

Impact assessments and due diligence are ex-ante instruments that represent precautionary principles for dealing with the uncertainty of digital developments that may pose significant risks for society.

Impact assessments are particularly important in the field of AI, which has a profound impact on core human values, including the preservation of human life (autonomous weapons), human dignity (respect for privacy), human well-being (mental health, reducing poverty), human agency (labour rights, and the rights to choice and decision making), our natural habitat (climate change, e-waste), and human diversity (protection of vulnerable and marginalised groups). Impact assessment mechanisms contribute to trust-building if they are transparent, inclusive, and evidence-based.

While all actors, including companies and academia, can establish impact assessment mechanisms, governments are responsible for setting the framework for these activities and leading impact assessment on digital technologies that may pose major risks for the public order, health, and overall well-being of human society.

There are new practices and initiatives for digital impact assessments. The UNESCO Recommendation on the ethics of AI (UNESCO, 2021) provides elaborate proposals for impact assessment in AI development. UNESCO is also developing a methodology for the Ethical Impact Assessment (EIA) of AI technologies. Businesses can develop impact assessments by following the *UN Guiding Principles on Business and Human Rights*.

**Due diligence** is a well-established legal principle that includes taking all necessary steps to prevent negative outcomes, such as cybersecurity risks or misuse of the system. It does not guarantee that prohibited developments will not occur, but it provides immunity from legal responsibility for companies if they have proactively taken all due diligence measures.

## Oversight instruments

Once a digital technology is deployed, it requires oversight of its impact. Oversight instruments follow pre-deployment impact assessments. National regulators perform oversight in many sectors. In addition to telecommunications and data, regulators are increasingly covering the cross-cutting impact of digitalisation on finance, market access, and security.

AI governance initiatives emphasise the need for human oversight as a primary requirement, with special significance in the use of autonomous weapons and juridical decisions. Oversight is also important for minimising the bias of AI in automated systems.

One overlooked and underutilised system for digital and AI oversight is the SDG system of goals, targets, and indices, as discussed earlier in this section. It provides quantifiable criteria for the oversight of the cross-cutting impacts of digitalisation on society.

**Whistle-blowers** have historically been and continue to be important contributors to oversight. In particular, their insights on the workings of tech companies, including business decisions and the development of AI, are providing useful input for parliaments and the general public for digital policy actions. Given their importance for future digital developments, **tech whistle-blowers should enjoy special legal protection.**

## National, regional, and global strategies

Digital strategies build awareness and put all actors on national, regional, and global levels on, if not the same, at least a closer policy page. As digital topics came into focus, national and other strategies started appearing. Ten years ago, cybersecurity strategies emerged to address the challenges and vulnerabilities of cyberspace. Five years ago, the main focus was on data strategies. Today, countries worldwide are adopting AI strategies to regulate and steer the development of AI and AI-based technologies.

The OECD.AI Policy Observatory contains over 700 policy initiatives from different countries and territories and the EU. While different national initiatives prioritise different topics, many focus on the following common values and objectives: leadership in AI,[23] international cooperation,[24] the future of work,[25] data,[26] ethics,[27] research and development,[28] and sustainable development.[29]

## Regulatory sandboxes and policy prototyping

Regulatory sandboxes are used to deal with new technologies that do not yet have a clear and certain governance direction. New norms are developed, deployed, and monitored in an agile way in a closely monitored policy environment. Based on constant feedback, norms are adjusted and re-deployed.[30] For example, Spain volunteered to serve as a testing ground for the implementation of the new EU regulation on AI ( Archyde, 2021).

## Dispute resolution and mediation

In addition to the courts, alternative dispute resolution (ADR) and online dispute resolution

[23] Canada aspires to global leadership on ethical AI; Norway and Finland aim to take leading positions in innovative applications of AI; the United Arab Emirates' strategy aspires to leadership in investment in AI.

[24] Spain stresses the need for participation in the global debate on human-centric AI, while the Danish AI strategy calls for cooperation with other countries to promote the responsible use of AI. International cooperation is key to ensuring alignment with international standards and principles on AI, as reflected in the Serbian government initiative.

[25] The adoption of AI technologies and the increased automation of work are set to disrupt many industries. This is why the majority of national AI initiatives raise the issue of the future of work, emphasising the need for the skilling and reskilling of the workforce, raising awareness, and adapting curriculums to the AI era, attracting AI talent and the like.

[26] India's AI strategy emphasises privacy, security, and data anonymisation. Since data forms the backbone of AI solutions, datasets used in AI need to be compliant with ethical principles as highlighted by Luxembourg's AI strategy.

[27] Many national strategies call for an *ethics by design* approach, stressing the need for applying the principles of ethical, responsible, comprehensive, transparent, safe, and secure AI during the early stages of the design of AI systems. Moreover, AI solutions should be human-centric, i.e. developed and used for the benefit of humanity, as emphasised by the national AI initiatives of Japan, Lithuania, the Czech Republic, and many other countries.

[28] In the area of research and development, countries underscore the importance of supporting national scientific centres and setting up dedicated AI research centres that attract specialised researchers from other countries. France aims to counter the brain drain by providing more resources for public research.

[29] Sustainable development cuts across all national AI initiatives as countries increasingly recognise the potential of AI in accelerating the attainment of Agenda 2030. France, Qatar, and Egypt considered the environment to be one of their priority areas.

[30] Singapore developed mechanisms that enable continuity, dialogue, feedback loops, and agility in decision-making, particularly in relation to the experimentation or piloting of new technologies.

(ODR) mechanisms are used extensively for solving disputes and conflicts in the digital realm. Compared to traditional courts, ADR and ODR offer more flexible, less expensive, and faster ways of settling disputes. It is also easier to enforce arbitration decisions following the *New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, as national courts are now obliged to enforce arbitration awards (UNCITRAL, 1958).

Typically, digital cases are addressed in traditional arbitration using a well-developed system of rules and institutions when dealing with commercial disputes. However, there are new types of dispute resolution mechanisms such as Uniform Dispute Resolution Procedure (UDRP), developed by the World Intellectual Property Organization (WIPO) and the Internet Corporation for ASsigned Names and Numbers (ICANN), as the primary dispute resolution procedure in issues related to domain name registrations.

ODR mechanisms have been used for some time. The EU introduced a new dispute resolution platform in 2016. The Online Dispute Resolution Platform, operational since February 2016, helps consumers and businesses settle their online domestic and cross-border purchase disputes (European Commission, n.d.).

Many internet companies (e.g. Google, Facebook, and Twitter) have also developed their own mechanisms. Following the CJEU ruling on the right to be forgotten, Google established a special procedure allowing individuals to request the removal of websites from search results. So far, Google has received over 1.1 million requests for removal, making it the biggest 'juridical' system in history (Google, n.d.).
The COVID-19 crisis has accelerated the use of ODR instruments as traditional courts could not meet in person. We will see the impacts of this change in ODR resolutions in the future.

# TEN clusters of policy topics

From core values and operation principles via policy instruments, we come to concrete policy topics organised in ten clusters. Policy topics are supplemented by an indication of where, by whom, and how they are addressed.

## Critical infrastructure

The COVID-19 pandemic has vividly shown that **digital infrastructure is the critical infrastructure of modern society.**[31] Many vital services from food supply to health assistance and education were delivered online. As our lives shifted online during the lockdowns, the importance of a safe and running internet increased.

This section addresses the main policy topics that support the smooth operation of the internet infrastructure illustrated by three main layers[32]: (a) the *telecommunication layer*, which carries all digital traffic (e.g. a medium like fibre cables or wireless signals); (b) the *technical standards (internet) layer,* which enables computers to communicate with each other and exchange data (like the Domain Name System (DNS) and TCP/IP; and (c) the *content and standards layer,* which enables computers to communicate with users, including, for example, HTML for web browsing Figure 6).

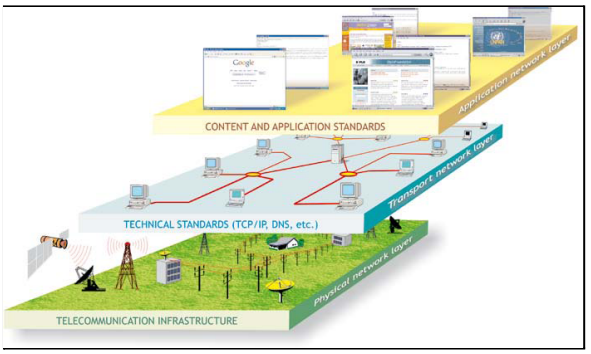


Figure 6. Internet layer structure

The **telecommunication layer** encompasses **a wide range of technologies and systems that carry digital traffic, including landline and mobile telephone networks, power grids, undersea cables, and satellite links**. Frontier technologies in this field include 5G mobile networks; innovative wireless solutions, such as balloons (e.g. Google's 'Project Loon') and low-orbit satellite networks providing access to remote areas; and smarter use of unused frequencies in the radio spectrum (e.g. white spaces). With the fast growth of the internet, the telecommunication infrastructure has and continues to expand with more cables and satellites providing increased bandwidth and speed.

The **internet layer** ensures the **flow of data among internet applications**. This flow is possible thanks to the main standard for coordination between internet networks in the form of TCP/IP. TCP/IP and other internet standards are set by the IETF. Given the core relevance of these standards to the internet, they are carefully and constantly reviewed by the IETF. Any changes to TCP/IP require extensive prior discussion and proof that they are an effective solution (i.e. the 'running code' principle).

Internet protocol (IP) numbers are unique numeric addresses that each device connected to the

[31] On the Common Heritage of Mankind and the Internet's critical infrastructure, see statement by Dr Alex Sceberras Trigona, Malta

[32] This is a simplified version of the seven Open Systems Interconnection (OSI) model layers: physical, data link, network, transport, session, presentation, and application layer. For non-engineers, the three-layer model outlined here is sufficient, yet, fundamental for understanding both how the internet works and what its policy challenges are.

internet must have; each address specifies how to reach a network location (e.g. a website) via the internet routing system. Generally speaking, two devices connected to the internet cannot have the same IP address.

One of the main challenges to the system is the depleting pool of internet protocol version 4 (IPv4) numbers and the slow transition to version 6 (IPv6) due to lack of backward interoperability and the expense involved. Pressure for a swift transition towards IPv6 will continue to increase as users demand more IP numbers due to each user utilising more devices, as well as future IP number needs for IoT-connected devices.

There are also ongoing discussions – within the technical community and SSOs – about the need to ensure that TCP/IP is robust enough to handle the rapid growth of the internet and the emergence of IP-based technologies. To this end, some work is being carried out on designing 'new protocols', one example being the Industry Specification Group on Non-IP Networking established in the framework of the European Telecommunications Standards Institute (ETSI).

**The content and application layer** is the top layer, which facilitates development and uses web applications, apps, and other tools. **The user experience of digital technology comes through apps and web pages on this layer**. The main standard for running the web is HTML, which is managed by W3C. The main challenge will be on the use of these standards for content policy, including dealing with fake news and filtering hate speech. Accessibility for people with disabilities is also managed on the content and application layer of the internet infrastructure.

**Net(work) neutrality** refers to the principle that all data transported on the internet should be treated equally and that internet service providers (ISPs) should not intentionally throttle or block content for commercial or political reasons. Under certain circumstances, exceptions due to technical reasons (e.g. to prevent congestion) or legal reasons (e.g. orders issued by courts) can be accepted. Net neutrality is in some cases regulated and enforced by governments: Brazil (Marco Civil, 2014), the EU (2015), and India (Srinivasan, 2016).

# Security and safety

> *We have the freedom needed to limit and direct technology; we can put it at the service of another type of progress, one which is healthier, more human, more social, more integral.*
>
> Pope Francis, *Laudado Si* [33]

**The vulnerability of the internet is the vulnerability of modern society.** With more than 3 billion users, the internet is the critical infrastructure (CI) of today's society. The financial sector, governmental services, the security sector, schools, hospitals, and citizens are increasingly and irreversibly dependent on the internet. A cyberattack on a hospital during the pandemic crisis can result in the loss of human lives (Hojstricova, 2021) , while attacks on financial institutions can destabilise the entire economy of a country (Henriquez, 2021).

However, security has mostly been an afterthought since the early days of the internet as many market-driven tech companies employed a 'release now, patch later' approach. The growing use of cyberspace by state and non-state actors for malicious purposes threatens peace and security, trust in the digital economy and services, and the potential for the digital transformation of societies and economies.
Security risks for citizens, companies, and countries are interrelated. Vulnerabilities used by criminals can easily slide into a military arsenal and vice versa. Thus, effective digital security requires a holistic approach to better tackle the interplays between security, economic development, human rights, as well as sociocultural and infrastructural aspects.

Three main sets of topics are covered in security and safety online: international peace and security, cybercrime, and child safety online

[33] Pope Francis (2015) Encyclical Letter *Laudato Si* of the Holy Father Francis on care for our common home. Available at http://www.vatican.va/content/dam/francesco/pdf/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si_en.pdf.

**Cybersecurity and development**

The security of the internet is as strong as its weakest link. Very often, the weakest links are found in small and developing countries that do not have the expertise, resources, and institutions to cope with security risks. For example, only 14 out of 56 countries in Africa have operational Computer Security Incident Response Teams (CSIRTs) (SEI, n.d.), which are often the key actors in dealing with cybersecurity threats. Developing countries are much more vulnerable to cyberattacks against CI such as electricity supply systems.

**Cybersecurity and resilience should be considered as development issues benefiting not only the economic well-being of small and developing countries, but all countries; cyber risks in one country affect all.**

## International peace and security

As countries invest in defensive and offensive cyber capabilities, their impact on international peace and security is intensively discussed. These capabilities range from developing cyber tools to attack the information security of other parties (Figure 7) or protecting from such attacks, to leveraging technologies such as AI, robotics, and 3D printing in the context of military operations. It is in this context that cyber conflicts and responsible state behaviour in cyberspace are now placed high on the agendas of regional and international organisations, as states attempt to agree on key issues such as **conduct in cyber conflicts** (How can existing international law be applied to cyberspace? Should new legal instruments be developed as well?); **humanitarian law** (How can the *Geneva Conventions* be applied to cyber conflicts? Should new instruments be devised?); and **weapons and disarmament** (How can cyberweapons be introduced into the disarmament process?).

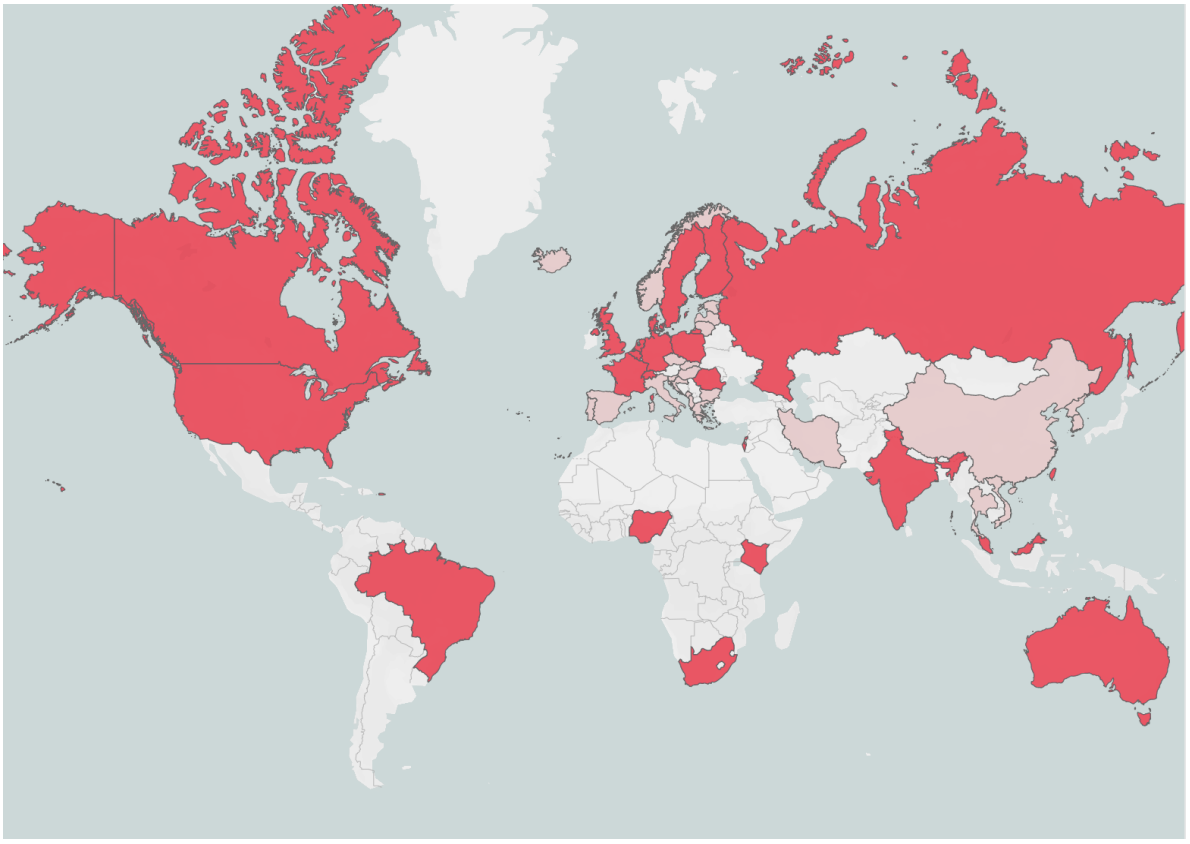

Figure 7. Offensive cyber capabilities map
(red: evidence – 23 countries; pink: indicators – 24 countries)

Digital technologies also impact the use of nuclear technology and associated risks. Another area of security and safety concerns is the use of facial recognition technology (FRT) and biometrics. The use of FRT without proper checks and balances, and outside of the rule of law, can lead to mass surveillance and the violation of human rights.

Most discussions on cybersecurity **norms** are conducted in the framework of the **UN GGE** and **OEWG**; **GGE LAWS** addresses the **use of AI and robots in cyberconflicts**; and **confidence and capacity development activities are undertaken** in regional organisations (OSCE, OAS, ASEAN Regional Forum, SCO).

Forums, such as the Meridian Process and the Global Forum on Cyber Expertise (GFCE), connect governments, the private sector, and other stakeholders for the exchange of knowledge and best practices and the development of policies.

Plurilateral forums (such as the G7 and the G20), as well as some bilateral agreements, increasingly address cyber issues. Multistakeholder initiatives and frameworks include the Paris Call for Trust and Security in Cyberspace and the Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue, n.d.). A greater interplay among these various forums will be fundamental to future success.

## Cybercrime

Cybercrimes are crimes committed via the internet and computer systems. It includes old, i.e. traditional, crimes now conducted through cyberspace (like various frauds), crimes that have evolved through the use of technology (e.g. credit card frauds and child abuse), new crimes that have emerged with the internet (e.g. denial-of-service attacks and pay-per-click frauds), and cybercrime tools that are used to facilitate other crimes (e.g. botnets).

The main international legal instrument for cybercrime is the Council of Europe's *Cybercrime Convention*, which has in turn inspired the development of many national and regional cybercrime regulations. For example, the negotiations on the new UN Cybercrime Convention will start in 2022. There are also regional regulations such as the *African Union Convention on Cyber Security and Data Protection.* Countries are also modernising Mutual Legal Assistance Treaties (MLATs) to use them in the fight against cybercrime. The UN Office on Drugs and Crime (UNODC), Interpol, and other regional organisations coordinate a wide range of activities against cybercrime and tech companies are also active participants in fighting cybercrime and making cyberspace more stable and secure.

## Child safety online

Combating online child sexual abuse and exploitation is the most developed area of international cooperation against cybercrime. Many efforts focus on education and awareness raising to increase the safety of users, in particular children (who make up a third of online users), and to prevent cybercrime, scams, and cyberbullying.

The protection of children online summons the most intensive international cooperation in the digital policy field, involving tech companies, civil society, governments, and international organisations.

Mechanisms include instruments such as the Council of Europe's Convention on Cybercrime and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), and a plethora of international non-governmental organisations (NGOs) and networks that are involved in preventing crime, tracing perpetrators, issuing warnings, and raising awareness among children and caregivers.

### Cybermediation and conflict resolution

Digital technologies can be used in support of safety and security efforts around the world. For example, AI applications are being used to support the work of mediators in multiple ways from supporting knowledge management to enabling a better understanding of the conflict and the parties to the conflict (Hone, 2019). Likewise, VR has significant potential to aid in mediation and peace processes. It could, for instance, enable conflict parties to better understand the consequences of the conflict for non-combatants, and learn lessons from other conflicts (Gregory, 2020).

# Human rights and digital identity

> *The world was relentlessly moving towards an economy that, thanks to technological progress, sought to reduce 'human costs'; there were those who would have had us believe that freedom of the market was sufficient to keep everything secure. Yet the brutal and unforeseen blow of this uncontrolled pandemic forced us to recover our concern for human beings, for everyone, rather than for the benefit of a few.*
>
> Pope Francis, *Fratelli Tutti*[34]

**'The same rights that people have offline must also be protected online'** is a widely accepted principle in human rights law (HRC, 2016). Online, like offline, the value of freedom, as an expression of the singularity of each human being, is respected when every member of society is permitted to fulfil their personal vocation; seek truth and profess their religious, cultural, and political ideas; express their opinions; choose their state of life and, as far as possible, their line of work; and pursue initiatives of an economic, social, or political nature.

The impact of digital technology on modern society is mixed. It has helped connect the world and create new opportunities for billions of people. Digital infrastructure has enabled the normal functioning of society during the COVID-19 pandemic; for example, it helped millions of students to attend school during lockdowns.

Whereas the digital realm has opened new possibilities for the advancement of human rights and freedoms, it has also triggered and amplified infringements of the very same rights. Our fundamental rights are now subject to increased risks. To illustrate, social networking platforms have made it easier to exercise our right to freedom of expression and information, but they also make censorship, violence against journalists, and internet shutdowns possible. Moreover, the **use of surveillance technologies** that gather our sensitive information, **and the extensive amassing of personal data by social media and tech companies has made the exercising of our right to privacy increasingly complex**. The right to privacy itself underpins other rights and freedoms, including the freedoms of association and belief.

**The right to privacy** and data protection came into sharper focus after the revelation of the extensive amassing and use of personal data by social media and other tech companies. The right to privacy underpins other rights and freedoms, including the freedoms of expression, association, and belief. The EU's GDPR, which came into force in May 2018, strengthened data protection and privacy worldwide by inspiring new policy conversations and the adoption of new laws.

[34] Pope Francis (2020) Encyclical Letter *Fratelli Tutti* of the Holy Father Francis on fraternity and social friendship. Available at http://www.vatican.va/content/francesco/en/encyclicals/documents/papa-francesco_20201003_enciclica-fratelli-tutti.html

**Data protection and/vs privacy**
Privacy is usually defined as the right of citizens to control their personal information and decide whether to disclose it. Data protection is a legal mechanism that ensures privacy. Privacy is a fundamental right, recognised in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and in many other international and regional human rights conventions. **Data protection discussions usually revolve around communication privacy (no surveillance of communication) and information privacy (the right of individuals to determine the handling of their personal data)**.

Figure 8 illustrates which countries have or are in the process of establishing legislation on data protection and privacy as of January 2018. Over 100 countries have adopted data protection and privacy laws pertaining to personal information in electronic and physical form.[35] Some 40 countries are in the process of doing so (Banisar, 2018).

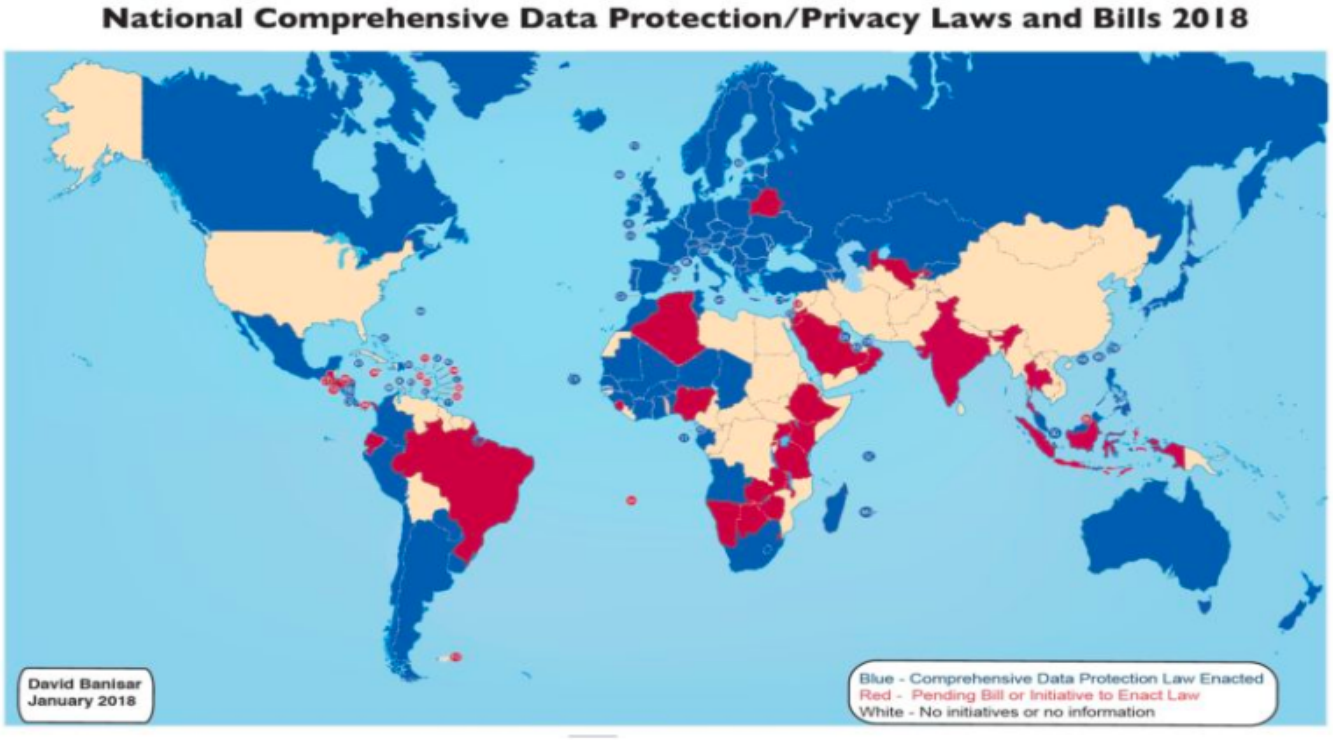


Figure 8. Data protection/privacy laws and bills map
Source: Banisar (2018)

The right to privacy builds on existing international instruments on privacy protection that apply online. In addition, there are new instruments such as the *UN Resolution on Right to Privacy in the Digital Age* (UNGA, 2015), and the OECD's *Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data* (OECD, 2013). Given the centrality of personal data in issues such as privacy and consumer protection, **the issues of big data, e-commerce and digital business models, freedom of expression, AI, IoT, and emerging technologies are very relevant to this right**.

[35] Brazil, Bahrain, and St Kitts and Nevis have also adopted Data Protection/Privacy Laws in the meantime.

**Gender rights online** address a major gender gap that digital developments have amplified. Fewer women access the internet than men, particularly in developing regions. For instance, in Africa 22.6% of women have access to the internet compared to 33.8% of men (Ugwuede, 2020). In addition, tech industry jobs, especially decision-making positions in tech, are mostly held by men. A recent study shows that women in the USA only account for 21.57% (Richter, 2019) of tech jobs in major tech companies.[36] **Gender rights online are also important for containing increasing online violence against women and young girls**.

Several organisations and initiatives focus on gender equality in the tech sector, including UN Women, ITU's EQUALS network, the W3C Foundation's Women's Rights Online network, and the IGF's Dynamic Coalition on Gender Rights. The 2016 *Report of the UN Special Rapporteur on violence against women, its causes and consequences*, noted online violence against women as a new challenge (HRC, 2016).

**The rights of people with disabilities** were strengthened with new online tools and services that can overcome disabilities barriers. Yet, **there are still major obstacles due to the limited accessibility of some of the platforms and tools**. The main framework for digital cooperation is provided by the *Convention on the Rights of Persons with Disabilities* (UN, 2006). Many activities are conducted by the IGF's's Dynamic Coalition on Accessibility and Disability; the Internet Society Disability and Special Needs Chapter; and the International Center for Disability Resources on the Internet. International standards in web accessibility are developed by W3C through its Web Accessibility Initiative.

**The right to be forgotten** derives from the right to erasure, a long-standing principle in EU data protection laws. In 2014, the CJEU extended this right to what is known today as the 'right to be de-indexed' (EC, 2014). **Users can request platforms to de-index names (i.e. remove them from search results) in justifiable circumstances**.

[36] Major tech companies considered in this study include Google, Microsoft, Apple, Uber, Facebook, Twitter, Amazon, and Netflix.

The right to be forgotten is now also regulated by the EU GDPR, which entered into force in May 2018. In other regions, several countries (such as Indonesia and South Korea) have codified this right into law. Court cases have also been interpreting and applying this right to other online spaces, such as online company registries and court databases.

**Children's rights online** are of high importance as one-third of internet users are under 18 years of age (Livingstone, 2016). **The human rights approach introduced a new angle to the previously predominant focus on child security and safety**. The main international instrument is the *Convention on the Rights of the Child* (1989). The UN Children's Fund (UNICEF), together with academia, civil society, tech and the tech sector, leads intensive cooperation in this area.

At regional level, the Council of Europe has developed a Strategy for the Rights of the Child.

**The rights of the elderly online** are gaining new relevance due to a rapidly increasing elder population. **By 2035, the number of people aged 65 and above will outnumber those under the age of 18 in the world**. Online technologies can help the elderly to live independent, autonomous, dignified lives; improve their emotional well-being; and increase their access to education and lifelong learning. The rights of the elderly have gained relevance worldwide and, in particular, in Japan and China due to the fast ageing populations in those countries. Discussions on digital and ageing should be built on existing mechanisms such as WHO's *Active Ageing Framework*.

## Digital identities

Digital identities shape human rights and the overall participation of individuals in digitally driven economic and social life. Digital identity refers to identifying individuals directly via an ID or online credentials or indirectly through transactions we conduct (contacts, transfers of money) or digital artefacts we use (mobile, driverless cars, home appliances). Digital identity solutions are provided by tech platforms and governments.

Tech platforms, such as Facebook and Google, filled the gap in digital identity by providing credentials to access to many digital platforms and services.[37] This role of an 'identity broker' gives tech companies significant power over data and, in turn, a deep understanding of individuals' economic, political, and social activities. Digital identities and associated data are used as the basis for business models by leading tech companies.

Governments, as traditional providers of citizen identities, have tried to issue digital identities as well. One of the most developed systems is India's Aadhaar and India Stack, which aim to provide a digital identity to 1.3 billion citizens as part of public services with the necessary mechanisms for the protection of identity, privacy, and security of citizens (Stacey, 2018). Based on this publicly owned infrastructure, businesses and other actors can provide their services, such as e-commerce or inclusive finance.

**Digital identity opens many *policy issues***. These include the protection of privacy and anonymity of biometric data, the protection of children, and potential risks of misuse of digital identity in the case of conflict and crisis (e.g. attacks against minorities).

# Development

> *How wonderful would it be if the growth of scientific and technological innovation would come along with more equality and social inclusion.*
>
> Pope Francis, Vancouver[38]

Development and technology have been twins of progress for centuries. More technology means more development. The record of tech-driven progress is impressive in many segments from improving our well-being to great innovations and economic growth.

While technology has contributed to alleviating poverty and improving the well-being of many, however, it has posed risks for society. For example, technologies like AI may challenge the centrality of human beings in the growth of society and, consequently, the relevance of progress. As the singularity movement argues, humans may have to share their unique rule with artificial systems. Progress may take on a different shape, becoming a more ethical than technological issue.

In this context of the need for a holistic approach to digital development, we focus on the following aspects: the digital divide, inclusion, inequalities, and capacity development

## Digital divide

The digital divide can be defined as a rift between those who have access and the capability to use digital technology, and those who, for technical, political, social, or economic reasons, do not. The OECD refers to the digital divide as 'the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the internet for a wide variety of activities' (OECD, 2001, p. 5).

The COVID-19 crisis exacerbated digital divides. Many communities in rural, remote, and low-income areas remained unconnected at a time when the rest of the world shifted online. Already achieved levels of access to education, health, and markets deteriorated as they remained disconnected.

## Inclusion

Inclusion starts with access to networks as a precondition of all other inclusions. But it is far from being sufficient. A study that investigated why internet adoption has stagnated in sub-Saharan Africa, despite the improvements in connectivity infrastructure and affordability (Internet Society, 2016), points to the importance

[37] Many apps and online services can be accessed by existing Facebook or Google profiles or credentials. Users do not need to provide new usernames and passwords.

[38] Pope Francis (2017) Video message of His Holiness Pope Francis on the occasion of the TED Conference in Vancouver. Available at https://www.vatican.va/content/francesco/en/messages/pont-messages/2017/documents/papa-francesco_20170426_videomessaggio-ted-2017.html

of fostering locally created content, in familiar languages (which are often different from the official national language). It also recommends that content is adjusted to the local cultural context, to enable individuals to perceive the usefulness and relevance of connecting to the internet. Cultural diversity can facilitate economic dynamism and financial inclusion in local communities.

The promotion of multilingualism online requires technical standards that facilitate the use of non-Latin alphabets, as well as the implementation of these standards by developers, vendors, and service providers.

It has limited impact, however, if there are no other policy and educational conditions to maximise on the use of digital technology. The gap between the developed and the developing world is more significant in the area of knowledge contribution than, for example, access to the internet. For example, Hong Kong (SAR China) provides more content to Wikipedia than all of Africa combined, although Africa has 50 times more internet users (Kurbalija, 2016).
Inclusion has various aspects including **financial inclusion,** i.e. access to affordable, useful, and trusted financial and banking services; and **economic inclusion,** i.e.participation of all individuals, groups, and communities in the labour market, equal access to entrepreneurship opportunities and other business activities in the digital economy. **Policy inclusion** requires the development of individual and institutional capacities to formulate and execute policy initiatives around issues of concern of specific communities, such as women, the elderly, or youth.[39]

[39] Inclusion often boils down to the simple participation of a few missing actors in the events. Very often, it does not imply representation of these communities. Thus, genuine representation would require much more bottom-up capacity development and discussions, which should probably take place first at the national level, through associations (e.g. student unions, associations of indigenous groups), etc. The conclusions of these discussions would feed into the global debate (the individuals travelling to events would be carrying a more mature message forward, due to previous discussions). This is clearly stated by advocacy groups for persons with disabilities' stipulation: *Nothing about us without us.*

## Inequalities

Digital technology tends to amplify existing **inequalities.** When the developed world takes advantage of the benefits offered by technology, those who do not have access to such technology become even more vulnerable. Since its outbreak, the COVID-19 pandemic has exposed and exacerbated existing socio-economic inequalities, such as the **digital divide**. Many communities in rural, remote, and low-income areas remained unconnected at a time when the rest of the world shifted online. Without adequate infrastructure and affordable internet access, there is no digital economy. This is why the existing gap between the digital 'haves' and 'have nots' conditions the development of the digital economy in low-income countries, preventing them from reaping the benefits of the digital economy.

According to the *Global Risks Report 2020*, published by the World Economic Forum (WEF, 2020), digital power concentration and digital inequality are among the top ten major risks that are likely to pose a threat to global stability. This means that a more balanced distribution of the wealth generated by the digital economy is not only a matter of improving justice, fairness, and equality but also a strategic decision that would benefit both developing and developed countries.

## Capacity development

In the context of this white paper, our focus on capacity development[40] is for active and impactful participation in digital governance, policymaking, and overall digital cooperation.

A locally developed programme anchors capacities in local cultural dynamics, which provides motivation for action. For example, in India, the Digital Empowerment Foundation (DEF, n.d.) has developed the capacity of the local police and

[40] In the context of digital cooperation, the Swiss Agency for Development and Cooperation's (SDC, n.d.) definition of capacity is useful: 'The ability of people, organizations, systems of organizations, and society as a whole to define and solve problems, make informed choices, order their priorities, plan their futures, and to implement programmes and projects to sustain them.'

community officials by building their understanding and skills to deal with digitally triggered local violence. It involves training, coaching, and the development of institutional capacities to deal with digitally triggered social violence. Practical activities include monitoring social media, engaging with influencers, and creating connections with tech companies.

For inclusive participation in global governance, there is a need to have simpler entry points for actors with limited human and institutional resources, in particular from, but not only from, small and developing countries.

Digital governance help desks should be established to help prepare new policies, draft new legislations, participate in negotiations, and implement digital norms and standards. Digital governance help desks should be established on global, regional, and national levels.[41]

[41] At national level 'entry point' could be established in the cooperation of UN country offices.

# Environment and the ecosystem

> *We need a conversation which includes everyone, since the environmental challenge we are undergoing, and its human roots, concern and affect us all.*
>
> Pope Francis, *Laudato Si*[42]

New technologies can help expand peace by enhancing environmental sustainability, thereby mitigating the effects of climate change and sparing the world the geopolitical instability that is intrinsically linked to the degradation of our ecosystems. The transition to a low carbon economy can be made more quickly via the effective deployment and use of technologies, particularly among communities and nations that depend on fossil fuels and other environmentally degrading practises.

However, how can we use these new technologies for the good of the many and not for the profit of the few? How can we hope to benefit from the use of these technical advancements if the ethical and spiritual roots of our environmental problems are not clear to ourselves? Moreover, is it realistic to speak of environmental sustainability and the green transition if in employing digital technologies, we do not consider the broader impact they have on people and societies? How can we be sure not to leave anyone behind in this transition?

Digitalisation has a multifaceted impact on nature and the environment. While technologies such as AI and big data can monitor and preserve endangered species on land or detect overfishing practises and pollution levels in ocean habitats, rapid digital transformation comes at a cost to our environment. In part, the answer to this challenge lies in developing technologies that are sustainable by design to help move the needle towards a more sustainable and circular economy.
The nexus between environment and digital could be followed in the following aspects of environmental policy: atmosphere, biodiversity, climate change, energy consumption, food and agriculture, land and deforestation, oceans and seas, use of rare materials, pollution and e-waste, and water. However, three policy areas stand out, and cover the lifecycle of digital products and infrastructure: energy consumption and its relationship to climate change, raw material extraction and e-waste, and the pursuit of a circular economy.

## Impact of digital growth on energy consumption and climate change

Digitalisation consumes a lot of energy. This is even more so the case with the latest tech developments, such as AI, blockchain, and cryptocurrency. At present, estimates show that if the internet were a country, it would rank 5th or 6th globally in terms of electricity usage (FRANCE 24 English, 2017).

High levels of energy consumption and therefore greenhouse gas emissions also apply to other digital technologies. As noted earlier in this paper, bitcoin mining alone consumed some 64.15 TWh of electricity in 2019 (Vincent, 2019), exceeding the energy demand of countries like Chile, Switzerland, New Zealand, and Bangladesh. Data centres, for their part, are responsible for 2% of global electricity consumption and forecasts expect demand to increase to 8% by 2030 (Elegant, 2019).

Digitalisation's demand for energy will only grow as more integrated systems emerge, especially as 5G and the IoT are adopted and developed. Thus, there is a need for action aimed at both reducing energy consumption and ensuring it comes from renewable sources.

Immediate possibilities for reducing energy consumption can be found in the manufacturing phase. Eighty per cent of

[42] Pope Francis (2015) Encyclical Letter *Laudato Si'* of the Holy Father Francis on care for our common home. Available at http://www.vatican.va/content/dam/francesco/pdf/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si_en.pdf

energy consumption associated with mobile phones (OpenMind, 2020) is tied to the manufacturing phase, including the mining and extraction of raw materials and their transportation to industrial facilities worldwide. Technologies like blockchain can help reduce energy consumption by making digital production supply chains more traceable and transparent.

On the supply side of energy, digital technologies can be implemented in smart grid and virtual power plants (Power, 2020), allowing for two-way communication between utilities and their customers, as well as the use of sensors for more effective electricity transmission thus ensuring better demand response.

## E-waste and the use of raw and rare earth materials

Digital hardware requires the extensive use of raw and rare earth materials, particularly when it comes to the production of microprocessors, cameras, hard disks, batteries, and electronic displays, among others. For example, a smartphone contains most of 16 of 17 rare earth elements (Rohrig, 2015).

The use of raw and rare earth materials has a two-fold impact on the environment. First, their extraction process is toxic and expensive. 'Rare' is not related to their availability in nature, but rather their toxic and expensive extraction process. Second, the recycling of raw and rare earth materials has become a significant issue when it comes to digital products, resulting in significant amounts of so-called e-waste.

Out of the over 50 million tonnes of e-waste generated annually, only 20% is recycled (Ryder and Houlin, 2019), while the remainder is tossed into landfills or incinerated, degrading our earth, air, and water. This is a long-term threat to human nature, as heavy metals such as mercury, lead, bromine, and arsenic seep into the soil and groundwater.

We must also consider the inequality in e-waste practices – most e-waste is sent to developing countries, meaning that the greatest consumers of digital products (developed countries) are largely spared its adverse effects. To this end, both the production and disposal of raw and rare materials open a wide range of environmental and human rights issues (Penke, 2021). Sustainable by design and circular economy approaches are essential in reducing the impacts associated with digital products. Far greater efforts must be made in ensuring the longevity of digital products and the effective recycling of such products.

## Circular economy as a holistic solution for digital technology and the environment

The circular economy (Figure 9) is often considered an integral solution that can protect the environment while maximising the use and potential of digital technologies.

**Definition of a circular economy**

Looking beyond the current take-make-dispose extractive industrial model, a circular economy aims to redefine growth, focusing on positive society-wide benefits. It entails gradually decoupling economic activity from the consumption of finite resources and designing waste out of the system. Underpinned by a transition to renewable energy sources, the circular model builds economic, natural, and social capital. It is based on three principles: design out waste and pollution; keep products and materials in use, and regenerate natural systems.

*Ellen McArthur Foundation* (n.d.) definition of circular economy

A circular economy opens new possibilities, including reducing pressure on the environment, improving the security of the supply of raw materials, increasing competitiveness, stimulating innovation, boosting economic growth, and creating jobs.

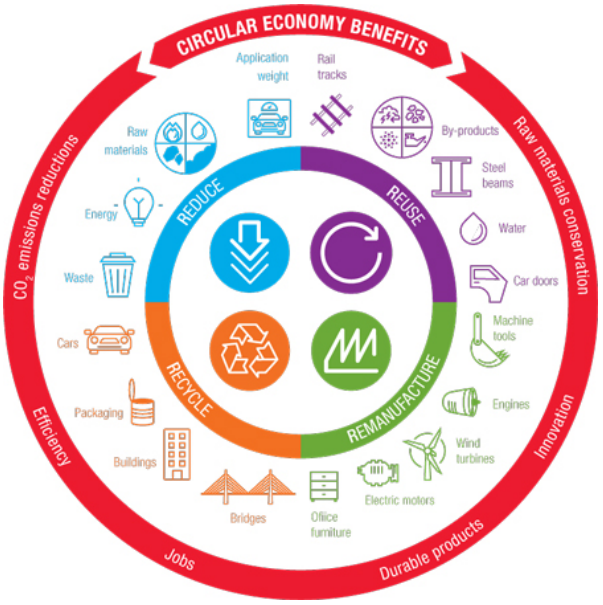


Figure 9. Circular economy scheme[43]

## Main instruments and forums that address the interplay between digital technology and the environment

The 2030 Agenda for Sustainable Development (2015) provides a broad framework to address the complex interplay between digital technology and the environment. For its part, climate change is addressed in the process initiated by the UN *Framework Convention on Climate Change* (UNFCCC, 1992) with numerous subsequent protocols and agreements, including the highly prominent *Paris Agreement (2015).* For e-waste, the main instrument is the *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal* (1992) that, among other provisions, outlaws the export of e-waste from developed to developing countries. On the regional level, the EU has issued its *Circular Economy Action Plan* (CEAP, 2020) as part of the European Green Deal.

International organisations like the World Meteorological Organization (WMO), the UN Environment Programme (UNEP), and ITU are also addressing the relationship between digital technology and the environment.

SDOs are focusing on the nexus of digital and environment as well. ISO, the IEC, and ITU, in particular, are developing standards intended to encourage the development of digital technologies that are more environmentally friendly and energy-efficient. These standards could have a direct impact on the production of digital devices that are sustainable by design.

At the ITU Telecommunication Standardisation Sector (ITU-T), one of the 11 study groups (technical bodies where standards are developed) – SG 5 on the environment, climate change, and circular – is dedicated to developing standards to guide the use of ICTs in an eco-friendly way and to reduce the adverse environmental effects of e-waste, among others. At ISO, the organisation's General Assembly adopted, in September 2021, the *London Declaration to combat climate change through standards*, highlighting the role of ISO standards in supporting the climate agenda. In November 2021, all three SDOs expressed their readiness to support the work of the group of experts announced by the UN Secretary-General to 'propose clear standards to measure and analyse net-zero commitments from non-state actors' (Naden, 2021).

[43] Source: https://unctad.org/topic/trade-and-environment/circular-economy

## Economy and labour

**The impact of digitalisation on the economy is cross-cutting and profound.** On the one hand, **digital technology is a major enabler of economic dynamism. Humankind can use technology** to boost innovation, increase consumer choices, and enhance human well-being. In addition, during the COVID-19 pandemic, the digital industry played an important role in providing critical services for society, from the delivery of food to online learning and work.

On the other hand, the **benefits of the digital economy – in terms of productivity and labour opportunities, for instance – are neither as big nor as evenly distributed as often claimed.** According to the World Bank's (2016) *World Development Report 2016: Digital Dividends*, the gap between the promises of digital technology and its real impact on the economy is widening. For example, the increase in productivity is only 2% in the digital era, compared to the 6% of productivity increase generated by previous innovations in electricity and transportation (ibid.). There is a persistent concentration of digital assets, such as data sets, in the hands of certain large technology companies located in a few jurisdictions, and market forces alone have not been able to ensure the structural change and technological upgrading of developing countries.

In addition, the centralisation of the economic power of tech companies increases as digitalisation penetrates other segments of the economy from services to manufacturing, transportation, and traditional retail. Through mergers and acquisitions, large companies are consolidating further across sectors, and the data they amass in each sector gives them even more of an edge (James, 2020). Apple, Microsoft, Amazon, Alphabet (Google), Facebook, Tencent, and Alibaba are increasingly investing in all parts of the global data value chain: data collection through platform services; data transmissions through submarine cables and satellites; data storage (data centres); and data analysis, processing, and use (UNCTAD, 2021).

The first step in amplifying potential and managing risks is to understand which companies generate profits, and how related regulatory issues affect them (Table 3).

**Table 3. The main digital business models**

| Business model | Examples of companies | Source of revenue | Regulations |
|---|---|---|---|
| The e-commerce model | eBay, Amazon, Alibaba Taobao, Marketplace, Spotify | Income from sales of goods and services through online stores and marketplaces | Most existing regulations apply. Open issues: consumer protection for cross-border sales, taxation, algorithm pricing |
| The hardware and software provider model | Microsoft, Oracle, SAP, Symantec, Totvs, Huawei, Apple | Cost, fees, and subscriptions for the use of hardware and software | Most existing regulations apply |
| The internet access model | ISPs worldwide, such as Verizon, Telefonica, Swisscom, and China Telecom | Subscriptions for gaining access to the internet | Most existing regulations apply |
| The cloud service model | Amazon Web Services, Salesforce.com, Microsoft Cloud | Fees for renting server spaces and for making use of services in the cloud | Open issue: data protection, jurisdiction |
| The internet advertising model | Facebook, Google, Twitter Flickr, Telcent | Income from advertising based on data provided by users | Issues: data protection (especially in the context of cross-border data transfers), competition policy, content policy |
| The internet platform model | Uber, Airbnb, Turo (formerly RelayRides), Amazon Mechanical Turk, TaskRabbit Handy | Fees from linking customers to providers, or otherwise un- and underutilised resources (also known as sharing economy platforms) – a business model that was made possible by the internet | Issues: consumer protection, competition policy, labour rights |

One of the main challenges is to regulate data-driven internet business models in which there is no direct financial transaction between consumer and tech platforms (Figure 10). Instead of money, a user contributes their data, which is then processed by tech companies. Intelligence extracted from data is sold to vendors for advertising and other purposes. Thus, internet users end up providing data free of charge and paying for advertising by purchasing goods and services.

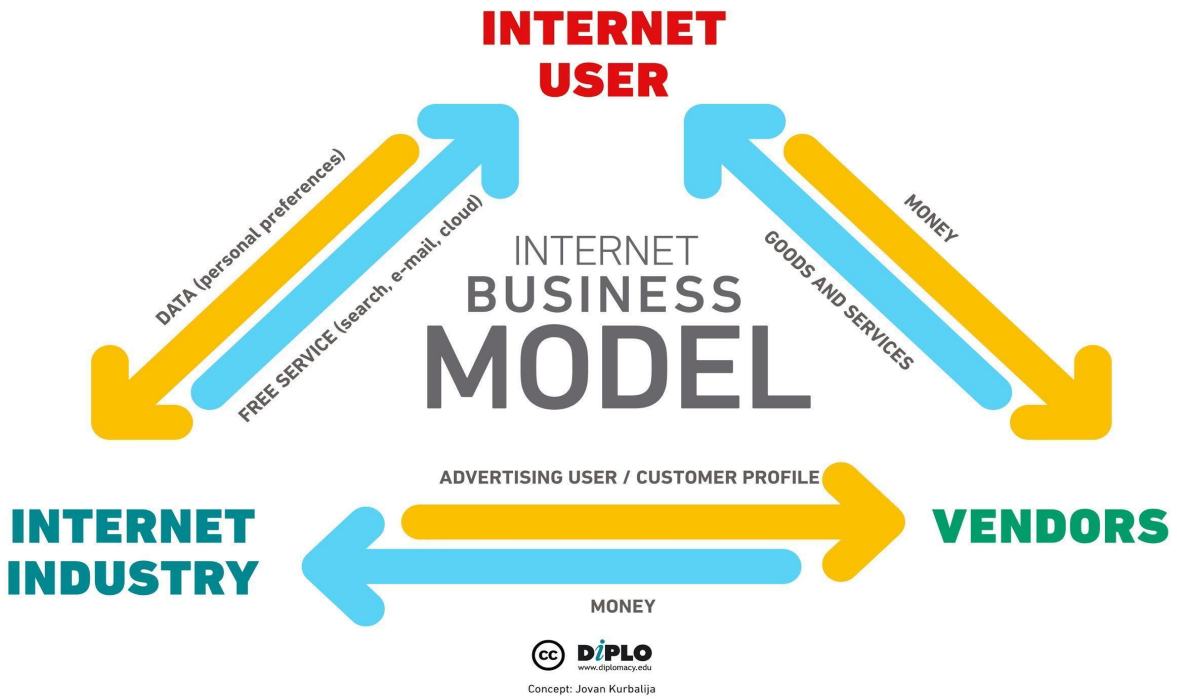


Figure 10. Schema of the internet business model

## Competition policy and anti-monopoly

Market regulators worldwide from Beijing to Brussels and Washington DC are trying to curb the market domination of tech monopolies and ensure the vibrancy and innovation of global economic life.

The tech sector is prone to concentrating economic power naturally as it benefits from the networking effect by which each additional user adds to the value of companies *exponentially*. This also triggers the *data-network effect*. Companies use data to attract more users, who then generate more data, which in turn helps improve services, and ultimately, attract more users. This dynamic creates new market distortions, in particular through the use of data in the context of AI systems.

The main underlying challenge is that the data-network effect creates natural monopolies that strengthen consolidation and concentration in the digital economy and distort market competition.

**How do we deal with tech monopolies?**
In dealing with digital antitrust cases, many competition authorities are entering uncharted terrain facing the following main challenges. They have to develop a trial-and-error approach with fast-feedback loops and the need to quickly adjust approaches and policies in a way that reflects the fast-changing digital economy. They face the following specific challenges:
First, current competition regulatory mechanisms are very slow. Taking five years or more to issue a decision in a competition case, for instance, is almost an eternity compared to the fast-changing digital industry.

Second, the evidentiary requirements imposed on competition authorities, while justified by the need to make these authorities adopt responsible behaviour, are very strong. A case in point is preemptive mergers, where dominant firms may swallow up their future rivals. As the latter often have not yet sold anything or are operating in a very limited market niche, no data can be brought to bear on a decision and so such mergers cannot be challenged.

Third, most small and developing countries cannot have their own competition policy in the digital realm mainly due to a lack of capacity in the field of digital regulation. But the absence of adequate competition policy could endanger their economic and social stability as many local and traditional bricks-and-mortar businesses might be overtaken by global tech giants. Competition policy can support gradual and well-managed economic transitions and could facilitate the growth of digital small and medium enterprises (SMEs) in small and developing economies.

**How do we avoid monopolies and increase competition among existing and new social media platforms?**

Technical, data, and market interoperability can foster competition across different tech platforms and prevent user lockdown in one of them. For example, interoperability among social media platforms such as WhatsApp and Telegram can help users to move freely with their data and network of users (friends). While a user can export their data from most existing platforms, there is no solution to maintain the same network of friends after moving from one to another platform. Technical solutions for this interoperability among social media platforms are possible. For their implementation, **there is a need to adopt data/network sharing standards and make compliance with these standards a precondition for access to national and regional markets.**

## Taxation

Three major developments have put taxation in the focus of digital policy**.** First, governments worldwide are searching for new fiscal streams to supplement countries' budgets hit by public deficits and austerity measures, particularly after the 2008 financial crisis. Second, traditional industries, such as advertising and retail, are increasingly digitalised and often operating beyond national jurisdictions, leading to shrinking fiscal revenues for governments. Third, the tech industry is shifting profits offshore to avoid paying taxes in the countries that host their economic activities. According to a study by the US Public Interest Research Group, the top 30 US companies with the most money held offshore include 10 major internet companies (McIntyre et al., 2015).

**The traditional model of taxation is based on the jurisdiction where tech companies are legally incorporated.** For example, in Europe, many tech companies are legally incorporated in Ireland, which is, therefore, also the country where they are taxed. However, this model is not sustainable as many countries in the EU and beyond require taxation in jurisdictions where value is generated, which is where the users of tech services are located.

At the global level, the OECD is the main policy space for addressing international digital taxation issues. The 1998 OECD Ottawa Principles, the main international document on digital taxation, specifies that offline tax regulation apply online.[44] In October 2021, over 140 countries agreed to a new set of global tax rules jointly developed by the OECD and the G20.

These taxation rules establish a new procedure for deciding the jurisdiction(s) where very large multinational companies – those generating more than €20 billion in revenue – should pay their taxes. Rather than the jurisdiction in which they are incorporated, it will be those countries where the companies are the most economically active; this will be determined by a complex formula. Second, the new OECD rules will oblige countries to impose a minimum tax rate of 15% on companies earning more than €750 million in revenue. The new rules will take effect in phases, starting in 2022. This major global tax reform, which is expected to be implemented in 2022, aims to ensure that profits are distributed more fairly and to promote healthier tax competition among countries.

[44] The OECD Guidelines restate the applicability of core taxation principles online: taxation of digital commerce should be based on the same principles as taxation for traditional commercial activities: neutrality, efficiency, certainty and simplicity, effectiveness and fairness, and flexibility; Organisation for Economic Cooperation and Development [OECD] (1998) *Electronic Commerce: Taxation Framework Conditions.* Available at https://www.oecd.org/ctp/consumption/1923256.pdf

## Trade regulation and e-commerce

In a post-pandemic scenario, the shift towards e-commerce is considered an opportunity to boost economic recovery. Nevertheless, the acceleration of e-commerce has significantly occurred mostly in developed economies and relatively high-income developing economies. Even though the pandemic has pushed more consumers in developing countries to buy online, many e-commerce businesses in these nations have seen a slump in sales due to the sharp fall in disposable income (UNCTAD, 2020).

SMEs and retail businesses were less able to scale up their processes and respond to increased demand for online shopping for goods and services. At the same time, big internet companies – whose business models are data-intensive – have seen their profits rise during the pandemic. Some of them, such as Facebook, saw their shares reach all-time highs in 2020, after the launch of online shopping features (Bursztynsky, 2020), a development that further blurs the line that separates e-commerce and the data-centred business model of social media platforms. The disparity regarding internet usage growth during the pandemic corroborates the magnitude of the digital divide.

The uneven digital leap forward taken by many industries and countries risks widening the gap between the technological haves and have-nots, threatening to scale back progress on reducing global poverty and inequality and further damage social cohesion and global cooperation (WEF, 2021). In this scenario, international and regulatory cooperation are of key importance not only to facilitate seamless cross-border trade but also to foster inclusion in the digital economy.
Trade agreements create an enabling environment for e-commerce, but they also result in significant redistribution and create winners and losers. The influence of a few countries from the developed world on agenda-setting and norms-making, and the influence of private sector special interest groups on the formulation of trade policy suggest that concentration trends could be reinforced, both in terms of economic and political power. Without proactive policies to tackle the digital and data divides, social and economic inequalities are likely to increase.

As the key policy player in modern global trade, the World Trade Organization (WTO) has established a system of agreements that provides the legal architecture for the liberalisation of international trade. At the WTO, discussions on e-commerce take place on two parallel tracks: the WTO Work Program on Electronic Commerce (WPEC), launched in 1998 with a non-negotiating and exploratory nature, and the Joint Statement Initiative (JSI) on e-commerce, which aims to produce a binding agreement among its members.

Some – mainly developed – countries argue that the WTO should negotiate legally binding rules for e-commerce. Others, mainly developing countries, argue that it is premature to adopt legally binding rules before open issues are addressed, such as the distinction between services and digitised goods now sold online – books, music, films – and before the problem of access and capacity development for digital commerce is tackled.

Currently, the total number of WTO members formally participating in the e-commerce JSI negotiations is 87. These account for slightly more than half of all WTO members and 90% of global trade (WTO, 2020a; 2020b). There are four participants from least developed countries (LDCs), namely Benin, Lao PDR, Myanmar, and Burkina Faso. The number of participating WTO members from Africa has increased to six over the last few years: Benin, Nigeria, Côte d'Ivoire, Kenya, Cameroon, and Burkina Faso. The regions that are least represented in the JSI are Africa, with X, and the Caribbean, which has no participants. In addition, none of the developing Pacific Island countries are part of the JSI.

So far, one of the main challenges in e-commerce negotiations is the cross-cutting nature of this regulatory field. Namely, the e-commerce agenda – whether global or regional – encompasses several elements that go well beyond the traditional trade agenda, such as technical standardisation, data flows, cybersecurity, data protection, and privacy (Figure 11).

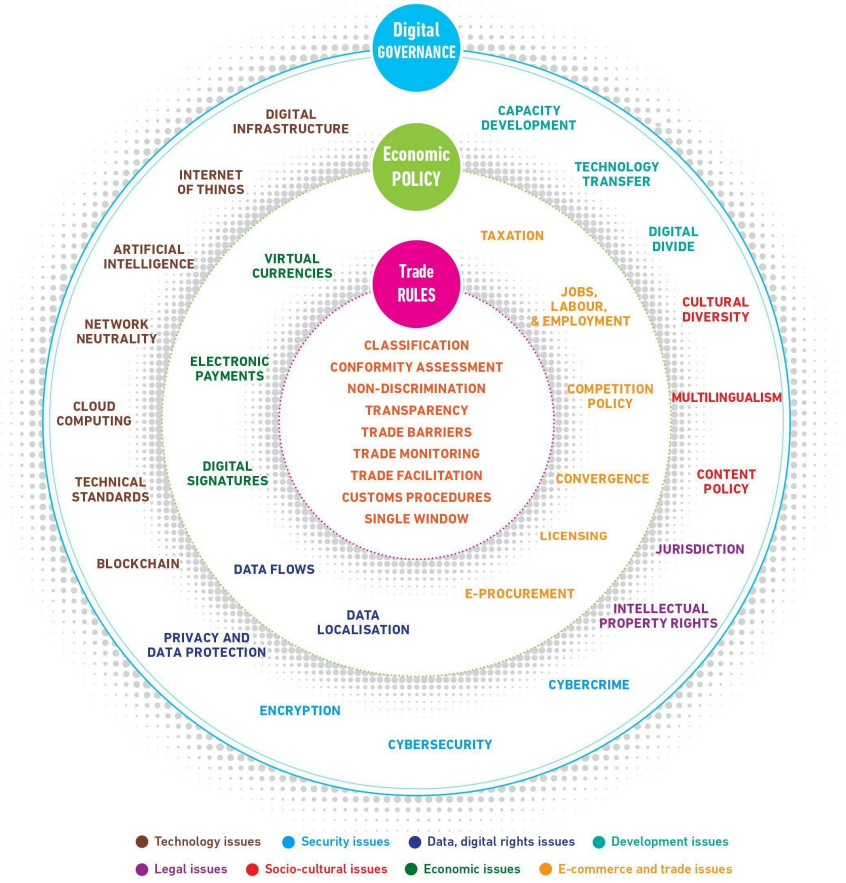


Figure 11. Digital economy schema

To meet such a level of complexity with appropriate responses, it seems essential to develop multiplayer and multilayer governance and policymaking mechanisms, and to provide developing countries and LDCs with the necessary capacity development and support, so they can meaningfully engage in trade negotiations, voicing their development-oriented priorities. In a scenario of growing inequality, e-commerce norms cannot be only a mechanism for online trade liberalisation; they also need to assist in promoting growth, development, equality, and human dignity.

## Future of work and labour issues

Another challenge that comes with the digital economy is related to the future of work and the threat of potential job loss with the rise of AI, robots, and automation. **Some estimates indicate that by 2022, around 54% of all employees will need to adapt or acquire new skills** (WEF, 2018a)**.**

One of the characteristics of the emerging labour market will be polarisation towards, on the one hand, highly specialised top experts, and on the other, manual workers. The machinery of the middle layers, especially in administration and management, is likely to shrink in size and importance. There is a hope that this shift will free some time for creative work instead of repetitive tasks. While it remains to be seen if this promise will be realised, the immediate focus should be on assisting transitory generations. Every industrial revolution from textile factories till today had a lost generation that got caught in the middle of the transition.

In the fast-changing labour landscape, sharing economy platforms (also known as platforms operating in the gig, access, or collaborative economy) have given rise to new types of jobs. Companies operating in the sharing economy have three main features in common: the prevalence of contractual and temporary employment, a digital

platform or app for (quasi) peer-to-peer transactions, and a rating system for evaluating the quality of the service provided. While these features have helped companies grow, the sharing economy also brought sharper focus to issues related to the protection of workers' social well-being and labour rights.

Shifts in the labour market also have gender aspects, with a prediction that 57% of the workers expected to be affected by disruptions in the labour market will be women (WEF, 2018b).

The International Labour Organization (ILO) is leading the efforts in preparing the job market for changes in the volume and type of work, and in the protection of labour. International and regional organisations and national courts are also contributing to shaping the market and the rights of labourers.

# Education, culture, and science

Education, culture, and science should help create a creative and ideal foundation for the digital empowerment of citizens, communities, and countries worldwide. These are separate but interrelated policy topics.

**Education** provides the necessary skills, knowledge, and awareness for the effective use of the internet. There are many capacity development and training initiatives aimed at providing digital skills; however, only a very few focus on the less practical, but essential aspects of the ethical, critical, and responsible use of digital technologies.

The emergence of new technologies and their rapid advance in the labour market is changing the nature of work and requires the adoption of new technological skills, and knowledge to keep pace with and make the most of future technological changes. Studies estimate that 65% of the children in primary school today will have jobs that do not exist yet (Devaux et al., 2017).

**Adjusting to the digital era should be highly prioritised by states and should therefore be ingrained in their respective educational curricula.** For instance, a number of countries, such as France and Norway, have already integrated digital literacy into their national curriculum (Ibid.). Nonetheless, educational institutions are not the sole responsible actors on this matter. Education on the effective use of technologies should be encouraged and promoted throughout society and as such is the responsibility of everyone.

Acquiring necessary skills and knowledge is also critical for bridging the digital divide and turning it into a 'digital opportunity for all' (WSIS, 2003). Therefore, digital empowerment is a key component for both economic growth and social development worldwide.
The widespread use of digital technologies following the outbreak of the COVID-19 pandemic has shed light on the fundamental right to access education. About 463 million children (31% of schoolchildren) worldwide do not have access to technologies needed for online learning (UNICEF, 2020).

## Education and capacity development

In response to the spread of COVID-19, authorities have taken a set of measures ranging from travel restrictions to city shutdowns. Education is another area of social life that has been affected by the outbreak.

Schools and universities across the world are resorting to online learning. In Italy, a number of schools have closed down since the outbreak and the authorities have resorted to different digital tools and platforms, such as Skype, Google Suite for Education, and Office 365 Education to keep the classes going. The Ministry of Education has called on school directors to activate, for the duration of the suspension of teaching activities in schools, distance teaching methods, with particular attention to the specific needs of students with disabilities (Pellegrini and Maltinti, 2020).

In China, telecom carriers developed online learning solutions to enable students to continue their studies from home while regular classes have been suspended at schools (Si, 2020).

However, a number of schools are experiencing difficulty in providing online learning to their students for several reasons ranging from lack of necessary infrastructure (Shapiro and Gold, 2020), appropriate training for educators (Lowen, 2020), and the general absence of digitalised teaching content . Furthermore, students lacking access to broadband will not be able to join and participate in the new learning environment (McGill, 2020).

Data shows that many more children worldwide were kept out of the education system in 2020 compared to previous years (DW, 2020). It is estimated that half of the total number of learners affected by school closures do not have access to a household computer, and 43% have no internet access at home (UNESCO, 2020).

# Humanitarian assistance

Humanitarian assistance has been affected by digitalisation on numerous levels. Tech tools and platforms became effective tools for spreading awareness of local and global issues, especially to communities which would normally be out of the reach of traditional print or audio media. It is especially relevant to outreach to youth, and to people disaffected by the way the mainstream media presents news and opinion.

Social media is also widely used by humanitarian organisations, including the IFRC, the ICRC, National Societies, IGOs, NGOs, and community groups. In the search for digital innovation, the ICRC and the American Red Cross partnered with popular online video game Fortnite (estimated 70 million players per month) to allow players to play the game as an ICRC worker, 'saving lives rather than taking them' (ICRC, n.d.). The game aimed to raise awareness of the core activities of the ICRC and the importance of IHL.

**The nature of crisis response has been changed by social media.** During crisis situations, social media allows for the timely sharing of reports and updates from the crisis scene, dissemination of updates to affected people, and galvanising international support. These tools were first used extensively in the aftermath of the 2010 earthquake in Haiti, when images and information were quickly propagated through social media platforms to help relief efforts, such as the American Red Cross's appeal to donate through text messaging. In the context of a humanitarian crisis, it is important to maintain interest through social media after the immediate crisis as well as to direct people towards where they can help most effectively.

Information and data gathering, and monitoring, are part of disaster response and also important at other times. Smartphones, VoIP, and ordinary SMS technology are used in many countries for reporting on the development of events, the scale of damage after a natural or man-made disaster, and the mobilisation of opinion or response. For example, the crowdsourcing platform Ushahidi is used by many organisations for elections monitoring and crisis response. It was developed by a non-profit company to map reports of violence in Kenya after elections in 2008. A more simple example that any organisation can use is to follow certain hashtags (#) to keep track of social media conversations surrounding a particular issue or topic.

**Data governance** came into focus with the use of big data, geospatial data, and crowdsourced data, to more accurately assess the impact of emergencies and to better target aid to the right recipients. In emergency response operations, success largely depends on the availability of timely information.

Big data can make a big difference here. For example, Cox's Bazar public health and information management professionals, UN Global Pulse, UNHCR Innovation, OCHA, Durham University, and the IBM/MIT Watson AI Lab are modelling the spread of Covid-19 and the impact of various public health measures in refugee camps. Using data about demographics and patterns of interaction, these models simulate the effects of different interventions. The results can help determine the most effective public health interventions and mitigation measures in environments characterised by overcrowding and insufficient sanitation facilities.

OCHA has established the Humanitarian Data Exchange (HDX), supported by the Ministry of Foreign Affairs of the Netherlands, as a platform on which data can be collected and shared among the humanitarian community (OCHA, n.d.).

**Privacy and security** are essential in dealing with humanitarian data. Humanitarian organisations generally deal with vulnerable populations, and the breach of their personal data can be a matter of life and death. This knowledge has not prevented 'many of the world's most important and trusted institutions taking irresponsible, at best, and illegal, at worst, risks with some of the world's most sensitive data' (McDonald, 2016, p. 2).

# Health and social well-being

The impact of digital technology on health came into focus during the COVID-19 crisis. Here is the survey of the main digital policy issues pertaining to health.

**Data** played a central role in taking epidemiological measures against COVID-19 pandemics from lockdowns to preventive measures. Data includes the number of infected people, vaccinations, and economic impacts, among others.

Much of the attention is accorded to data collection that enabled the prediction and identification of the pandemic. As noted above, on the basis of data collected by BlueDot, early warning of the virus was communicated to the WHO (Tong, 2020). Similarly, data collected by medical centres on patients' geographic location and infection status was entered into a government database known as the 'National Infectious Disease Monitoring Information System Database' ultimately helped Chinese authorities identify where the initial COVID-19 outbreak had started (Secon, 2020).

Data visualisation has also been put to use. Online data platforms have been created to track the spread of the Coronavirus worldwide. Data on the number of COVID-19 cases, deaths, number of tests, vaccines and many other related metrics are available on numerous platforms, presented in the form of a table or an interactive map, which are updated regularly.

In response to the Coronavirus outbreak, other calls for and initiatives regarding data sharing have surfaced. The Director-General of the WHO Tedros Adhanom Ghebreyesus invited health ministers of member states to improve data-sharing measures related to COVID-19 (Nebehay, 2020). Academia and the private sector are for their part involved in data sharing. Data has been shared through Github by Harvard Medical School, the Institute of Health Metrics and Evaluation, and Metabiota, a risk analysis company (McDonnell, 2020).

More data, however, does not mean more balanced and evidence-based policies. Very often, especially in dealing with risks, we miss context and reference. These situations could devolve into panic as is happening currently with the cancellation of flights. The coronavirus death rate is estimated at around 2% (WHO, n.d.) which is significantly lower in comparison to 14–15% in the case of SARS (Ross, 2003), 50% for ebola (WHO, 2021), or 35% during the MERS epidemics (WHO, 2019). There is not enough data to make informed and reasonable policies in proportion to current and potential risks. That said, AI may help us put data in the right context of risks and societal priorities and in turn facilitate evidence-informed policymaking.

**Artificial intelligence** has been in the focus of a few pandemic measures showing the importance of AI for health protection. When the pandemic first broke out, China's top tech giants opened their AI and cloud computing solutions to researchers (Henan, 2020) for free to unlock the full potential of these technologies to predict the course of the development of the disease and to find a vaccine.

Canadian AI company BlueDot published early warnings on pandemics based on AI-powered algorithms that process an enormous amount of unstructured data from about 100,000 news articles in 65 languages on a daily basis (Prosser, 2020). Its massive pool of data includes animal disease, temperature, and climate information, as well as flight records that all help to predict viral spread patterns.

There have been examples of AI being deployed in the form of tiny robots serving food and providing medical help to quarantined people in China (News18, 2020), or as chatbots that screen individuals and tell them whether they should be evaluated in case of possible infection (Robbins and Brodwin, 2020).

**Cybersecurity** risks increased during the COVID-19 crisis (Mamiit, 2020). Betting their chips on fear, cybercriminals are said to exploit the situation and spread malicious content with misleading information about the coronavirus. Some of the factors that have contributed to the increase in cyberattacks are higher security risks due to remote working or learning, delays in cyberattack

detection and response, exposed physical security by working from public spaces and using free internet, and the like (Deloitte, n.d.).

As COVID-19 vaccines started being approved and administered, multiple authorities have warned about cybercriminals exploiting the situation, including Interpol, Europol, and the FBI. According to the warnings, cybercriminals have taken to advertising and selling fake vaccines in exchange for money and data.

Additionally, nation-states going after other countries' vaccine supply chains has become a concern. In September 2020, hackers began a phishing campaign targeted at organisations associated with a COVID-19 cold chain (a temperature-controlled supply chain necessary to keep vaccines from spoiling in high temperatures) (Zaboeva, 2020). In 2021, US adversaries have been trying to interfere with Operation Warp Speed, the US government operation distributing the vaccines.

**Content policy** came into focus with the term 'infodemic', describing misinformation about the outbreak of pandemics. Tech giants like Facebook, Twitter, and Google also joined efforts to address fake news. Through the activation of an 'SOS alert' for searches linked to Corona virus outbreak, Google has provided users with the latest tweets, advisory information, and other relevant resources provided by the WHO.
The growth in online acts of hate speech have also contributed to the 'Coronaracism' phenomenon, as well as the rise of stigmatisation on social media. To study such negative developments, Twitter has recently announced that it will be providing researchers with free access to data (i.e. public tweets that contain such content).

**Human rights** were impacted by, for example, measures to prevent the spread of what some actors have dubbed as 'rumours' on social media that have affected the right to freedom of expression of many. According to several sources, activists have been detained, harassed, and intimidated by the authorities for pandemic-related content they posted online.

The pandemic has also given way to concerns of violations of the right to privacy and data protection. In 2020, a heated debate regarding contact tracing apps took place with much attention being paid to privacy issues pertaining to collection and storage of data through the previously mentioned apps.

## Content policy and media

Content policies have come into focus of the global public, especially when such content affects or disrupts elections and the political process of a country. COVID-19 has also triggered 'infordemics' that challenges prevailing consensus around facts and scientific findings. Tech platforms have been placed under intense scrutiny – especially by governments – over their ability to identify and remove such content as swiftly as possible. In some countries, legislation is replacing the self-regulation approach, which is being deemed insufficient.

Content issues are addressed from various perspectives, including constitutional (who can decide what 'truth' is), government policies on content (motives for filtering include national security, public order, the protection of the democratic system, and politically motivated censorship), human rights (the impact of content policies on rights such as freedom of expression and the right to communicate), and technological tools (such as the use of AI for content filtering).

Social media has accelerated the spread of **false information** and online acts of **hate speech**. Supported by new technologies such as AI, misinformation is spread today at an unprecedented scale and pace, inflicting harm on human dignity, health and well-being, targeting certain communities and vulnerable groups, and eroding trust in democratic institutions. According to a substantial study on *The spread of true and false news online*, whilst the truth reached not more than about 1,000 people, 'the top 1% of false-news cascades routinely diffused to between 1,000 and 100,000 people.' **Demystifying the truth behind fake news and disinformation is one of the main challenges in the digital age.**

Content policy issues are covered mainly on a national level. For instance, Germany has introduced a new law against hate speech. Others are considering regulating fake news and hate speech, and introducing content policy. These issues are particularly thorny in the context of protecting the democratic system and electoral processes. On an international level, the 'Our Common Agenda' proposes establishment of a global code of conduct that promotes integrity in public information.

Content issues should be addressed in short, medium, and long term perspectives.

Short-term, urgent measures should be taken to end the use of social media for inflaming conflict with potential risks to human lives and the security of society. Such measures should be exceptional, taken for a limited time in full compliance with the law.

Medium-term, countries should adopt necessary laws and regulations to govern content policy. Because content policy is so important for democracy and freedom of expression, all content policy measures must be governed by clear legal safeguards.

Long term, content policy and the fight against fake news must be addressed via media literacy, critical thinking development through education.

# Conclusion

The twofold aim of this white paper and toolkit is to initiate dialogue by providing background for the main dilemmas of the digital age and a policy toolkit for dealing with them practically.

Conclusions will be drawn by each of us as we navigate through these concepts in the search for the answers to questions such as whether we can predict the impact of specific ethics and values on AI or what is the best use of legal instruments for dealing with Big Tech priorities, or how we can develop appropriate policies for data use and the common good, to name a few. Each of us will find our path through the core values, approaches, instruments, policy topics, and technologies.

As we cannot reach *one* conclusion, here I will share some questions that I ask myself as I discuss with diplomats, academics, colleagues, friends and others how this fast growth of technology will shape our future, and what really matters. Conclusions derive from echoing questions that highlight our dilemmas and pave the way for important conversations that we must have in every sphere of influence, from our families to global community forums.

# Reference list


Archyde (2021) Spain, European testing ground for artificial intelligence. Available at https://www.archyde.com/spain-european-testing-ground-for-artificial-intelligence-companies/

Awad E et al. (2018) The Moral Machine experiment. *Nature International Journal of Science* 563, pp. 59-64. Available at https://www.nature.com/articles/s41586-018-0637-6

Banisar D (2018) *National Comprehensive Data Protection/Privacy Laws and Bills in 2018*. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

*BBC* (2018) Germany starts enforcing hate speech law. 1 January. Available at: https://www.bbc.com/news/technology-42510868.

Brazil's Civil Rights Framework for the Internet [Marco Civil] (2014). Law n°. 12.965, of April 23, 2014.

Brundtland G (1987) *Report of the World Commission on Environment and Development: Our Common Future*. United Nations General Assembly document A/42/427.

Catholic Relief Services (n.d.) 'ICT4D in Our Work'. Available at https://www.crs.org/our-work-overseas/ict4d/ict4d-media

CBINSIGHTS (2021) Our Meatless Future: How The $2.7T Global Meat Market Gets Disrupted. Available at: https://www.cbinsights.com/research/future-of-meat-industrial-farming/

Devaux A et al. (2017) *Education: Digital technology's role in enabling skills development for a connected world*. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE238/RAND_PE238.pdf

Digital Empowerment Foundation [DEF] (n.d.) Website. Available at http://defindia.org/

Deutsche Welle [DW] (2020) 260 million children miss out education: UNESCO, 23 June. Available at https://www.dw.com/en/260-million-children-miss-out-education-unesco/a-53908881

Gong M et al. (2021) Quantum walks on a programmable two-dimensional 62-qubit superconducting processor, *Science*, Vol. 372, Issue. 6545, pp. 948-952. /doi/10.1126/science.abg7812.

Google (n.d.) Requests to delist content under European privacy law. *Google Transparency Report*. Available at: https://transparencyreport.google.com/eu-privacy/overview?hl=en

Group of 20 [G20] (2018) Digital Economy Ministerial Declaration. Available at http://www.g20.utoronto.ca/2018/2018-08-24-digital.html#annex3

Elegant NX (2019) The Internet Cloud Has a Dirty Secret. *Fortune*. Available at: https://fortune.com/2019/09/18/internet-cloud-server-data-center-energy-consumption-renewable-coal/

European Commission [EC] (2014) *Press Release Database.* Available at http://europa.eu/rapid/press-release_CJE-14-70_en.htm

European Union [EU] (2015) *Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120

Federal Ministry of Transport and Digital Infrastructure [BMVI] (2017) Ethics Commission –- Automated and Connected Driving, Berlin, p. 33. Available at https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected-driving.pdf?__blob=publicationFile

FRANCE24 (2017, March 3) The hidden pollution of the internet [Video]. *YouTube*. Accessible at: https://www.youtube.com/watch?v=GX8sOrz_-Fg&ab_channel=FRANCE24English

Geneva Dialogue on Responsible Behaviour in Cyberspace (n.d.). Available at https://genevadialogue.ch/

Green E (2020) Sallie McFague and an Ecotheological Response to Artificial Intelligence*. The Ecumenical Review, 72(2), 183–196.* doi:10.1111/erev.12502.

Gregory JA (2020) *Virtual reality and the future of peacemaking*. DiploFoundation Policy Papers and Briefs. Available at https://www.diplomacy.edu/sites/default/files/Policy_papers_briefs_14_JAG.pdf.

Henan S (2020) Chinese tech giants open cloud computing technology to researchers amid coronavirus emergency. *KrASIA*, 31 January. Available at https://kr-asia.com/chinese-tech-giants-open-cloud-computing-technology-to-researchers-to-help-fight-coronavirus-outbreak

Henriquez M (2021) Banking industry sees 1318% increase in ransomware attacks in 2021. *Security Magazine*. Available at: https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021

Hojstricova K (2021) Cybersecurity public-private partnerships in healthcare – Part 1. *DiploFoundation*. Available at: https://www.diplomacy.edu/blog/cybersecurity-public-private-partnerships-in-the-health-sector/

Hone K (2019) Mediation and artificial intelligence: Notes on the future of international conflict resolution. Available at https://www.diplomacy.edu/sites/default/files/Mediation_and_AI.pdf

Huang E (2018) *T*he East and the West have very different ideas on who to save in a self-driving car accident. *Quartz,* 1 November. Available at https://qz.com/1447109/how-east-and-west-differ-on-whom-a-self-driving-car-should-save/

Huawei (2019) *ICT Sustainable Development Goals Benchmark*. Available at https://www-file.huawei.com/-/media/corporate/pdf/sustainability/sdg/huawei-2019-sdg-report-en.pdf?la=en

Human Rights Council [HRC] (2016) *The promotion, protection and enjoyment of human rights on the internet* (A/HRC/32/L.20). Available at https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

International Committee of the Red Cross [ICRC] (n.d.) Fortnite Liferun. Available at https://www.icrc.org/en/fortnite-liferun

International Telecommunication Union [ITU] (n.d.) The ICT Development Index. Available at https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx

Internet Society (2016) *Promoting Content in Africa*. Available at https://www.internetsociety.org/wp-content/uploads/2017/08/Promoting20Content20In20Africa.pdf

Kant I (1998) *Groundwork for the Metaphysics of Morals*. Edited and translated by Mary Gregor, Cambridge, pp. 42-43.

Kharpal A (2018) A.I. will turn us into 'superhuman workers,' founder of secret Google X lab says. *CNBC*. Available at https://www.cnbc.com/2018/02/12/a-i-will-turn-us-into-superhuman-workers-founder-of-secret-google-x-lab-says.html

Kurbalija J (2016) *An Introduction to Internet Governance*, 7th edition. DiploFoundation. Available at https://www.diplomacy.edu/sites/default/files/AnIntroductiontoIG_7th%20edition.pdf

Livingstone S (2016) One in Three: Internet Governance and Children's Rights. *Office of Research – Innocenti Discussion Paper 2016-01.* Available at https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

Love MC (2020) *Global Issues Beyond Sovereignty*. Rowman & Littlefield.

Lowen M (2020) School's out: Parents stressed by Italy coronavirus shutdown. *BBC News*, 6 March. Available at https://www.bbc.com/news/world-europe-51751031

Martin E and Loudenback T (2017) The 9 richest billionaires who earned their fortunes in tech. *Business Insider*, 7 March. Available at https://www.businessinsider.com/richest-people-in-tech-2017-3?r=US&IR=T

Mamiit A (2020) Hackers taking advantage of coronavirus scare to spread malware. *Digital Trends*, 2 February. Available at https://www.digitaltrends.com/computing/hackers-coronavirus-malware/

McDonnell T (2020) Coronavirus is a proving ground for scientific transparency. *Quartz*, 1 February. Available at https://qz.com/1795103/coronavirus-is-a-proving-ground-for-scientific-transparency/

McGill MH (2020) Virus-driven shift to online classes brings home the digital divide. Axios. Available at https://www.axios.com/online-classes-coronavirus-85815ed5-7bf9-4453-a179-20bd1bf716d0.html

McFague S (1993) *The body of God: An Ecological Theology*. Minneapolis, Minn.: Fortress Press.

McIntyre et al. (2015) *Offshore Shell Games 2015: The Use of Offshore Tax Havens by Fortune 500 Companies*. Citizens for Tax Justice and U.S. PIRG Education Fund. Available at https://uspirg.org/sites/pirg/files/reports/USP%20ShellGames%20Oct15%201.3.pdf

Meyer R (2018) The Grim Conclusions of the Largest-Ever Study of Fake News. *The Atlantic*. 8 March. Available at https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

Milanovic B (2016) *Global Inequality: A New Approach for the Age of Globalization.* Cambridge: Harvard University Press.

Naden C (2021) Standards Need to Achieve Net Zero, said UNSG at COP26. *ISO*. Available at https://www.iso.org/news/ref2748.html

Nebehay S (2020) WHO calls for improved data-sharing on virus, says sending team to China. *Reuters*, 4 February. Available at https://www.reuters.com/article/us-china-health-who/who-calls-for-improved-data-sharing-on-virus-says-sending-team-to-china-idUSKBN1ZY2IG

News18 (2020) AI to the Rescue: China and US Use Robots as Waiters and Doctors to Combat Coronavirus, 29 January. Available at https://www.news18.com/news/buzz/ai-to-the-rescue-china-and-us-use-robots-as-waiters-and-medical-staff-to-combat-coronavirus-2477645.html

Organisation for Economic Co-operation and Development [OECD] (2001) *Understanding the Digital Divide*. Available at http://www.oecd.org/internet/ieconomy/1888451.pdf

OECD (2003) *Implementation of the Ottawa Taxation Framework Principles.* Available at https://www.oecd.org/tax/administration/20499630.pdf

OECD (2013) *Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data.* Available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD (2018) *Toward a Framework for Measuring the Digital Economy*. Available at http://www.oecd.org/iaos2018/programme/IAOS-OECD2018_Ahmad-Ribarsky.pdf

OpenMind (2020) The Hidden Environmental Toll of Smartphones. Available at:

https://www.bbvaopenmind.com/en/science/environment/the-hidden-environmental-toll-of-smartphones/

Pellegrini M and Maltinti C (2020) “School never stops”: Measures and experience in Italian schools during the COVID-19 lockdown. *Best Evid Chin Edu*, 5(2):649-663.

Penke M (2021) Toxic and radioactive: The damage from mining rare elements. DW. Available at https://www.dw.com/en/toxic-and-radioactive-the-damage-from-mining-rare-elements/a-57148185

Power (2020) The Role of Virtual Power Plants in a Decentralized Power Grid. Available at https://www.powermag.com/the-role-of-virtual-power-plants-in-a-decentralized-power-grid/

Prosser M (2020) How AI Helped Predict the Coronavirus Outbreak Before It Happened. *SingularityHub*, 5 February. Available at https://singularityhub.com/2020/02/05/how-ai-helped-predict-the-coronavirus-outbreak-before-it-happened/

Putnam R et al (1993) *Making Democracy Work: Civic Traditions in Modern Italy.* New Jersey: Princeton University Press.

Richter F (2019) *The Tech World is Still a Man’s World*. Available at https://www.statista.com/chart/4467/female-employees-at-tech-companies/

Robbins R and Brodwin E (2020) Chatbots are screening for the new coronavirus — and turning up cases of the flu. *Stat News*, 5 February. Available at https://www.statnews.com/2020/02/05/chatbots-screening-for-new-coronavirus-are-turning-up-flu/

Rohrig B (2015) Smartphones: Smart Chemistry. *ACS*. Available at https://www.acs.org/content/acs/en/education/resources/highschool/chemmatters/past-issues/archive-2014-2015/smartphones.html

Ross R (2003) Estimates of SARS death rates revised upward. University of Minnesota, Center for Infectious Disease Research and Policy. Available at https://www.cidrap.umn.edu/news-perspective/2003/05/estimates-sars-death-rates-revised-upward

Ryder G and Houlin Z (2019) The world’s e-waste is a huge problem. It’s also a golden opportunity. *World Economic Forum Annual Meeting*. Available at https://www.weforum.org/agenda/2019/01/how-a-circular-approach-can-turn-e-waste-into-a-golden-opportunity/

Schwab K (2016) *The Fourth Industrial Revolution: What it means, how to respond*. Available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Secon H (2020) A medical-surveillance system that China implemented after SARS led officials to discover the new coronavirus within 1 week — here's how it works. *Business Insider*, 3 February. Available at https://www.businessinsider.com/medical-surveillance-allowed-china-to-discover-novel-coronavirus-2020-1

Shapiro E and Gold M (2020) Thousands of Students in New York Face Shuttered Schools. *The New York Times*, 9 March. Available at https://www.nytimes.com/2020/03/09/nyregion/coronavirus-new-york.html

Si M (2020) Telecom carriers offer special services to help tame nCoV. *China Daily*, 24 February. Available at https://global.chinadaily.com.cn/a/202002/24/WS5e532980a310128217279b6f.html

Software Engineering Institute -.Carnegie Mellon University [SEI] (n.d.) National Computer Security Incident Response Teams (CSIRTs). Available at https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/

Stacey K (2018) India’s Supreme Court places limits on digital identity card. *Financial Times*, 26 September. Available at https://www.ft.com/content/de10c206-c165-11e8-95b1-d36dfef1b89a

Srinivasan V L (2016) TRAI rules out Facebook’s Free Basics project in India. *ZDNet*, 8 February. Available at https://www.zdnet.com/article/trai-rules-out-facebooks-free-basics-project-in-india/

Swiss Agency for Development and Cooperation [SDC] (n.d.) *Glossary Knowledge Management and Capacity Development.* Available at https://www.eda.admin.ch/dam/deza/en/documents/publikationen/glossar/157990-glossar-wissensmanagement_EN.pdf

*The Economist* (2019) 'The Inclusive Internet Index 2019'. Available at https://theinclusiveinternet.eiu.com/

Tong S (2020) Big data predicted the coronavirus outbreak and where it would spread. *Marketplace*, 4 February. Available at https://www.marketplace.org/2020/02/04/big-data-predicted-coronavirus-outbreak-where-it-may-go-next/

Ugwuede K (2020) More African women should be using the internet. *Techcabal*. Available at https://techcabal.com/2020/09/11/bridging-digital-gender-gaps-key-to-unlocking-femtech-in-africa/

United Nations [UN] (2021) *Our Common Agenda—Report of the Secretary-General*. Available at https://www.un-ilibrary.org/content/books/9789210010122

United Nations Children’s Fund [UNICEF] (2020) Education and COVID-19. Available at https://data.unicef.org/topic/education/covid-19/

United Nations Educational, Scientific and Cultural Organization [UNESCO], Recommendation on the ethics of AI – adopted by UNESCO member states in November 2021. Available at https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14

UNESCO (2020) Startling digital divides in distance learning emerge. Available at

https://en.unesco.org/news/startling-digital-divides-distance-learning-emerge

United Nations Conference on Environment and Development (UNCED) (1992) *The Rio Declaration on Environment and Development*. New York.

UN (2006) *Convention on the Rights of Persons with Disabilities*. Available at https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html

UN Commission on International Trade Law [UNCITRAL] (1958) *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*. Available at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/new-york-convention-e.pdf

UN High Level-panel on Digital Cooperation [UN HLP DC] (2019) The Age of digital Interdependence. Available at https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf.

UN General Assembly [UNGA] (2015) Resolution 69/166. *The right to privacy in the digital age*. Available at https://undocs.org/A/RES/69/166

UN Group of Governmental Experts on Information Security [UNGGE] (2013), *Government Group of Experts on Developments in the field of information and telecommunications in the context of international security: Note by the Secretary-General,* Sixty-eighth session, UN Doc A/68/98 (24 June 2013, reissued for technical reasons on 30 July 2013).

UN Human Rights Council [HRC] (2016) Report of the Special Rapporteur on violence against women, its causes and consequences. 19 April 2016, A/HRC/32/42. Available at https://digitallibrary.un.org/record/842657?ln=en.

United Nations Office for the Coordination of Humanitarian Affairs [OCHA] (n.d.) The Humanitarian Data Exchange. Available at https://data.humdata.org/

Vincent J (2019) Bitcoin consumes more energy than Switzerland, according to new estimate. *The Verge*. Available at https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

Vosoughi S et al. (2018) The spread of true and false news online. *Science*, Vol. 359, Issue 6380, pp. 1146-1151. Available at: http://science.sciencemag.org/content/359/6380/1146.

Wainwright O (2021) 'This is the age of waste': the show about our throwaway addiction and how to cure it. *Guardian*. Available at: https://www.theguardian.com/artanddesign/2021/nov/01/waste-age-exhibition-design-museum.

World Bank (2016) *World Development Report 2016: Digital Dividends.* Overview booklet. World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO.

World Health Organisation [WHO] (n.d.) WHO Coronavirus (COVID-19) Dashboard. Available at https://covid19.who.int/?gclid=Cj0KCQiA3smABhCjARIsAKtrg6Ip-M3-R35pN_SSYXaEqFNjusqJXrQStFznP7hTp58lYGKWBR4AOSkaAuRIEALw_wcB

WHO (2019) Middle East respiratory syndrome coronavirus (MERS-CoV). Available at https://www.who.int/news-room/fact-sheets/detail/middle-east-respiratory-syndrome-coronavirus-(mers-cov)

WHO (2021) Ebola virus disease. Available at https://www.who.int/news-room/fact-sheets/detail/ebola-virus-disease

World Economic Forum [WEF] (2018a) *The Future of Jobs Report 2018*. Available at http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf

WEF (2018b) *Towards a Reskilling Revolution: A Future of Jobs for All*. Available at http://www3.weforum.org/docs/WEF_FOW_Reskilling_Revolution.pdf

WEF (2020) *The Global Risks Report 2020*. Available at https://www.weforum.org/reports/the-global-risks-report-2020

Wenk E (1986) *Tradeoffs: Imperatives of Choice in a High-Tech World*. Johns Hopkins University Press.

World Summit on the Information Society [WSIS] (2003) *Declaration of Principles – Building the Information Society: a global challenge in the new Millenium (WSIS-03/Geneva/Doc/4-E).* Available at http://www.itu.int/net/wsis/docs/geneva/official/dop.html.