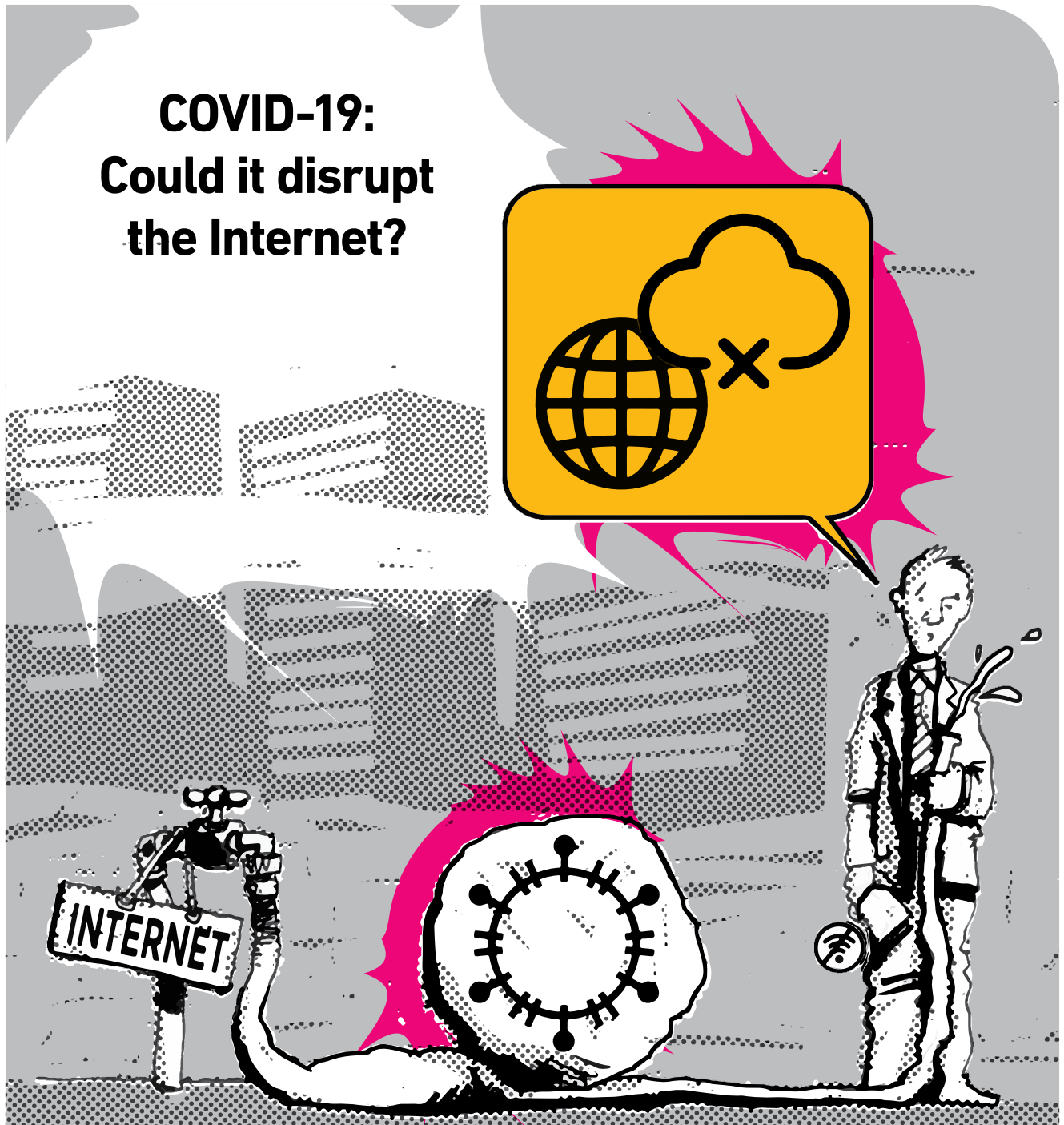# COVID-19: Could it disrupt the Internet?

EDITORIAL

The current crisis is a stress-test for the Internet and its governance. Can it pave the way for a strengthened digital governance space?

More on page 2

COVID-19 & DIGITAL POLICY

The impact of the COVID-19 pandemic is profound and cross-cutting, affecting almost all areas of digital policy.

More on pages 3-10

DATA ANALYSIS

COVID-19 featured highly on the *Digital Watch* observatory in March, with most updates covering privacy, content policy, and digital education.

More on page 11

ONLINE MEETINGS

As online meetings gain new relevance, we offer a concise guide to planning and running them effectively.

More on page 12

Preparing for the 'day after'

In less than a few weeks, COVID-19 almost rebooted our lives. What was unthinkable yesterday, such as restrictions of movement, is unavoidable today in order to contain the spread of the virus. Thus, it is not surprising that this issue of the *Digital Watch* newsletter is dedicated exclusively to digital and COVID-19.

DiploFoundation and the Geneva Internet Platform (GIP) reacted quickly to the crisis by offering our experience and expertise in organising online meetings, running online courses, and following the impact of COVID-19 on digital policy. This crisis is a pivotal moment in global diplomacy, as it could pave the way towards more inclusive and transparent global policy-making. Faced with threats to their lives, people worldwide are asking for transparent, professional, and inclusive leadership of societies from local to global levels. This was echoed by the call from the UN General Assembly President Tijjani Muhammad-Bande for 'more - not less - transparency' and for the inclusion of all 'legally allowed' in the UN shift towards online meetings in this time of crisis. In responding to these calls, Diplo's Conference Tech Lab provides assistance in organising online meetings through help desks, surveys of online meeting platforms, and coaching in the moderation of online meetings. After realising the need for training, we initiated a just-in-time course on online meetings in diplomacy and global governance.

Coming back to this newsletter, we have adapted it to the current situation by covering the impact of COVID-19 on digital policy issues. As you will read in the following pages, the impact of this crisis is profound and cross-cutting, from increased pressure on the Internet infrastructure to challenges in respecting human rights online, the risk of fake news spreading,

the impact on digital commerce, and the risks for cybersecurity. Almost all areas of digital policy are being affected by the Coronavirus crisis.

The crisis is a stress-test for the Internet and its governance. The good news is that the Internet has managed to sustain the sharp increase in traffic. Yet, on issues such as dealing with fake news, fighting cybercriminals, or using data as a commons, the lack of global digital coordination is more pronounced. In preparing for the 'day after' this crisis, the international community should revisit the need for a strengthened digital governance space where businesses, governments, and other actors can come together and address the crisis and other regular issues.

COVID-19 has already taught us a few lessons. First, without harnessing the interdependence of modern society, we will fail. Digital interdependence, as the UN High-level Panel on Digital Cooperation highlighted, is one of the core elements of global interdependence. Second, people and countries worldwide are keen to take their destinies in their hands. Third, digital governance should involve all concerned and affected parties, ranging from local communities to governments and businesses. The digital policy community should rise up to this historic occasion. We at Diplo and the GIP will continue to provide data and expertise for inclusive, informed, and impactful discussions on digital governance and other pressing issues of global policy.

COVID-19 & digital policy

In this thematic overview, we look at how the COVID-19 pandemic and the related crisis are impacting different digital policy areas. We explore the interplay between the measures taken to manage the situation and various digital policy issues, based on the *Digital Watch* taxonomy.

INFRASTRUCTURE AND TECHNOLOGY

Handling the increase in Internet traffic

As more and more countries implement lockdowns, and most of our social and professional lives shift online (people working from home, children taking online classes, etc.), the pressure on the Internet is constantly increasing.

An unprecedented growth in Internet traffic has been registered at both global and national levels. Nokia estimates there has been a 20–40% increase in peak traffic in impacted regions over the last four weeks – a significant increase given that 'most networks see 30–35% growth over a year'. Large operators around the world are reporting major network traffic increases, too. For example, Verizon and Vodafone reported a 20% and 50% week-on-week growth, respectively, while Orange said that the number of users connecting to its network remotely has increased by 700%. In Spain, major telecom operators reported that Internet Protocol networks were experiencing a nearly 40% increase, and that voice and data usage in mobile networks were up 50% and 25%, respectively, after the first week of lockdown.

Can these traffic increases lead to major congestions that disrupt or even break the Internet? At the local level, Internet traffic can be throttled by multiple heavy users while everyone is at home (e.g. parents working, children playing online games or watching e-school streaming). While some smaller local and sub-regional Internet service providers (ISPs) may experience problems, bigger telecom providers are confident that they can handle traffic surges and are taking measures to avoid disruptions in their services. Spanish providers, for instance, are strengthening their network infrastructure. French operators say they have sufficient capacity to deal with increases in Internet traffic, while Telecom Italia argues that its network can cope with a surge in traffic. Similar statements have been made by many other operators, especially across the developed world.

The situation tends to be different in developing regions. In Nepal, for instance, assessments say that providers do not have the appropriate infrastructure for higher demand, and that they depend on India to increase the bandwidth. And while major Internet Exchange Points (IXPs) (e.g. DE-CIX Frankfurt, AMS-IX Amsterdam, and LINX London) apparently have more than sufficient resources to handle higher traffic peaks, national IXPs (especially in developing countries that rely heavily on them) may need to add more capacities to cope with the increase and adequately manage traffic at the local and national level.

As operators consider measures to strengthen the resilience of their networks and services, they are also called to respect existing rules, especially when it comes to throttling traffic. The Body of European Regulators for Electronic Communications (BEREC), for instance, noted that EU net neutrality regulations continue to apply, but explained that telecoms are allowed to introduce 'exceptional traffic management measures [...] to prevent impending network congestion and to mitigate the effects of exceptional or temporary network congestion' while equally treating 'equivalent categories of traffic' and if the measures are necessary.

Asking what other actors can do

Users, too, should be aware that the Internet is not an unlimited resource and it should be used as a commons. Public awareness in this regard is important. Authorities and operators are asking citizens to use the Internet responsibly (e.g. avoid video streaming, games, and large attachments in peak hours). Such calls have come from the European Commission, the Serbian and UK telecom regulators, and operators in Nepal and Spain, among others.

Content providers are also being asked to act responsibly. The EU, for example, has called on streaming platforms to ease the pressure on Internet capacity. Netflix, Facebook, YouTube, Apple, Amazon Prime, and Disney have taken measures, in Europe and elsewhere, to lower the bandwidth utilisation, for instance by switching from high to standard definition for video streams. And other types of businesses have been invited to consider prioritising certain types of traffic over others.

Governments should act when the Internet infrastructure is at risk and all other actions do not help. For the time being, they are taking actions to help operators cope with the situation. For example, BEREC and national regulators in Europe are setting up 'a special reporting mechanism' to monitor traffic and react quickly, in co-operation with businesses and users. The International Telecommunication Union (ITU) is establishing a Global Network Resiliency Platform to help governments and the private sector in ensuring the resiliency and availability of telecom networks and services during the crisis. And the US Federal Communications Commission (FCC) has launched the Keep Americans Connected Pledge, inviting operators to commit to not penalising users with termination of Internet services if payments are delayed.

As lockdowns are introduced in more and more countries, increases in Internet traffic are likely to continue. It is a good sign that operators and authorities are taking measures to handle potential bottlenecks and ensure the availability of Internet services, which are now more critical than ever. But the resilience of the Internet will continue to be tested in the weeks to come.

Putting emerging technologies to use

Over the past few months we have seen many examples of artificial intelligence (AI) applications being put to use as part of the efforts to manage the COVID-19 crisis, from AI-powered scanners deployed to track fevers and other symptoms, to machine learning models used to predict protein structures for the virus.

But AI is not the only advanced technology found to be useful in this crisis period. In Spain, the police are using drones to monitor cities and urge citizens to respect quarantine rules. An Italian hospital is using 3D printed valves for their ventilators to deal with the shortage of supplies. Virtual reality is being used to uncover how the virus affects lungs, and to help hospitals treat quarantined patients while limiting physical interaction. Major tech companies, including IBM, Microsoft, and Google, in partnership with several US universities and labs have launched the COVID-19 High Performance Computing Consortium, an initiative aimed to provide scientists with access to supercomputing resources.

These are all encouraging initiatives, demonstrating both the ability of technology to help in times of crisis, as well as the commitment of the tech community to play their part in the fight against the virus.

On 25 March 2020, Diplo's Conference Tech Lab organised a web discussion asking the question: Could COVID-19 disrupt the Internet? Discussants addressed potential challenges to connectivity and what must be done by national Internet providers, major regional Internet hubs, and tech platforms. Read the summary of the debate or watch the recording.

CYBERSECURITY

Facing distributed denial of service attacks and ransomware campaigns

Is the COVID-19 crisis moving us to an increasingly insecure cyber-world? While the sudden shift to online will bring unprecedented changes to our work and communication habits, the change also brings certain risks.

Critical information infrastructure and digital services are already under stress due to the surge in use. Distributed denial of service (DDoS) attacks against health systems such as the US Health and Human Services, e-school platforms such as the Croatian academic network Karnet, or MyGov portal of Australia, aggravate this stress. Nevertheless, it is always worth double-checking if the system failed due to sudden overuse, attack, or both. Security companies warn organisations and private entities to put additional focus on the security of their Virtual Private Networks (VPNs) that allow remote access to employees, as these will likely become more targeted by DDoS and other types of attacks.

It is not new for ransomware campaigns to target hospitals, exploiting generally outdated and vulnerable systems and locking down their data and computers until the ransom is paid. The bad news is that such campaigns continue even as the global pandemic expands: the second largest hospital in the Czech Republic was a victim of ransomware, as well as a private hospital in Illinois, USA, though luckily without major consequences; a similar attack was attempted against

a hospital in Spain, and Hammersmith Medicines Research – a company which tested for Ebola and is waiting to do medical trials on a possible COVID-19 vaccine.

In the current situation, when the healthcare systems around the world are already under stress to handle the exploding number of citizens infected by COVID-19, however, such attacks may be fatal to dozens, if not hundreds of patients. In response, outraged security professionals warned ransomware operators to stay away from medical organisations, or else they will use all their resources to hunt them down. Interestingly, some of the known cybercriminal groups confirmed they will not target the health sector – thus some solidarity in times of crisis might be found among criminals as well.

Exploiting users' fear

Humans remain the weakest link, however. Our demand for more information and action on COVID-19 makes us easy victims of smartly put phishing messages. Europol's report on how criminals are exploiting the crisis underlines numerous cases of phishing campaigns; security companies report particular cases: an invitation to install a bogus Folding@home app (that claims to use computer power to help research new drugs against diseases), which in fact is a malware; false requests and bogus links related to Coronavirus spread impersonating health authorities and even the World Health Organization (WHO); and phishing messages customised to local environments, such as in Italian, with infected attachments. Reports also show a big number of Coronavirus-related new Internet domains, many of which are being used for malicious purposes. In one case, attackers penetrated a number of insecure home and office routers, changing the DNS settings of channel users to a Coronavirus-related bogus domain which hosts malware. Even the Corona Antivirus emerged, which allegedly prevents users from the real COVID-19 infection thanks to 'AI development to combat the virus using a windows app'!

Identifying other risks

There are also indications that some governments might be using the Coronavirus situation for their phishing campaigns, in particular to tempt officials of other states to launch malware. Others are blamed for using Coronavirus-related apps to unlawfully monitor their citizens, including their movements. Yet, there is very little reliable information available.

The confidentiality of communications is also being brought into question, especially as institutions, organisations, and companies move en masse to online meetings through proprietary platforms like Zoom, Adobe Connect, Cisco Webex, Microsoft Teams, and others. Similarly to messaging apps, most online meeting platforms have embedded encryption between the device and the server – yet not all offer full end-to-end encryption. This means that hosting companies – and some law enforcement agencies (LEAs) – may still be able to access the communication records stored on their servers.

These and other issues will be addressed in a web debate on 'Cyber(security) and the shift to online'. *Join us on 9 April and contribute to the discussion.*

HUMAN RIGHTS

COVID-19: What about my rights?

As nationwide lockdowns and social distancing become the new norm amid the outbreak of the Coronavirus, human rights emerge as a central feature of the crisis. Citizens and governments, alike, are caught in a limbo, having to choose between the basic right to health and all the other rights and freedoms that are essential to the proper identity, dignity, and security of a person.

The fine line between privacy and national security

The right to privacy is perhaps at most risk from precautionary and emergency measures declared worldwide in response to the rapid spread of the pandemic. Media articles are reporting about data collection and exchange tools, such as tracking apps and surveillance systems, implemented to monitor infected individuals and reduce the impact of COVID-19.

To illustrate, the Israeli government made headlines when it passed an emergency law that allows security services to track infected people through their mobile data. Serious concerns were also raised over text messages sent by the South Korean authorities to individuals that included information on their whereabouts. In line with the EU General Data Protection Regulation (GDPR), slightly less intrusive monitoring steps are to be taken in the EU, as the European Commission has asked mobile operators to share 'anonymised mobile data to help analyse the patterns of diffusion of the Coronavirus'. Mobile phone operators in Austria, Germany, and Italy, for instance, have already started sharing data about their customers with authorities, to help track their movements.

While gathering and exchanging data may be necessary in such circumstances, one cannot but wonder what cost such a course of action bears for privacy. The Electronic Frontier Foundation, for example, has cautioned that governments should be granted surveillance powers only if 'they can show the public how these powers would actually help, in a significant manner, to contain COVID-19'.

A hush on free expression

COVID-19 has also reduced the space to exercise freedom of expression. A number of countries have imposed restrictions on media coverage of the pandemic including the suspension of newspaper production and distribution in Jordan, Oman, and Morocco, while laws have been or are being enacted on prison sentences for those in South Africa and Hungary who publish false information about the COVID-19 crisis.

Much as statistics show that social media is the third most used news source worldwide, ahead of international organisations including WHO, censorship of social networking platforms is impacting access to information and free expression. These rights are even more limited due to Internet shutdowns. Global pleas have been made to lift Internet bans in the Oromia region of Ethiopia, in Jammu and Kashmir, Myanmar, and Bangladesh, as they are preventing rapid co-ordination and the minimisation of potential harm caused by the pandemic.

Other human rights affected

Privacy and freedom of expression are not the only rights whose exercise is affected in the context of the COVID-19 crisis. Discrimination is another concern, as misinformation and unproven theories about the source of the virus spread online, leading to racist and xenophobic attacks on Asian communities. As illustrated by the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, such attacks have taken the form of 'online harassment, hate speech, proliferation of discriminatory stereotypes, and conspiracy theories'. WHO also noted that 'there are an increasing number of reports of public stigmatization against people from areas affected by the epidemic.' WHO's Director-General called on people to 'fight in unison', saying that stigmatisation 'is more dangerous than the virus itself'.

The right to education is also being threatened as a result of the transition to online education. Children, in particular those living in poorer conditions, may not be able to participate in this new educational environment on equal terms if they lack access to the Internet and appropriate technological equipment.

Most popular news and informations sources worldwide on COVID-19

Source	
Major news organisations	
National government sources	
Social media	
Global health organisations like the WHO	
National health authorities like CDC	
Friends and family	
Local government sources	

Source: Statista

In view of all these developments, Diplo-Foundation organised a web discussion on 'Technology and human rights in times of crisis'. The summary and recording of the discussion are available.
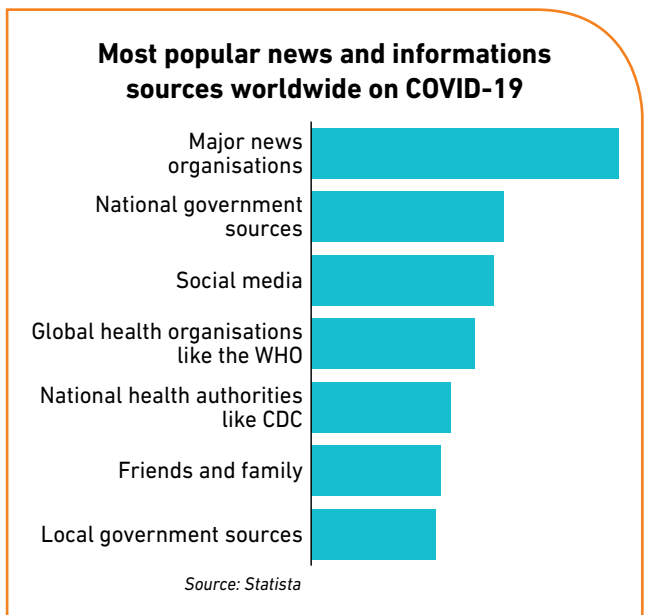
ECONOMIC

Views of the broader picture

COVID-19 has triggered a downturn of economic activities, with many businesses being endangered and stocks falling. While it is too early to predict the course of the economic downturn, a recession seems inevitable. Some analysts affirm that it will likely dwarf the 2008 financial crisis. This is being used to justify the unprecedented policy actions undertaken by governments worldwide, not only to quickly mobilise societies in strategies of rapid response, such as confinement policies, but also to make available the economic resources necessary to safeguard firms, jobs, and workers' incomes.

In the midst of the crisis, the technology industry has provided products and services that underpin some governmental strategies of response, such as the use of AI to identify and track potential carriers of the virus on the streets, or to quickly diagnose patients whose lungs have been compromised by the disease. Many tech start-ups are pioneering health projects to help fight the virus, such as BenevolentAI, which is using AI to suggest potentially useful medicines to alleviate the symptoms, and Blue Ocean Robotics, currently deploying disinfection robots in hospitals. In response, the European Commission has allocated emergency funds to support tech start-ups and small and medium enterprises (SMEs) in tackling the Coronavirus outbreak.

Effects on SMEs and the gig economy

Despite incoming aid, the consequences of the crisis for digital start-ups and SMEs will be extremely diverse, depending on the sector. While telemedicine applications, fitness apps, smart robot makers, and remote meet-up solutions are capturing more clients, tourism platforms, and transport and accommodation booking services are facing difficulties. This is also true for giants operating in the gig economy, such as Uber, Lyft, and Booking.com. Uber is facing a 60–70% decline in demand for its car-hailing service; however the demand for food-delivery is rising, and the company has declared it has enough resources to get through the crisis.

The situation is far more serious for gig workers. Those who cannot afford to take time off without compromising their survival are demanding paid sick leave during the Coronavirus outbreak. Uber started by temporarily suspending the accounts of riders if it believed they may have come into contact with someone carrying the virus. More recently, the company announced that it will compensate drivers and delivery workers who are either diagnosed with COVID-19 or personally asked by a public health authority or licensed medical provider to self-isolate for up to 14 days. In spite of this, there are criticisms about the efficacy and implementation of the measure, as it has failed to provide support to the most vulnerable workers. These arrangements may affect the relationship between companies and gig workers even after the pandemic. Calls for a more stable contractual relationship between platforms and gig workers may get louder, with gig economy platforms pressed to give workers more security.

Implications for big tech companies

Large social media companies are also under pressure to fight misinformation online. Facebook, Twitter, YouTube, and TikTok have announced measures against fake news on the Coronavirus. Some of them have pledged to be further engaged in the fight against the consequences of the crisis. Facebook announced a USD$100 million programme for small businesses impacted by the Coronavirus.

The post-crisis scenario for Internet companies is not totally gloomy. Some powerful and mostly Silicon-Valley-based firms are likely to gain more clout, such as Microsoft, Apple, Facebook, and Alphabet. Their huge financial buffer will allow them to maintain high investment as other firms cut back. Acquisitions of smaller companies may increase, strengthening concentration, and governments may be too busy fighting unemployment to prioritise antitrust concerns.

Some giant platforms are witnessing a stark increase in business revenues, even during the crisis. Self-isolation has provided a boost to e-commerce. In the USA alone, Amazon is hiring 100 000 workers to meet the rising demand in e-commerce. As governments retreat behind national borders and prioritise support for national champions, e-commerce may be even more important to global trade and to the future economic recovery.

Challenges for ensuring consumer protection

This shift to online transactions will enhance the importance of consumer protection. Consumer authorities are very active, adopting measures against the spread of fake anti-COVID-19 products online⬈ and seeking to provide clarity to consumers on issues such as the cancellation of contracts, travel, and tenancies. They will probably need to continue being proactive with regard to online transactions after the crisis has passed.

Governments will also be important in seeking the root cause of the crisis and what can be done to mitigate the rise of similar viruses in the future. Researchers note that the destruction of natural habitats created the conditions for the emergence of the Coronavirus and other viruses.⬈ The relationship between indiscriminate economic exploitation, environmental destruction, and pandemics needs to be unveiled.

DEVELOPMENT

Digital divides in the spotlight

The Coronavirus is conceivably the first major global crisis with a digital dimension. Social distancing measures have accelerated the shift to online learning and teleworking. While the transition may seem a reasonable and logical approach to preventing the spread of the virus, with over 46% of the world's population lacking access to the Internet,⬈ the response does not add up for everyone.

As Human Rights Watch recently noted, 'in this time of crisis it is essential to ensure immediate access to the fastest and broadest possible [Internet] service.'⬈ Some governments and companies have started taking measures to reduce the digital divide. For example, in Kenya, Google and local operator Telkom are deploying Google balloons to provide 4G Internet access across the country.⬈ Across Africa, several operators are offering free access to essential websites (not adding the traffic related to accessing this website towards data caps), or removing fees for mobile money transfers.⬈

The Coronavirus crisis has not only made the digital divide more visible in the North-South dynamics, but it has also shed light on digital divides in developed countries. For instance, it is said that the pandemic laid bare 'America's digital divide'⬈ given that 44% of lower income households in the USA do not have home broadband and 46% lack personal computers.

Moreover, the pandemic is driving deeper the corporate digital divide,⬈ i.e., between businesses that rely on manual labour and those that have been digitalised. Recent reports of 3.3 million people filing for unemployment⬈ in the last week of March in the USA are a bleak depiction of the digital haves and have nots, which in turn raises the question for many on how to exercise

their fundamental right to education and right to work when the physical world is replaced by a virtual one.

The green side of the Coronavirus crisis

In just a short span of time, from busy offices and buzzing streets, the world stopped. Almost everything shut down and moved online as the world transitioned quickly to social distancing.

Even though the economic repercussions of the emergency measures undertaken amid the Coronavirus outbreak are still unknown, our environment stands to make the most of it as countries worldwide remain on lockdown.
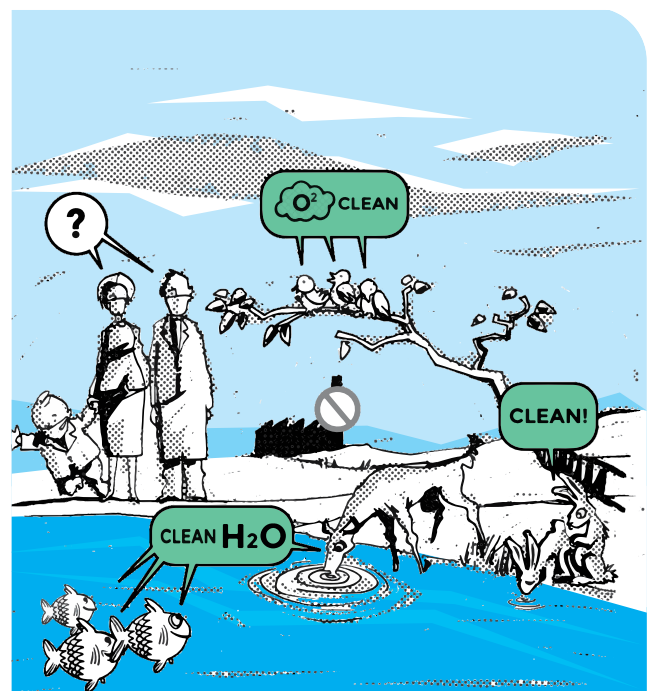
Estimates show that over the past month greenhouse gas emissions (GHGs) declined by 25% in China while recent data indicate a drop in air pollution in the USA, the UK, South Korea, and Italy. That said, the World Meteorological Organization (WMO) highlighted that reductions in emissions as a result of the ongoing COVID-19 situation should not be in any way regarded as 'a substitute for concerted climate action'.

The Executive Director of the United Nations Environmental Programme (UNEP) Inger Andersen was also quoted as saying that the virus is a 'clear warning shot' from nature and that as much as fighting the pandemic takes priority, our long-term attention should be paid to habitat and biodiversity issues, given that 75% of all emerging infectious diseases come from wildlife.

The grey side of digital pollution

Although the so-called green virus may have caused a rapid decrease of GHG emissions, the surge to teleworking, online conferencing, and online learning is far from environmentally benign.

Often referred to as hidden or invisible pollution, the Internet, massive data centres, and emerging technologies such as Bitcoin all play a part in GHG emissions. Digital technologies are said to represent 4% of global carbon emissions, which exceeds the emissions from much more talked about industries such as aviation. The mining of Bitcoin alone consumes 58.77 TWh of electricity per year, which exceeds the annual energy consumption of entire countries like Switzerland, Greece, or Bangladesh.

Then, there is the more visible aspect of digital pollution. Regarded as the fastest-growing waste stream in the world, e-waste such as outdated electronic equipment, including computers and smartphones, constitutes perhaps the biggest environmental challenge from a digital perspective. A study by the World Economic Forum (WEF) indicates that around 50 million tonnes of e-waste are produced annually, of which a mere 20% is recycled. The rest ends up in e-dumps, in most cases, in developing countries.

Having said that, it is not all black and white. There are many shades of grey in between. Digital technologies such as AI, big data, the Internet of Things (IoT), and blockchain are revolutionising our approach to the conservation of biodiversity, the development of clean energy, and the management of natural disasters.

Climate change activism goes digital

In response to the lockdowns and social distancing measures implemented by governments worldwide, climate activist Greta Thunberg called on activists to avoid gatherings and engage instead in digital strikes so as to flatten the curve and avoid the spread of the virus.

The 50th anniversary of Earth Day, like many other events and gatherings, has been moved online. Among other things, the first-ever digital edition of Earth Day will also consist of virtual climate protests.

To keep track with updates on the pandemic and the implications of digital technologies on environmental sustainability, consult our trend pages on COVID-19 and digital and environment.

SOCIOCULTURAL

How the pandemic is changing society

The COVID-19 pandemic is having an unprecedented impact on society. It is dramatically altering our daily routines, shifting our day-to-day activities from offline to the online arena. It has changed educational systems around the world overnight and has led to the first social media 'infodemic', influencing public opinion worldwide.

The hunt for misinformation intensifies

Ever since the outbreak of COVID-19, social media companies have tried to curb the spread of rumours and fake news related to the disease. Instagram said it would remove Coronavirus-related content and accounts from recommendations and its 'explore' option, unless the content belonged to a credible health organisation. Earlier this month, Twitter barred users from posting

misleading information about the Coronavirus, while Facebook announced that the company would give WHO as many free ads as it needed, and provide ad credits to organisations that are working to convey accurate and timely information on the virus. WhatsApp recently launched the WhatsApp Coronavirus Information Hub offering general tips and resources for users worldwide to reduce the spread of disinformation and find accurate health information. Moreover, major social media companies and their parent corporations issued a joint statement on their efforts to fight the Coronavirus infodemic.

Governments have also taken measures to address this issue. In the UK, a specialist unit has been set up by ministers to counter disinformation about the Coronavirus. The National Health Service (NHS) has also taken action against Coronavirus-related fake news. Misinformation has been tackled by the EU as well. The Rapid Alert System, an EU tool for monitoring disinformation, has been put into use as a response to the growing number of disinformation campaigns on the Coronavirus outbreak.

The pandemic of misinformation has also been addressed by world leaders. Russia's President Vladimir Putin claimed that Russia has been targeted by misinformation about the Coronavirus organised from abroad to 'sow panic'. On the other side of the globe, US President Trump's administration claimed there was a 'deliberate effort by a foreign entity to sow fears of a nationwide quarantine amid the virus outbreak'.

An alternative way of accessing public services

To deter the spread of the Coronavirus and ensure the continuity of public services, governments across the globe are increasingly relying on the use of citizens' digital identities. In the United Arab Emirates (UAE), the government encourages citizens to use a digital identity to access government services remotely. The UAE Pass app, a national digital identity solution, allows for smartphone-based verification of a user and enables them to e-sign documents. In Estonia, the authorities keep citizens informed on the status of their e-residency cards and encourage them to use Smart-ID to manage their business if their e-residency card is about to expire.

Moreover, demand in online ID verification has spiked since the outbreak of the virus. Passbase and Onfido are among the digital identity start-ups that have experienced
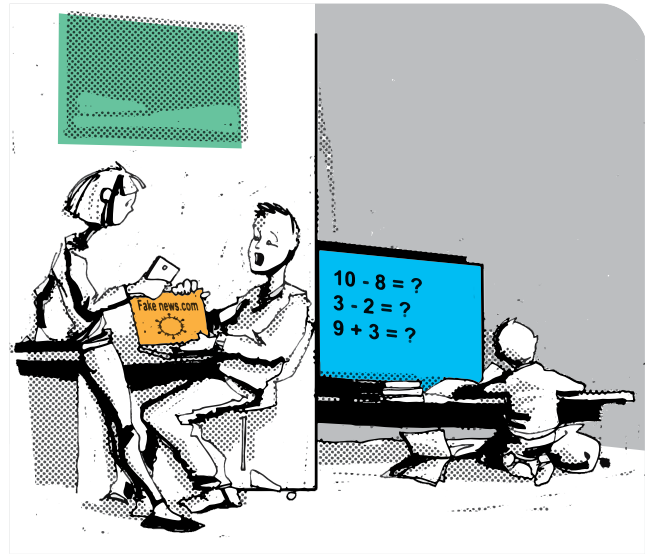
a steady increase in demand, especially from the health-care sector. Yoti, on the other hand, pledged its digital identity services free for the next three months to any public health organisation, emergency service, and community initiative tackling the COVID-19 crisis.
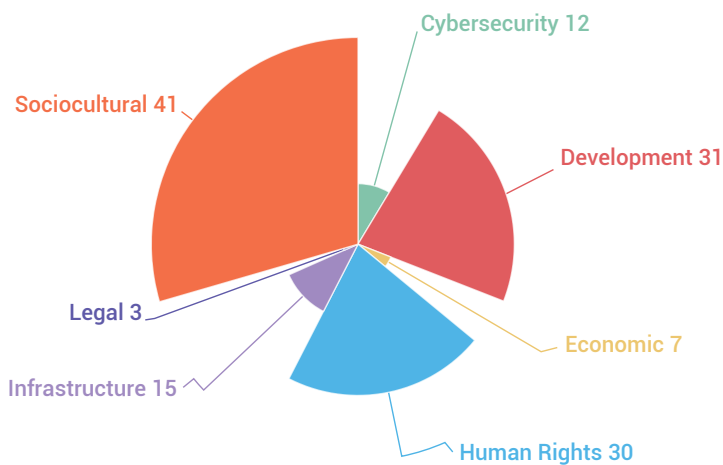
Schools go digital

As the epidemic spread, more and more countries decided to shut schools and universities. Italy was among the first. At the beginning of March, the Ministry of Education called on school directors to activate distance teaching methods, for the duration of the suspension of teaching activities in schools, with particular attention to the specific needs of students with disabilities. A number of countries, such as UAE, Japan, and Egypt have provided students with free access to online learning platforms for the duration of the pandemic.

But the shift from a predominantly offline to a completely online learning environment poses a challenge for many countries. To that end, Estonia's Ministry of Education and Research has decided to share its online learning tools and expertise with educational facilities in countries affected by school closures. At the international level, the United Nations Educational, Scientific and Cultural Organization (UNESCO) has established the Global COVID-19 Education Coalition to provide advice and technical assistance to governments working on securing education for students out of school. The coalition includes multilateral partners and the private sector, including Microsoft and GSMA.

Digital Watch observatory:
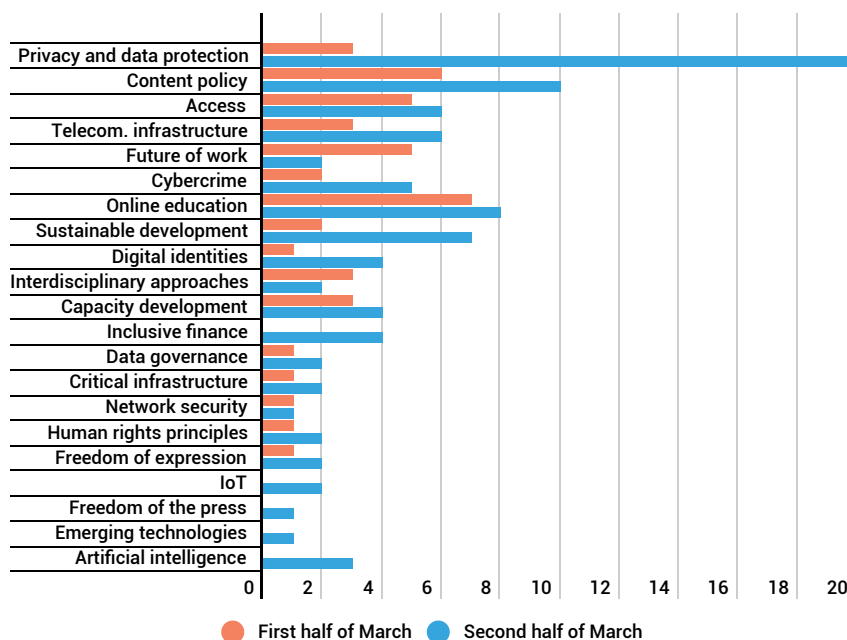# What do COVID-19-related updates tell us?

Over the past two months, the *Digital Watch* observatory has been monitoring the COVID-19 outbreak from a digital policy perspective. We have covered major developments that illustrate the connections between the outbreak and digital technology and policy. ⬀

Baskets covered in COVID-19-related updates

Cybersecurity 12
Sociocultural 41
Development 31
Legal 3
Economic 7
Infrastructure 15
Human Rights 30

COVID-19 has featured highly on the *Digital Watch*: 102 COVID-19-related updates were posted on the observatory in March, which accounts for a little less than a third of all updates posted during the month. These 102 updates covered 21 digital policy issues. Sociocultural, development, and human rights issues took the lead as the vast majority of Coronavirus-related updates focused on the spread of misinformation, access to information, and privacy concerns. On the other hand, economic and legal issues were less prominent this month.

Issues covered in COVID-19-related updates

- Privacy and data protection
- Content policy
- Access
- Telecom. infrastructure
- Future of work
- Cybercrime
- Online education
- Sustainable development
- Digital identities
- Interdisciplinary approaches
- Capacity development
- Inclusive finance
- Data governance
- Critical infrastructure
- Network security
- Human rights principles
- Freedom of expression
- IoT
- Freedom of the press
- Emerging technologies
- Artificial intelligence

● First half of March   ● Second half of March

During the first half of March, the most prominent issue was online education, as most updates focused on shifting to an online learning environment. Content policy came in second (with topics addressing the pandemic of misinformation), followed by the future of work (with topics related, for instance, to how the crisis is affecting gig workers), and access (given in particular the concerns over the resiliency of the Internet in the context of more and more activities switching to the online space). The second half of the month was marked by a steady increase in updates tackling privacy concerns, as governments and other actors started focusing more on ways of using personal data in addressing the global health crisis. Content policy remained in second place, whereas online education dropped to third.

Online meetings: A survival kit in time of crisis

While online meetings are nothing new, they are gaining new relevance with COVID-19 social distancing and lockdown measures. Here's some advice from Diplo's Conference Tech Lab on how to organise effective meetings.

Conference Tech
L A B

1. CHOOSE THE RIGHT PLATFORM

The best platform for you depends on many factors, such as the type of meeting, how small or large your group will be, the level of engagement you expect, and the duration of the meeting. Think also about formality: protocol and procedural rules may be needed.

2. DON'T RELY ON TECH SIMPLICITY

Starting a meeting is relatively simple. Running a good meeting takes skill. Bad meetings could affect the working modalities of your organisation and ultimately waste a lot of time (and money). Plan properly, consider the available time, and integrate elements to make your meeting effective and engaging.

The Conference Tech Lab's guide offers just-in-time assistance and how-to advice on transitioning from onsite to online in an effective, efficient, and smart way.

Access the Lab's resources

3. CREATE DIGITAL EMPATHY

Online meetings need to recreate the room atmosphere online, and bring in as much social and emotional context from traditional meetings as possible. Use simple tricks, from sharing photos from the window of your home, to using video and animation.

TIP: TURN OFF THAT FILTER!

Take a good look at your surroundings. People switching on their filters by mistake, or inadvertently leaving them on, are often the subject of memes. Don't forget to turn off your filters (unless you want to inject some humour into your meeting).

Geneva Internet Platform
DigitalWatch

The Geneva Internet Platform is an initiative of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

RÉPUBLIQUE ET CANTON DE GENÈVE

UNIVERSITÉ DE GENÈVE

ETH zürich

DiPLO
www.diplomacy.edu