

Digitalisation and Civic Space: Chances and Challenges



Imprint

Publisher

Brot für die Welt
Evangelisches Werk für Diakonie
und Entwicklung e. V.
Caroline-Michaelis-Strasse 1
10115 Berlin, Germany
Telephone +49 30 652110
info@brot-fuer-die-welt.de
www.brot-fuer-die-welt.de

Authors Kai Schächtele,
Ingo Dachwitz, Felix Zimmermann,
Chris Köver, Christine Meissler,
Martina Hahn, Sven Hilbig

Editors for the English Edition

Camila Sanchez Ugalde,
Christine Meissler, Karin Saarmann,
Silke Pfeiffer

Responsible According to German Press Law Klaus Seitz

Photos picture alliance/dpa (title);
Geert Vanden Wijngaert/picture
alliance/AP Photo (p. 17); Talukdar
David/Shutterstock (p. 21); Fabian
Bimmer/picture alliance/Reuters
(p. 28); Edgard Garrido/Reuters (p. 30);
Teun Voeten/Panos Pictures (p. 33);
Ajeng Dinar Ulfiana/Reuters (p. 36);
Fotomontage: fizkes/Shutterstock
2020/Brot für die Welt (p. 39); Marco
Longari/AFP/Getty Images (p. 42);
Mark Henley/Panos Pictures (p. 45);
Valentyn Ogirenko/Reuters (p. 48);
Alexey Pavlishak/Reuters (p. 51);
Valentyn Ogirenko/Reuters (p. 52)

Layout János Theil

Translation Translationes

Editorial Deadline of Original

German texts 15 February 2022

Donations

Brot für die Welt
Bank für Kirche und Diakonie
IBAN: DE10 1006 1006 0500 5005 00
BIC: GENODED1KDB

ANALYSIS

Digitalisation and Civic Space: Chances and Challenges

Content

- Preface..... 5
- Summary..... 6
- The internet and civil society: Digital space is narrowing 7
- Is the constitutional state caught in the web? 12
- Facebook: A catalyst for conflicts 16
- Biometric surveillance..... 19
- The surveillance state: Made in Europe 22
- “Data and money flow in one direction only” 23
- This is how our data is collected: past and present 24
- When machines make decisions about humans 26
- Mexico – Bugged and spied on..... 30
- Indonesia – An all-purpose weapon against criticism 36
- Tanzania – As if someone had pulled the plug 42
- Ukraine – Lies as a weapon 48
- Our demands 54
- Endnotes..... 56

Preface

Civil society organisations are increasingly suffering from restrictions and repression: Never before have so many partner organisations of Brot für die Welt lost their registration or been unable to renew it as in 2021. Never before has so much staff been forced to leave the country to avoid being arrested. And never before have so many partner organisations had to close down in their country of origin and continue their work from abroad. Yet, human rights and civil society initiatives are essential for democracy, development and peace. To highlight the state of civil society worldwide, and to make the situation better known to a broad public in Germany, Brot für die Welt, together with CIVICUS, annually publishes the “Atlas der Zivilgesellschaft”, an in-depth analysis of the state of civil society based on the data of the CIVICUS Monitor. This publication “Digitalisation and Civic Space. Chances and Challenges” reproduces key parts of the analysis initially published in the “Atlas der Zivilgesellschaft 2022”.

Today, digitalisation makes it even easier for autocrats to censor opinions, to spy on and to repress people. Internet shut-downs have become a widespread tool to block people’s right to information. But digital tools also bring opportunities for activists: with the help of modern communication channels, they can inform, mobilise and network more directly and successfully. As the Protestant Church in Germany (EKD) rightly stated: Digitalisation is an important building block for sustainable development; provided that barriers to access are removed and human rights are respected.

Because of its global importance, in its fourth edition, this analysis focuses on chances but also on challenges of digitalisation for civil society. In addition to reports from Indonesia, Mexico and Tanzania, we have a closer look at the situation in Ukraine. The report, which was initially written for the “Atlas der Zivilgesellschaft 2022” and whose editorial deadline was mid-February 2022, clearly demonstrates the consequences, past and present, of Russian or pro-Russian disinformation. The consequences of fake news campaigns and years of repression of activists can currently be seen above all in Russia. Censorship, disinformation and the shut-down of political dissent have helped to make the current war in Europe possible.

For all the challenges linked to digitalisation, one thing is clear: human rights organisations and Tech NGOs are working tirelessly to ensure that digital tools enrich our lives and minimise harm. Whether it is non-discrimination in automated decision-making and artificial intelligence, better export regulation for surveillance technologies, biometric recognition or big tech companies, prevention of hate crime, preservation of data protection or freedom of expression online. Here, too, civil society initiatives fulfil an important watchdog function. They ensure that people worldwide benefit as much as possible from technological developments – and that human rights are being respected in the process.

CHRISTINE MEISSLER

Policy Advisor Protection of Civil Society
Brot für die Welt

SILKE PFEIFFER

Head of Human Rights and Peace Unit
Brot für die Welt

Summary

Civil society in the digital space

Multifaceted, uncensored, promoting democracy – that is the internet, many people had long hoped. But from today's perspective, this is not true – or only partially. Because the big digital platforms and the world wide web are both: media of freedom and control. In many places, they support civil society, but often they also pose a massive threat to it.

On the one hand, civil society organisations, activists and bloggers use digital tools to organise their work and make it more efficient: Through them, they disseminate reports and campaigns and exchange information. On the other hand, governments restrict freedom of expression and the press through online censorship: They block access to certain websites or platforms or shut down the internet entirely and monitor activists and journalists with digital technologies, often made in Europe.

Policymakers, platforms and civil society face major challenges: They have to negotiate and decide how to deal with hate on the web and in social media without compromising freedom of expression. How more people, especially in the Global South, can get better access to the internet. And, how the data collection frenzy of the big tech companies and the dangers posed to democracy by Facebook & Co can be contained. Civil society voices call for more human rights based regulation and containment of digital capitalism.

Countries

Four country examples illustrate the opportunities, but also the challenges, for civil society engagement and fundamental freedoms in the digital space: In Mexico, numerous human rights defenders and journalists were monitored with the spy software Pegasus. In Indonesia, laws restrict freedom of expression on the internet and social media. In Tanzania, the day before the 2020 presidential elections, the government shut down the Internet for several days. And in eastern Ukraine, the spread of fake news contributed to the escalation of the conflict. Surveillance in the digital space, censorship, internet shut-downs and disinformation violate fundamental freedoms. They make the work of our partner organisations more difficult and reduce their scope for action. But civil society is also using digital tools to defend itself against state repression. It builds networks and develops new formats to work more effectively. The Brot für die Welt partner organisation

Mental Health Service, for example, has used digital instruments to treat people traumatized by the war in eastern Ukraine. And in Indonesia, the organisation KontraS informs the public via social media despite restrictive IT laws and censorship, and exchanges information with other organisations through these channels. In this way, it also puts pressure on the government.

Our political demands

To ensure that human rights are respected and independent civil society is able to engage worldwide, policymakers must take action. Governments and parliaments must uncompromisingly commit to an independent civil society and universal human rights – also in the digital space. Embassies should strengthen their efforts for human rights, their defenders and civil society. The responsibility regarding human rights for political decision-makers begins with their own policies. They should ban the export of surveillance products except for individual case authorizations. They should ensure that algorithmic systems that make autonomous decisions or assist in decision-making are only introduced after a risk assessment and do not violate fundamental rights. In addition, development cooperation should promote access to the internet for all.

Our political representatives should also advocate that banning individual services and shutting down the internet should be outlawed as human rights violations. At the global level, an international legal framework should be created that defines the duties of the states and the responsibilities that companies have in the digital space – and which guarantees that these are in line with international human rights.

The internet and civil society: Digital space is narrowing

The idea of the internet as a medium for freedom has suffered. Authoritarian regimes use digital technologies as a tool for control. However, the internet does still hold significant emancipatory potential.

An outdated narrative tells us: The internet is uncensorable. Many people used to believe that the decentralised organisation of its infrastructure means it is immune to being controlled. The global diversity of voices, so the story went, will almost automatically ensure democracy, and the virtuality of encounters, an end to discrimination. “We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity,” wrote the US civil rights activist John Perry Barlow in 1996 in his “A Declaration of the Independence of Cyberspace”¹

15 years later, at the dawn of the Arab Spring, it seemed as if this utopia was coming true. It was when the streets of North Africa and the Arabian Peninsula were filled not only with tens of thousands of demonstrators and the whiff of tear gas, but also with the idea of decentralised and coordinated mass protests. More and more people took to the internet to express their discontent at repressive policies and the catastrophic economic situation, arranged demonstrations and shared pictures of them that the state-run media withheld. For a moment, it looked as if the Arab world would shake off its autocratic rulers with the help of digital media.

Less and less internet freedom

In hindsight, we know that the hope that the uprisings might have a lasting effect on democratising the region’s political structure did not come to pass. Activists from the region soon understood how Eurocentric Western talk of the “Facebook and Twitter revolutions” was. While social media may have acted as an amplifier of the protest, the backbone of the uprisings were local structures and often entirely analogue networks of resistance.

Above all, however, the uprisings were a wake-up call for the world’s dictators to digitally upgrade their regimes: They installed internet blockers and seized the digital infrastructure, passed censorship laws and bought surveillance technology from the West. Protest posts that had already appeared online were soon used as evidence: Countless bloggers and online activists have been jailed in the last decade. In 2021, for the twelfth year running,

the NGO Freedom House stated that there is less internet freedom now than in the previous year.²

Internet: Both help and danger

Today we know that the internet is both: A medium of freedom and a medium of control – depending on its exact technical, social and political manifestation. In many democratic countries, the internet has helped further democratisate the public sphere. More people than ever before have easy access to knowledge, culture and discourse. This has also allowed the scope for civil society actors to organise and mobilise to broaden and has given marginalised groups a voice to be heard. The hashtags of social media platforms such as Twitter turned the many individual voices of African Americans into a political movement. Brought together by the catchphrase #BlackLivesMatter, they became a powerful chorus decrying everyday racism and police violence. Another example of collective power of hashtags are feminist initiatives like #Aufschrei in Germany, #ShutItAllDown in Namibia³ or #MeToo worldwide. While this alone does not bring about a change in circumstances, the fact is that never before have people been able to make their everyday experiences of sexualised violence and discrimination heard as effectively as today.

However, right-wing populist and extreme right-wing actors also know how to utilise these new opportunities, often with the aim of silencing the marginalised who had only just found empowerment. Studies show that women, queer people and people with a migrant background in particular are exposed to hostilities online and are increasingly withdrawing from the digital public sphere.⁴ Meanwhile, there is probably no politician who has benefited from social media as much as former US president Donald Trump. The phenomenal reach of the platforms’ targeting tools helped his 2016 election campaign to demobilise African Americans in particular,⁵ and Facebook’s algorithms rewarded his polarising rhetoric and blatant disinformation.

It is by no means a given that the actors who would quite like to undo the process of democratisation will not ultimately prevail in the battle for a democratic public

sphere. The situation is further complicated by the fact that the social media, the most important arenas of the online public sphere, are run by just a few hypercapitalist corporations. For a long time they moderated online discourse simply as they saw fit, guided by profit. For this reason, policy-makers have been battling for years with how to regulate platform companies and thus the digital public sphere.

Quite often, they overshoot the mark despite their noble intentions. Germany for example, with its Network Enforcement Act (NetzDG), which it enacted in 2017, is pressuring Facebook and other platforms to delete illegal content as quickly as possible. But to distinguish legal from illegal content is often rather difficult. The platform staff doing the clicking often only have seconds to make a decision, and so, if in doubt, they prefer erring on the side of deleting too much.⁶ It was not until 2021 that the law was reformed and obliged companies to provide their users with proper appeals procedures and to restore unlawfully removed content. Meanwhile, even in democracies, interior ministers never tire of expanding government surveillance of digital spheres. And so, they seek access to encrypted

emails and messaging services, are obliging telephone and internet providers to retain usage data without reason, and are also trying to keep an eye on the analogue world with facial recognition and similar technologies.

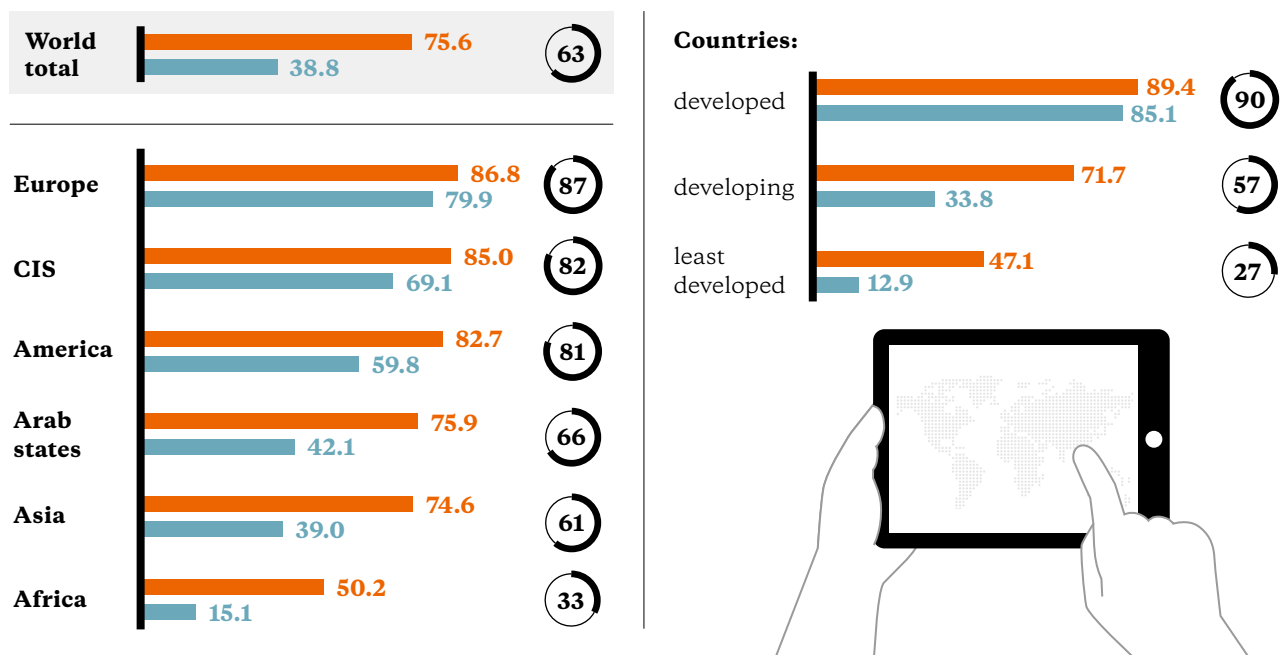
Digital call, analogue protest

Despite this growing pressure for control, the emancipatory impact of the internet predominates in many liberal democracies. Citizens use their smartphones to document police violence and racist attacks, activists force the state to be transparent, and bloggers create civil society counter-publics.

Even the successes of global environmental movements such as Fridays for Future or Extinction Rebellion would be virtually inconceivable without digital tools. Messaging apps and collaborative online tools are essential for planning campaigns, organising local groups and coordinating demands. Moreover, young climate activists know how to integrate analogue protests and civil disobedience

Internet usage worldwide

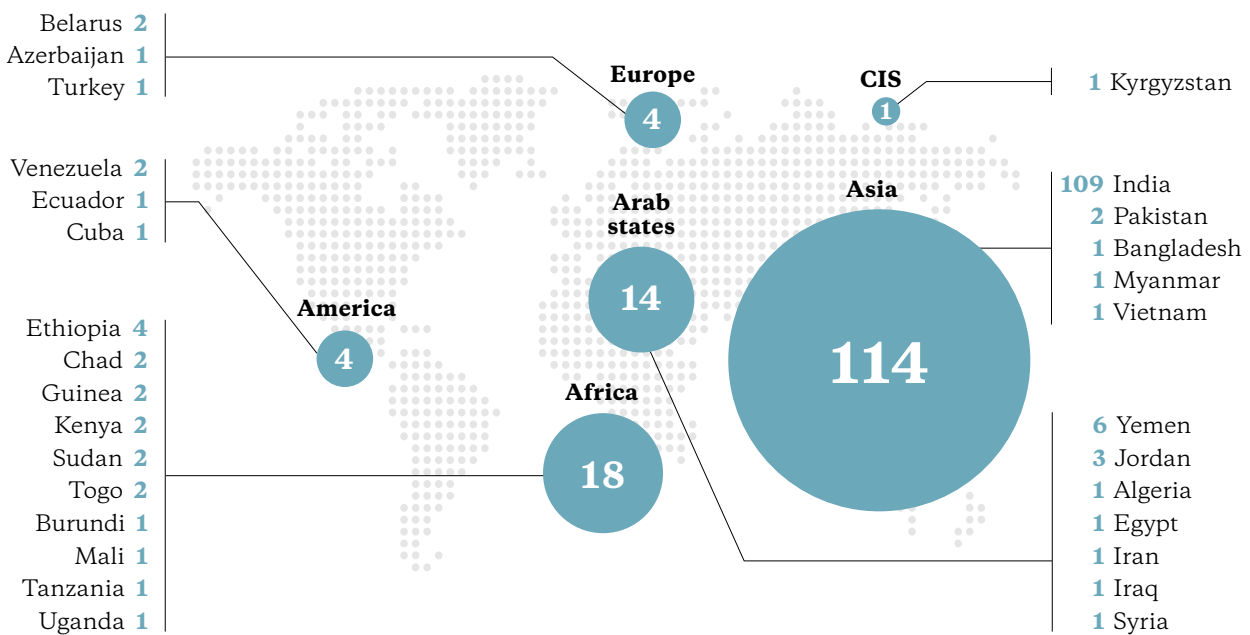
Percentage of people who use the internet



Source: International Telecommunications Union (UN ITU) (2021): *Measuring digital development, Facts and Figures*

Internet shutdowns worldwide

According to the NGO Access Now, governments blocked access to the internet 155 times in 29 countries in 2020.



Source: Access Now (2021): *Shattered Dreams and Lost Opportunities. A year in the fight to #KeepItOn*

campaigns with digital media better than anyone before them. Young people also go on strike for the climate in countries like Uganda and India, making clever use of social media. But while the activists want to use facts to persuade, the social media in many countries of the Global South have become a breeding ground for disinformation, hate and violence. This is because the platforms in these countries take even less effective action than they do in the USA and Europe.

In 2021, the Facebook Papers showed how the corporation failed to stop misleading posts and calls to violence in India or Ethiopia. The company simply does not invest enough in fact checkers, moderators and algorithm recognition systems with the relevant language skills. And because their sorting algorithms reward content that is especially emotional and polarising, they often act as catalysts.

Despite this, people in more repressive countries continue to find ways to use social media for their resistance efforts. In Iran, for example, women posted photos

and videos on Instagram of themselves dancing and without headscarves to protest the mullah regime's sexist moral politics.⁷ Or in Nigeria in 2020, when mostly young people got together on Twitter under the hashtag #EndSARS to draw attention to the violence committed by the Special Anti-Robbery Squad (SARS) police unit and to organise protests.⁸

The rulers generally react to such actions in the same way: they use the power they have over the telecommunications infrastructure and block access to these services. Iran blocked Facebook and Twitter some time ago, and Instagram was also blocked for a while. President Muhammadu Buhari of Nigeria blocked access to Twitter for a period in response to the protest, and in Turkey, Wikipedia was blocked for a number of years. Some people manage to circumvent these blocks using encryption and anonymisation tools, but internet blockers are often an effective tool against mass online protest.

Lucrative markets, inadequate controls

Governments regularly take even more drastic measures and shut down the internet entirely in the whole country or individual regions. According to the NGO Access Now, there were 155 such shutdowns in 2020 alone, from Belarus to Myanmar to India, with the latter topping the list with 109 internet shutdowns. There were over 3,000 days of internet shutdowns that year – especially before elections and during protests (see page 9).⁹ The censorship laws that many countries use to curb access to social media and other digital spaces are almost as severe. Such laws often go under the cloak of measures against terrorist propaganda, cybercrime or fake news. But their vaguely formulated guidelines and threatened sanctions almost always aim to control online discourse without having to block the services altogether. It is not uncommon for leaders such as Russian President Vladimir Putin or Turkish head of government Recep Tayyip Erdogan to make explicit reference to Germany and its Network Enforcement Act (NetzDG) as a model.¹⁰ The online platform companies in the US quite often comply because they do not want to lose access to lucrative markets.

A technical cat-and-mouse game

And finally, surveillance completes the toolbox of state control over the digital realm. This is the case in Hong Kong for example, where the democracy movement organised its protests via encrypted messaging apps and Bluetooth communication, and the devices of arrested members of the opposition were sent to China for analysis. And then, there is Mexico (see page 30), where opposition activists, journalists and members of the clergy were placed under surveillance with the Pegasus spyware. It is not just this scandal that makes it clear that it is often Western companies, including German corporations, that help fan the flames of the surveillance state in the Global South (see page 22).

More than a decade after the Arab Spring, we know that such digitally enabled mass protests are virtually impossible now in many places. The grip autocrats have on the internet is too tight, and digital technologies are too easy to use as a means of control. And yet, the internet's emancipatory potential as a medium for freedom has not

vanished from sight altogether. Many activists now play a technical cat-and-mouse game with the authorities, circumventing censorship with anonymisation services and encrypted messaging apps.

It should be one of the tasks of the Western countries to reinforce the emancipatory potential of the digital realm. All too rarely do they consider how their own regulatory decisions affect the digital sphere in less democratic countries. When German authorities, for example, keep knowledge of vulnerabilities in widely used IT systems to themselves rather than close these security gaps because they need them for digital weapons, then this also makes the devices of opposition members in authoritarian systems vulnerable to attack. If the calls made by interior ministers in Europe to build backdoors to encrypted messaging apps and emails are implemented, then this will also jeopardise freedom of communication for journalists in repressive states. And, when the EU requires media platforms to install automatic upload filters to protect against copyright infringements, then illiberal rulers will be delighted about such an infrastructure that can easily be abused for censorship. European and US governments and companies have a shared responsibility for the digital infrastructures around the world.

“We use tools that are easy to access”



Interview with **Palesa Ramolefo** activist at Brot für die Welt partner amandla.mobil (<https://amandla.mobi>)

Ms Ramolefo, your organisation Amandla.mobi mainly supports low-income women in South Africa. You campaign around issues like gender-based violence, economic justice, police brutality, food security, corruption and climate change. What digital tools do you use for your campaigns?

Palesa Ramolefo: Above all, we use tools that are easy to access. We want as many people as possible to be able to participate in our campaigns. And that is why our most important digital tools are very simple means of communication such as SMS, WhatsApp and social media channels.

How do they help you?

Palesa Ramolefo: An example: There are public parliamentary hearings before a new budget is prepared. An old woman from the countryside may not have the opportunity to travel to Cape Town to go to the parliament. She also does not have a smartphone or enough data to attend the Zoom meetings of the hearing, but she would like to take part. That is where we come in; we give her the opportunity to pass on her contribution to the hearing, for example via SMS or WhatsApp, so that her voice can be heard – and not just the voices of people who have enough money and can manage without our help.

Has this been successful?

Palesa Ramolefo: Oh yes; our campaigns can exert a lot more pressure with the participation of many people and therefore achieve noticeable change. For example, we managed to get VAT on hygiene products such as tampons and sanitary towels to be abolished, a major success for many low-income women. And our successful Data Must Fall campaign resulted in 30 million people gaining easier access to the internet. The major mobile operators were required to reduce the costs of their products. Previously, the costs had been too high for people on low income.

Is the constitutional state caught in the web?

Members of marginalised groups in particular need to be protected from provocateurs looking to stamp out all online dissent. But at what point does this infringe on fundamental rights such as freedom of expression or freedom of occupation?



Interview with **Josephine Ballon**, lawyer and Head of Legal at HateAid, and **Felix Reda**, Project Leader at Gesellschaft für Freiheitsrechte (GFF, Society for Civil Rights)

Ms Ballon, your organisation looks after victims of online hate speech. With your support, Green Party politician Renate Künast secured a victory at the German Federal Constitutional Court at the beginning of February 2022. The Constitutional Court decided that the rulings of the Regional Court and Court of Appeal of Berlin contained serious errors: The courts had deemed the mostly anonymous sexist abuse Künast was subjected to in response to a meme she did not create and that contained a misquotation as being covered by freedom of speech. Do you think the ruling of the chief justices will deter people from posting egregious insults in the future?

Josephine Ballon: I do hope so! After the ruling of the Federal Constitutional Court, the authors of the ten comments that were complained about will hopefully have wet their pants. The Court of Appeal now has to re-examine these comments. But of course we hope that this will empower the people involved. And, that it tells offenders that there will be consequences to their actions. They now realise that there is no such thing as total anonymity on the internet.

Mr Reda, your work at the Society for Civil Rights (GFF) focuses on the dynamic and problematic relationship between freedom of speech and legal violations on the internet. What is your view of the verdict?

Felix Reda: I am also pleased with the outcome of the proceedings. The fact that Facebook did not make the

decision on its own whether to pass on the personal data is a good thing. Nevertheless, the criticism of the regional court's first ruling was justified. Even if you think that the arbitrariness with which online platforms block opinions at times is a concern, it nonetheless makes sense and is in everyone's interest that the courts, when weighing up fundamental rights, take into consideration the situation as a whole and when necessary conclude that a particular statement was not okay. If they did not do that, it would be virtually impossible for people who are politically active or express a position on socially contentious issues to participate in public discourse.

In another case, the messaging service Telegram blocked 64 channels under pressure from the German government. You once warned that such proposals and actions are generally the preserve of autocratic regimes like Russia. The call for technical solutions to a social problem, you thought, risks jeopardising fundamental rights. Why is it justified in this case?

Felix Reda: My comment referred to something else. It was about a federal interior minister's call to have Telegram blocked completely in Germany. This is completely different from what Telegram has actually done: namely to block individual channels which repeatedly had illegal content on them. In the first case, it would be like taking a TV channel offline because one of its programmes was illegal. It is a different thing to politically influence a platform like Telegram so that it complies with European law. You also have to take into consideration the history of such a platform. Telegram was founded as a dissenting voice to the Russian regime. From an international perspective, it is not easy to simply say that as long as everyone abides by the legal rules and regulations, freedom of speech is taken care of. There are many countries in the world where a counter-public is needed.

What criteria are used to decide what gets blocked?

Felix Reda: This continues to be a major work in progress. Not just when it comes to Telegram, but pretty much all platforms – including Facebook, Instagram, TikTok and

YouTube. On all these platforms, the people affected by the blocks often do not know why it happened. There may be good reasons in individual cases. But you still have a right to know why a decision was made and to contest it. It is becoming increasingly clear that online platforms are not ordinary private-sector companies; they are important spaces of discourse which for certain groups are the basis for exercising their freedom of speech or freedom of occupation.

Could you name an example?

Felix Reda: We were dealing with a group of Turkish journalists in exile who run a YouTube channel from Germany for the public in Turkey. The channel takes a critical look at the policies of the Erdogan government. YouTube kept blocking the videos, allegedly because they violate copyright laws. The journalists found it extremely difficult to talk to an actual person at YouTube. With our help, they got in touch with someone who looked into this case and decided that the blocking rules were unwarranted. They were clearly politically motivated to prevent critical reporting. The larger a platform, the greater its responsibility to ensure that fundamental rights can be exercised on it.

Ms Ballon, how do you deal with the tension that arises between hate messages that must be prosecuted and the fundamental right of freedom of expression?

Josephine Ballon: We know that this is where the crux of our work lies. But freedom of expression is not a one-way street. Even according to the Grundgesetz [German Basic Constitutional Law] it has its limits. And these limits are drawn where the rights of others are deemed more worthy of protection. We see freedom of expression mostly being abused on social media by groups working strategically. A lot of such content comes from the right-wing or the extreme right-wing. According to the Federal Criminal Police Office, 62 percent of recorded politically motivated instances of hate speech came from the right and far right in 2020. There are guidelines circulating in these circles telling people, among other things, to target young female students in particular, because they are especially easy to silence. Studies carried out across Europe tell us that it is not just the people themselves who are attacked in this way who then think twice about expressing an opinion on certain topics, but also the people who just witness how defenceless other people are when they are exposed to digital violence. According to a survey held in 2019, half of the internet users in Germany now shy away from expressing their political

opinion on the web. We therefore need to create the right conditions that allow all sides of the political spectrum to safely navigate social media. They have, after all, become the most important platforms for public discourse. If we do not do this, it will mainly be marginalised groups and people who stand up for social values who will withdraw from these platforms: activists, journalists and politicians, especially at the local level. We know that as much as 19 percent of local politicians in Germany do not want to run again or even want to resign because of digital violence.

Mr Reda, the Network Enforcement Act, or NetzDG, was passed to create such conditions. The act is highly controversial, however, because it clearly leads to overblocking, meaning even legal content gets blocked. What do you think?

Felix Reda: The NetzDG act has both upsides and downsides. Some basic things were done right. For example, platforms are not directly liable for each individual piece of content. If this were the case, platforms would simply block everything on request to avoid the risk of liability. The platforms have to meet certain duties of care, so that in the case of obvious legal violations they are also immediately subject to a duty to control – but not in cases that courts would argue about for years.

And the downside?











Felix Reda: This includes the obligation of platforms to pass on information to the Federal Criminal Police Office. In my view, this violates fundamental rights. Because it means that we are passing on private data of people about whom we do not yet know whether they have said anything illegal. What's more, inflexible deletion deadlines incentivise platforms to block too much rather than too little if in doubt. And a third point: Germany led the way with this law and in a sense provided other countries with a blueprint: Turkey, for example, defended its platform law by referring to the NetzDG act – even though its law imposes massive restrictions on freedom of expression.

Ms Ballon, what is your view on this?

Josephine Ballon: The NetzDG act is a good start, but it has some teething problems; some of them are now being rectified, but other changes have made it worse. I do not think it is such a bad thing that Germany has pressed ahead with this. If that had not happened and some other countries had not followed suit, there would not have been the will in Europe to enact the Digital Services Act.

This is what needs to be taken into account when regulating tech groups

Proposals and warnings of the NGO Freedom House

Good practices	Bad practices
 Transparency on content moderation, data use, and advertising practices	 Requirements to remove political, social or religious content
 Robust encryption and privacy standards	 Obligation to hand over data without judicial oversight
 Due process safeguards and avenues for appeal	 Broad rules on data localization and retention
 Strong protections against intermediary liability	 Mandates for automated content moderation
 Obligations tailored to match companies	 Onerous requirements for registration and in-country representatives

Source: *Freedom on the Net (2021): The Global Drive to Control Big Tech*

And, where do you see the weak points?

Josephine Ballon: I think it is a shame that there is little willingness at the European level to address the lessons learnt from the NetzDG act. And unfortunately it is the case that whenever you give the platforms scope for interpretation, this is exploited for their benefit as much as possible. I do not feel particularly sorry for the platforms when people say: the poor platforms, they are not judges – how are they supposed to decide what is illegal and what is not? Then you just have to get the necessary expertise in order to counter these social dangers.

What do you think is missing?

Josephine Ballon: Clear deletion guidelines, with deadlines, if possible. Unfortunately, the Digital Services Act does not provide for this, since there is no political will for this at the European level. They say it is not possible because it would result in overblocking on a large scale. But there is no evidence that this would happen.

Mr Reda, do you also believe this is a weak point?

Felix Reda: No. The reason why the Digital Services Act does not include deletion deadlines is quite simple: The NetzDG act is a special law aimed at very specific large commercial platforms, and it imposes procedural obligations on them in order to combat certain criminal offences. The Digital Services Act, on the other hand, is precisely not the European reaction to the NetzDG act. It is a comprehensive horizontal regulatory instrument that affects all online services: from internet access providers and website operators to large social media platforms and other services such as Amazon. To set such rigid deletion deadlines for such a variety of platforms and content would indeed lead to overblocking. We have seen the NetzDG act being abused, too: As soon as private sector companies are required to automatically respond to certain outside input, mass reporting of accounts of marginalised groups by provocateurs can lead to the blocking of accounts because it is not possible to properly assess the content.

And does the Digital Services Act properly address the regulation of online services?

Felix Reda: One positive aspect is that platforms can set their own rules in the form of general terms and conditions. It would be wrong to deal with it the way, for example, the Polish government has proposed, namely to leave everything online as long as it does not violate any laws. This is too simplistic.

Why?

Felix Reda: It would mean that Wikipedia, for example, is not allowed to delete anything that does not violate any laws. However, more criteria apply to an encyclopaedia than just whether a piece of content is legal – for example whether it can be verified or fits the topic of the entry. According to the Digital Services Act, platforms can make their own rules, but they have to be enforced in a transparent way. They must not act arbitrarily and must respect fundamental rights.

Can the Digital Services Act have an impact beyond the EU?

Felix Reda: It will continue to be a problem for countries in the Global South in particular that they are simply not economically important enough for these companies to be able to enforce their own rules to the same extent. But we can hope that laws like the Digital Services Act have an impact beyond Europe. It is often easier for platforms to implement certain changes globally than just in a single country or just in the EU.

What do you think, Ms Ballon?

Josephine Ballon: There should be a social component to it as well. We had long hoped that the platforms would eventually develop a social conscience; unfortunately, we came to realise that that is not happening. On the other hand, we have seen that advertising revenue is an enormously important tool, especially for the big platforms. Campaigns like Stop Hate for Profit have clearly made a difference: Major companies pulled their advertising budgets from Facebook to demand improvements. And there are more and more companies that do not want their products to be advertised alongside a video showing a beheading.

And what about the users?

Josephine Ballon: There is already a major trend towards sustainability, for example, in our society. Strong social awareness can also help put pressure on platforms. It works. Because ultimately, their goal is not to interconnect the world, their goal is to make profit.

Network Enforcement Act (NetzDG) and Digital Services Act: How the EU and Germany regulate the internet

Network Enforcement Act (NetzDG): The “German law on improving legal enforcement in social networks” has obliged social media platforms to take action against unlawful posts since 2017. Among other things, they must delete “obviously unlawful content” reported by users within 24 hours. Otherwise they risk fines in the millions. The NetzDG act applies to platforms with more than two million users in Germany. The federal government does not have an exhaustive list. But the mandatory transparency reports were published by Facebook, Twitter, YouTube, Instagram, Reddit, TikTok, Change.org and SoundCloud. Since 2021, companies have had to offer their users an appeals procedure, and since 2022 they have had to report potentially criminal content including IP address to the Federal Criminal Police Office.

Digital Services Act (DSA): The Digital Services Act is intended to impose comprehensive rules for online service providers in the European Union. The proposed regulation submitted by the EU Commission at the end of 2020 also covers the area of the NetzDG act, but it goes further. The DSA is intended not only to standardise how illegal content is to be dealt with, it also contains more far-reaching provisions on the liability of companies for the content of their users, on online advertising, on the operation of online marketplaces and on state supervision of these services. At the time of editorial deadline, the legislative process had not yet been completed.

Facebook: A catalyst for conflicts

Hate speech, abuse of data, disinformation – Facebook promises cohesion. But we see that the platform corporation is a danger to democracy and society not just in the Global South.

According to its own mission statement, Meta wants to bring the world closer together. And indeed, the flagship of this platform company, which was called Facebook until recently, is probably the first truly global social network: Facebook is used by people all over the world; the service has almost three billion monthly users. And then, there is WhatsApp and Instagram. If Facebook were a country, it would be the most populous one by far.

But whether its population would be safe, whether they would live in peace and justice, is questionable. While in the aftermath of the Arab Spring, the focus for a long time was on the opportunities Facebook offered for mobilising civil society, ten years later criticism of the company's founder Mark Zuckerberg is louder than ever. Facebook's mission proved to be its own downfall. Rather than connecting people and empowering them, the platform all too often fosters chaos and violence. Even the company itself came to this conclusion. Numerous internal documents leaked by former Facebook employee Frances Haugen in 2021 show that while Instagram has a toxic effect on young

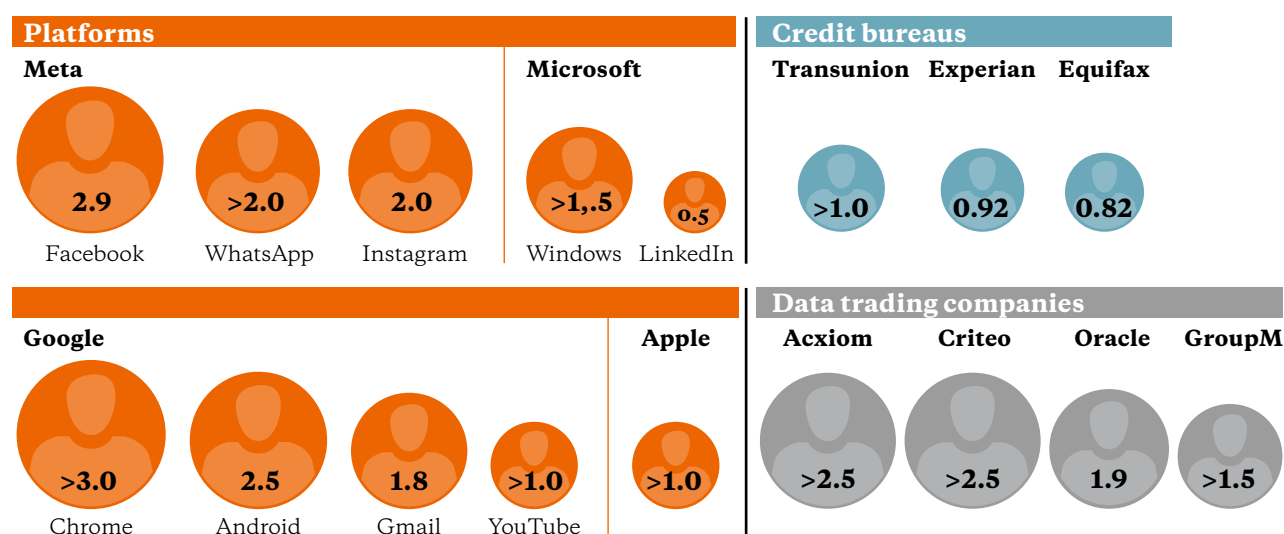
people's mental state, Facebook often has a similar effect on the social climate.¹¹ Activists in the Global South have been warning for years that while in liberal states with a strong democratic public sphere, the platform may have a damaging effect – keyword: Donald Trump, in regions that are politically more fragile and where Facebook is often the only digital public sphere, it has a devastating effect.

Conquering markets one by one

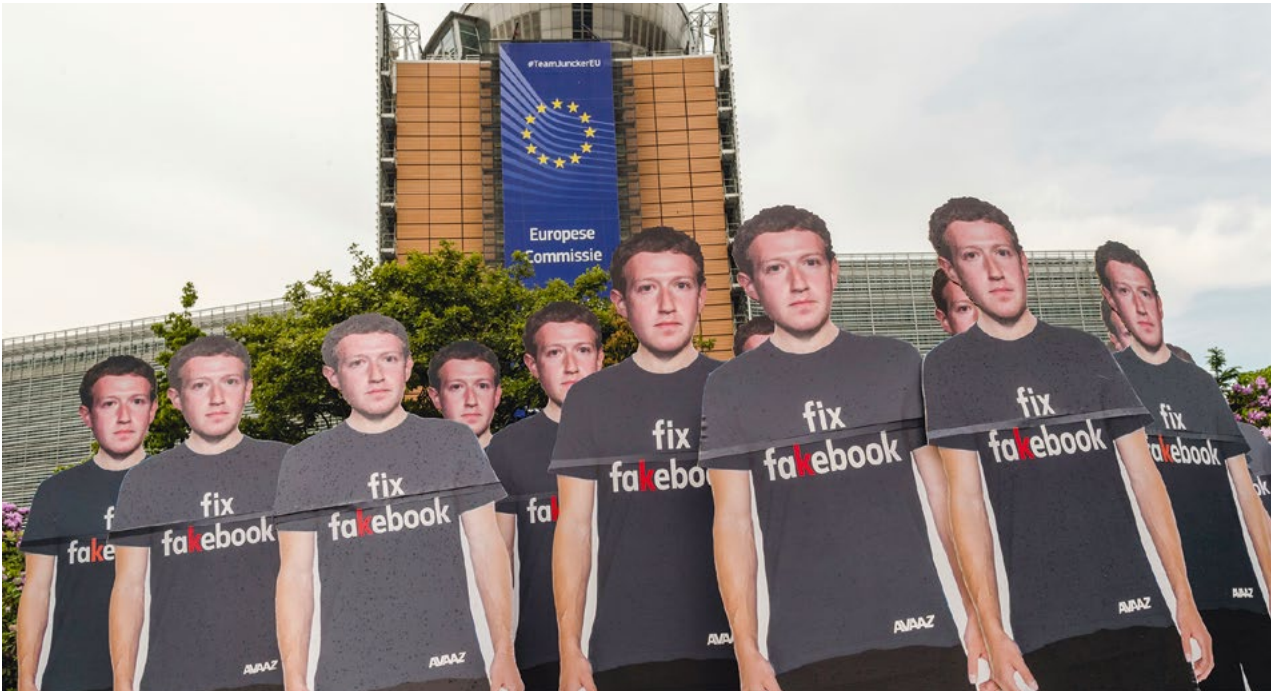
In line with Zuckerberg's motto "Move fast and break things", Facebook has conquered one market after another over the past decade – without caring about cultural specifics or political situations. The company estimates that more than 70 percent of its users live outside Europe and North America. Meanwhile, Facebook spends 87 percent of its misinformation classification budget on the U.S., according to the Facebook Papers. This leaves 13 percent for the rest of the world.

The data collection mania of the tech corporations

The companies gather data on billions of people.



The figures are based on information provided by the companies over the past years.



Global citizens movement Avaaz display life-sized Zuckerberg cutouts near the EU Commission to protest against fake Facebook accounts spreading disinformation on the platform, in Brussels in 2018.

In Myanmar, for example, where genocide has been committed against the Rohingya minority since the mid-2010s, Facebook allowed the spread of calls for violence against this ethnic group. A group of Burmese NGOs and a report by the UN Human Rights Council noted in 2018: Facebook's lack of moderation contributed substantially to the violence.¹² The company did not have enough moderators with the right language skills to enforce its own rules and contain hate speech.

Posts that call for violence

As the Facebook Papers show, similar things are happening in Ethiopia, where civil war has been raging since late 2020.¹³ Network staff repeatedly alerted to the fact that "problematic actors" are spreading disinformation and inciting violence. But Facebook did not change its moderation practices. They only had six fact checkers with the right language skills for a population of 115 million. For a long time, Facebook's algorithms did not understand hate speech in Oromo and Amharic, the country's most widely spoken languages.

According to Facebook's own investigations, the platform not only failed to contain conflicts, it often acted as their catalyst. The stirring up of emotions, polarisation and disinformation is an integral part of the platform's business model.¹⁴ That is because Facebook makes money by selling its users' attention to advertisers. And to do that, Facebook has created one of the world's largest data pools. The thing that helps advertisers to reach people that are most easily swayed is also susceptible to abuse and manipulation. What's more, Facebook adjusts its processes so that people stay on the platform for as long as possible. This means that the algorithms that sort through the communication flows on Facebook prefer posts that get a lot of likes, shares, comments and emoji reactions. But according to an internal report from 2020, viral posts are four times more likely to contain misinformation.¹⁵

It is this combination of datafication and drawing maximum attention that makes Facebook so dangerous and so successful at the same time. The company is one of the most valuable in the world, making a net profit of 29 billion dollars in 2020 alone. It is unlikely that Facebook will change its course of its own accord.

“Critical analysis, comparing sources”



Interview with **Marisol Castañeda**: President of the Brot für die Welt partner CALANDRIA (www.calandria.org.pe)

Ms Castañeda, your organisation CALANDRIA trains NGOs and journalists in Peru in communication. Is this working better now than 30 years ago thanks to digitisation?

Marisol Castañeda: Yes. Digital media have several advantages for our educational work. We reach a lot more people through learning platforms like Moodle or Classroom. Digitisation enables the communication and exchange of knowledge. And it gives more autonomy to our target groups.

Are there disadvantages?

Marisol Castañeda: People consume more information today, including fake news. For us, this means that we need to teach digital skills in our courses even more than before: critical analysis, comparing sources.

Do you reach everyone you want to reach?

Marisol Castañeda: No. There are groups that are digitally excluded and therefore unable to attend meetings or workshops. They are mainly older people, illiterate people – and women. Here the digital divide is particularly big. They do not have a smartphone. Or have to share it with their children or their husband so they can attend virtual classes or go to work. Only one in seven Peruvians owns a PC or laptop. In the Amazon region, and also in the Andes, 70 to 80 percent of all households do not even have internet. For these areas, you still need to make calls, send text messages or use the community radio to reach people.

Do you also need to have face-to-face meetings?

Marisol Castañeda: Yes. I understand educational processes and communication to be dialogue, and that means empathy and getting to know each other. No digital tool can fully replace physical meetings. While you hear what someone is saying in the video meeting, you do not really find out anything about what kind of a person you are seeing on the screen. Something gets lost.

What advice do you have for other NGOs?

Marisol Castañeda: Promote media education and strengthen digital literacy, including our own.

Biometric surveillance

In India, if you do not show your fingerprint you will not get subsidised cooking gas or a pension. Other countries are also digitising their social benefits, often with the help of private companies. The risks are immense.

There are few other technologies that get European human rights organisations and activists to spring into action as much as facial recognition and biometric data capture. “Take your face back!” is the call of a joint campaign run by tens of organisations standing up for fundamental rights in the digital space and currently aiming to collect a million signatures. They want the EU to ban all forms of biometric surveillance in public spaces. They argue that biometric mass surveillance threatens fundamental rights such as freedom of speech, freedom of assembly and privacy.

But while the EU is arguing about the uses and dangers of biometrics and is proposing to regulate the high-risk technologies of artificial intelligence (the AI Act; see page 26), other countries are already deploying biometric identification on a grand scale.

The largest biometric database in the world is located in India. According to the Indian government, the Aadhaar database contains information about around 1.4 billion people – that is 99 percent of the population. The construction of the database was financed with funds from the World Bank’s ID for Development (ID4D) project, which develops digital identification systems worldwide.¹⁶ For India’s head of government Narendra Modi, the database is an important cornerstone of his Digital India campaign, which is designed to make India fit for the future. Such systems, however, carry social risks: They can threaten the protection of personality rights and social security, fears IT for Change, a partner organisation of Brot für die Welt in India.

A 12-digit number for every person

How does the system work? India’s Unique Identification Authority (UIDAI) assigns a twelve-digit number (Aadhaar) to each registered person, under which it stores information such as name, gender, date of birth and address, as well as biometric data such as fingerprints, iris scans and photos. UIDAI outsources this work to registrars: public authorities as well as private companies such as banks and insurance companies.

The registrars, in turn, can hire subcontractors to enter citizens into the Aadhaar system. Although to this day, India does not have the protection of privacy enshrined in law that would prevent the data stored in this way from being passed on or stolen, entry in the biometric database is a precondition for many government services. Without Aadhaar, people do not have access to subsidised cooking gas, pension payments, scholarships or jobs. More and more private companies are now also asking for the Aadhaar numbers: Banks ask for them if you want to open an account or apply for credit, telecom companies ask for them if you want a SIM card, insurance companies to get insurance cover and start-ups to use their services.¹⁷

The digitalisation of government services poses a particular threat to the social security of the poorest people in India. Millions of people have been denied food rations, children have been denied enrolment in school or school meals and elderly people did not receive their pensions. The readers used to check fingerprints are often as unreliable as the country’s internet or mobile phone connections. The fingerprints of people who do hard manual labour are often difficult to scan. And, the iris scanners often do not work on people with eye diseases.

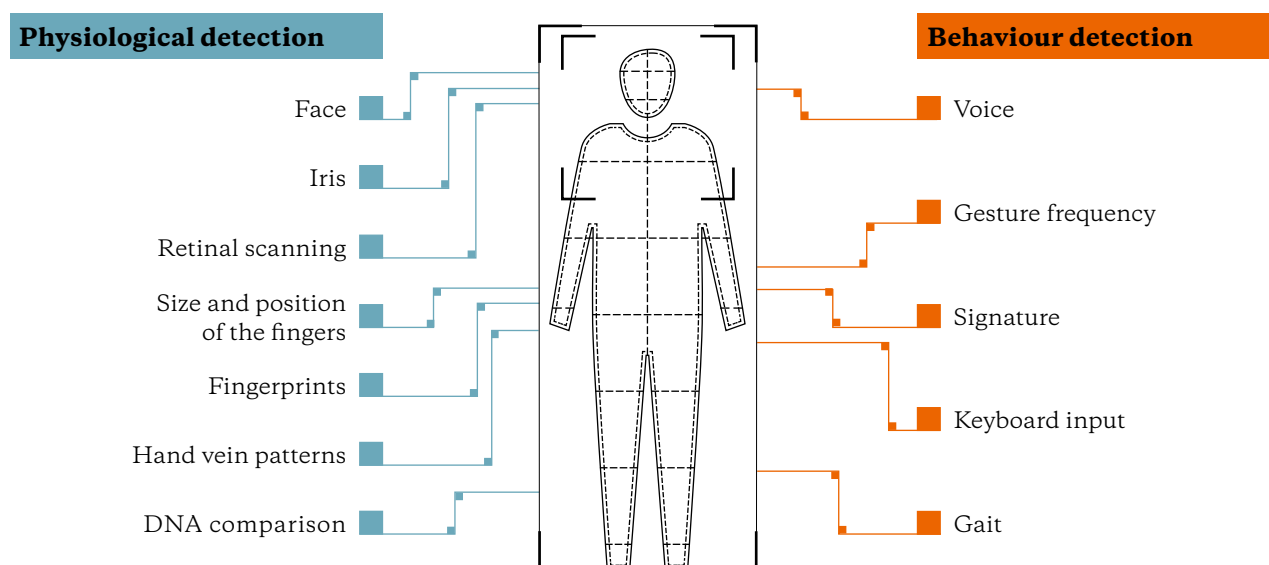
Security flaws: Data leaks and fundamental rights

There have already been numerous scandals that uncovered the security gaps of the Aadhaar systems: You could purchase personal Aadhaar data online for less than the equivalent of ten euros. Millions of Aadhaar numbers along with personal information were published on over 200 government websites. Another reason why Amnesty International believes that fundamental rights are threatened is because the UIDAI can disable the numbers for a variety of reasons. The people whose numbers are disabled lose access to state benefits.¹⁸

Biometric technologies are also being used in other countries of the Global South to verify the identity of social security recipients. In Mexico, the 55.6 million people insured by Seguro Popular, the national health insurance

This is how machines recognise people

Every person is unique - this fact is often abused.



Source: Brot für die Welt

scheme for the country's poorest, must share their biometric data with the authorities. In South Africa, 17.2 million recipients of social assistance are given biometric smart cards. Social Security agencies and private companies such as MasterCard or Visa often enter into commercial agreements to develop smart cards for social welfare programmes or to enable companies to accept them. In South Africa, for example, the biometric card for social assistance is a MasterCard. Such agreements do not generally include remedies for data and information misuse. Private companies, donor agencies, and the World Bank justify the expansion of digital identification systems by arguing that iris and fingerprint scanners or facial and voice recognition, along with the integration of databases, increases efficiency, combats fraud and reduces costs.

Easily done: interlinking law enforcement authorities

This has far-reaching consequences: Using a common identifier, biometric data, once stored in the database of a social welfare programme, can be linked to other systems, such as law enforcement systems. Nigeria's national identity database, for example, is linked to several databases – including the one managed by law enforcement agencies to search for criminals, for example. This means that video cameras in public spaces would be able to match each recorded face against millions of faces in the database and trigger an alert when a wanted person is spotted. The pressure to share sensitive social security data, including biometric identity data, with law enforcement (domestically and internationally) is further heightened by concerns over terrorism and migration. This not only compromises the privacy of millions of people worldwide, it also infringes on civil liberties.



An iris scan is taken to link an Aadhar card with the National Register of Citizens (NRC) in Barpeta, Assam, India.

This is how face recognition works

Facial recognition is a biometric method that can be used to identify people or confirm their identity. First, the face of a person is technically captured by a camera. Then the geometry of the face is analysed by a software. Important factors include the distance between the eyes or between forehead and chin. The characteristic features of a face are then converted into data, the face becomes a mathematical formula and is as unique as a fingerprint.

The print can be matched against a database of other known faces to determine a correspondence. A distinction is made between 1-to-1 matching (is the person the one who it says it is?) and 1-to-many matching (is this person on a list of wanted people?). The latter is often used by law enforcement agencies.

The surveillance state: Made in Europe

Autocrats around the world are using technology from Europe to oppress their populations. The market for surveillance products is growing, and the European Union is struggling to effectively control exports.

The Pegasus scandal shined a spotlight on surveillance technology manufacturers in 2021. The high-performance spyware is produced and distributed by the NSO Group, a company based in Israel. The USA is also considered a hotspot for producers of surveillance products. What is more, according to a ranking of the global surveillance industry published by Privacy International in 2018, Germany and Europe are among the top players. German and European companies are evidently as likely to supply their products to Western intelligence agencies as to criminals and autocratic rulers.⁴⁹ In Germany, the manufacturers of digital weapons systems have such illustrious and frequently changing names as Advanced German Technologies, Trovicor or FinFisher. While they shy away from the public eye, their products regularly crop up in places where human rights are under pressure.⁵⁰ In 2017, for example, the Trojan software Finspy from the Munich-based company FinFisher was found on websites in Turkey. The sites pretend to be part of the Turkish opposition movement; they ask activists to download a networking app, which then secretly installs the surveillance program. It is seen as likely that the Erdogan government is behind this, but there is no concrete evidence.

From Trojans to lie detectors

In Germany, meanwhile, a civil society alliance is suing the manufacturer for not having an export license for Turkey.⁵¹ FinFisher denies having supplied surveillance products to the Bosphorus, and prosecution authorities have been investigating the case since 2019. In 2020, the authorities searched the company's headquarters, and at the end of 2021 FinFisher filed for insolvency. Observers suspect that this move was designed to pre-empt a conclusion to the criminal proceedings; the parent holding company continues to exist under the new name of Vilicius.⁵² But the fact that things even went this far is considered a success.

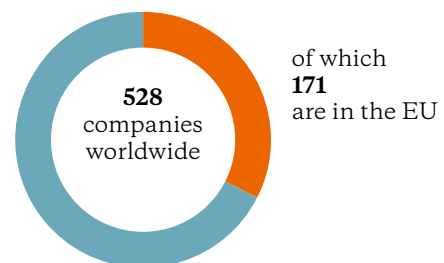
The EU has been wrestling over how to control the export of surveillance products for years. The market is growing, with offerings ranging from Trojans to biometric video surveillance to smart lie detectors. Surveillance technology is not considered legally problematic in and of itself. Rather, this is about products that can be used by the

military and the police, but can also be put to use for civilian purposes. Such dual-use products are not illegal. Following tough negotiations, revised rules for the export of such products have been in force in the EU since September 2021.⁵³ The Dual-Use Regulation now explicitly also covers surveillance technology. Since then, exports are subject to new transparency requirements and manufacturers are obligated to assess risks to human rights. The regulation also stipulates for the EU Commission to have a checklist of specific technologies and destination countries for which exports must be approved in advance. The list must be adopted unanimously by all EU countries, but does not oblige them to ban such exports.

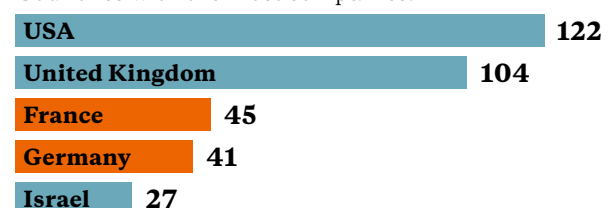
Human rights organisations consider this a disappointing compromise.⁵⁴ They had called for more binding control requirements and more comprehensive duties of care, and they fear that European companies will continue to sell products to authoritarian regimes. Whether the EU is indeed willing to put human rights above market potential is yet to be seen.

Registered office of exporters

One in three companies selling surveillance technologies is based in the EU.



Countries with the most companies:



Source: Privacy International (2018): *The Global Surveillance Industry*

“Data and money flow in one direction only”

We are witnessing a new, digital, colonialism. It, too, exploits people in the Global South.



Interview with **Renata Avila** CEO of the Open Knowledge Foundation (<https://okfn.org>)

Ms Avila, quite a number of development cooperation actors, including the World Bank, see the digital transformation as a major opportunity to reduce poverty and inequality in the Global South. Do you share this euphoria?

Renata Avila: It depends on which development model you are advocating. I believe in a sustainable, feminist and just digital future – and that is in stark contrast to the model that is being imposed on the Global South. That model only benefits China and the USA. The South provides them with the materials, labour and data to build their digital empires. In addition, the tech giants benefit from global trade agreements and complicated tax structures and pay very little taxes to the Global South.

Is this a new kind of colonialism?

Renata Avila: It's a continuation of the colonialism of the past, only this time it is digital. Resources, data and labour are once again exploited in the South. Only today, it is technology empires that rule the world by controlling critical digital infrastructure, data and ownership of computing power. They are assisted by an imperial world trade system that favours the leading powers and forces small countries to compete on unequal terms. It is a system in which companies have more influence than entire regions. All this is happening with the full recognition and complicity of the states, and they even appoint tech ambassadors to Silicon Valley.

How does this digital colonialism manifest itself?

Renata Avila: Let us take the example of education. Children around the world are passively learning technologies that they cannot improve, adapt or develop. Most of the

technologies used in schools are not based on free software, the software belongs to Big Tech. This acts as a break to digital innovation. Instead of building blocks, children are given a ready-made digital black box – and most parents think that is a good thing. The result is that the tech corporations do not just shape the children. They are also the ones who harvest the data, which they can use to develop even more products, rather than collecting educational data for the common good. In this form of digital colonialism, data and money flow in one direction only.

What does the dominance of the tech industry mean for democracy and development?

Renata Avila: Countries have lost control of important spaces: Most digital election campaigns, debates and even public health campaigns take place on private platforms. These are usually subject to California law, which everyone must then comply with. Election and health authorities do not meet local needs. What is more, the system is susceptible to encroachment by those in power, as was the case with Cambridge Analytica. Plus: Small, local businesses don't stand a chance. When WhatsApp announces new terms of use, everyone has to agree. This is a blatant abuse of their dominant market position.

How can developing countries become digitally sovereign?

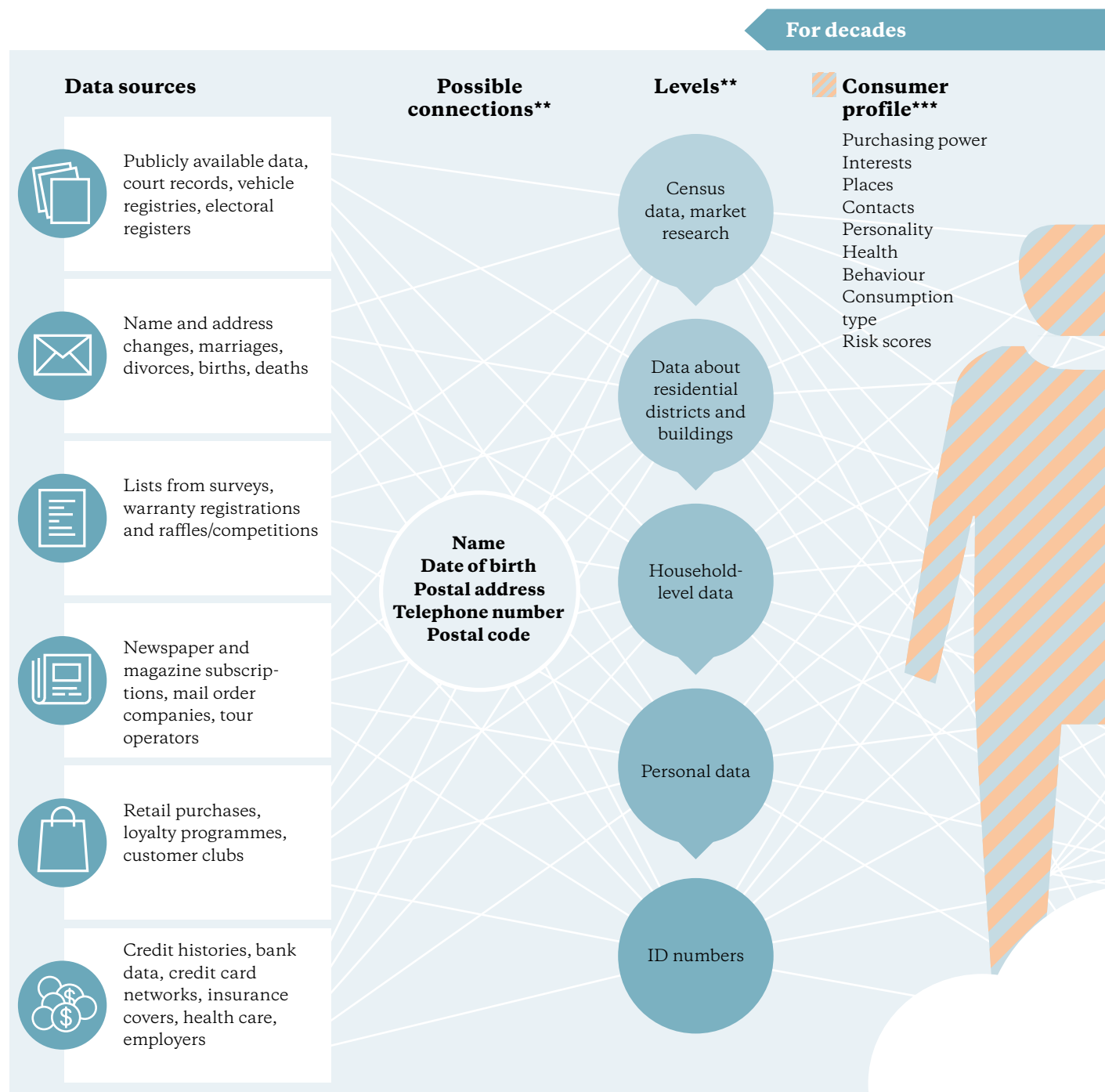
Renata Avila: That is not possible without political or economic sovereignty. For now, this means that we must stop the advancement of digital colonialism. Citizens must learn to make new technologies their own and demand to have a say in their regulation.

What must Germany and the EU do to achieve this?

Renata Avila: They should lift trade restrictions that shackle developing countries. It is unfair and cruel to restrict access to knowledge, the right to repair devices, the right to make copies of content or the right to tinker with technologies, just so that the monopolies can get richer. Developing countries need flexible rules to be able to innovate. And, they need space to develop technologies – without the prices and restrictions imposed by tech corporations worldwide. The Sovereign Tech Fund which Germany is now financing is a step in the right direction. The money helps the Global South to develop a more just, a decolonised technology.

This is how our data is collected: past and present

Companies use data to try to predict the behaviour of customers. They have been collecting information for a long time. In the digital age, countless new data sources and traders complete the profiles.

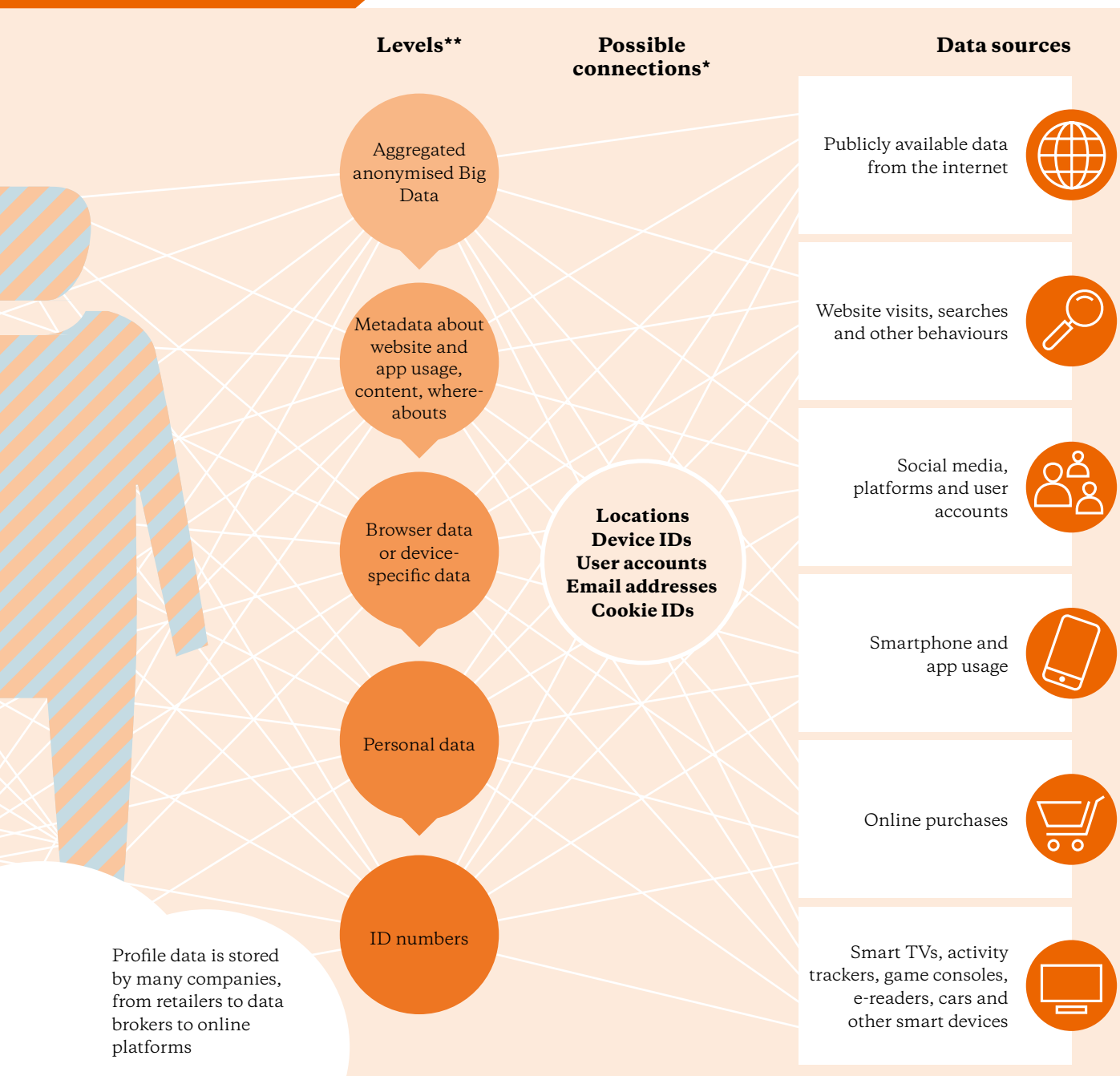


* The data are linked to each other using different identification codes ("identifiers")

** Data flows in at different levels, from anonymised to personalised

Source: Pascale Osterwalder and Wolfie Christi, "Corporate Surveillance in Everyday Life" (Cracked Labs, 2017)

Since the 2000s



*** Data from different sources and contexts are merged into individual profiles.

When machines make decisions about humans

In Austria, unemployed people are automatically sorted into categories; in the Netherlands, the local authorities used automated searches to find benefit fraudsters. What does it do to civil society when countries turn high-tech tools against their own people?

Is it legitimate to categorise unemployed people according to age, gender or the number of children they have and then – depending on which category they fall into – deny them further training? In Austria, this question has been with the Supreme Administrative Court since the beginning of 2021.²⁵ It is to decide whether the Austrian labour market services (AMS), the equivalent of Germany’s job centres, will be allowed to use a computer system across Austria that automatically sorts unemployed people into groups to help advisors decide what to do next.

From a technical point of view, this is not complicated. The labour market opportunity mode, as it is officially called, divides job seekers into three categories. It was developed by a company in Vienna, which fed the system with labour market data from previous years, including gender, age, nationality, place of residence and whether people have care responsibilities for children or relatives.²⁶ Based on this data, the system makes a prediction about how likely a new job seeker is to find work within a certain period of time. Only people whose chances are reasonable will be given support, such as further training. This turns a human being into a statistical probability.

Is a state allowed to treat its citizens like this?

Technologically, this may be simple. However, the AMS’s actions raise difficult moral and legal questions. Is a state permitted to deny support to its people based on such predictions? And should an algorithm, a machine-generated decision, be the judge of that? Whether you are given support or are basically being given up on has an enormous impact on the rest of your life.

The answers to such questions have far-reaching consequences. Not just for each individual, but also for civil society as a whole. In Austria, researchers and civil rights organisations had criticised the system from the outset.²⁷ In their view, it discriminates against those who are already disadvantaged in the job market. Older people and women

are penalised automatically – the latter even more so if they have children. Men are not affected by this.

Is that sexist? Is it discrimination? AMS head Johannes Kopf does not think so. All the system does, according to him, is reproduce the real existing conditions on the labour market.²⁸ Paola Lopez, a mathematician who conducts research on this topic, describes the AMS algorithm as a “discrimination barometer” that could easily be put to good use, namely by giving extra support to the most disadvantaged.²⁹ Instead, the system cuts them off.

No one thinks about the rights of those affected by this

The people mostly affected by such decisions are therefore often members of marginalised and socially disadvantaged groups. It is already more difficult for them to participate in decision-making processes or to campaign for equal treatment, social security or access to information. Automated decision-making processes make it even more difficult for them to secure the material foundations of a self-determined life.

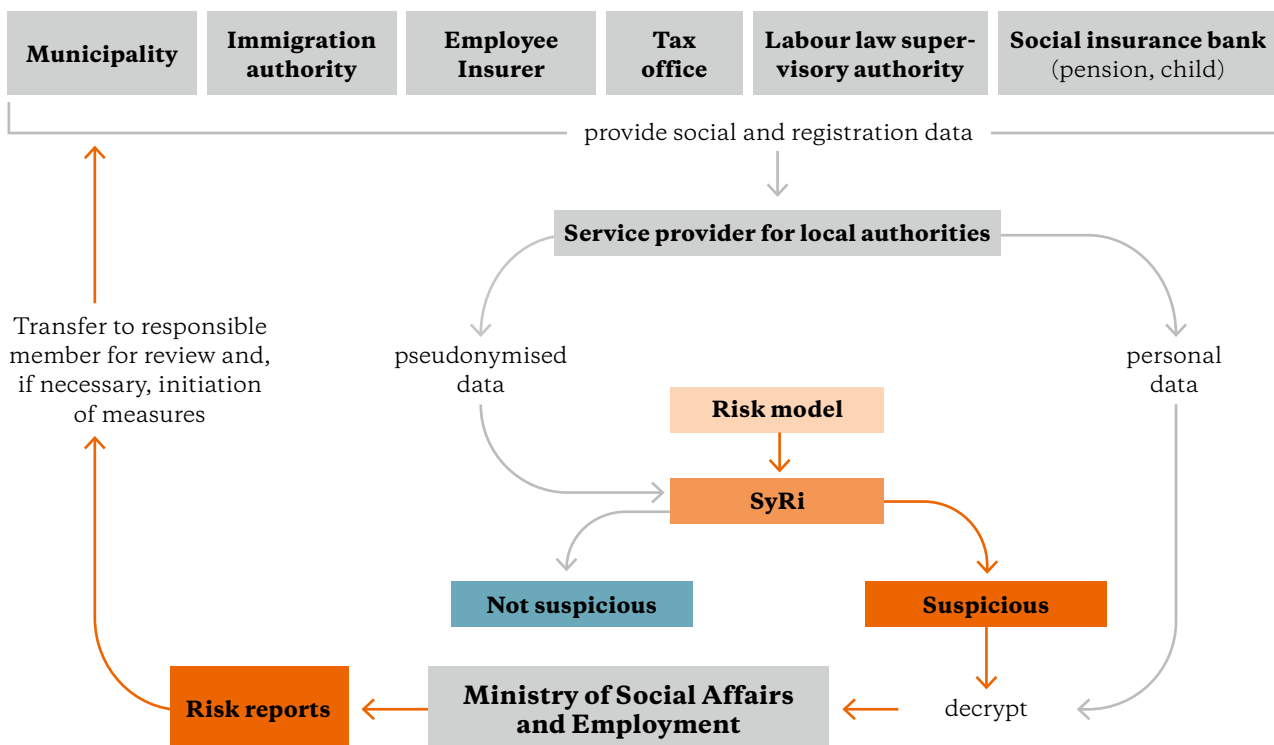
A bitter battle has been raging in Austria for more than a year. Following a trial run, the AMS was planning to introduce the model across Austria at the beginning of 2021. Then the data protection authority intervened. What the AMS does is “invasion-of-privacy relevant profiling” of people, the authority believes, and this requires a legal basis that does not yet exist. The trial run had to stop. A short while later, the Federal Administrative Court overturned the ban. The AMS is indeed allowed to feed data of job seekers into the model to assess support requirements, the court ruled in December 2020. Only automating the decision entirely is illegal. In theory, this paves the way for the introduction of the system.

Agency officials keep emphasising that no automated decisions are being made. The system only helps the advisors make their decision; a human being makes the ultimate decision. Critics are not convinced. They point to

First a suspect, then discriminated against

In the Netherlands, local authorities used the Big Data analytics tool SyRi (see below) to track down benefit fraudsters – and created a risk profile for each individual. The result: People who came under suspicion of fraud this way - often mistakenly – received less state benefits.

Members of the cooperative association:



Source: Image/CC-BY, Algorithm Watch

studies that show that when a machine makes a prediction, people do not tend to override it.

The fact that we even know so much about the AMS algorithm is very unusual. Because generally, such automated decision processes are problematic in another way altogether. They are a black box for the people involved, and non-transparent from the outside. We know about the AMS algorithm because the company responsible for it has published the example formulas for some cases.³⁹ And the examples also show that transparency alone is not enough. There also needs to be the opportunity to object. What good is it to a job seeker in Austria knowing that the system puts her at a disadvantage? She still cannot remove herself from the assessment or object to the prediction.

Suspicious per algorithm

Human rights organisations and activists are therefore calling for clear rules on when such systems can be used at all – whether by companies or states. The dispute surrounding the AMS has become a case study in what can go wrong when public agencies use automated predictions to provide or deny access to services. They are currently operating in a legal grey area.

The German financial regulator BaFin, for example, monitors the algorithms used in high-speed trading on the stock exchange. But when a municipality or public authority decides to use automated processes to track down benefit fraudsters and undeclared work, i.e. turning algorithms



Protesters take part in a rally against human rights abuses in China before the official opening of the CeBIT trade fair in Hanover March 15, 2015.

against members of the public, no one monitors this. This is what happened in the Netherlands; for years, the Dutch ministry of social affairs used a program called SyRi, short for Systeem Risico Indicatie, to analyse all kinds of sensitive social and registration data in order to flag people who might have been wrongly claiming unemployment or housing benefit.³¹ Anyone who flashed up in SyRi's data analysis was likely to soon receive a home visit. And, the people were not told that they were under suspicion. What is more, the ministry refused to disclose exactly what data was analysed and how the system arrived at its findings.

We see the same pattern here of such a system being used against people who are already disadvantaged. The system was used primarily in what are considered problem districts: districts with a poor population and a disproportionately large number of immigrants who often rely on government assistance. Only the ruling of a court in The Hague³² in early 2020 put an end to such risk scoring in the middle of Europe.³³ The court found that it violates the European Convention on Human Rights. It is possible, according to the court, that the scheme discriminates against poor people and migrants. Prior to the ruling, activists and civil society organisations had fought against it for years.

A legal framework full of gaps

Can companies and public authorities really unleash algorithms on their customers and citizens completely unchallenged – even when it is about such important matters as loans and social benefits? In theory, a legal framework to protect the people in the EU from such automated processes is already in place. When personal data is involved, the EU's data protection rules apply and they prohibit fully automated decisions. The two examples from Austria and the Netherlands show that this rule offers little comfort.

With the EU's AI Act, a set of rules for artificial intelligence is heading for the home stretch. The act is intended to place greater focus on high-risk systems such as biometric facial recognition in the future. However, human rights organisations like Human Rights Watch fear that specifically algorithms in connection with social security may fall through the cracks.³⁴

“We can tell more precisely who owns what land”



Interview with **Dimgong Rongmei** Head of Development at Brot für die Welt partner RNBA (<https://rnba.in>)

Mr Rongmei, you work with the Rongmei Naga Baptist Association in the Indian state of Manipur on land rights – and you use digital tools. Why do you need these tools?

Dimgong Rongmei: 90 percent of Manipur consists of hills – land whose ownership is not officially documented and instead governed by customary law. The village and clan chiefs have absolute power, also over the land. This makes everything related to the land very complicated. Now a few mega projects are coming up: railway routes, dams and roads. For this, the government needs land and pays huge sums as compensation. Since the village chiefs and clan leaders have the power, conflicts arise over land and money, also between the villages, each claiming the land for itself. It is difficult when the boundaries are based on customary law that is passed down through the generations orally. We try to create reliable land registers. To do this, we use mobile apps with GPS. And, based on these data, we create land ownership certificates with the local government, and village and clan leaders.

Does that help resolve land conflicts?

Dimgong Rongmei: Yes, because it creates clear ownership. The land is distributed transparently – including people who had not owned any land in the village. We also encourage women to own land, because they have a right to it. We talk to the clan leaders and clarify it with them. This way, single women also benefit from the digitalised and trustworthy recording of ownership.

Do the clan leaders accept the new certificates?

Dimgong Rongmei: Most of them do.

And if not?

Dimgong Rongmei: Then we talk to them and give advice. We gather as much information as possible from customary law using the app and can then say more precisely who owns what land. People accept that.

Mexico

Bugged and spied on

No country has used the Pegasus spyware more excessively than Mexico. The government has unsettled and weakened civil society with its digital surveillance system.

Pegasus is the name of the winged horse in Greek mythology that faithfully stands by the gods. It makes springs burst forth, delivers thunder and lightning, and is ready for action wherever it is needed. The god father Zeus rewarded it for its services. It has been a miraculous creature and a constellation in the sky ever since, as if quietly watching over everything.

And that is what Pegasus did in Mexico in our time, and this time for those in power. It hears everything, sees everything and does everything they want – and also makes springs burst forth, but no water flows from them. Pegasus is a malware that does its work secretly and silently, and spies on people.

In the summer of 2021, an international research consortium discovered that this software is used worldwide.

It is installed on smartphones, remaining unnoticed and eavesdropping on its victims. In Mexico, we can observe exactly how Pegasus works. It shows us how digital surveillance helps to eliminate political opponents, how it weakens civil society and sows distrust, how powerful people use sinister methods to further their power and pressure people who fight for a freer country.

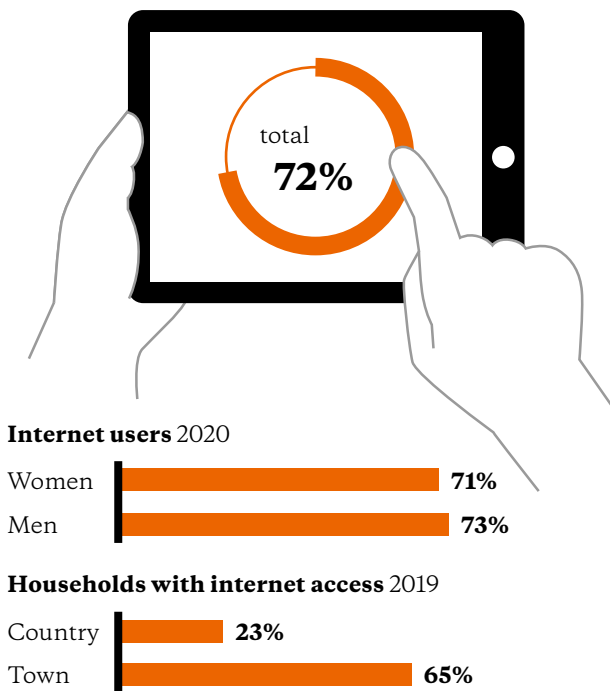
In Mexico Pegasus can be detected on the smartphones of people in the immediate vicinity of the then opposition politician and current president Andrés Manuel López Obrador. Pegasus was found on smartphones of the family members of the 43 students of a teaching seminar who were abducted in 2014 by police officers in league with organised crime. No one is safe from the software; the human rights organisations Consorcio Oaxaca, a partner of Brot für die



“Listening to Aristegui is an act of rebellion”, reads the placard during a protest against the dismissal of journalist Carmen Aristegui. Her team had previously uncovered a real estate scandal the president is involved in.

Access to the internet

Percentage of people in Mexico who use the internet (2020)



Source: International Telecommunications Union (UN ITU): www.itu.int/en/ITU-D/Statistics/Dashboards/ (accessed in December 2021)

Welt, alone has so far identified 109 human rights defenders and 27 journalists who have been spied on with Pegasus.

The investigations by an international network known as the Pegasus Project are based on a data leak of 50,000 phone numbers of people targeted by the spyware worldwide. 15,000 of those phone numbers are Mexican.

The software is produced by the Israeli NSO Group. In 2020, the numbers were leaked to Amnesty International and the non-profit media organisation Forbidden Stories, and the story was picked up on by media outlets around the world. In Mexico, Amnesty International and Forbidden Stories shared the data with Aristegui Noticias, the online investigative magazine named after its founder, Carmen Aristegui. And it was Aristegui who detected one of the first Pegasus infections on her phone after reporting on shady property deals concluded by controversial

ex-president Enrique Peña Nieto. In 2015/16, she received more than 20 text messages with innocuous looking but malicious links, revealed the University of Toronto's Citizen Lab in 2017³⁵, an institute dedicated to securing digital rights. The phones of Aristegui's colleagues and family members were also attacked, even that of her then 16-year-old son. "It's a malware that activates your camera, your microphone, everything that is an integral part of your life," she said, explaining in a nutshell what makes this software so insidious. It turns an infected smartphone into a bug without anyone noticing.

War on drugs as a pretext

Countries, both democratic and authoritarian, use Pegasus primarily to fight crime or terror. The fact that they also use it on a large scale to spy on regime critics, opposition members and civil society initiatives only became known as a result of the investigations. The spyware market is entirely unregulated. Internet freedom and digital rights experts such as netzpolitik.org are calling for these companies to be banned because their products endanger life and limb.

The NSO Group's first major customer is Mexico. The country stocked up on cyber espionage products as early as the 2010s, ostensibly to tackle its rampant drug crime. In July 2017, Aristegui Noticias published details of the contract between the NSO Group and the Mexican Attorney General's office,³⁶ which had acquired Pegasus in 2015 for 32 million US dollars in order to gradually equip not only the Attorney General's Office itself but also its secret service and ministry of defence. In total, the Mexican authorities paid NSO around 300 million US dollars. Pegasus pervades Mexican society. If you start at the top of the hierarchy, you will probably come across the spyware's most prominent victim – the current president, López Obrador, commonly known as AMLO. When he was still an opposition politician and the top candidate for the centre-left Morena party, his surroundings were a potential spying target. He stood up for ordinary people and wanted to end the 77-year rule of the Institutional Revolutionary Party (PRI).

Obrador also promised to take care of the case of the 43 students who disappeared from the Escuela Normal Rural "Raúl Isidro Burgos". They were being trained as primary school teachers in the state of Guerrero. Few other crimes have captured public attention in recent years in Mexico as much as this one. The school, which was founded in 1926, has a socialist orientation and has been

a thorn in the side of all governments. Most of the students come from rural regions with indigenous populations, and Marxist views are widespread among the lecturers.

Unbearable uncertainty

On the day of the kidnapping – on 26 September 2014 – the 43 students were on their way to a demonstration to protest the Mexican government’s unfair pay and hiring practices. On the way, they were stopped by the police, who immediately opened fire. Six students died, 43 were abducted, and to this day, no one is quite sure what happened to them. Most likely they were murdered. Investigations revealed that the students were kidnapped by police and the Guerreros Unidos drug cartel.

Shortly after the kidnapping, the students’ parents joined forces to put pressure on investigators to solve the crime. They organised many demonstrations in the country’s capital. There are photos of Cristina Bautista, one of the mothers, carrying a placard with a picture of her son Benjamin and the inscription: “You took him away alive, we want him back alive!” The uncertainty is almost unbearable, but the state is doing nothing to shed light on it – and Obrador has not yet kept his promise to solve the case either.

To the parents, one person is to blame: Tomás Zerón, former head of Mexico’s criminal investigation agency. He is said to have participated in the kidnapping and torture of the 43 students and tampered with evidence. In April 2020, the Attorney General issued a warrant for his arrest. In December 2020, it became known that Zerón had fled to Israel. The Zerón case is sensitive and tricky, because he

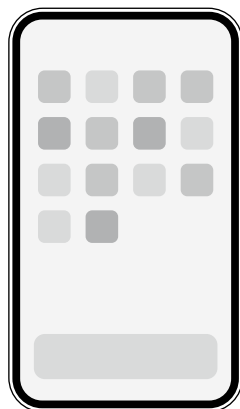
This is how Pegasus works

This surveillance technology accesses all data of users via their smartphones.

Attack vectors

Pegasus can be installed on a phone through vulnerabilities in common apps, or by tricking a person into clicking on a malicious link

-  SMS
-  WhatsApp
-  iMessage
-  Unknown vulnerability



Abilities

Once installed, Pegasus can in theory intercept all data on the device and send it back to the attacker

-  Reading text messages
-  Recording emails
-  Monitoring WhatsApp chats
-  Extracting photos and videos
-  Switching on the microphone
-  Activating the camera
-  Recording calls
-  Reading GPS data
-  Combing through the calendar
-  Tracking contacts

Source: Guardian (2021): UAE linked to listing of hundreds of UK phones in Pegasus project leak

Pegasus are useful to fight organised crime, he said. But without government control mechanisms, such surveillance tools can be abused.⁴⁰

When details of the surveillance activities emerged, the affected NGOs filed criminal charges with the federal prosecuting authorities in 2017, but they did not take action. One year later, a judge ruled that suspicions of espionage by government agencies against journalists and human rights defenders should be investigated and that the investigation should focus on the illegal use of the Pegasus software. So far, nothing has happened.

Great fear for relatives

Sofia de Robina of the Center for Human Rights (ProDH), a partner of Brot für die Welt, which gives legal advice to the parents of the 43 students, gave a powerful description of the impact of state surveillance. In 2016, a conversation with relatives was leaked to the public and quoted out of context. “It seemed to imply a connection between the ProDH and organised crime that did not exist,” de Robina says. This incident alarmed the organisation for a number of reasons: “Not knowing how much information these malicious actors had and how they planned to use it was a concern.” And which consequences the leak might have for Centro ProDH’s litigation strategy and the families affected. In their daily work, the risk of being targeted by the state and the military is always present. People also greatly fear for their family members and friends, who cannot always be protected. Because the encroachments on civil society are happening on such a grand scale, several organisations (including Consorcio Oaxaca, another partner of Brot für die Welt) are calling for independent investigations by the UN or the Inter-American Commission on Human Rights. They call on all federal agencies to cooperate with investigators, disclose the Pegasus deal files and provide journalists and human rights defenders with better protection.

These are demands placed on a state they could not rely on – but calling for the rule of law is still their strongest weapon.

“Through me they entered people’s homes and private spaces”



Interview with **Yesica Sánchez Maya** Director of Consorcio Oaxaca

Ms Sánchez, you were under surveillance by the Pegasus spyware. How did you find out about it?

Yesica Sánchez Maya: A journalist who worked on the Pegasus investigation project told me that my number was on the list. Looking back, there were obvious signs that my phone was being spied on. There were photos and videos on my phone, which I never took. Apps suddenly disappeared or I suddenly saw them in mirror image. What is more, we kept having to deal with attacks and sabotage, and we did not know where the attackers got the information they needed for this. Now we know.

Why did the state spy on you?

Yesica Sánchez Maya: Consorcio Oaxaca is a feminist human rights organisation. We document violence against women and expose the severe human rights crisis in the country. We say it as it is, and we denounce the situation and the failure of the government publicly, and also internationally. This made us a thorn in the side of Peña Nieto’s government. It used the spyware to keep an eye on its “enemies” and intimidate them.

What does that mean for your work?

Yesica Sánchez Maya: It means that all the victims of human rights violations, all the people I was in contact with at the local and international level, very likely also became victims of espionage. And it means a violent intrusion into my professional, family and personal life.

How do you cope with it?

Yesica Sánchez Maya: I am deeply concerned, because we offer the victims protection and support, and create a safe space. That is why people come to us. Now we do not know what the state knows about them and what it does with that information. Such uncertainty is difficult to bear. I feel as if someone had held a large magnifying glass over me for years. Knowing that I was the gateway for espionage that targeted not only me but all the people who communicated with me is difficult. Through me they entered many people's homes and private spaces.

Does the state protect your organisation?

Yesica Sánchez Maya: No. After we had denounced a femicide in Oaxaca and the involvement in it of government officials in 2020, we found a pig's head outside our office with a message saying that we are next. We reported it, but so far we have heard nothing from the prosecuting authorities. This shows the depth of the entanglements. They want us to give up.

What do you demand from your government?

Yesica Sánchez Maya: The state must tell us who is responsible for the spying attacks – and conduct criminal investigations. It must be transparent about what information was intercepted about us and our contacts. And governments need to get together and put a stop to the surveillance of journalists and human rights defenders. This is central to defending democracy.

In brief

Our partner: Consorcio Oaxaca

Origins: In 2003 from an association of feminists

Project area: The state of Oaxaca

Focus: Consorcio Oaxaca brings together feminist activists of all generations and advocates for gender justice at the national and international level. The organisation also provides protection and psychosocial support for human rights defenders.

Further information <https://consorciooaxaca.org>

Indonesia

An all-purpose weapon against criticism

In Indonesia, the government is combating undesirable voices on the internet with a law that was introduced to regulate online commerce. Today, the law is used to silence civil society.

When Joko Widodo was sworn in as president of Indonesia in October 2014, high hopes were pinned on him. From 2005 to 2012, he was the mayor of his hometown of Surakarta. During his seven years in office, Widodo, the founder of a furniture company, established a political style that placed emphasis on dialogue, fought corruption and focused on economic growth. Jokowi, as he is known, seems to favour policies that encourage large infrastructure projects and attract investors from abroad.

On 5 October 2020, his government thus passed the so-called Omnibus Law. Citing the economic impact of the corona pandemic, among other things, labour and environmental laws were being deregulated and industry-wide minimum wages scrapped to stimulate the economy.⁴ The changes are reflected in 1,244 articles and 79 legislative texts. Without consulting expert bodies nor civil society, they were rushed through parliament.

Protests against the legislative package erupted throughout the country. Hundreds of demonstrators were arrested. Their criticism is ignited by the fact that environmental standards, such as mandatory environmental impact assessments, are being suspended and workers' rights, the rights to information and freedom of expression weakened. There is a lack of transparency, they feel. What is more, civil society actors complain that the Omnibus Law concentrates power with the national government and undermines the power of local governments to act and make decisions.

That this criticism is legitimised shows a case that occurred in the summer of 2021 in New Guinea, the second largest island on earth with an area of 786,000 square kilometres. The eastern part of the island belongs to Papua New Guinea. The western part, West Papua, is part of the island archipelago of Indonesia. The island is rich in



The so-called Omnibus Law – passed in October 2020 – is intended to create an investment-friendly climate for international companies. But people all over the country are protesting against it.

mineral resources: Oil, natural gas, copper and gold. This makes the Indonesian part economically important for the country. The world's largest gold mine is in the highlands of Papua. There are also major liquid gas reserves here. At the same time, 80 percent of the people in West Papua are poor: About 2.4 million people live largely on what they grow themselves. In comparison, only ten percent of the overall population live below the poverty line of \$1.90 per day, according to the national statistics office.⁴²

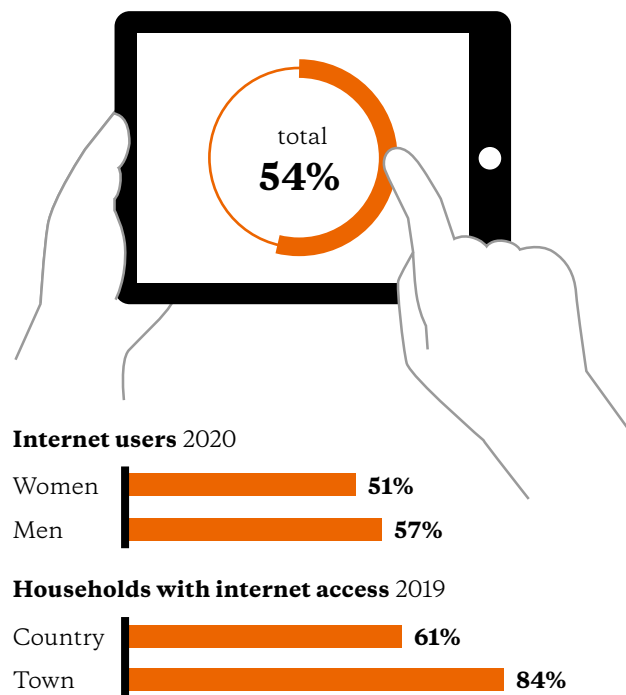
Business with the military

In the summer of 2021, nine NGOs published a study, including Greenpeace Indonesia, the Indonesian Legal Aid Foundation and the human rights organisation KontraS (The Commission for the Disappeared and Victims of Violence), a partner of Brot für die Welt. According to the study, military and police bases have been built conspicuously close to mining areas for years. Furthermore, there are close ties, the study says, between the military, retired generals in particular, and the companies that are active on the ground. The report lists four companies. Two of them are gold mines with proven business links to the military, including the current Minister of Maritime Affairs and Investment, Luhut Binsar Panjaitan, a former general.⁴³ The allegation: The government uses its power not only to boost the economy but also to further personal interests. The study led to a public discourse about what is going on in West Papua. Authors were invited to interviews. But the government did not react. In mid-August, human rights defender Haris Azhar and Fatia Maulidiyanti, coordinator at KontraS, sat down in front of a web camera and spoke to one of the study's researchers. Then they uploaded the just under 30-minute recording onto the internet.

Now the minister and former general Panjaitan reacted. He reported the two activists to the police for defamation. A month after the publication of the video, Haris Azhar and Fatia Maulidiyanti receive a summon: In it, they are asked to explain the motives behind the publication, to publicly apologise within five days via the YouTube channel and in the print and online media, and to promise not to repeat what they said.⁴⁴ The politician said he filed the complaint because he cannot allow his children to think badly of him. A few days later, Azhar and Maulidiyanti receive another summon almost identical in content. The possible punishment: up to six years in prison.

Access to the internet

Percentage of people in Indonesia who use the internet (2020)



Source: International Telecommunications Union (UN ITU): www.itu.int/en/ITU-D/Statistics/Dashboards (accessed in December 2021)

Through their lawyers, they explain that their criticism was not directed against Panjaitan as a private individual, but rather in his capacity as minister. His actions in West Papua, they said, give the impression that he is abusing his office to use the military to secure his private interests. But Panjaitan maintains that he has to defend his personal reputation (see interview).

And he relies on a law that is playing an increasingly important role in restricting online freedom of expression. The Information and Electronic Transaction Law (ITE Law) was passed in 2008 and revised in 2016. It was originally created to regulate hate crime, fake news and pornography within the new field of e-commerce. The law states: Any person who intentionally and without authorisation disseminates information with the intent to sow hatred or discord against individuals or groups on the basis

of ethnic and social group affiliation, religion, or race is punishable by imprisonment for up to six years or a fine of up to one trillion rupiahs – the equivalent of about 60,000 euros. It was said at the time that all modern countries need such a law to keep the net free of the things that poison society. Now the Indonesian government is using it to suppress criticism.

Because the law leaves a lot of room for interpretation. It does specify what is punishable and what is not. Article 27, for example, defines defamation. Article 28 deals with fake news and hate crime. However, the articles are written in such a way that enables the authorities and the police to suppress freedom of expression.

Chat followed by arrest

The case of Fatia Maulidiyanti and Haris Azhar is not the only illustration of how great the power imbalance is between those who denounce human rights violations and corruption, and government representatives. In July 2021, the state president’s chief of staff filed charges against the human rights defenders Egi Primayogha and Miftachul Choir.⁴⁵ They had disclosed on the website Indonesia

Corruption Watch close ties between him and a pharmaceutical company that had developed a controversial covid drug.⁴⁶ The politician referred to the defamation article and declared this to be a private vendetta that he was incapable of ignoring: “I have a wife and children.” And in November, two Greenpeace activists were charged. They had criticised the president for downplaying the consequences of deforestation at the climate summit in Glasgow.⁴⁷

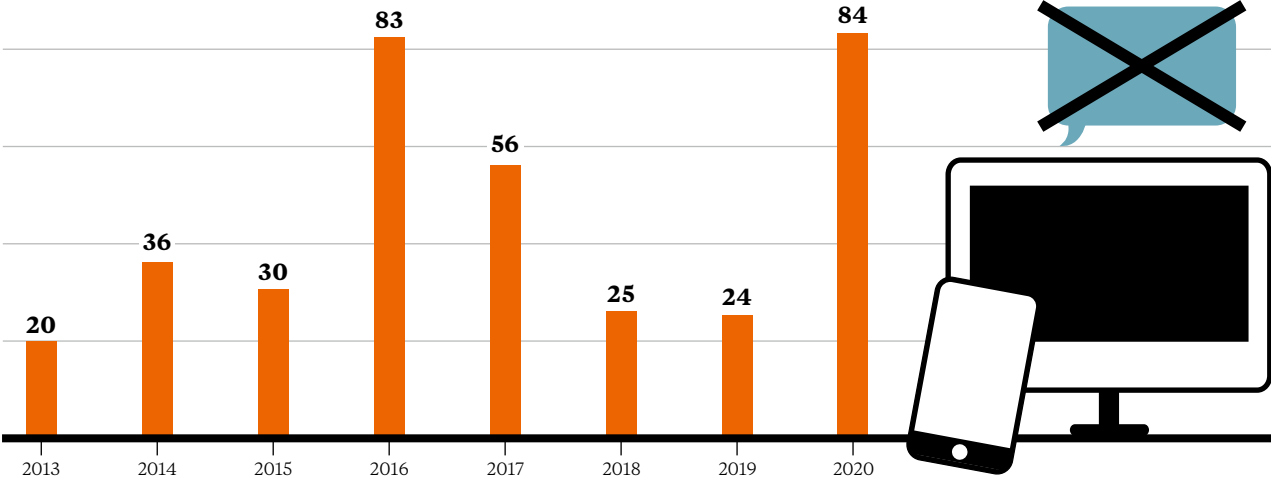
The case of university lecturer Saiful Mahdi shows that if you express criticism in a semi-public chat group you are already under threat. In a message to his colleagues via a messaging service, the engineer complained about the hiring process for lecturers in his faculty. “I have received sad news about the death of common sense,” and “Why is a faculty that was once so glorious now so faint-hearted?” This landed him in jail for three months.

Police get a separate cyber unit

In 2020, Amnesty International registered 119 cases of alleged violations of freedom of expression under the ITE Law, with a total of 141 suspects, including 18 activists and four journalists.

No freedom of expression online

Number of cases in which people were criminalised by the ITE Law



Source: SafeNet (2021): Indonesia Digital Rights Situation Report 2020



In August 2021 human rights defenders Fatia Maulidiyanti and Haris Āzhar denounce corruption in a video. They have been persecuted by members of the Indonesian government ever since.

The result is an atmosphere of intimidation, in which people generally as well as human rights defenders censor themselves before making grievances public.

While the ITE Law is the most well-known law to contribute to this development, it is not the only one. Under the Indonesian constitution, all citizens have the right to express their opinions and access information freely. However, article 154 of the Indonesian criminal code states: “Any person who publicly expresses feelings of hostility, hatred or contempt towards the government of Indonesia faces a prison sentence of up to seven years” – this is contradictory to the constitution, Indonesia’s constitutional court ruled in 2007.

All attempts by civil society to persuade the government to change course and revise the ITE Law failed. On the contrary: Since February 2021, a dedicated police cyber unit has been combing through social media and chat apps in search of allegedly criminal content.⁴⁸ This is done on the request of the Minister for Political, Legal and Security Affairs.

The minister had announced the year before that the government would set up a special police unit to counter

the spread of misinformation online, as this has the potential to ruin public order. Today, if you voice criticism online you may get a message saying: If you do not delete this post immediately, you will be penalised under the ITE Law.

As early as April 2021, the police unit sent such warnings to 200 social media accounts, mainly of users who criticised the government. Most people deleted the content immediately.⁴⁹

“More and more people are realising that it makes a difference whether you get involved or not”



Interview with Auliya Rayyan Head of the International Advocacy Division at the human rights organisation KontraS (The Commission for the Disappeared and Victims of Violence)

Ms Rayyan, what is your view of what has been happening in Indonesian civil society for years?

Auliya Rayyan: I could give a very long answer to this question, but I will try to be brief: We are seeing a significant decline in democracy. Our president and the security forces tolerate violence. They do not see it as a violation of human rights, but rather as a legitimate form of punishment or a means to achieve certain goals. Between September 2019 and September 2021, the state arrested 5,389 people for expressing their opinions, for example, by participating in demonstrations or rallies. Some were immediately released again. Others were given lengthy prison sentences.

What is the significance of the digital sphere in Indonesia for civil society and for your work?

Auliya Rayyan: The internet is an important place for us to exchange information with other organisations, to keep our followers up to date and interact with them. We can of course also criticise using the official channels, such as petition letters to the government. But using the social media channels is often faster and people can respond immediately. And the pressure for the government to respond is greater.

The government has repeatedly shut down the internet entirely. What are the consequences of this for your work?

Auliya Rayyan: The shutdown of the internet shows how insecure the government is about the free flow of information. Because it cannot control it, it shuts down the internet instead. This makes it difficult for us to monitor human rights violations and pass on news to a wider audience. We can only do our work when we know the details of a specific case.

There is strong opposition in Indonesia to the ITE Law, the most well-known law politicians use to try to defend themselves against unwelcome criticism. How is the government responding to the protest?

Auliya Rayyan: It says it is open to revising the law if civil society objects. But so far we have not heard anything about the law being revised.

What are you doing to get the government to review it?

Auliya Rayyan: We have applied for a judicial review and this process is accompanied by campaigns. We also sit in the hearings, and so are international organisations.

What happens to those who risk coming out from under cover with their criticism of the government?

Auliya Rayyan: They are persecuted. For example, many individuals and human rights defenders criticised the government's handling of the corona pandemic. In April, the WhatsApp account of a human rights defender was hacked. The police then accused him of having provoked riots. He tried to get to a safe place. But the police caught him and threw him in jail. What happened to him was entirely arbitrary. Many people demanded his release until he got out of prison.

What are the consequences of such attacks for your work?

Auliya Rayyan: We get a lot of hate messages on our social media channels. That is why we introduced some safety measures. For example, we drive directly to the office without taking any detours. Because it is only at home or in the office that we are truly safe. And we pay even more attention to what we post. But it is fair to say that we are staying strong and continuing our work.

What are you doing to maintain that strength?

Auliya Rayyan: I personally get a lot of support from our international network. But we also get support from local human rights or research organisations in the form of webinars or discussions. We try to be there for one another, and we also get psychological support when we feel we are at risk of burnout.

How, specifically, do international organisations support you?

Auliya Rayyan: It varies and ranges from legal advice to support for our campaigns and safe accommodation when the situation becomes too risky.

Are you optimistic or pessimistic about the future?

Auliya Rayyan: Personally, I do not see any improvement when it comes to the protection of human rights in my home country. But there is one positive aspect: more and more people are joining the human rights movement. They realise how the situation in our country is deteriorating and that it makes a difference whether you get involved or not. This helps us to put more pressure on the government.

But young people in particular prefer to look for jobs in government or business in Indonesia. Why did you choose KontraS?

Auliya Rayyan: Many people at my university looked down on NGOs, especially the local ones. They wanted to work for ministries or startups with nice offices and free lunches. But in my case, it has always been my dream to do something that gives people hope.

In brief

Our partner: The Commission for the Disappeared and Victims of Violence (KontraS)

Origins: Founded in 1998 in Jakarta

Project area: Nationwide and international advocacy

Focus: The goal is a legal and political system based on the sovereignty of the people and free from fear, oppression, violence and human rights violations. Their work covers topics such as the protection of activists, reform of the security sector and right to land.

Further information: <https://kontras.org/en>

Tanzania

As if someone had pulled the plug

When elections were held in Tanzania in October 2020, everything pointed to a victory for the incumbent president. He still shut down the internet. This is just one step of many to weaken the opposition, civil society and human rights in the country.

It was the 27th of October 2020; the next day was to be an important one for Tanzania. A new parliament is up for election as well as the president. It is very likely that John Magufuli and his Chama Cha Mapinduzi (CCM) party will be re-elected; he has been in power for five years, and the party has dominated the country since its independence in 1961. The last hours before the polls open are important – initiatives and NGOs can now once again remind people to vote, explain the electoral system and campaign for the right to co-determination.

Election observers and journalists are working at full speed: Will everything run correctly? In 2015, Magufuli had campaigned on fighting corruption and inefficiency,

but instead he interfered heavily with civil liberties: journalists disappeared, political opponents were beaten up, opposition members were not allowed to hold rallies and new laws restricted freedom of assembly and freedom of expression. Magufuli's most important opponent, Tundu Lissu, also felt the severity of these measures: for one week he was excluded from the election campaign.⁵⁹

Election day was around the corner – and suddenly it was as if someone had pulled the plug. The internet was down, and nothing worked anymore. Social media and messaging services, used for quick communication, sharing observations, mobilising voters, were dead; online news sites that compile information were also down. The



In a controversial election, President John Magufuli is re-elected on 28 October 2020, with an 84.4-percent share of the vote. Here, a woman is casting her vote in Stone Town, Zanzibar.

incumbent government was depriving the population of the last opportunity to gather information and to connect with other people. Through its telecommunications authority, the government ordered an internet shutdown that was to last for more than a week. This is how teacher and social media influencer Godfrey Abely Magehema described the impact of these measures: “I had no access to reports and information.” But what do you do as an influencer when you cannot post on your news feed? Or Idd Ninga, a social worker in Arusha: “The shutdown of internet services violated my right as a citizen to access information, especially during an election. It was extremely difficult to keep up to date, especially since not everyone always has access to traditional media such as television or radio.” Governments around the world keep shutting down the internet in recent years, especially in African and Asian countries – in 2020, there were 109 shutdowns in India alone. Governments, directly or through their telecommunications authority, instruct internet providers to restrict access to certain services for their users. This primarily affects the social networks, but it can also be extended to make the entire internet inaccessible.

The Tanzanian government relied on the “Electronic and Postal Communications Regulations” of 2020 for the election shutdown. It authorised the Tanzania Communications Regulations Authority (TCRA) to order service providers to block or filter content if the agency considered the content illegal. If providers did not comply, they risked a penalty.

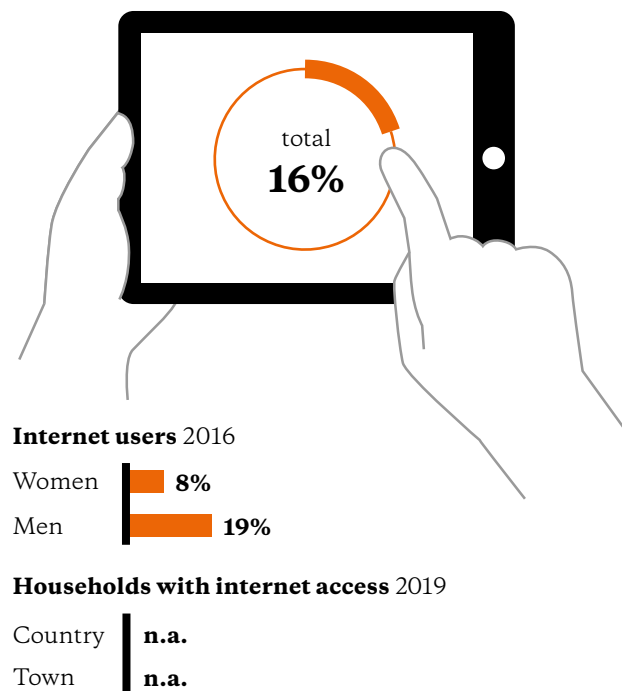
An official from the TCRA- who asked not to be named – confirmed to Deutsche Welle that the shutdown was approved by President Magufuli. Looking at the developments in the years leading up to the 2020 election, this is not surprising. Since the beginning of Magufuli’s term in office in 2015, freedom of expression and freedom of the press have been restricted step by step. Bloggers, for example, have had to register with the TCRA since 2018 and pay the equivalent of 800 euros for a license. This alone is an obstacle to writing a blog at all.

An “Unpatriotic” report

An entire legislative package also fundamentally interferes with basic civil rights. Under the Media Service Act, media companies can be suspended, journalists arrested and publications banned, among other things. The reasons for this can be “false or misleading news” – but who defines

Access to the internet

Percentage of people in Tanzania who use the internet (2017)



Source: International Telecommunications Union (UN ITU): www.itu.int/en/ITU-D/Statistics/Dashboards/ (accessed in December 2021)

that? In any case, the law is being applied – in 2019, the Citizen Newspaper reported on the devaluation of the Tanzanian currency and was suspended for a week. In May 2020, two journalists were arrested for conducting interviews on the difficult Covid situation. The reason: Such “unpatriotic information” could have a negative impact on the country’s security, unity and economy.

The restrictions affect journalists as well as people who stand up for their country working in NGOs and other organisations. Human rights defenders are imprisoned, lawyers are suspended and opposition activists are fined. All it takes is to express a view that is different to that of the government.

Members of Magufuli’s government argued that the laws were aimed at combating hate speech and other online crime such as cyberbullying and pornography.⁵⁴

Magufuli had already indirectly announced the shutdown two years before the election: “I was wishing that angels descend from heaven one day and close all these platforms, so that when they are reopened after one year, we have already built our new Tanzania.” The internet was shut down the day before the election and continued to be down for more than a week. It was executed at various levels: The TCRA ordered the telecommunications service and internet providers to use filters to restrict access to services like Twitter, WhatsApp and Telegram; previously, providers had been ordered to block access to SMS and voice messaging services. According to the NGO Access Now (which campaigns worldwide for unrestricted access to the internet and digital rights), the TCRA installed devices that throttle the internet, block websites and limit data traffic to such an extent that large data packets containing videos or photos cannot be transmitted at all.⁵² This deprived millions of people in Tanzania of their usual means of communication.

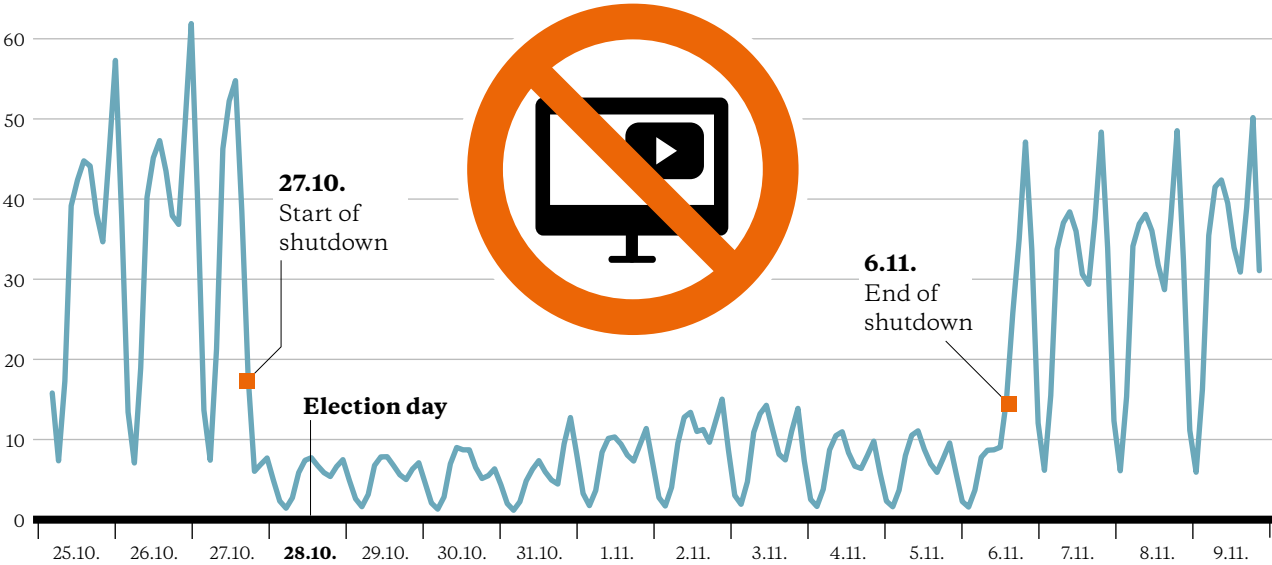
No reports about the election

Analyses of real-time data showed that services such as Twitter, WhatsApp, Instagram as well as Google services such as Gmail and Google Translate were indeed completely or partially unavailable via the leading Tanzanian network operators. The data also indicate a general disruption of the services of the state-owned Tanzania Telecommunications Corporation.

The victims of the internet shutdown were the people of Tanzania: businesspeople unable to go about their business, causing economic losses; journalists, NGOs and initiatives unable to freely report on the election – such as the Christian Council of Tanzania (CCT). Without social media they were unable to gather and disseminate information and report on problems before, during and after the election. To make matters worse, the CCT was not approved as an election observer. But the shutdown also affected people who simply wanted to meet friends or talk to their

Eleven days without internet

YouTube Traffic shows: There was virtually no internet access in Tanzania around the time of the 2020 presidential election.



According to Google, *traffic* here refers to the ratio between the request rate from Tanzania and the worldwide request rate. A request is an attempt to access a web page, not access itself.

Source: Google Transparency Report, *Traffic and disruptions to Google*



The internet is an important source of information for many people in Tanzania. A shutdown like the one around election time in October 2020 is thus a severe encroachment on basic rights.

families – a blatant disregard for basic human rights. But why does a government do such a thing and what for?

We are familiar with the usual arguments from other countries: shutdowns are designed to curb the spread of “fake news, hate speech or content promoting violence.” According to observers, however, this is just a pretext; shutdowns, they believe, aim to restrain protests, for example as a result of military action, to channel rising violence due to local conflicts and to prevent political instability.⁵³ In Tanzania itself, the shutdown was justified by “national security and concern for the fairness of the electoral process” – ultimately just empty phrases to gloss over human rights infringements.⁵⁴

The protests did not happen – there was too much fear

The bare figures are known: Magufuli won the election with 84.4 percent of the vote. Tundu Lissu of the opposition party

Chadema came in second with 13 percent. Magufuli was able to significantly increase his share of the vote – in 2015 he had received 58.5 percent of the vote. Interestingly, voter turnout in 2020 was 50.7 percent, well below the 67.3 percent turnout in 2015, even though the number of registered voters had increased by seven million compared with 2015.

The election that took place in Tanzania on 28 October 2020 was not fair, and it was directly manipulated via the internet shutdown. The shutdown also had a major impact on the coverage of the election, according to the observer group Electoral Institute for Sustainable Democracy in Africa (EISA). It was simply not possible to gather and disseminate adequate information about the election; there were fewer opportunities to report incidents in time for lawyers to intervene, for example.

How did Tanzanian civil society react to the election and the shutdown of the internet? Were there protests, demonstrations? No, says Gloria Mafole of the CCT, “there was no public response, people were simply too afraid.” And people couldn’t connect with each other without the internet and messaging services. Only people who were

able to set up a VPN tunnel, a protected network that can bypass the blockage, could communicate, Mafole says. Although such VPN tunnels were banned, during the shutdown the demand for VPNs increased by 18,823 percent.

Official reports stated that Magufuli died in March 2021 in Daressalam. Two days after his death, his Vice President, Samia Suluhu Hassan, was sworn in as Tanzania's first female President.⁵⁵ The 61-year-old is from the semi-autonomous island of Zanzibar, worked in the Ministry of Planning and Development and pursued a career in Zanzibar's regional government. In 2010 she was elected to the Tanzanian parliament and became Magufuli's Vice President five years later. Many people who were disappointed by Magufuli are pinning their hopes on Suluhu Hassan.

On the positive side, Hassan abolished the school ban for pregnant girls and young women in the autumn of 2021.⁵⁶ But when it comes to freedom of expression, she falls short of many people's expectations: none of the laws restricting freedom of expression and freedom of the press have been weakened or abolished since the start of her presidency; journalists are still being arrested and persecuted by the authorities. And in July 2021, eleven representatives of the opposition party Chadema were charged with financing and planning terrorist activities – including its leader Freeman Mbowe, who is still in prison.

Tanzania's first female president is an opportunity for the country, media wrote after Magufuli's death.⁵⁷ So far, Samia Suluhu Hassan has disappointed any hopes for the easing of restrictions. The FAZ newspaper put it succinctly: "Magufulism lives on".

“There was chaos”



Interview with Gloria Mafole Programme manager for Good Governance and Lobbying at the Christian Council of Tanzania (CCT)

Ms Mafole, what was your experience of the internet shutdown on the day before Tanzania's election on 28 October 2021?

Gloria Mafole: As soon as we woke up in the morning we noticed that something was wrong. The internet was not running and the messaging services were unavailable. There was chaos.

What did this mean for you?

Gloria Mafole: The shutdown severely restricted our work around the election. This time, our organisation was excluded from the election observation. This is one of the measures the Magufuli government used to restrict some of the most basic human rights. That is why we had to rely on our own network and on the pastors and staff of the member churches to gather information about the election – they all went to the polling stations. The internet shutdown meant that this information could not be passed on or published. This went on for seven days, by which time the election was long over.

Did civil society protest?

Gloria Mafole: No, that did not happen. People were afraid of punishment. After all, the Magufuli government repeatedly arrested and intimidated critics and members of the opposition. What is more, because of the internet shutdown it was virtually impossible to communicate, to coordinate, to arrange to meet up. Only the people who had the possibility to set up a VPN tunnel were able to use the messaging services. But that was also banned.

Why is election observation so important in a country like Tanzania, which was long considered a model of democracy and human rights... ?

Gloria Mafole: Things changed in 2015. Magufuli's government passed many laws that bolster the system and make life difficult for members of the opposition and independent journalists. The country has slipped to 124th place out of 180 countries in the press freedom rankings of Reporters Without Borders.

And the elections?

Gloria Mafole: The shutdown, which was ordered the day before the election, says a lot. And you see, the election commission is biased, it is part of the politics that is controlled by the ruling party. That is why election monitoring is important, and that's why we were not approved for it.

President Magufuli died in March. He was succeeded by his long-time vice president, Samia Suluhu Hassan. Has the situation improved since then?

Gloria Mafole: Not in the way we had hoped. The laws that systematically restrict civil society are still in place and government critics are in prison; we do need changes. At least Suluhu Hassan abolished a law prohibiting pregnant girls from going to school. They can now go to school again. It is a small but important change. But it is not enough. What we need now is the reversal of the draconian laws that have been depriving us of our fundamental rights since 2015. And a new constitution.

In brief

Our partner: Christian Council of Tanzania (CCT)

Origins: In 1964 as an umbrella organisation of the country's most important Protestant churches and church organisations

Project area: Nationwide

Focus: CCT sees itself as the mouthpiece of its member churches vis-à-vis the state and society. Project and lobbying activities on gender, health, climate change, the environment, food security, peace and good governance.

Further information: www.cct-tz.org

Ukraine

Lies as a weapon

Since the beginning of the conflict in eastern Ukraine, fake news have been a key element of Russian warfare. A vibrant civil society has developed methods to resist this. It thus fills a void in the Ukrainian state, which at times succumbs to authoritarian temptations itself.

On 5 July 2014, the Ukrainian army marched into Slovyansk, a city in eastern Ukraine with a population of just over 100,000. They rounded up the population in the city centre on Lenin Square; some were brutally tortured, a three-year-old was crucified.

One woman managed to escape the city. She contacted the pro-Kremlin television station Channel One Russia. Her eyewitness accounts shocked many people in Ukraine. There was just one catch: None of it was true, neither the torture nor the crucifixion. Slovyansk doesn't even have a Lenin Square. The witness turned out to be an actress, the wife of a pro-Russian member of the military.⁵⁸

Disinformation has been an important weapon of Russian warfare since the outbreak of the war in eastern Ukraine in the spring of 2014. Fake news is designed to divide Ukrainian society and create a general mood that says Ukraine's proximity to the European Union is a danger which the partner in Russia can protect them from. But a vibrant Ukrainian civil society has been working against this for just as long and with lots of energy. There is a popular joke in Ukraine that goes: "Without Vladimir Putin and Russian aggression there would be no civil society here at all". There is more truth to this joke than the Russian president might like.



On the anniversary of its independence in August 2021, citizens in the Ukrainian capital of Kyiv took part in the March of the Defenders of Ukraine. What may look like folklore is actually a serious political concern.

The armed conflict, which is still ongoing, started in November 2013. It started in Kyiv with protests against a decision by then-President Viktor Yanukovich. The Ukrainian government had been negotiating an agreement with the EU to forge closer economic ties between them for years. But Yanukovich rejected the agreement, which was all but signed. People came to the Ukrainian capital to protest from all over the country. One of their slogans: “Ukraine belongs to Europe, not Russia.” As security forces quelled the demonstrations, more people arrived. The Maidan became the centre of their months-long protests. In February 2014, Yanukovich fled the country.

In Crimea, too, supporters as well as opponents of closer cooperation with the EU take to the streets – until troops in unmarked green uniforms take control of the peninsula. Later, Russian President Vladimir Putin was to argue that he needs to protect Russian citizens and Russian speakers in Crimea and south-eastern Ukraine.

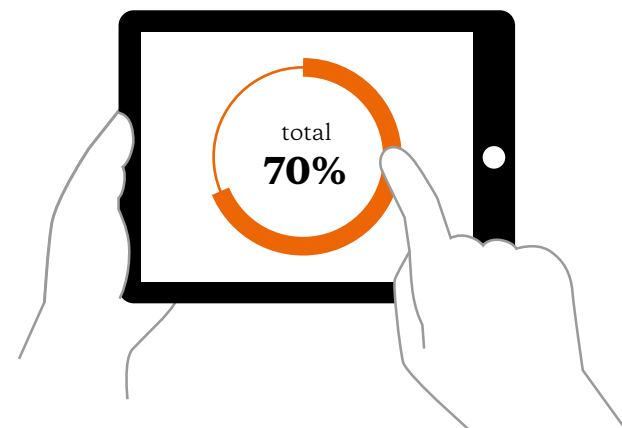
In a controversial referendum held in mid-March 2014 in Crimea, more than 95 percent of the voters were reportedly in favour of joining Russia, even though only 62.9 percent had identified themselves as Russians in a previous census.⁵⁹ However, the decision for or against the annexation was not made along ethnic lines. The decisive factors were economic and political, promises of prosperity and better pensions were made. Crimean Tatars and civil society actors feared for their freedom.

Fighting ensued between Russian-backed separatists and the Ukrainian military, which soon spread into eastern Ukraine. According to the Global Conflict Tracker of the Council on Foreign Relations, more than 10,300 people died and nearly 24,000 were injured between April 2014 and November 2021.⁶⁰ Other sources put the death toll up to 14,000.

From as early as March 2014, Russia has been using fake news to sow mistrust and deepen social division. While people in Kyiv protested against corruption and anti-Western propaganda, the Russian news media popular in Crimea, such as Russia 24, NTV, Channel One Russia and Russia-1, paint a very different picture: Kyiv is the aggressor, they say. And Ukraine is a fascist and nationalist country, controlled by the EU and the US, oppressing the Russian-speaking population. Such messages are reinforced by trolls who spread pro-Russian, anti-Western content on social media, forums and blogs.

Access to the internet

Percentage of people in Ukraine who use the internet (2019)



Internet users 2019



Households with internet access 2018



Source: International Telecommunications Union (UN ITU): www.itu.int/en/ITU-D/Statistics/Dashboards/ (accessed in December 2021)

Citizen journalism is booming

All that escalated into a war of information. Many fake reports are first published in Russia, picked up in Ukraine by Russian-language TV stations and news portals backed either by the Russian state or Ukrainian oligarchs close to the Kremlin, such as Viktor Medvedchuk, and then shared online on Facebook groups, anonymous and personal chat channels, and YouTube channels. To broaden their influence, Russian-controlled broadcasters, including their websites, and pro-Russian Facebook pages cooperate with each other. This creates an echo chamber where statements reinforce each other and lend each other legitimacy.

But Russia is not the only country that spreads fake news. Such fake reports also often originate from Ukrainian

Ukraine today

Since 2014, several regions of Ukraine have been occupied or annexed.



Source: Federal Agency for Civic Education (2019):
Ukraine-Konflikt: Der vergessene Krieg im Osten Europas

politicians and businesspeople who favour close ties with Russia. The Opposition Platform – For Life party, for example, is considered one of the main sources of pro-Russian propaganda. One of its chairmen is the oligarch Viktor Medvedchuk.

The example of the fact-checking organisation StopFake shows the energy with which Ukrainian civil society is fighting back against this invisible but extremely effective weapon. At the beginning of March 2014, prospective digital journalists talked about what is going on in their country in a Facebook group; they thus followed a common spirit that had also characterised the atmosphere on the Maidan six months earlier. Because no one knows which information can be trusted, the new types of citizen journalism emerged during the protests, which scrutinise every piece of information.

Civil society fills the gaps left by the state

Digital journalists came up with the idea of a website that unmasks fake news using verifiable sources. Soon it was up and running. News of its launch spread quickly. Several tens of thousands of fake news items have appeared there since then. The website now has more than 30 people working for it and publishes its findings in 13 languages. StopFake has also exposed the lie of the crucified boy. The website founder, Olga Yurkova, travelled to Slovyansk especially for this purpose.

StopFake is one of many organisations that make it their mission to educate Ukrainian society. As well as with journalists, they work with analysts, open-source experts, social media initiatives, cyber activists and IT companies with special software skills. Among other things, they work against Russia's distorted account of history, provide information about Russian troop movements in eastern Ukraine and promote data security. They also teach media skills, for example at universities for prospective journalists. They thus fill a gap that the Ukrainian state was unable to fill itself, especially at the beginning of the conflict.

But it is not only the defence strategies of Ukrainian civil society that have become more professional. Propaganda has also become more sophisticated. Initially, fake news were generally obvious lies, such as the crucified boy or the Ukrainian fighter jet that is said to have shot down the Malaysian airliner MH-17 and 298 people died as a result; the latter had also been spread by Channel One Russia. StopFake proved that the alleged photographic proof had been retouched.⁶¹ Extensive analyses by the German research agency Correctiv and the Bellingcat digital forensic journalism network revealed that a Russian-made anti-aircraft system, operated either by Russian separatists or Russian forces on Ukrainian territory, was responsible, and that the anti-aircraft system was later returned to Russia.

Over the years, the propaganda has become more complex. According to an analysis of the Ukraine Crisis Media Center and the Estonian Center of Eastern Partnership, there are a number of narratives that regularly make it into the news.⁶² One is of a thriving Nazism in Ukraine that tramples all over the legacy of their ancestors who once fought against Hitler's Germany. According to another narrative, Ukraine is in a civil war, has become a squalid money laundering centre and is headed for state bankruptcy. The

Russian media cite experts and studies and use the assessments of rating agencies to support their claims. And because Ukrainian media sometimes lack the professionalism to check sources, they also pick up on such reports. This way, fake news turn into truths.⁶³ Civil society actors also come under fire in such campaigns: StopFake is said to be an organisation with a fascist agenda.

Disinformation on all channels

However, there is no reliable answer to the question of what kind of disinformation has what effect or how many people are even reached by such campaigns. According to a study carried out in May 2021 by the independent platform Texty, websites with pro-Russian content get more than 110 million visits per month.⁶⁴ Similar YouTube channels get 120

million views. The Russian-controlled RT television channel says it reaches 700 million people in more than one hundred countries. This would give it a wider reach than the BBC, but without its journalistic standards.

However, a joint research project by the Center for Security Studies at the ETH Zurich, the London School of Economics, the Shorenstein Center for New Media at Harvard, and Internews Ukraine suggests that digital media are much less effective at spreading such disinformation than traditional media. As part of the project, the researchers tracked 17 disinformation narratives on social media and chat apps. While 20 to 30 percent of the Ukrainian public agreed with them in whole or in part, the more often respondents encountered such narratives, for example on TV channels of Viktor Medvedchuk, the more they tended to believe them. The authors thus concluded: “These findings suggest that fears around the effectiveness of digital



On 25 December 2019, residents of Sevastopol, the largest city on the Crimean peninsula, celebrated the arrival of the first direct train from St. Petersburg. The placard reads “Motherland! Freedom! Putin!”.



A woman sits with a baby stroller next to an infantry fighting vehicle of Ukrainian Armed Forces, which was damaged during fighting between Ukrainian government forces and pro-Russian separatists, and then installed as a monument in a park in Kramatorsk, Ukraine, November 2021.

disinformation are likely to be overblown and threaten to distract from the role of traditional media as a tool of influence that is at least as important.⁶⁵

Ukrainian government has authoritarian traits

Since 2014, all presidents – including the current one, Volodymyr Zelenskyy – have been taking action against the channels that are considered distributors of fake news in Ukraine. Then-president Petro Poroshenko, for example, banned the broadcast of Russian television in Ukraine. More than 70 broadcasters were blocked, and three years later, so were popular portals such as Vkontakte, the Russian version of Facebook, the Russian email provider mail.ru and the Russian search engine Yandex.

This raises the question of what the situation is like in Ukraine itself when it comes to freedom of expression and freedom of the press. In addition to curbing fake news, for example, Ukraine banned 25 books published in Russia on the grounds that they contained propagandistic historical narratives. What is more, entry bans were imposed on Russian and international journalists whose work allegedly undermines the territorial integrity of Ukraine.⁶⁶ In late 2019 and early 2020, two draft laws of the ruling parliamentary majority and the Ministry of Culture and Information Policy also provoked controversy: both were authoritarian in nature, as they would have granted government agencies broad powers to identify and sanction fake news and statements that the government considered a threat to Ukraine's territorial integrity. Following pressure from civil society and advice from other governments, the laws were not passed.

“The propaganda is everywhere”



Interview with **Oksana Khmelnytska** Psychologist, founder and head of the professional association Mental Health Service

Ms Khmelnytska, you are one of the initiators of Mental Health Service, which trains and provides networking in trauma therapy and psychological care for people in eastern Ukraine. How did that come about?

Oksana Khmelnytska: In 2014, several female trauma therapists and psychologists – in Ukraine these are almost exclusively female professions – joined forces to support people in eastern Ukraine who look after people with mental illness.

How did you go about that?

Oksana Khmelnytska: For many people, psychological knowledge and trauma therapy are considered things imported from the West. For this reason, Ukraine did not have the structures in place or the specialists to care for people who suffered from the consequences of the war. We ourselves were not trained to deal with such crisis situations. And so we had international organisations from Germany, Georgia and the USA teach us this knowledge and exported it to the East.

Kyiv, where you work, is 800 kilometres from eastern Ukraine. Would you even be able to do your work without digital tools?

Oksana Khmelnytska: No. We could not do our work just using a phone. Due to the pandemic, digitisation made a great leap forward. We talk to each other in closed chat groups, collaborate on online documents and use chat apps and video conferencing. I look forward to being able to meet people face to face again after the pandemic. But many digital tools will remain.

How do you judge the success of your work?

Oksana Khmelnytska: Our success is that people are willing to use such services instead of drinking alcohol or taking drugs. After the war broke out people were only interested in material support. Our work is essentially to show people what options even exist when they experience domestic violence, post-traumatic stress, depression or anxiety.

And what are the consequences for society of the constant disinformation campaigns?

Oksana Khmelnytska: The propaganda is everywhere. It keeps finding new topics. This brings with it additional anxiety and destabilisation. This results in a loss of trust in the government and a loss of solidarity. This not only divides Russia and Ukraine, it reaches deep into families. Forecasts suggest that a reconciliation, if it is possible at all, will take at least two generations.

In brief

Our partner: Mental Health Service

Origins: In 2014 (under current name since 2019)

Project area: Southeast Ukraine, Kyiv region and Belarus

Focus: Therapeutic work with people traumatised by war, torture, flight, division and the ongoing crisis. Further training, exchange of ideas and mutual support with professional colleagues. Civil conflict management and reconciliation.

Further information: <https://mhs.org.ua/>

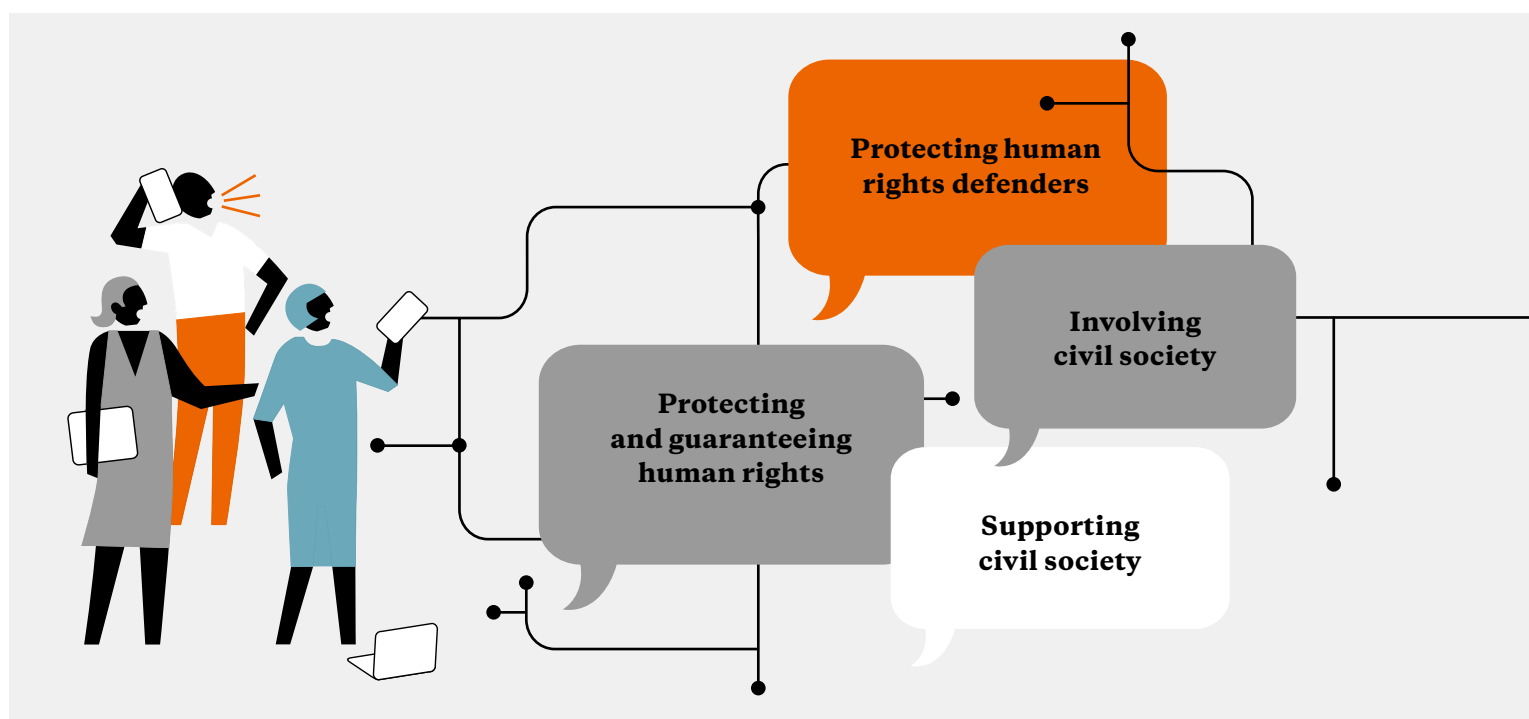
Our demands

Governments and Parliaments should ensure that...

- universal **human rights** are protected and guaranteed, including in the digital space.
 - civil society actors are promoted and enabled worldwide to stand up for just and sustainable development **without fear** of persecution and repression.
 - civil society and particularly vulnerable and **disadvantaged** groups can effectively participate in political, social and economic decision-making.
 - **embassies** around the world strengthen their efforts to promote human rights, human rights defenders and the scope for action of civil society.
 - its own **foreign economic** and foreign policy decisions do not violate human rights.
 - the **export** of surveillance products is prohibited, except on a case-by-case basis, if guaranteed that they do not violate human rights.
 - the development and use of non-commercial digital social infrastructures is promoted as an **alternative** to platforms like Facebook.
 - they do not use nor authorise internet blockers, **upload filters** and other regulatory measures for the digital realm that can be misused as censorship.
- algorithmic systems that make autonomous decisions or help make decisions are introduced only once they have undergone comprehensive **risk assessment** to ensure that they do not violate fundamental rights or lead to discrimination.
 - companies and government agencies always actively inform people of any decision that has been made about them based on algorithms. There needs to be **transparency** about input data and prognostic parameters.

In their international relations, governments should step up their efforts to ensure that...

- other governments **release** human rights defenders who are imprisoned for their work.
- civil society and particularly vulnerable and **disadvantaged** groups can effectively participate in political, social and economic decision-making in all countries.
- an international legal framework is created in which the obligations of states and the **responsibility** of companies in the digital sphere are in conformity with international human rights norms and standards.



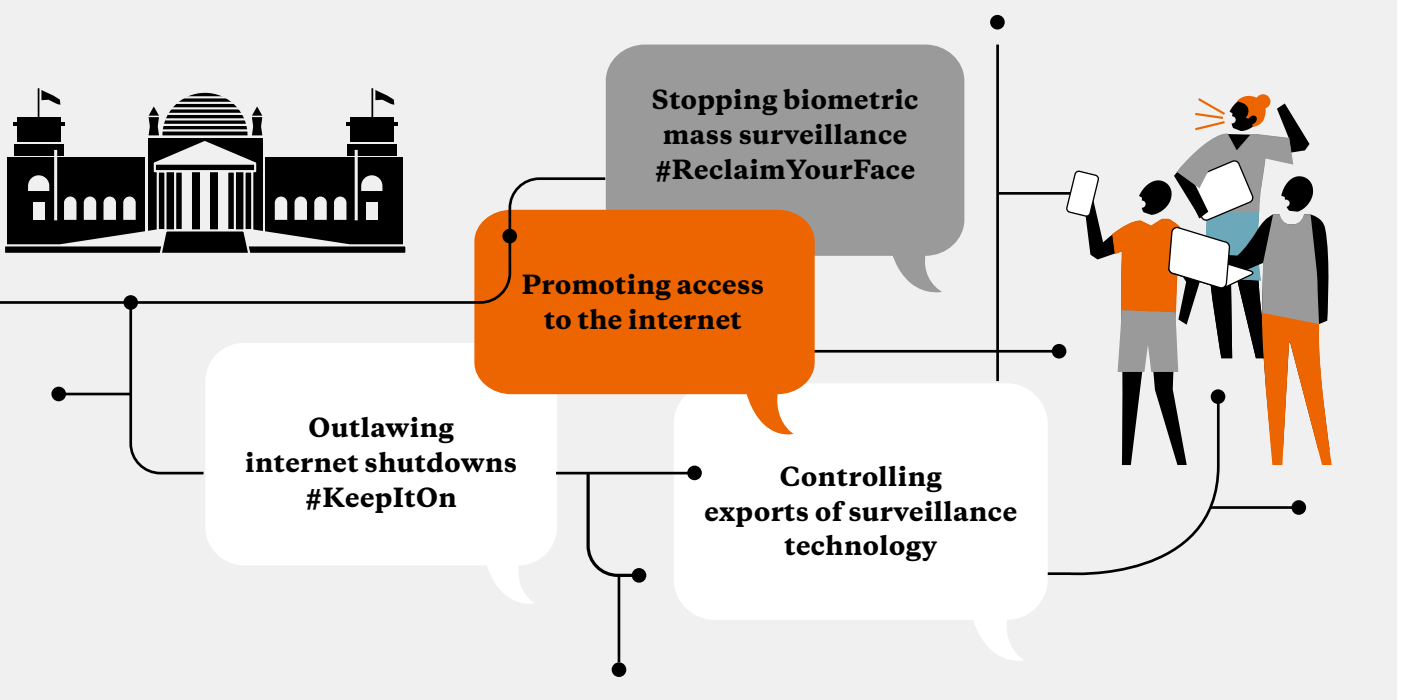
- governments of other countries adopt and implement regulations that protect personal data and the right to **privacy**.
- censorship of individual services and internet shutdowns are **outlawed** as violations of human rights.
- **surveillance-proof** digital infrastructures become the standard worldwide and an international right to encrypted communication is introduced.
- governmental and multilateral development cooperation organisations take a critical look at the promotion of **biometric** databases, which are prone to security vulnerabilities and misuse.
- the promotion of digital projects in the Global South in the context of development cooperation places greater focus on effective consumer and **data protection**.

Donor governments should ensure that...

- access to the internet and the fostering of media and **digital skills** become key components of development cooperation. This should be done, among others, by providing training for journalists and human rights activists in digital self-defence or through fact-checking projects.

EU Member States should strengthen their efforts so that...

- the EU keeps in check by democratic means the power of large social media platforms, including stipulations regarding the quality of content moderation, the ban of behavioural micro-targeting and the **disentangling** of dominant market players.
- the EU institutions classify **face recognition** and other forms of biometric surveillance as high-risk technology under the AI Act and adopt a moratorium on the use of such technology in public spaces.
- the EU leads by example when it comes to regulating communication platforms and the digital public sphere; this includes a clear definition and delimitation of prohibited content, the **obligation** to make available mechanisms of appeal and put-back, no automation of difficult balancing decisions on freedom of expression.



Endnotes

- 1 John Perry Barlow: A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, 08/02/1996, www.eff.org/cyberspace-independence
 - 2 Freedom House: Freedom on the Net 2021, 2021, https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf
 - 3 Nashilongweshipwe Mushaandja: Legt alles still, Analyse und Kritik, 11/11/2020, www.akweb.de/bewegung/shut-it-all-down-namibia-proteste/
 - 4 Reset.pollytix: Hass in Sozialen Medien, 16/07/2021, https://public.reset.tech/documents/210802_Reset_pollytix_Hass_im_Netz.pdf
 - 5 Jana Ballweber/Ingo Dachwitz: Microtargeting. Wie Trump Millionen Schwarze Amerikaner:innen mit gezielter Werbung vom Wählen abhalten wollte, Netzpolitik.org, 01/10/2020, <https://netzpolitik.org/2020/microtargeting-wie-trump-millionen-schwarze-amerikanerinnen-mit-gezielter-werbung-vom-waehlen-abhalten-wollte/>
 - 6 Thomas Rudl: Studie zeigt Schwächen bei Gesetz gegen Hassrede auf, Netzpolitik.org, 24/03/2021, <https://netzpolitik.org/2021/netzwerkdurchsetzungsgesetz-studie-zeigt-schwaechen-bei-gesetz-gegen-hassrede-auf/>
 - 7 Suzanne Maloney/Eliora Katz: Iran and the headscarf protests, The Brookings Institution, 24/01/2019, www.brookings.edu/opinions/iran-and-the-headscarf-protests/
 - 8 Chika Oduah: The revolution will be hashtagged, Rest of the World, 09/12/2020, <https://restofworld.org/2020/the-revolution-will-be-hashtagged/>
 - 9 Access Now: Shattered Dreams and Lost Opportunities. A year in the fight to #KeepItOn, 03.2021, www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf
 - 10 Zeit Online: Human Rights Watch kritisiert türkisches Social-Media-Gesetz, 01/10/2020, www.zeit.de/politik/ausland/2020-10/meinungsfreiheit-tuerkei-social-media-gesetz-kritik
 - 11 David Pierce/Anna Kramer: Here are all the Facebook Papers stories, Protocol Media, 25/10/2021, www.protocol.com/facebook-papers
 - 12 United Nations Human Rights Council: Report of the independent international fact-finding mission on Myanmar, 17/09/2018, www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf
 - 13 Elisa Mackintosh: Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show, Cable News Network, 25/10/2021, <https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html>
 - 14 Shoshana Zuboff: Im Zeitalter des Überwachungskapitalismus, Netzpolitik.org, 12/06/2019, <https://netzpolitik.org/2019/im-zeitalter-des-ueberwachungskapitalismus/>
 - 15 Jeremy Merrill/Will Oremus: Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation, The Washington Post, 26/10/2021, www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/Kontrolle-durch-biometrische-Überwachung
 - 16 World Bank Group: ID4D. G2Px.2021 Annual Report,2021, <http://id4d.worldbank.org>
 - 17 Pam Dixon: A Failure to 'Do no harm' - India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., in: Health and Technology, Volume 7, Issue 4, p. 539-567, 12.2017
 - 18 Human Rights Watch: India: Identification Project Threatens Rights, 13/01/2018, www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights
- ## The surveillance state: Made in Europe
- 19 Privacy International: The Global Surveillance Industry, 16/02/2018, www.privacyinternational.org/explainer/1632/global-surveillance-industry
 - 20 Andre Meister: Wie westliche Firmen den syrischen Überwachungsstaat aufgebaut haben, Netzpolitik.org, 13/12/2016, <https://netzpolitik.org/2016/arabischer-fruehling-als-jagdsaison-wie-westliche-firmen-den-syrischen-ueberwachungsstaat-aufgebaut-haben/>
 - 21 Luisa Podsadny: Illegaler Export von Überwachungssoftware, Gesellschaft für Freiheitsrechte, 04/09/2020, <https://freiheitsrechte.org/export-von-ueberwachungssoftware/>
 - 22 Sebastian Grüner: Trojanerhersteller geht in Insolvenz und wechselt Namen, Golem.de, 12/12/2021, www.golem.de/news/finfisher-trojanerhersteller-geht-in-insolvenz-und-wechselt-namen-2112-161735.html
 - 23 EUR-Lex: Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck (Neufassung), 11/06/2021, 1, <https://eur-lex.europa.eu/legal-content/DE/TXT/?toc=OJ%3AL%3A2021%3A206%3A-TOC&uri=uriserv%3AOJ.L.,2021.206.01.0001.01.DEU>
 - 24 Alexander Fanta: EU verwässert neue Regeln für Überwachungsexporte, Netzpolitik.org, 10/11/2020, <https://netzpolitik.org/2020/dual-use-verordnung-eu-verwaessert-neue-regeln-fuer-ueberwachungsexporte/>

Facebook: A catalyst for conflicts

- 11 David Pierce/Anna Kramer: Here are all the Facebook Papers stories, Protocol Media, 25/10/2021, www.protocol.com/facebook-papers
- 12 United Nations Human Rights Council: Report of the independent international fact-finding mission on Myanmar, 17/09/2018, www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf
- 13 Elisa Mackintosh: Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show, Cable News Network, 25/10/2021, <https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html>
- 14 Shoshana Zuboff: Im Zeitalter des Überwachungskapitalismus, Netzpolitik.org, 12/06/2019, <https://netzpolitik.org/2019/im-zeitalter-des-ueberwachungskapitalismus/>

When machines make decisions about humans

25 Alexander Fanta: Jobcenter-Algorithmus landet vor Höchstgericht, Netzpolitik.org, 28/01/2021, <https://netzpolitik.org/2021/oesterreich-jobcenter-algorithmus-landet-vor-hoehchstgericht/>

26 Jürgen Holl/Günter Kernbeiß/Michael Wagner-Pinter: Das AMS-Arbeitsmarktchancen-Modell. Dokumentation zur Methode, Synthesis Forschung, 10.2018, www.ams-forschungsnetzwerk.at/download-pub/arbeitsmarktchancen_methode.%20dokumentation.pdf

27 Florian Cech et al.: Dem AMS-Algorithmus fehlt der Beipackzettel, Futurezone.at, 03/10/2019, <https://futurezone.at/meinung/dem-ams-algorithmus-fehlt-der-beipackzettel/400636022>

28 Chris Köver: Streit um den AMS-Algorithmus geht in die nächste Runde, Netzpolitik.org, 10/10/2019, <https://netzpolitik.org/2019/streit-um-den-ams-algorithmus-geht-in-die-naechste-runde/>

29 Chris Köver: Mal sehen, was der Computer sagt. Netzpolitik.org, 30/11/2019, <https://netzpolitik.org/2019/mal-sehen-was-der-computer-sagt/>

30 Jürgen Holl/Günter Kernbeiß/Michael Wagner-Pinter: Das AMS-Arbeitsmarktchancen-Modell. Dokumentation zur Methode, Synthesis Forschung, 10.2018, www.ams-forschungsnetzwerk.at/download-pub/arbeitsmarktchancen_methode.%20dokumentation.pdf

31 Ilja Braun: High-Risk Citizens, Algorithm Watch, 04/07/2018, <https://algorithmwatch.org/en/high-risk-citizens/>

32 The Hague court ruling of 05/02/2020, <https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:RBDHA:2020:1878>

33 Koen Vervloesem: How Dutch activists got an invasive fraud detection algorithm banned. Algorithm Watch, 06/04/2020, <https://algorithmwatch.org/en/syri-netherlands-algorithm/#:~:text=How%20Dutch%20activists%20got%20an%20invasive%20fraud%20detection,-public%20organizations%20to%20think%20about%20less%20repressive%20alternatives.>

34 Human Rights Watch: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers, 10/11/2021, www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net

Mexico: Bugged and spied on

35 Forbidden Stories: Carmen Aristegui. Mexico, o. D., <https://forbiddenstories.org/journaliste/carmen-aristegui/>

36 Aristegui Noticias: Filtran contrato que comprueba que PGR compro Pegasus, 29/06/2017, <https://aristeguinioticias.com/editorial/2906/mexico/filtran-contrato-que-comprueba-que-pgr-compro-pegasus/>

37 Oded Yaron: Wanted Mexican Official Linked to NSO Spyware Deal 'Seeks Asylum in Israel', Haaretz, 26/01/2021, www.haaretz.com/israel-news/tech-news/.premium-wanted-mexican-official-linked-to-nso-deal-asks-for-asylum-in-israel-1.9483711

38 John Scott-Railton et al.: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware, The Citizen Lab, 10/07/2017, <https://citizenlab.ca/2017/07/mexico-disappearances-nso/>

39 Nina Lakhani: Fifty people linked to Mexico's president among potential targets of NSO clients, The Guardian, 19/07/2021, www.theguardian.com/news/2021/jul/19/fifty-people-close-mexico-president-amlo-among-potential-targets-nso-clients

40 Dana Priest/Craig Timberg/Souad Mekhennet: Private Israeli spyware sued to hack cellphones of journalists, activists worldwide, The Washington Post, 18/07/2021, www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Indonesia: An all-purpose weapon against criticism

41 Asienhaus: Indonesisches Omnibusgesetz: Solidarität mit den Protesten gegen Sozialabbau und Umweltzerstörung, 10/10/2020, www.asienhaus.de/nc/aktuelles/detail/indonesisches-omnibusgesetz-solidaritaet-mit-den-protesten-gegen-sozialabbau-und-umweltzerstoerung/

42 The EcoSoc Institute: Country Study Indonesia for Brot für die Welt, 2018

43 Westpapua Netzwerk: NGO-Studie belegt wirtschaftliche Interessen hinter illegalen Militäroperationen in Intan Jaya, 26/08/2021, www.westpapuanetz.de/aktuelles/1814-ngo-studie-belegt-wirtschaftliche-interessen-hinter-illegalen-militaeroperationen-in-intan-jaya

44 Stop the Criminalization, Protect the Right to Freedom of Expression in Indonesia!, o. D., www.change.org/p/stop-criminalization-against-human-right-defender-protect-the-right-to-freedom-of-expression-in-indonesia-poldametrojaya-jokowi-dr-moeldoko?utm_source=share_petition&utm_medium=custom_url&recruited_by_id=8782f440-c7c2-11e9-a985-4bb917b5e87f

45 Front Line Defenders: Human rights defenders Egi Primayogha and Miftachul Choir reported to the police on charges of defamation, o.D., www.frontlinedefenders.org/en/case/human-rights-defenders-egi-primayogha-and-miftachul-choir-reported-police-charges-defamation-o

46 Voi: Sit Down On The Case Of Moeldoko's Report To ICW And The Latest Developments In This Case, 11/09/2021, <https://voi.id/en/bernas/84189/sit-down-on-the-case-of-moeldokos-report-to-icw-and-the-latest-developments-in-this-case>

47 Sydney Allen: Indonesian official tries to silence Greenpeace activists, changes course amid criticism, Global Voices, 19/11/2021, <https://globalvoices.org/2021/11/19/indonesian-official-tries-to-silence-greenpeace-activists-changes-course-amid-criticism/>

48 Tri Indah Oktavianti/Budi Sutrisno: New 'virtual police' adds to fears over loss of online civic space, civil freedoms, The Jakarta Post, 19/03/2021, www.thejakartapost.com/news/2021/03/19/new-virtual-police-adds-to-fears-over-loss-of-online-civic-space-civil-freedoms.html

49 Freedom House: Freedom on the net 2021. Indonesia, 2021, <https://freedomhouse.org/country/indonesia/freedom-net/2021> Tanzania: As if someone had pulled the plug

50 Johannes Dietrich: Wahlen in Tansania. Wie ein Oppositioneller tapfer gegen die Regierungspartei antritt, 27/10/2020, www.tagesspiegel.de/politik/wahlen-in-tansania-wie-ein-oppositioneller-tapfer-gegen-die-regierungspartei-antritt/26313844.html

51 Fumbuka Ng'wanakilala: Tanzania orders all unregistered bloggers to take down their sites, Reuters, 11/06/2018, www.reuters.com/article/us-tanzania-internet-idUSKBN1J71W6

52 Dickens Olewe: Tanzania 'using Twitter's copyright policy to silence activists', BBC News, 22/12/2020, www.bbc.com/news/world-africa-55186932

53 Zaina Foundation: Report on internet shutdowns in Tanzania, 09/09/2020, <https://zainafoundationtz.org/report-on-internet-shutdowns-in-tanzania/>

54 Moses Owiny/Sheetal Kumar: Disconnecting from Cyberstability. An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability, The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, 09.2021, <https://cyberstability.org/wp-content/uploads/2021/09/Disconnecting-From-Cyberstability-1.pdf>

55 France 24: Samia Suluhu Hassan sworn in as Tanzania's first female president, 19/03/2021, www.france24.com/en/africa/20210319-samia-suluhu-hassan-sworn-in-as-tanzania-s-first-female-president

56 Alloyce Kimbunga: Auch Mütter dürfen lernen, taz.de, 02/12/2021, <https://taz.de/Maedchenbildung-in-Tansania/!5819663/>

57 Fritz Schaap: Eine Chance für Tansania, Der Spiegel, 27/03/2021, www.spiegel.de/ausland/tansania-samia-suluhu-hassan-ist-eine-chance-fuer-das-land-a-f5fedoeb-eef9-49e8-92fo-80bfeoc9007c

Ukraine: Lies as a weapon

58 Andrew Higgins: Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote, The New York Times, 16/02/2017, www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html

59 Bundeszentrale für politische Bildung: Vor fünf Jahren: Russlands Annexion der Krim, 18/03/2019, www.bpb.de/politik/hintergrund-aktuell/287565/krim-annexion

60 Council on Foreign Relations: Conflict in Ukraine, o. D., www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

61 Viktoria Morasch: „Die meisten Leute sind naiv“, taz.de, 27/07/2015, <https://taz.de/Journalistin-ueber-gefaelschte-Nachrichten/!5215634/>

62 Evolution of Russian Narratives about Ukraine and their export to Ukrainian Media Space, https://drive.google.com/file/d/1x5y7qQjIFWosCHwjzJoDU_5LL29WZZZd/view

63 Erik Albrecht: Evolution of Russia's informational warfare in Ukraine: Interview with Olga Yurkova of StopFake, Deutsche Welle, 02/07/2019, www.dw.com/en/evolution-of-russias-informational-warfare-in-ukraine-interview-with-olga-yurkova-of-stopfake/a-49443961

64 „Hunderttausende. Wie groß ist das Publikum der (pro) russischen Medien in der Ukraine?“, https://texty.org.ua/projects/103537/pro-audytoriyu-prorosijjskyh-media-v-ukrayini/?fbclid=IwAR3sp95Wwum4i9hznZHgUzwDot67Fh8hKJIBsPLtFbvDs3Z_SuvoBJc3CwZc

65 Lennart Maschmeyer: Digitale Desinformation: Erkenntnisse aus der Ukraine, CSS Analysen zur Sicherheitspolitik, no. 278, 02.2021, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse278-DE.pdf>

66 Toni Michel: Graustufen, Konrad-Adenauer-Stiftung, 28/09/2021, www.kas.de/de/web/auslandsinformationen/artikel/detail/-/content/greyscales

