DIGITAL RIGHTS ARE HUMAN RIGHTS

Right to equal enjoyment of human rights

Right to life

Right to be free from slavery

Right to be free from cruel, inhuman or degrading treatment

Right to a fair trial

Right to seek and enjoy asylum

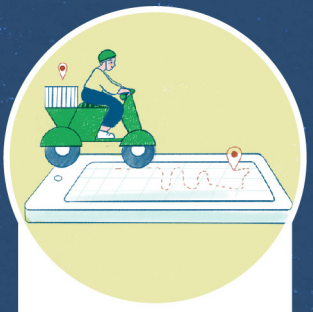
The right to own property

Right to freedom of expression

Right to privacy

Right to assembly and association

Right to political/ public participation



Right to work

Right to health

Right to social security

Right to education

Right to freely participate in cultural life

DFF Digital Freedom Fund

10 DECEMBER 2020

DFF celebrated Human Rights Day 2020 with a count-down that kicked off on 24 November and ran until 10 December. Each day for 16 days, we published a short article illustrating how digital rights are human rights. Each bite size post was written by an esteemed guest author in our network. Collectively, the series shows how the 1948 Universal Declaration of Human Rights remains relevant today, with the digital age presenting many new and urgent challenges to our human rights. The mini-series was inspired by the excellent Privacy Matters project from Privacy International.

List of Contributors

Sarah Chander	European Digital Rights (EDRi)
Rasha Abdul Rahim	Amnesty Tech
Chloe Setter	Global Alliance (WPGA)
Samantha Newbery	University of Salford
Griff Ferris	Fair Trials
Ilia Siatitsa	Privacy International
Lea Beckmann Gesellschaft	Freiheitsrechte (GFF)
Ivan Stepanov	Max Planck Institute for Innovation and Competition
David Kaye	University of California
Ilia Siatitsa	Privacy International
Nora Mbagathi	Open Society Justice Initiative
Jędrzej Niklas	Data Justice Lab
James Farrar	Worker Info Exchange
Lotte Houwing	Bits of Freedom
Jen Persson	defenddigitalme
Adele Vrana and Anasuya Sengupta	Whose Knowledge?

The right to equal enjoyment of human rights

UDHR Articles 1-2

By Sarah Chander, Senior Policy Advisor at European Digital Rights (EDRi).

Articles 1 and 2 of the Universal Declaration of Human Rights tell us that all human beings are equal. Unfortunately, we know that in our world, we are still a long way from realising these rights.

Across the world, discrimination in many forms persists – and new technologies and dynamics in the digital sphere further complicate this issue.

The increased power of global technology companies and social media platforms has had a direct impact on whether we really do have an equal ability to express ourselves and make political statements online, as the recent Zoom censorship case shows.

Further, the increasing and disproportionate experience of abuse and harassment online of many marginalised groups, fuelled by business models which amplify toxic content, are a direct barrier to the equal enjoyment of rights to free expression and assembly.

With the increased resort to automated decision-making in many different areas of public life, discrimination will be heightened, and perhaps new forms created. The flip side to the "innovation" and enhanced "efficiency" of automated technologies is how they, in effect, differentiate, target and experiment on communities at the margins. In the world of work, the roll-out of a range of automated decision-making systems has been shown to enhance and optimise surveillance of people working in already precarious contexts.

In other cases, data-driven tools exacerbate monitoring and profiling of already over-policed communities, including people of colour, migrants, and sex workers.

The testing of new tools, from facial recognition lie detectors to iris scanning and beyond, of people at the borders highlights how we do not all experience these new technologies in empowering ways. Our enjoyment of rights to privacy, freedom of movement, the prohibition on cruel, inhuman or degrading treatment and arbitrary arrest, is always highly differential and unequal, especially with the increased use of digital tools.

These are just some of the ways the digital context brings challenges for the full realisation of our right to equality and equal enjoyment of human rights. They show us that we need to think about digital rights as human rights, and vice-versa.

The right to life

UDHR Articles 3

By Rasha Abdul Rahim, Co-Director (Acting) at Amnesty Tech.

With a global public health emergency and so many human rights crises happening around the world right now, it is easy to overlook other pressing human rights threats on the horizon. One of these threats is the development of autonomous weapons systems, which, once activated, can select, attack, kill and wound humans, all without meaningful human control.

As our lives have stood still during the pandemic, the development of AI military technologies, including fully autonomous weapons, continued to race ahead. In a recent interview, the Head of the UK armed forces said that a military designed for the 2030s could include large numbers of autonomous or remotely controlled robot soldiers.

These rapidly developing weapons systems could not only change the nature of warfare. They also raises serious human rights concerns, undermining the right to life, enshrined in Article 3 of the UDHR, as well as human dignity. Fully autonomous weapons would delegate life and death decisions to machines, programs, and algorithms – crossing an ethical red line, contravening laws designed to protect civilians in warfare and policing operations, and destabilising global security.

Our personal data is also extremely valuable to the tech companies and governments that are quietly building increasingly autonomous weapons. Location data, image data, and our online activities may contribute to the development, production, and fine-tuning of algorithms powering fully autonomous weapons.

Only recently, an investigation by Motherboard uncovered how the U.S. military is buying granular location data of people around the world, harvested from seemingly innocuous apps, such as a Muslim prayer and Quran app (with more than 98 million downloads worldwide), to support Special Operations Forces missions overseas.

This is made all the more concerning in light of the US lethal drone programme, which has relied heavily on signals intelligence to locate and kill "targets", with a disproportionate number of these targets being marginalised groups.

Surveillance and the invasion of our right to privacy may therefore be feeding into the very development of autonomous weapons. Protecting our digital rights today is therefore essential to guarding against tomorrow's threats to our right to life.

Amnesty and partner NGOs in the Campaign to Stop Killer Robots continue to call on states to commence negotiations on a new treaty to pre-emptively ban fully autonomous weapons and retain meaningful control over the use of force.

Amnesty is convinced that a legally binding instrument is the only effective way to address the multiple legal, ethical and security risks posed by autonomous weapons systems. Not only is it achievable, it is a moral and legal imperative.

The right to be free from slavery

UDHR Articles 4

By Chloe Setter, Head of Policy at WePROTECT Global Alliance (WPGA).

When the UDHR was proclaimed by the United Nations General Assembly in Paris in December 1948, the internet was decades away from being invented. The drafters of Article 4 – the right not to be held in slavery or servitude, or made to do forced labour – could not have foreseen the role of future technology in the abuse of generations to come.

Fast forward to 2020, and the internet part of most of our daily lives: there are now over five billion unique mobile users and more than four billion internet users in the world today. Children (those under 18) account for an estimated one in three internet users around the world, whilst evidence suggests that children are going online at increasingly younger ages.

The world wide web is a land of opportunity for young people, offering connectivity, learning and, for many, freedom. Yet the reality is that it also brings with it the threat of harm and child rights abuses. The internet can be used to directly facilitate child sexual exploitation and trafficking, can provide a safe space for offenders to convene and acts as a readily available repository of abusive material.

Yet in this modern era of online-facilitated child sexual abuse and exploitation, the established framework of human rights is as relevant as ever: a child's right to be safe from violence applies in a digital context to the same extent as any other. In this way, states have a responsibility to establish appropriate legal frameworks and strategies to protect children in the digital environment.

In 2019, the United Nations Committee that monitors the Convention on the Rights of the Child launched new guidelines designed to help states better implement the Convention's Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography*. Policies and strategies have had to evolve, just like technology has, in order to deal with the new threats facing children.

Despite international efforts, evidence shows that the "scale, severity and complexity of online child sexual exploitation and abuse is increasing at a faster pace than those aiming to tackle the activity can respond".

Now more than ever, a collective response is needed. It is for this reason that WePROTECT Global Alliance exists: an organisation that unites civil society, law enforcement, governments and businesses in a single movement dedicated to ending online child sexual abuse and exploitation.

As we honour Human Rights Day 2020, we must urgently acknowledge that our ability to protect children from sexual abuse and exploitation both online and offline depends on how globally we can adapt and respond to the ever-changing technological landscape.

The right to be free from torture

UDHR Articles 5

By Samantha Newbery, Reader in International Security at the University of Salford.

The unsettling images brought to mind when torture or cruel, inhuman or degrading treatment or punishment (CIDT) are mentioned tend to involve the victim and perpetrator being together in the same room. These abuses are commonly understood to take place face to face, with perpetrator and victim in close physical proximity to one another, for motives that include revenge, sadism, or interrogations designed to collect intelligence.

Despite these conventional understandings, the proliferation of digital technology in our daily lives has shown that these abuses can happen remotely.

Although definitions of torture and CIDT can be disputed, guidance is available. The United Nations' Convention Against Torture, which came into force in 1987, defines torture first by stating that it is "severe pain or suffering", specifying that this can be physical or, indeed, it can be mental. The key to understanding that torture and CIDT can happen by digital means is that severe mental suffering can constitute torture.

Victims can be reached remotely using social media or emails for instance, on devices they carry with them all day long. Mental suffering, sometimes severe enough to meet the "severity" threshold for torture, can be caused through persistent online harassment that targets the victim on the basis of protected characteristics such as gender or age, online threats, accusations, blackmail, or a combination of these and more.

There may be times when those who are inclined to carry out torture can fulfil this element of the definition through digital means. There are no barriers to the other elements of the definition being met through digital means, namely that it is intentional, is carried out for specific purposes such as punishment, and is carried out by, at the instigation of, or with the consent of, someone acting in an official capacity.

In light of how digitisation has changed how we live, the common understanding of torture, and of CIDT, must undergo a significant shift in order to better prevent these serious violations.

The right to a fair trial

UDHR Articles 6-10

By Griff Ferris, Legal and Policy Officer at Fair Trials.

You wake up to the police breaking down your door. They arrest you for something you haven't done – yet.

A police computer system – an algorithm – created by a profit-driven company, sold to a cash-strapped and under-pressure law enforcement agency, programmed using criminal justice data which reflects the daily racism and inequality found in policing and criminal justice, has analysed information on you and your background – and labelled you as at "high risk" of committing a crime in the future.

After your arrest, another police algorithm analyses more data about you and decides that if released, you are again at "risk" of committing a crime, and shouldn't be released on bail.

You're held in detention awaiting trial for months while the courts deal with the many other offenders arrested over minor issues because they too have been deemed "risky" by a police algorithm.

When you go to trial, you still don't fully understand the reasons for your arrest or the evidence against you, hidden as it is within an algorithm-generated profile and the computer system on which it runs, with justice authorities promising that the system is "neutral", "fair" and "unbiased" – it's just a computer system, after all.

The case is conducted online, via a video-link. You didn't have enough time to speak to your lawyer because the connection kept dropping, and you aren't able to properly communicate with the judge and protest your innocence due to the restrictive online video format. You are not able to appeal or challenge your sentence, because it was based on an algorithm, which cannot be wrong, and anyway, the reasons behind the decision are hidden in the complexities of the system.

This may seem a dystopian daydream, but these technologies and algorithmic tools are increasingly being used by police and in criminal justice systems in Europe and the US. The use of new technologies in policing and criminal justice, both in the process and procedure, has serious implications for fairness, equality and justice.

Predictive and profiling systems completely undermine the presumption of innocence, labelling people and places as "criminal" based on historic information. In doing so, they also re-entrench the existing discrimination and inequality inherent in policing and criminal justice, causing already oppressed and overpoliced communities and groups

to be subjected to the same treatment again and again, as these predictions are used to justify arbitrary arrest and other punishment, such as eviction.

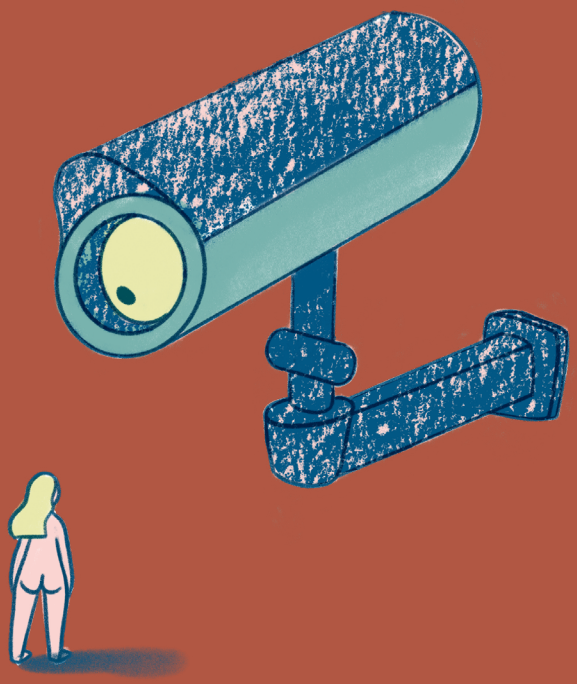
Online courts can certainly assist and support justice, but equally, they can be the cause of injustice, preventing marginalised defendants from being properly heard or assessed, and ultimately preventing fair and public hearings.

We must ensure that any new technologies in the criminal justice system actively help to level the playing field and guarantee equality and fairness for all those involved, and do not merely preserve or exacerbate the structural and institutional racism and inequality that undermines justice worldwide.

No-one should be labelled as a criminal or profiled as a "risk" by an algorithm, and criminal justice should only be served by a completely independent, impartial court or tribunal, under a process which is transparent and accountable, and which can be challenged by any individual subject to it. Any new technologies that do not advance or protect these minimum standards, or that undermine them in any way, have no place in a justice system.

The right to privacy

UDHR Articles 12



By Ilia Siatitsa, Legal Officer at Privacy International.

There is a digital footprint to almost every aspect of our life today: where we go, who we communicate with, what we buy, what we search, read and watch online, what health conditions we have. And governments seek access to these digital footprints, with no regard to whether we are suspected of wrongdoing and, as a result, threatening our autonomy, dignity, and basic democratic values.

Today, governments indiscriminately collect, analyse, and/or generate data on large numbers of people, instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing. This indiscriminate data collection can be described as mass surveillance and directly interferes with our right to privacy.

Privacy is foundational to who we are as human beings, and every day, it helps us define our relationships with the outside world. It gives us space to be ourselves free of judgement and allows us to think freely without discrimination. It gives us the freedom of autonomy, and to live in dignity.

Privacy is also a right that enables our enjoyment of other rights, and interference with our privacy often provides the gateway to the violation of the rest of our rights. Forms of mass surveillance used today by governments directly threaten the very core of our right to privacy, as protected by Article 12 of the Universal Declaration of Human Rights as well as other human rights instruments.

By systematically monitoring people's lives, mass surveillance enables the potential for unchecked state power and control over us. Many might answer that we have "nothing to hide". But knowledge is power, meaning that mass surveillance gives governments unprecedented power over us: they can profile us for our risk of committing crimes, based on factors entirely beyond our control, or use facial recognition to monitor dissent at every demonstration we attend.

Mass surveillance affects some groups in society more than others, from journalists exposing government corruption scandals to minority groups protesting against racial and ethnic discrimination. But nobody is safe from potential abuses of mass surveillance. Governments change, and so do their agendas, meaning that it's simply impossible to know that they won't take a sudden interest in us further down the line.

That's why resisting mass surveillance should be a priority for all of us now, and not when it's already too late.

The right to seek and enjoy asylum

UDHR Articles 14

By Lea Beckmann, human rights lawyer at Gesellschaft für Freiheitsrechte (GFF).

According to Article 14 of the UDHR, everyone has the right to seek and to enjoy asylum. The declaration is regarded as a milestone in international human rights law.

Since then, the right to asylum has been incorporated in countless international treaties and constitutions. Despite this, the right to asylum and the human rights of migrants and refugees have continuously been the centre of violent political attacks.

To shirk their legal responsibilities, countries have built walls, barbed wire fences, armies and border control agencies.

Refugees who make it beyond those obstacles oftentimes find themselves placed in centres and isolated campsites with no access to doctors or legal representation; their children often going without adequate education.

On top of this, governments and state agencies have begun to seriously invade the privacy rights of refugees. They have started to buy, implement, and test invasive technologies on this particularly vulnerable group.

In Europe, the European Union has built up excessive police and migration data bases, which it aims to broaden and interlink. For years, the European Asylum Support Office illegally monitored social media data from refugees to detect and obstruct flight routes – until it was stopped by the EU data protection supervisor. Nonetheless, Frontex, the infamous European Border and Coast Guard Agency, has already publicly announced its interest in continuing such monitoring.

All over the world, governments are analysing smart phone data of migrants and refugees: to confirm flight routes and to verify identity and nationality, but possibly for a variety of other reasons as well. In Germany, GFF is challenging the phone data analysis in court.

Human rights are inseparable and interlinked. The right to asylum is worthless if other human rights of asylum seekers are not respected, and refugees should not have to accept infringements of their privacy rights any more than anyone else.

The right to own property

UDHR Articles 17

By Ivan Stepanov, PhD Researcher at the Max Planck Institute for Innovation and Competition.

The "accept all cookies" button: a recurring and pesky interruption that we quickly dispose of before continuing to use the internet. But clicking this button is not as trivial as it might seem.

Cookies are small pieces of information that we generate while surfing the internet. They are designed to make website use easier for us. However, cookies can store important personal information: our internet habits, our location, our financial details, and even our names.

By clicking the button, we agree to share our data with the website. These data are valuable, as companies can use them to send us targeted advertising or in other ways tailor their services towards us.

Such practices raise a number of concerns, particularly when if you consider just how often we click that button. Firstly, we don't really know what happens to the data. Who sees, controls and uses them?

Secondly, if the data have economic value, what are we getting in return? Is an improved surfing experience really a fair compensation?

One way to resolve these issues is to institute a property right over data. Property rights are the cornerstone of economic empowerment, personal and economic security, and overall prosperity in a society. If we have the right to own and reside in our homes or to enjoy the fruits of our labour, should the same not apply to data?

Data ownership seems appealing, as it provides us with clear legal tools to assume full control over who uses our data and what we get back in return.

However, there are some pitfalls to such a solution. We live in a world of unequal economic, informational and bargaining power. The chances are that when we exchange data, we are interacting with a big corporation, with all its economic and legal might behind it. In this case, how much say do we really have in such interactions? Would our current position really improve if our data were recognised as our property? Would property rights be a fix for these imbalances, or would they just formalise and entrench the status quo?

The solution could be found halfway. In intellectual property, concepts like fair use or compulsory licenses exist precisely to provide some balance in cases of economic and other inequalities. Therefore, if property rights over data are introduced, they should be crafted in a way that properly reflects the person's economic and privacy interests.

As a principle, the person should be guaranteed a way to monitor the use of their data even beyond the point of initial transfer, and the ability to rescind the consent for the use of data when their essential personal interests are at stake. By providing the abilities of oversight and partial control over the data, the economic and legal imbalances previously mentioned could be, to some extent, alleviated.

The right to freedom of expression

UDHR Articles 20

By David Kaye, professor of law at the University of California and former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

I like to imagine the drafters of the Universal Declaration of Human Rights gathered around a virtual conference table, whether it's Zoom or Teams or BlueJeans or some other platform for the pandemic. Eleanor Roosevelt gavels in the meeting.

"René. René! Are you here? Please mute yourself. OK. I suppose I have everyone's consent to the language here in Article 19, yes?" she queries in her authoritative and recognisable cadence.

And indeed she did, for everyone has agreed that the United Nations should declare everyone's right to hold opinions without interference and "to seek, receive and impart information and ideas through any media and regardless of frontiers."

The drafters of this language would be comfortable in their digital environment. They would understand how the rights to browse, download and post map neatly onto seek, receive and impart. They doubted stasis, understanding the reality of an always evolving information space (any media) and a borderless information environment (regardless of frontiers).

Eleanor Roosevelt and her colleagues, however, did not seal off the right to freedom of expression from the other rights the Declaration articulated. They understood that they were crafting a whole, a document promising that everyone should enjoy "all the rights and freedoms" they set forth, "without distinction of any kind" (Article 2). They specified but did not limit the Declaration to oppose discrimination based on "race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

The online platforms of the moment have massive power. Even as they claim to rest on the freedom of expression, a convenient right on which to base a business model of engagement and attention, their owners cannot ignore the possibility that their products may interfere with other rights – they may discriminate, they may interfere.

They may do so unthinkingly, by creating automation tools that are simply unable to make the kinds of distinctions that both promote expression and resist discrimination, hate, incitement. They may do so negligently, by failing to account for the vast experiences of their users and the publics where they operate, or by ignoring the contexts of harassment and violence and misogyny that the words themselves do not reveal to rulemakers thousands of miles away.

As with every Human Rights Day, it's useful to remember that the Declaration was not written merely for its moment in 1948. It was meant to last, to be applied by the powerful in order to promote and guarantee all of its rights and to protect everyone who needs its protection. Today that is a message that must be heard, with a set of rights that must be protected, by governments, by private platforms, and by those who build and govern today's internet.

The right to assembly and association

UDHR Articles 20

By Ilia Siatitsa, Legal Officer at Privacy International.

When we are watched, we are controlled. Nowhere is this more clear than in the application of mass surveillance tools such as facial recognition, gait analysis, and other developing technologies.

If these tools are widely adopted, it becomes more likely that the police will use them to gather information on us when we go to protests and demonstrations, and potentially penalise us for taking part in activities that challenge the actions of the state.

Research has found that people are more likely to avoid places where police are using facial recognition cameras. Here in the UK, Liberty's client, who recently won the world's first case against police use of facial recognition, was scanned at a protest against the arms trade. Protesting is a vital means to express ourselves. Facial recognition in public spaces poses a significant threat to us doing that.

Despite unprecedented restrictions due to the pandemic, this year has seen a rising wave of protests around the world, in large part driven by Black Lives Matter and the movement against societal racism. In many countries this right to protest is under threat, and enhanced surveillance such as facial recognition creates an alarming new element to this.

Our privacy protects us and ensures we can voice dissent as well as speak out against threats to our other rights. We should all be able to attend a protest or political meeting without being tracked by the police, without being caught in a web of surveillance, and without the fear our actions are will be reported to our families, employers or state agencies. Privacy matters because it allows us to speak freely and stand up to power.

The right to political and public participation

UDHR Articles 21

By Nora Mbagathi, Associate Legal Officer at Open Society Justice Initiative.

In today's world, our lives increasingly take place online. While the internet offers endless opportunities, our social media and online lives create equally as many possibilities to exploit the regulation gaps harbored by the digital world. In the election context, such gaps can mean the difference between a freely and fairly elected government, or a win based on a manipulative social media campaign built on lies and falsehoods.

Election campaigns no longer are confined to ads on posters, in newspapers, or on radio and TV. They have found their way onto our personal devices: on our Facebook, Twitter and other social media feeds. Sometimes, they aren't recognisable as political ads, and they can be targeted through algorithms that have studied our profiles and learned our preferences. The Cambridge Analytica scandal and concerns over the misuse of personal information for microtargeting in the UK Brexit referendum are a good example.

In the online world, elections are run and controlled by private companies, often outside the reach of traditional regulatory mechanisms. Sometimes these companies are specifically excluded from regulation. In Bulgaria, for example, the 2019 election code regulates 'media service providers' and defines media services as the "creation and distribution of information and content which are intended for reception by, and which could have a clear impact on, a significant proportion of the general public". But a few lines later, the code states that "the social networks: Facebook, Twitter and other such, and the personal blogs shall not be media services" leaving it up to the companies to decide if and how to regulate targeted or misleading election advertising – something Facebook has in the past declined to do.

So what can we do? We must ensure that existing laws on privacy and equality, as well as sector specific normative frameworks such as electoral codes, also apply in the digital context to hold states accountable. We must also hold corporations to account for their online actions.

We should also ensure collaboration between groups working on issues such as equality and non-discrimination and those with tech expertise, working on issues such as privacy and data protection. Marginalised communities are the first to feel the negative impact of online manipulations. They are scapegoated, targeted for exclusion, or worse.

Free and fair elections form the very baseline of democracy and the rights enshrined in Article 21 of the Universal Declaration on Human Rights, which ensures that people have a say in the governance of the country they live in. In the context of elections, digital rights and regulations are the gateway that make or break access to all human rights.

The right to social security

UDHR Articles 22

By Jędrzej Niklas, postdoctoral researcher at Data Justice Lab.

Coming out of Second World War trauma, the international community announced in the Universal Declaration of Human Rights (UDHR) that everyone should have a right to social security. Back then, it meant that the basic needs of all people must be fulfilled, and societies should do whatever they can to make this possible.

The right to social security is deeply connected to the idea of the welfare state and distributional justice. It includes creating "social safety nets" such as cash transfers and benefits that help communities deal with life's challenges related to unemployment, illness, old age or parenthood.

But today's welfare state is very different. The extensive use of digital technologies has led to significant changes in social security. Algorithms, machine learning and AI are more and more often used to predict social risks, automate eligibility checks, calculate benefits or detect welfare frauds.

Big data and automated cost-effectiveness analyses play a crucial role in creating new policies and making meaningful governmental decisions. From Indian Aadhaar and Dutch SyRi systems to Kenyan biometric schemes and Polish profiling of unemployed tools – countries all around the globe practice digital upgrades of welfare administration.

With the promise of greater efficiency, these new systems often produce flawed results and reduce our ability to challenge and negotiate unfair computerised verdicts. The use of technologies often replicates old hierarchies, power relations, and inequalities. Exclusive online applications and services in welfare administration also mean that those deprived of connectivity or digital skills face exclusion from necessary social support.

These changes often go hand in hand with budget cuts, austerity measures, and punitive welfare policies. They increase the power of technological corporations, strengthening their ability to replace legislators and governments in shaping crucial public decisions.

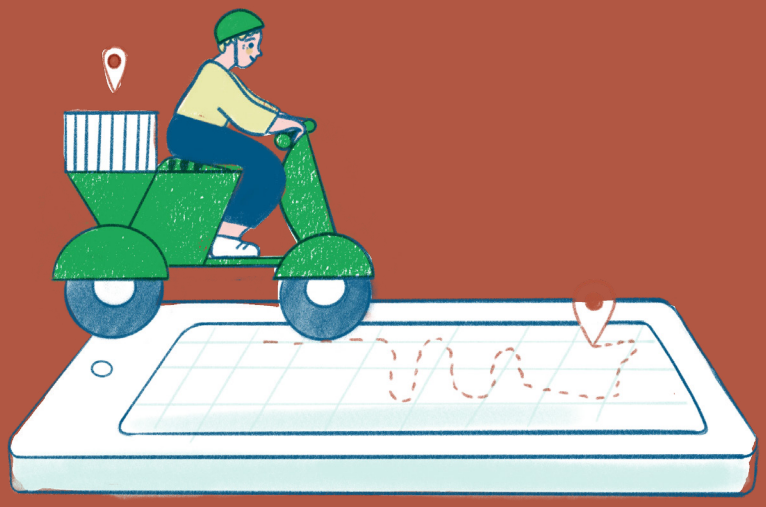
The right to social security creates a framework for understanding and responding to these issues.

Social rights can address some of the issues that mainstream digital rights issues, such as data protection or due process safeguards, neglect. Such issues often focus on procedural aspects, such as consent, better control of information processing, and the possibility to appeal. In contrast, the right to social security can highlight actual harms and losses experienced by people, be it reduction of social benefits or the loss of assistance in the event of unemployment and illness. Through this lens, we can consider the role of automated systems in meeting people's basic needs, or their impact on the adequate distribution of public services.

In this context, social rights go beyond procedural concerns and provide the necessary "material end" – relating to everyday, tangible struggles – when thinking about digital rights and justice.

The right to work

UDHR Articles 23



By James Farrar, Founder of Worker Info Exchange.

The so-called "gig economy" is truly a post-truth phenomenon that purports to have re-invented work through digital means. At the tap of an app, it promises to unleash us from the bonds of a fixed workplace, to offer us limitless flexibility to earn and the freedom of being our own boss.

But the deceit at the heart of this gig economy rhetoric is the idea of a job as merely a "gig" – a take it or leave it side hustle. And it is this caustic casualisation of the idea of employment and attendant rights that is exactly the problem.

The reality of gig work is harsh. It is 90-hour work weeks on less than minimum wage with no rights or protections. It is often hazardous transport work where occupational safety protections are ignored by the employer and where fatigue is an ever-present threat. The gig economy workforce is disproportionately made up of people of colour and migrant workers who too often face assault and abuse on the job. In London, more than half of all minicab drivers have been assaulted at work and 83% have suffered abuse because of their racial or religious identity.

Prospective gig workers find themselves entering a veritable contractual hall of mirrors when they sign up to work for a gig economy app. Misclassification is the name of the game, and app employers use language carefully to create a new reality where no legally enforceable contract of employment exists. You are "on-boarded" as a "partner" for an "economic opportunity to earn" where your performance is "rated by customers" and a violation of "community standards" can eventually see you summarily "deactivated".

Technology is deployed to keep the lie going with management control concealed in algorithms. System-generated profiles determine the quality and quantity of work offered, if any at all. Platform employers have abused their asymmetrical bargaining power over labour to depress wages and mostly refuse to cooperate with trade unions seeking to represent their workers.

Misclassification and algorithmic control has enabled platform employers to side-step legal obligations of employment such as the minimum wage, holiday pay, sick pay, paternity pay and pensions as well as protection from unfair dismissal and the right to freedom from discrimination. Many in precarious employment can never take a holiday or even a short break.

Perhaps the biggest lie of all is that technology has changed work and made employment law and its human rights underpinning obsolete. The opposite is true: never has it been more relevant. In passing the 1875 Employers and Workmen Act, the British parliament recognised that a category of workers might precariously lie between the boundaries of employment and self-employment, just as gig economy workers do today. They understood that such workers are vulnerable to exploitation and deserve protection. And so, we find nothing new under the sun. More than ever before, we must ensure that both technology and the law serve us, not vice versa.

The right to health

UDHR Articles 25

By Lotte Houwing, Policy Advisor at Bits of Freedom.

In the discussion of COVID-19 apps, the right to health has popped up frequently. In most cases, it has arisen alongside the right to privacy. The logic so often went as follows: in the interests of protecting public health, surely we can afford to sacrifice our right to privacy?

However, this doesn't do justice to what privacy means for our society. Privacy protects and enables other essential democratic rights. It secures our possibility to freely develop dissenting opinions, safely figure out who we are, develop our personality, and freely process our faith. But it also plays an essential role in the context of the right to health: Would you be honest with your doctor if you weren't sure that they would be discreet with your personal health information To guarantee safe access to healthcare, privacy is essential.

Privacy has had a rough time during the COVID-19 pandemic. After all, it's hard to argue against the protection of public health. But the wrong frame has been set for the discussion. We need both privacy and health, and they should complement one another.

We should start to reframe the discussion by, firstly, asking ourselves whether technology is always the right solution. We have a tendency to cling to technology, hastily treating it as a magic fix whenever we're overwhelmed by issues we don't quite understand. That's why the prospect of a big and scary pandemic being restrained by technology is so comforting at first glance. Unfortunately, though, this tech-solutionism can often lead us down the wrong path.

We should be very careful with the introduction and normalisation of surveillance infrastructures in our societies, and we should be wary of big data monopolists selling technologies that gather our health data to strengthen their position of power as a solution for our societal problems. We should keep in mind that surveillance is not a medicine, and that a healthy society entails both a right to health and a right to privacy.

The right to education

UDHR Articles 26

By Jen Persson, Director of defenddigitalme.

Everyone has the right to education, but COVID-19 has widened an existing divide in realising this right worldwide.

Long before coronavirus, lost learning hours were routine for children in marginalised communities, with additional educational needs, or living in poverty.

Making digital the default means of delivery has consequences for those who can continue to learn outside the classroom, and for those who cannot.

Under Article 26, education shall be free, at least in the elementary and fundamental stages. If digital infrastructure is a prerequisite to states meeting their obligations, its delivery should be universal, but in practice, the cost of online access falls on families privately. Underfunded schools can have too little hardware to lend, and tell families to buy school-defined hardware.

Deprivation, family choices, or the constraints of physical network and systems' capacity to meet growing demand can mean some children have no access to devices or to the internet.

In addition to physical access to infrastructure, when it comes to education software and services, products can be inaccessible due to design, or staff or pupils' capability.

The rapid shift has also had broader consequences for children, schools, society and state parties.

Schools under pressure to support distance learning fast but without new funding or training often procured "freeware" without due diligence.

Some free products come at the cost of children's human rights, dignity and freedoms. Economic exploitation of their personal data, products with intrusive advertising, invasive behavioural surveillance or discrimination by-design are routine. These consequences reach beyond the school grounds and into private and family life.

Furthermore, proprietary providers can lock in limitations on the control of future services, choices or costs, with long-term implications for the sustainable delivery of state education and the political power of companies in educational reform.

And the imposition of a digital-first approach has undermined parents' right to autonomy under Article 26, who had chosen no-tech or low tech teaching for their children.

Rapid digital adoption has supported learning for some children, but has also created new barriers and unintended consequences.

Data protection frameworks give state parties common approaches to the enforcement of rights and it is timely that the CoE Committee of Convention 108 has adopted new Guidelines on Children's Data Protection in an Education Setting. But we need to look beyond data protection law for children in the digital environment and consider equality, competition and consumer laws.

States around the world must cooperate in and beyond this pandemic to uphold every child's universal right to education among their full range of rights, if we are to promote global human flourishing.

The right to freely participate in cultural life

UDHR Articles 27

By Adele Vrana and Anasuya Sengupta, Co-Directors and Co-Founders of Whose Knowledge?

There are over 7000 spoken languages in the world. Every one of them is foundational to the cultural heritage we offer each other every day. Our languages are a system of being, of doing, of communicating – and, most importantly, of knowing and imagining what we have passed on through generations. It is also a system of knowledge in itself: it is one of the critical ways through which we make sense of our world, how we act in it, and how we explain it to others.

Yet the internet we have today is not multilingual enough to reflect the full depth and breadth of humanity. At best, 7% of the world's languages are captured in published material, and an even smaller fraction of these languages are available online.

We must change this reality through the leadership of our communities who have been historically or currently marginalised by structures of power and privilege – women, people of colour, LGBT*QIA, indigenous communities, and the majority of the global south (Asia, Africa, Latin America, the Caribbean and Pacific Islands).

We often cannot add or access knowledge in our own languages on the internet. Most online knowledge today is created and accessible only through colonial languages from Europe, and mostly, that language is English.

This reinforces and deepens inequalities and invisibilities that already exist offline, and denies all of us the richness and textures of the multiple knowledges and cultures of the world.

This is why it is imperative to use Article 27 of the UDHR to recognise and work towards a multilingual internet, as an essential facet of cultural life.

About the Digital Freedom Fund

The **Digital Freedom Fund** supports strategic litigation to advance digital rights in Europe. With a view to enabling people to exercise their human rights in digital and networked spaces, **DFF** provides financial support for strategic cases, seeks to catalyse collaboration between digital rights activists, and supports capacity building of digital rights litigators. **DFF** also helps connect litigators with pro bono support for their litigation projects. To read more about DFF's work, visit: **www.digitalfreedomfund.org.**

DFF Digital Freedom Fund

E-mail:
info@digitalfreedomfund.org

Postal address
Digital Freedom Fund
P.O. Box 58052
1040 HB Amsterdam
The Netherlands