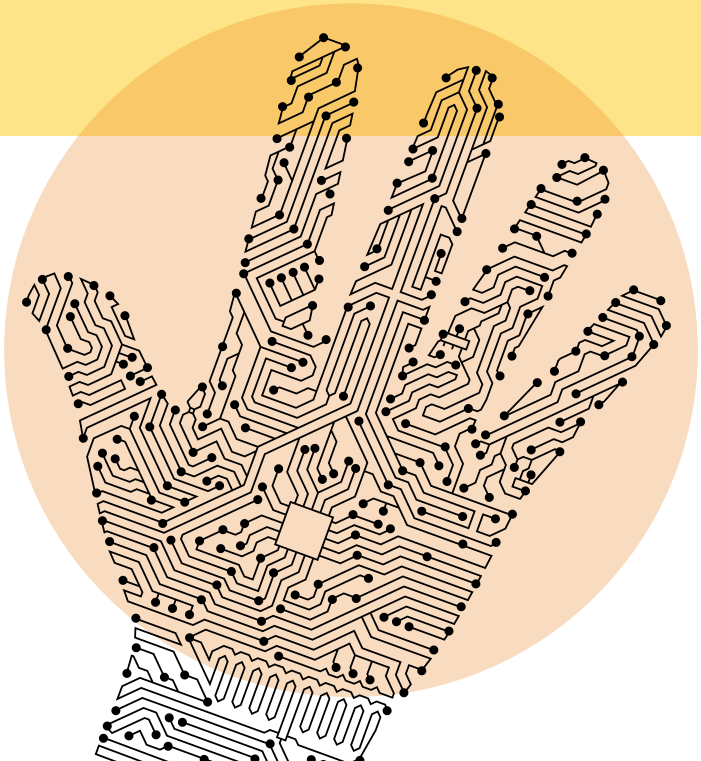
‘Digital human rights’ shaping standards in international cooperation

Guidelines for implementation



giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Contents

Introduction 3

Human rights in the digital space – potential and challenges for advisory services 7

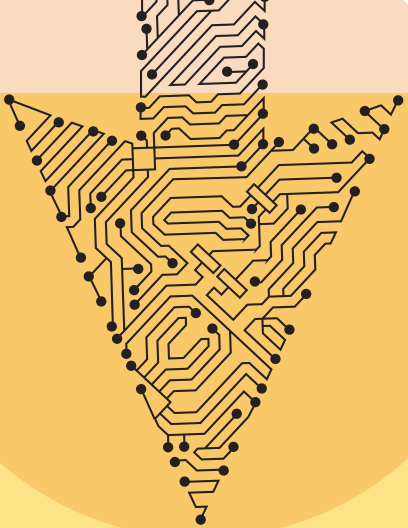
A. Principle of non-discrimination 8
B. Freedom of opinion and expression and right to information 9
C. Freedom of assembly and association, and political participation 10
D. Protection of privacy and personal data 11
E. Education 12
F. Participation in cultural life and cultural diversity 13
G. Protection of children 14
H. Protection of girls' and women's rights 15

Application: Illustrating the logic of the digital rights-based approach using examples 16

Case 1: Attacks on an online platform promoting employment among women 17
Case 2: Accessible communication to target groups 18
Case 3: Conflict contexts and data security 19

Conclusions and outlook 20

Annex: Sources 22



Introduction

Digital rights are a topic relevant to GIZ's advisory services in many respects. A large proportion of our work is now carried out online, and we use a range of digital media for communication and cooperation. Moreover, our state and civil society partners and the local population in our partner countries are increasingly using digital technologies. At the same time, national and transnational companies use digital tools too.

Digital transformation offers considerable potential with regards to human rights: the internet provides new opportunities for people across the globe to assert their rights to freedom of opinion and expression and access to information, freedom of assembly, education, health and work. Human rights institutions have emphasised that human rights apply online too. At the same time, the growing importance of the internet is also leading to an increase in human rights risks: human rights defenders are increasingly affected by online censorship and surveillance and by internet shutdowns. Other dangers include cyber attacks and misuse of data, targeted dissemination of disinformation and hate speech on the internet, cyber violence against women and children and the discriminatory use of algorithms. In addition, unintended negative consequences may occur, if the impacts of using digital technologies are not sufficiently analysed. Due to low standards of protection, poor regulation and a lack of digital skills, internet users in developing countries are particularly affected. Generally speaking, there is a digital divide between north and south, between urban and rural areas and between men and women; in particular, groups that are already marginalised may be left behind to an even greater extent.

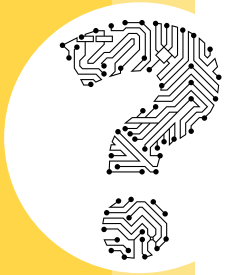
By ratifying human rights conventions, our partner countries and Germany too undertake to respect and fulfil human rights and to prevent third-party violations. However, as digitalisation is proceeding in unprecedented global dimensions and at a fast pace, accountability and responsibility for respecting human rights are more difficult to assign. Along with a shift from national to international level, control and responsibility are also being transferred from the public to the private sector: companies that dominate the market, such as Google, Facebook, Amazon, Apple, Alibaba and Tencent, have a considerable influence over how people navigate the internet and are leaders in developing innovative digital solutions. The basic human rights principle of nation states as duty bearers and individuals as rights holders is thus becoming more complicated. However, there is also a lack of consensus among experts in other contexts on the extent to which human rights also apply to (transnational) companies.

By adopting a human rights-based approach, GIZ has set itself the goal of mainstreaming the protection of human rights in our partner countries as a cross-cutting issue in all sectors and focus areas, which is why it is now vital to address the topic of digital human rights. In addition to questions at micro level, such as 'Which digital (social) media does my target group use to communicate with one another and what consequences does this have?', overarching issues also arise in connection with advisory services to our partners, for instance:

'What consequences should the infringement of human rights by a (trans)national company in the partner country have?'

'What new norms are necessary to protect human rights in the digital age?'

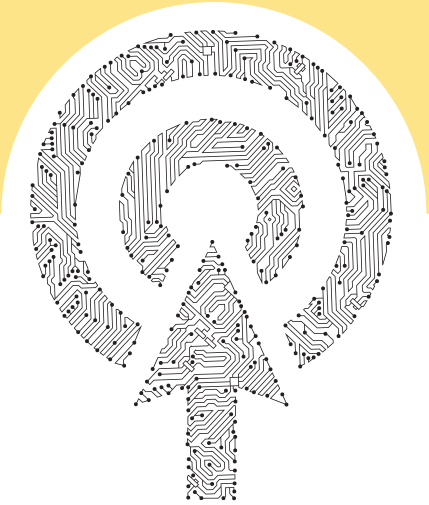
'How does the use of digital technologies impact for example marginalized groups and how can we reduce the negative effects on them, or even use digital approaches to empower them?'



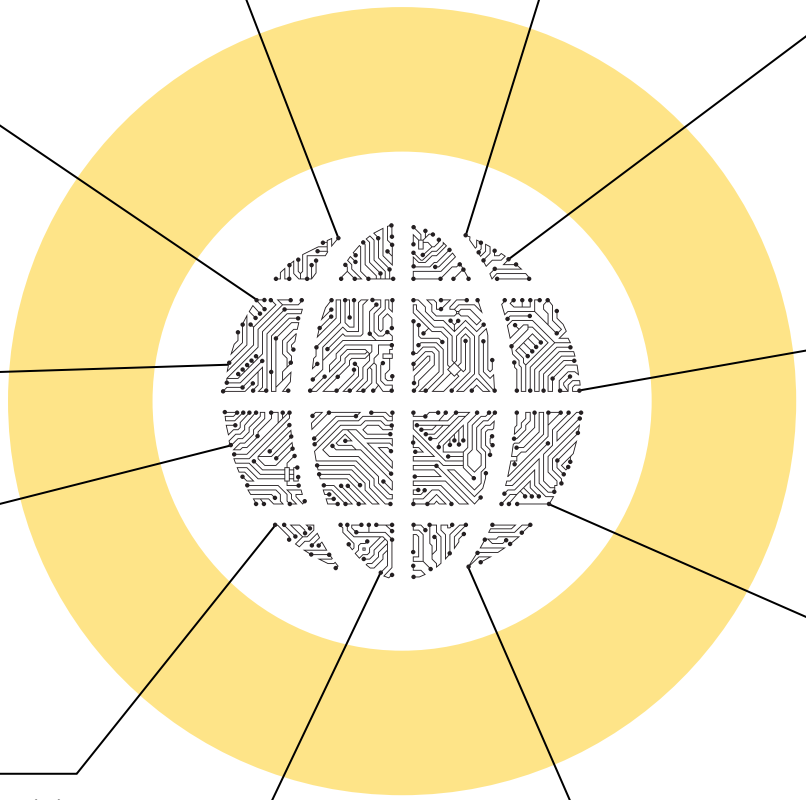
Questions such as these have been discussed since 2003 at events such as the World Summit on the Information Society (WSIS) and as part of the Internet Governance Forum (IGF). Many civil society initiatives have also made key contributions to the debate; large human rights organisations now have their own teams working on digital topics. The UN human rights institutions and the regional human rights systems also address the topic of human rights in the digital age, both through established structures and new thematic mandates. Resolution 20/8 of the UN Human Rights Council from 2012 explicitly stated for the first time that human rights also apply online and is thus regarded as a milestone.

The Principles for Digital Development were drawn up for the field of international cooperation; they contain nine guidelines on developing user-focused and responsible digital solutions and were signed by GIZ in February 2018. As a guide for working with (personal) data in partner countries, GIZ has developed the Responsible Data Guidelines. Human rights in the digital sphere are also playing an increasingly important role in our projects. Despite the important principle of Resolution 20/8 that all existing human rights agreements apply both online and offline, there is to date no internationally binding, explicit legal framework for 'digital rights'. Whether or not specific new agreements and declarations are required, or existing legal instruments can be interpreted accordingly is a matter of some controversy among experts.

These guidelines offer a brief overview of those human rights that are particularly relevant in the digital space, their implementation potential and the challenges involved.



The following diagram shows what a Universal Declaration of Digital Rights might look like:



Right to education & literacy

- Right to digital literacy
- Right to understand the implications of technology

Freedom from discrimination

- Right not to be discriminated

Right to privacy

- Freedom from profiling
- Freedom from bulk surveillance
- Right to use strong encryption
- Right to private digital communications

Right not to be judged by a machine

- Right to request a human override to algorithmic justice
- Right to delete the digital self

Right to challenge the algorithm

- Right to algorithmic transparency

Right to disconnect; Right to remain offline

- Right to live in a faraday cage from time to time
- Right to non-digital access to government services

Political participation

- Freedom from online manipulation
- Right to take part in political decision making online

Right to (digital) self-determination

- Right to control your own data
- Right to object to the use of personal data
- Freedom to move providers
- Right to challenge / opt-out of standard terms and conditions

Right not to be profiled

- Right to get information about your own data
- Right to keep your personal data protected
- Right to opt-out of profiling
- Right to anonymous access & participation

Right to participate in cultural life of community

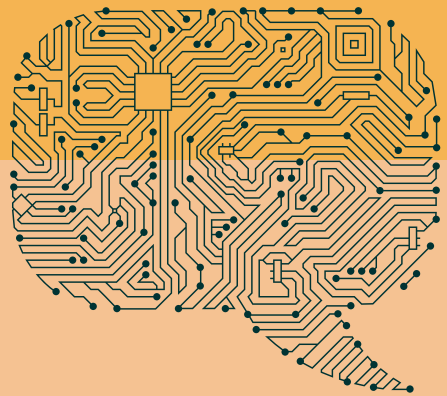
- Right to participate in digital expression
- Freedom to share and receive information
- Right to participate in online communities

Right to personal safety & security

- Right to digital security
- Right to bodily integrity
- Freedom from cyber bullying, trolling & abuse

This illustration is based on the following image: https://digitalfreedomfund.org/the-digital-rights-future-we-want-imagining-a-universal-declaration-of-digital-rights/

Human rights in the digital space – potential and challenges for advisory services



A. Principle of non-discrimination

Right

Right to freedom from discrimination/ principle of non-discrimination

Digital dimension

All discrimination on the internet based on skin colour, sex, language, religion, political or other convictions, national or social origin, property, birth or other status is prohibited.

Conclusion

Internet access must be non-discriminatory and affordable. Nobody shall be excluded from internet access against their will (exception: children, see below). People facing barriers to access, for example in rural areas or due to disabilities, are entitled to specific and needs-driven measures.

Potential offered by compliance with this right

- Facilitates political, social and economic participation for particularly disadvantaged groups, for example by providing a broader range of training measures.
- Creates new forms of access to information, for example on the basic legal aspects of the principle of non-discrimination or state services, such as through online portals.
- Helps to prevent discrimination by enabling people to remain anonymous, for example in online self-help groups.

Challenges

- Not everyone benefits from digitalisation to the same extent: groups that are already disadvantaged often do not have adequate access to the internet and/or can only use it to a limited extent. This is due to factors such as a lack of infrastructure, high costs, cultural obstacles, a lack of accessibility, relevance of content and low levels of digital literacy.
- Particular danger of increasing the digital divide between countries of the global South and North: only a fifth of the population in the least-developed countries use the internet compared with four-fifths in hyper-digitalised countries.
- Frequently inadequate and controversial legal position in connection with companies' commitment to the principle of non-discrimination. Danger that discrimination, for example on Facebook, has no legal consequences.
- Bias of data sets and algorithms in the use of artificial intelligence. Female candidates are thus excluded and put at a disadvantage compared with male candidates in the pre-selection process for job interviews, for example.
- Social media in particular often require photos and other information providing details about a person's skin colour, sex or national origin for instance. This facilitates discrimination. Moreover, slanderous and discriminatory online interactions often remain on the internet permanently.

Human rights sources

International: UDHR 1948 arts. 1, 2, 7; ICCPR 1966 arts. 2, 20; ICESCR 1966 art. 2; ICERD 1965; CEDAW 1979 arts. 1, 2; CRC 1989 art. 2; ICRMW 1990 arts. 1, 7; CRPD 2006 arts. 3–5
Regional: ECHR 1950 arts. 1, 14; CFR 2000 art. 21; ACHR 1969 arts. 1, 24; ACHPR 1981 arts. 2, 19; Arab CHR 2004 arts. 3, 11

B. Freedom of opinion and expression and right to information

Right

Right to freedom of opinion and expression and to information

Digital dimension

Everyone has the right to express their own opinion freely on the internet and to receive and impart information.

Conclusion

The state has an obligation to respect and protect the freedom of expression and information of internet users. Any restriction of this right must therefore not be arbitrary and must have a lawful objective, such as the protection of others (for example to the right to privacy). Restrictions must be publicised and justified and may not last longer than necessary.

Potential offered by compliance with this right

- Easier and faster access to (state) information and platforms for (political) discourse. Particularly people who are difficult to reach in terms of their location can express their opinion and can network and exchange information globally.
- Even controversial opinions can be disseminated, with the aid of encryption technologies, at less personal risk. Human rights defenders in particular are thus better protected.
- Critical information can be updated quickly and can be easily disseminated. This makes it easier for the state to protect its citizens, such as in the event of an earthquake or terrorist attack warning.

Challenges

- The quality of information is difficult to regulate. This means that information and knowledge gaps may easily arise, which may play a critical role, particularly in spreading targeted misinformation (fake news), for example in elections.
- Potential for misuse by criminals and their networks. For example, instructions on building bombs are easier to disseminate through the internet and can be accessed by more people.
- Restrictions of the right to freedom of expression in the event of disproportionate violations of the rights of other individuals lead to two problems:
  - Private infringements: those affected often have no way of seeking legal recourse against hate speech in social media, for example.
  - It is easy for states to use this argument to censor online content or even to restrict access to the internet or shut down the internet completely to prevent people from expressing their opinion, for example members of the opposition. They often cite law and order or public safety as justifications for such measures.
- Danger of surveillance by companies such as Apple, Microsoft, Google and Tencent, facilitated by the concentration of power in the hands of a small number of providers. Here, too, there is a danger of state surveillance and censorship, which in many countries also entails a danger to physical integrity, for example for users who are critical of the government. Too little transparency regarding cooperation between digital companies and states.

Human rights sources

International: UDHR 1948 art. 19; ICCPR 1966 art. 19; CRC 1989 art. 13; ICRMW 1990 art. 13; CRPD 2006 art. 21

Regional: ECHR 1950 art. 10; CFR 2000 art. 11; ACHR 1969 art. 13; ACHPR 1981 art. 9; Arab CHR 2004 arts. 30, 32

C. Freedom of assembly and association, and political participation

Right

Right to freedom of assembly and association; right to political participation

Digital dimension

Everyone has the right to assemble peacefully online (for example in group chats, blogs or social media groups) and to form associations.

Conclusion

States should facilitate and safeguard the use of information and communications technologies (ICTs) for political participation. States should develop and implement strategies to promote e-democracy, e-participation and e-government in democratic processes and debates. Any restrictions of this right must not be arbitrary and must have a lawful objective, for example the protection of others.

Potential offered by compliance with this right

- Stakeholder groups can find each other and share information and ideas more easily, even if they are located far away from each other. Transnational political campaigns can therefore be organised more easily, for example. In addition, it allows for greater diversity.
- Participation in debates within political, social and economic associations, for example by trade unions, is more easily accessible for marginalised groups, such as people in remote rural areas.
- Provides new options for democratic participation and potentially more transparent coordination processes, for instance in the field of e-participation.

Challenges

- The increasing shift of political, social and economic associations and political campaigns onto the internet carries the risk of excluding all those who do not have access to it. This can lead to a distorted, biased picture, for example in political debates on Twitter.
- The use of exclusively digital meeting processes, for example in chats or groups on social media, has been demonstrated to lead in some cases to a process of isolation, in which people shy away from engaging in controversial but often productive debates with others who do not share their own views. This effect is often exacerbated by information tailored to the particular user, for example through personalised newspaper article recommendations on Facebook, and can lead to social or cultural positions becoming entrenched.
- Alongside democratic processes such as e-democracy and e-government, there must always also be parallel analogue processes and opportunities for participation to ensure that no one is excluded.
- Moreover, the digitalisation of political processes opens up the threat of influence being exerted by external parties, leading to data protection, data security and manipulation risks, for example through bots.

Human rights sources

International: UDHR 1948 art. 20; ICCPR 1966 art. 21; ICESCR 1966 art. 8; CRC 1989 art. 15; ICRMW 1990 arts. 26, 40; CRPD 2006 art. 29

Regional: ECHR 1950 art. 11; CFR 2000 art. 12; ACHR 1969 arts. 15, 16; ACHPR 1981 art. 10, 11; Arab CHR 2004 art. 24

D. Protection of privacy and personal data

Right

Right to privacy and the protection of personal data

Digital dimension

Everyone has the right to the protection of their (online) private life, particularly their (online) personal data.

Conclusion

State institutions and private companies are obliged to comply with rules and procedures when processing personal data. This data should only be used if stipulated by law or if the individual concerned has provided explicit consent; information on this matter should be accessible to all. Internet users should be informed if personal data is passed on to third parties. Nobody shall be subjected to general surveillance or wiretapping. In exceptions stipulated by law, for example as part of criminal investigations, an individual's privacy may be restricted with regards to their personal data. The principles of legality, proportionality and the necessity of such restrictions must be adhered to, however.

Potential offered by compliance with this right

- Possibility of anonymity and use of encryption technologies to protect one's own identity. This is often the basis for realising other human rights, such as the right to freedom of opinion and expression.
- Access to digital data offers huge potential for evidence-based work and hence better access to disadvantaged groups and individuals, for example. These groups and individuals must be informed in a transparent way and must give their consent prior to any data processing.

Challenge

- Many users do not know enough about data protection. They are not aware of the amount of data they disclose every day and how this can be used to their disadvantage.
- The concentration of power in the hands of only a few digital providers and platforms makes it more difficult to regulate. Here, too, there is a danger of cooperation between the private sector and states to obtain sensitive data, for example for the state health system.
- Too little transparency in data use, processing and forwarding to third parties by internet providers and online platforms.
- Inadequate enforcement of data protection laws by data protection authorities due to a lack of independence and resources.
- A lack of measures to protect sensitive data. Hackers repeatedly manage to obtain such data unlawfully.
- On the other hand, encrypted messaging services, such as WhatsApp, do not provide any way of reporting problematic content.

Human rights sources

International: UDHR 1948 art. 12; ICCPR 1966 arts. 17, 25; CRC 1989 art. 16; ICRMW 1990 art. 14; CRPD 2006 art. 22

Regional: ECHR 1950 art. 8; CFR 2000 art. 7; ACHR 1969 art. 11; Arab CHR 2004 art. 21

E. Education

Right	Digital dimension	Conclusion	Potential offered by compliance with this right
Right to education	Everyone has the right to equal access to online education and to the development of their media skills in order to be able to assert their own rights and liberties on the internet.	States should facilitate access to information and communications technologies (ICTs) and promote education on using relevant technologies, particularly for children, young people and women. In particular, the dangers and risks of ICTs should be taught, for example how to take a critical approach to online information.	• Easily accessible availability of learning and training resources regardless of the user's location, often in several languages. This includes political education and knowledge about human rights, which can lead to the empowerment of rights holders. • Education portals offer exchange opportunities to enable students across the globe to connect and form networks. • Integrating internet use into curricula in schools and/or universities can ensure increasing and responsible media skills in society.

Challenges

- When preparing online study courses, alternative analogue services should always be designed alongside. Not all people have access to the internet, so there is a danger that the digital gap will increase, for example in areas without an adequate power supply or for lower-income population groups. The right to education shall not be withheld from individuals who can only use analogue education services due to disabilities or who do not wish to use digital education, for instance due to reservations about data protection.
- Taking a critical look at the dangers and risks of the internet is rarely taught to any adequate degree. Teaching sound and comprehensive media skills within state education may entail high costs, which some states find difficult to meet. For example, technical equipment needs to be acquired and teachers need to be trained for the new learning content.
- The quality of non-state education is difficult to regulate. Information and knowledge gaps or even misinformation can thus easily arise – either due to a lack of quality or intentionally due to fake news.

Human rights sources

International: UDHR 1948 art. 26, ICESCR 1966 arts. 13, 14; CEDAW 1979 art. 10; CRC 1989 art. 28; ICRMW 1990 arts. 30, 45; CRPD 2006 art. 24

Regional: ECHR 1950 art. 2 (Protocol 1); CFR 2000 art. 14; ACHPR 1981 art. 17; Arab CHR 2004 arts. 34, 41

F. Participation in cultural life and cultural diversity

Right

Right to participate in the cultural life of a community; right to cultural diversity

Digital dimension

Everyone has the right to participate in the cultural life of a community online too. This requires a certain cultural and linguistic diversity on the internet.

Conclusion

States should ensure that all cultural and linguistic minorities, including indigenous peoples, have equal access to the internet. This includes promoting the (linguistic) diversity of internet content, particularly in the provision of public online services. Free access to publicly owned digital cultural heritage should be guaranteed.

Potential offered by compliance with this right

- Easier access to cultural activities and potential to reach extensive and diverse target groups with these activities, in particular people from lower-income population groups who could otherwise not afford to take part in cultural activities.
- It is easier and less expensive to create and disseminate potentially high-value cultural offerings online, for example through video platforms such as YouTube.
- Cultural diversity, for example in the form of language, is easier to guarantee through free online translation services.

Challenges

- Risk of deepening inequalities: as a result of linguistic or other access barriers, particular cultures are (unintentionally) promoted, while others are not.
- Increase in intercultural tension online, as people often have fewer inhibitions about making provocative statements on the internet. Studies on the role of social media in conflicts indicate that problematic content is usually more popular and is thus also disseminated much faster than content offered by traditional and 'professional' media, among other things due to its strong appeal on an emotional level. As a result, there is also a danger that 'offline' violence may increase, for example between ethnic groups.

Human rights sources

International: UDHR 1948 art. 27; ICCPR 1966 art. 27; ICESCR 1966 art. 15; CEDAW 1979 art. 13; CRC 1989 art. 31; ICRMW 1990 art. 31; CRPD 2006 art. 30

Regional: CFR 2000 art. 22; ACHPR 2000 art. 17; Arab CHR 2004, arts. 25, 42

G. Protection of children

Right

Protection of children's rights

Digital dimension

Every child has the right to the protection of children's interests and needs online too.

Conclusion

Children (and young people) should have access to age-appropriate information, including through (social) media. They should be informed of their rights and, if necessary, should have access to effective legal assistance. With regard to age-inappropriate and harmful content and types of behaviour on the internet, children are entitled to targeted care and support.

Potential offered by compliance with this right

- Easier and more extensive access to appropriate and/or playful information and education about their own (children's) rights.
- Internet services enable the more comprehensive guarantee of other rights of children and young people, such as the right to freedom of assembly (for example in online youth groups) or the right to education (for example using educational computer games).

Callenges

- The internet is full of violent videos, discriminatory comments and pornographic content that are not appropriate for children and young people. Clear legislation and efforts by parents or guardians to teach children how to avoid content such as this are necessary in order to protect children's interests adequately.
- Many children and young people do not have the media skills required to deal with controversial content. They are often unaware of their own rights and cannot properly assess dangers, for example if they use their real name in chatrooms. In addition, they themselves risk violating the rights of others, for example the copyright of photographers if they post a photo on their own Facebook page. Comprehensive lessons to teach media skills are thus needed in order to protect children.
- Children and young people are exposed to the danger of being taken advantage of financially, for example if they buy virtual weapons with real money in computer games, and to cyber bullying and cyber violence. This can also have consequences in the offline world.
- Children without access to the internet, for example from lower-income families, should not be neglected. Greater equality can be achieved by providing internet access at schools; however, this entails costs for schools/the state.

Human rights sources

International: UDHR 1948 art. 25; ICCPR 1966 art. 24; ICESCR 1966 art. 10; CRC 1989; ACRWC 1990; ICRMW 1990 art. 45; CRPD 2006 art. 7

Regional: CFR 2000 art. 24; ACHR 1969 art. 19; ACHPR 1981 art.18; Arab CHR 2004 art. 17

H. Protection of girls' and women's rights

Right

Protection of the rights of women and girls

Digital dimension

Gender equality applies on the internet too. Discrimination on the basis of a person's sex and/or gender is not permissible online either.

Conclusion

States should ensure that women and girls have equal access to the internet and to services to support their digital skills. They should be made aware of their rights and, if necessary, should have access to effective legal assistance.
Steps must be taken to eliminate gender-based discrimination, for example concerning access to information and communications technology (ICT)-based jobs.

Potential offered by compliance with this right

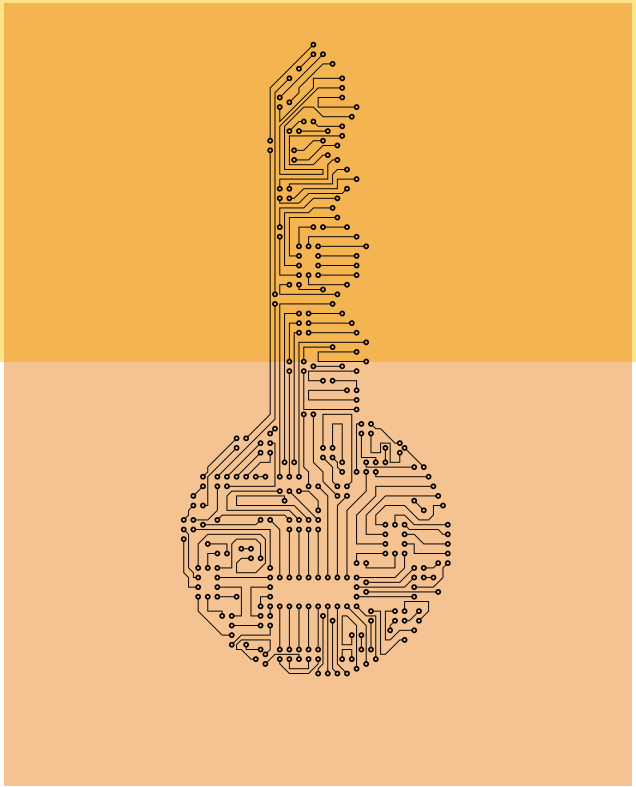
- Online media enable women and girls, and in particular activists, to contact one another and to share information and ideas and forge networks even across large distances.
- It is easier for women and girls to access information about their rights, for example in the event of discrimination, and to access education.
- The internet allows individuals to access help and advice while remaining anonymous, for example in the event of gender-based violence.

Challenges

- Risk of exacerbating existing disadvantages and marginalisation of women and girls. Many women cannot or are not permitted to acquire the necessary digital skills, which leads to or increases the digital gender gap.
- The ICT sector continues to be a male-dominated area. This is often based on discriminatory gender stereotypes and norms and discourages girls and young women from taking ICT courses or completing training, which in turn means that they are unable to benefit from the considerable growth in this sector.
- Women and girls are exposed to a higher risk of hate speech, cyber violence and harassment. Perpetrators often remain anonymous, and gender-based online violence is not uniformly or sufficiently criminalised. Across the world, almost three quarters of all women have already experienced cyber violence.
- Women's rights activists engaged in online activities are particularly often affected and are exposed to mental and physical danger – from both private individuals and the state.
- Disparaging of politicians and journalists, for example by using deep fakes – perfectly faked videos in which people appear to say invented statements or do things that never actually happened in the manner portrayed.
- The apparent objectivity in the use of artificial intelligence and algorithms, for example in pre-selection for job interviews, does not exist. Existing data sets used to teach algorithms often contain gender-specific bias and disadvantage women.

Human rights sources
International: ICCPR art. 3, ICESCR 1966 art. 3; CEDAW 1979; CRPD 2006 art. 6
Regional: CFR 2000 art. 23; ACHPR 1981 art. 18; Arab CHR 2004 arts. 3, 34

Application: Illustrating the logic of the digital rights-based approach using examples



Case 1:
Attacks on an online platform promoting employment among women

Situation: GIZ advises on employment promotion in a partner country with the aim of promoting economic participation and employment among women. In cooperation with a women's rights organisation and the counterpart ministry in the country, an online platform is set up through which women across the country can obtain legal and practical advice on all aspects relating to family and career. The platform is open and free of charge in order to reach as many women and girls as possible. In the event of disputes within the family, the platform also offers women initial advice. The names of the contact persons are given on the platform to ensure direct and fast contact and to create trust. In their mailbox and on their private Facebook accounts, the women working for the NGO, most of them young, have been receiving messages full of sexual comments or even rape threats every day since the platform went live. The police have suggested to them that dealing with bullying is part of their job. As the female staff were worried for their own safety and that of their families, the organisation decided to discontinue cooperation with the partner ministry and GIZ and to no longer provide its services on the online platform. The online platform was then closed.

Advisory approach: Women and girls are entitled to a life without discrimination and violence. They also have the right to express their opinion freely, both offline and online, and to network with other people online and offline. The online platform created the opportunity to provide many women with advice that meets their needs quickly and individually on questions about their economic participation. However, violent threats and hate comments against women who advocate for human rights on the internet often lead to them reducing their activities. This self-censorship restricts their right to participate in public life and to express themselves without restriction online. This is particularly true of young women and of women from disadvantaged population groups. In order to ensure that female activists are protected, state partners should be advised on fulfilling their responsibility to protect personal rights and human rights in the digital world – particularly the rights to freedom from discrimination and freedom of opinion and expression. They must take women's complaints seriously and initiate specific measures to help prevent this abuse from happening on the internet. State partner institutions should stipulate clearly what is classified as violence and misconduct and how they deal with complaints. Specific measures to protect against violations must always be developed with the particular context in mind. Consequently, in the present case, when setting up the online platform, care could be taken to protect the identity of the people involved and to not reveal their real names. At the same time, certain requirements for access could mean that only the target group can use the online platform. Accompanying education and awareness-raising measures could also promote acceptance in the population for the economic empowerment of women.

Case 2:
Accessible communication to target groups

Situation I: The Ministry of Foreign Affairs in another partner country is increasingly using digital communication channels to inform citizens about its duties and services to reach more people. Although more than 40 different indigenous population groups live in the country and more than 60 local languages are spoken, the information on the website is only available in English and access to the information is not barrier-free. The online form to apply for a passport is only available in English too.

Situation II: The citizen dialogue team at the German Federal Ministry for Economic Affairs and Energy (BMWi) recently wrote a post on Twitter that was difficult to understand; the (translated) wording was as follows: 'The aim of BMWi in recent months was to avoid predetermining a (negative) result through a level of ambition that was too high and unrealistic and through hidden pitfalls and to enable the result of monitoring to be meaningful. Citizen dialogue team.'

Situation III: Due to the COVID-19 pandemic and the associated measures (e.g. lockdowns), various in-person formats to promote social cohesion and to prevent violence in the context of displacement cannot be implemented. A project in a partner country therefore develops a digital tool that can be used to raise awareness among the target group about topics connected with the prevention of violence and peacebuilding. As most of the people in the target group do not own a smartphone and do not have access to the internet, a simple SMS tool is developed. In addition, dialogue formats are implemented with members of the local communities and the administrations online using MS Teams. Here, too, the digital skills of the participants are taken into account when choosing the tool.

Approach: Whether in our partner countries or in Germany: communication by the state is only free of discrimination if the different contexts and backgrounds of all people are taken into account. Discrimination-free access to information and public debate is particularly important to ensure that everyone can form a (political) opinion and make informed decisions. State services must also not have any access barriers and should be designed in a target group-sensitive way. An important condition in this context is met by developing multilingual and barrier-free information and communication services, for example for indigenous peoples or people with disabilities. People who cannot read must also be able to access and understand information. Information can therefore be made available in both written and spoken form. Simple and easy language helps make even complex content understandable for everyone. To avoid increasing the digital gap and disadvantaging people without access to the internet, both digital and analogue communication channels should be used. When cooperating with mobile communications providers, privacy and data security must be guaranteed. Particularly in the context of the COVID-19 pandemic, digital approaches offer a huge potential in terms of contin-

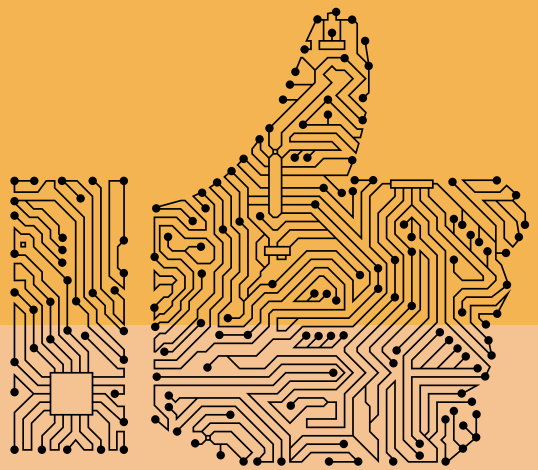
uing to reach target groups and implementing activities. However, the possibilities (infrastructure, digital skills, etc.) available to vulnerable target groups, such as refugees or internally displaced persons, but also to older people or poorer population groups, must be taken into account in order to comply with the principle of non-discrimination.

Case 3:
Conflict contexts and data security

Situation: As part of a project in the special initiative on displacement, registration of internally displaced persons is to be improved in a partner country in order to obtain an overview of the number of people and their needs. Many of them live in host communities rather than camps, which is why they have often not been systematically recorded to date. In order to rectify this situation, internally displaced persons are to be registered by means of a digital tool, for example using blockchain technology. However, this might lead to various unintended results that could have a negative impact on the target group. Internally displaced persons are often seen by staff of the local administration not as victims of a violent conflict but as collaborators of local non-state armed groups. The data gathered using the tool would be stored on the server of a state authority. There would thus be a danger that staff might be able to access personal data and that internally displaced persons might be discriminated against or even endangered. Due to these risks, after careful consideration, GIZ ultimately decided not to implement the digitalisation project.

Advisory approach: Particularly in the context of a conflict, in autocratic states and when dealing with especially vulnerable target groups, it is vital to ensure that protection of privacy and data security is guaranteed. On the one hand, better data on internally displaced persons offers huge potential to improve services, particularly for vulnerable groups who have not received much attention so far. On the other hand, data might be misused for unintended purposes, particularly in fragile, conflict-ridden and authoritarian states. In order to rule out discrimination or even danger to life and limb, relevant countermeasures should be taken. If technical or administrative solutions cannot be found, it is advisable to refrain from digitalised data collection (see also Responsible Data Guidelines). However, GIZ can also examine whether databases or platforms with sensitive data can be hosted in a safe third country to prevent unauthorised access by local conflict actors, including state authorities.

Conclusions and outlook



Basic principles such as 'do no harm' and 'leave no one behind' (LNOB) also apply to digital solutions. In view of the rapid and particularly far-reaching developments, there are particular challenges in assessing impacts and in human rights-based project design. Knowledge on the impact of new technologies on human rights and gender equality needs to be developed continuously, as should the specialized networks on these topics. Offline advisory services adapted to local contexts, for example on digital literacy, the creation of human rights-based regulatory frameworks and capacity building among human rights defenders and civil society actors, will remain relevant.

Digital exchange platforms and dialogue events offer great potential for carrying out activities, even in the context of remote management (inaccessible conflict regions or during epidemics/pandemics). It also allows people to take part who are unable to travel or who have family commitments. This safeguards the right to assembly and association and the right to (political) participation. At the same time, the protection of privacy and data security must be guaranteed in this context too, so that individuals are not exposed to risk or jeopardised if they make critical comments in these forums. A clear policy and relevant sanctions are also required for hate speech and sexual harassment. This also has implications for the work and costs involved (for example for developing policies and content or moderating forums), which need to be taken into account during planning.

'Technology is neither good nor bad; nor is it neutral.' (Melvin Kranzberg, U.S. technological historian)

Annex: Sources

Selection of sources on the topic of digital human rights:

- Resolution 20/8 of the UN Human Rights Council on 'The promotion, protection and enjoyment of human rights on the Internet'
- German Bundestag (2018) Documentation WD 2 – 3000 – 107/18 'Menschenrechte im Digitalen Zeitalter' ('Human rights in the digital age') (in German)
- Report by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, focusing on 'The rights to freedom of peaceful assembly and of association: The Digital Age'
- Principles for Digital Development (signed by GIZ in 2018)
- GIZ (2018) Responsible Data Guidelines (focusing on the protection of privacy and the responsible use of digital data)
- Council of Europe Commissioner for Human Rights (2018): Human Rights Comment "Safeguarding human rights in the era of artificial intelligence"

Websites of particularly relevant mandate holders:

- Special Rapporteur on the promotion and protection of freedom of opinion and expression (incl. reports on online hate speech, content moderation, artificial intelligence, digital surveillance, encryption, the role of the private sector, etc.)
- Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights
- Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights
- Thematic section on Freedom of Expression of the Council of Europe

NGOs und think tanks:

AccessNow
Tactical Tech
The Engine Room
Digital Freedom Fund
Electronic Frontier Foundation
Human Rights Watch Technology and Rights section
Amnesty International Freedom of Expression section

Published by: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Registered offices Bonn and Eschborn, Germany
Friedrich-Ebert-Allee 32 + 36
53113 Bonn
T +49 228 44 60 - 0
F +49 228 44 60 - 17 66

Dag-Hammarskjöld-Weg 1 – 5
65760 Eschborn
T +49 61 96 79 – 0
F +49 61 96 79 - 11 1

www.giz.de/en

Authors/Editors: Franziska Bertz, Rhea Franke, Dr Friso Hecker, Dr Elisabeth Leiss and Alexandra Steinebach, Competence Center Rule of Law, Human Rights, Gender, Security with contributions from Anna Scherer and Johanna Sztucki, Competence Center Peace and Emergency Aid

Design / Layout: Bettina Riedel, briedel64@gmx.de

Illustrations: istock

Translation: Internationaler Sprachendienst der GIZ

Contact:
Sectoral Department (FMB)
Competence Center Rule of Law, Human Rights, Gender, Security
Rhea Franke (rhea.franke@giz.de)

Eschborn 2020