RECOMMENDATIONS

- *Mainstream human rights for all into the development and dissemination of technologies, with a particular focus on the barriers that minorities and indigenous peoples face.* This requires a more holistic examination of technologies that assesses their social, economic and political implications as well as their technical capabilities. Accessibility, affordability, appropriateness and availability should be a central part of their function, measured through clear data on the proportion of minority and indigenous community members able to use these technologies freely in ways that meet needs or address concerns. This is especially important for technologies involved in public service delivery, such as the increasing use of smartphones in educational settings and health care: in these circumstances, lack of access could exacerbate exclusion further.

- *Focus on improving minority and indigenous inclusion, not only as end users of technologies, but also upstream in their design and production.* While it is vital to ensure that minority and indigenous community members are able to access available technologies, it is also important that their role extends beyond this to equitable participation in the production of these technologies at every stage of their development. At the moment, minority and indigenous representation in key sectors such as computer programming and software engineering remains very low. As a result, many members of these communities continue to be excluded from the economic benefits of employment in these fields, thereby entrenching existing power imbalances in society.

- *Promote a diverse and expansive approach to technology development that enables the creation of a wide range of products suitable for different communities.* At present, there is a tendency for smart technologies, web platforms and other widely used tools to be monolingual, mono-script and designed around the needs, values and assumptions of the dominant majority, particularly its male members. This is unlikely to change until members of minorities, indigenous peoples and other marginalized groups, including women and people with disabilities, are able to contribute equitably to these processes. Among other measures, this means ensuring products are available in minority languages, including sign languages, and are culturally appropriate for different communities.

- *Conduct human rights impact assessments as a necessary first step whenever digital technologies are being considered for adoption by public authorities.* These impact assessments must include a focus on inclusion as well as non-discrimination. They should be carried out with the meaningful participation of all affected minorities and indigenous peoples, including representatives of marginalized groups within these communities, in their design and implementation.

This is particularly crucial when AI and predictive algorithms are being adopted for public decision-making. In such cases, algorithmic impact assessments should be conducted ahead of any introduction of an automated decision system. These should be updated when systems are upgraded, and the results made publicly available. All appropriate measures must be taken to mitigate risks identified through the impact assessments. With governments increasingly outsourcing technological development and delivery to companies and research institutions, it is vital that they are not able to outsource their human rights obligations as well.

- *Ensure accountability and independent oversight.* Public authorities should only use digital systems that are auditable, in order to ensure that they are available for independent oversight. Legislation and administrative guidelines should be put into place making this a requirement in public tendering processes for the use of digital technologies.

- *Scrutinize the use of AI and automation in decision-making, with a focus on ensuring transparency and non-discrimination.* This is especially important in areas such as suspect identification, prison sentencing, access to essential services, migration management and other issues of public decision-making where the human costs are high and the potential for bias, given past trends, is markedly high. Crucially, automated processes and their assumed objectivity should always be questioned, with the same review and accountability mechanisms that would accompany a human-led decision. Given the widespread involvement of private companies and academic institutions in the development of these technologies, it is also important that clear requirements are established to ensure good conduct, including ensuring that data on their impacts is transparent and publicly available. If companies or public agencies use an automated recruitment or service delivery system that replicates inequalities around ethnicity, religion, gender or disability as a result of their algorithms, then the outcome is still discriminatory and should be penalized as such.

- *Establish and enforce clear protocols on the collection, retention and use of personal data by governments, companies and other actors.* Though privacy and freedom of movement are universal human rights concerns, the increasing use of biometric data, facial recognition and online monitoring to target particular groups has very direct relevance for minorities and indigenous peoples. While the Chinese government's intrusive surveillance of millions of Uyghur Muslims in the name of security is an especially egregious example, similar patterns of discriminatory policing are emerging elsewhere. Even seemingly innocuous interventions justified by efficiency or cost effectiveness, such as the growing trend for 'smart' development in cities, pose significant concerns for members of communities with a long history of discrimination against them. These issues have become even more pressing since the outbreak of the Covid-19 pandemic, as many technologies such as ‘track and trace’ applications could raise the danger of privacy intrusions if misused by governments or corporations.

- *Enshrine universal access to the internet as a right for all citizens, with a positive emphasis on accessibility and safety rather than censorship and surveillance.* The importance of the internet as a source of information, social connections, employment opportunities and public services means that lack of provision can directly affect the ability to access many basic rights. Governments therefore have a responsibility to ensure that all their citizens have ready and secure access to the internet, with a particular emphasis on poor, remote or marginalized communities currently excluded from its benefits. Governments need to increase steps to ensure that online spaces and platforms are used constructively and are not exploited to mobilize hate against any section of their community, and in particular are not used to organize or incite violence linked to racism, religious tensions, gender or any other protected characteristic. Along with rights follow responsibilities, and educational services need to ensure that public knowledge about fake news, hate speech and its effects keeps pace with levels of access and usage. While this should include the creation and enforcement of anti-hate speech provisions in national legislation, particularly in relation to incitement to violence, governments should not use hate speech as a pretext to target activists and political opposition groups to silence dissent. Nor should they use the existence of hate speech to access private information stored or shared online. Regulatory authorities applying such laws must be demonstrably independent and accountable.

- *Abstain from imposing blanket internet shutdowns in the name of security, especially for protracted periods.* Human rights law allows limitations to freedom of information in certain very limited circumstances. There have been multiple instances of internet shutdowns where the test to justify state intervention in freedom of speech (and an internet shutdown) has not been met. Any internet shutdown should be strictly limited to exceptional circumstances where there is strong evidence of imminent mass killings and where the internet is clearly playing an inciting role in those killings or attacks. Outside of these very narrowly defined exceptions, internet shutdowns are in breach of international standards on freedom of expression. These measures, being indiscriminate by nature, can effectively amount to a form of collective punishment and may increase impunity and insecurity by preventing the documentation and reporting of human rights abuses.

Businesses

- *Recognize that they have a responsibility to respect human rights and apply the UN Guiding Principles on Business and Human Rights.* ICT companies must act with due diligence and avoid the infringement of the rights of their users and the wider public. Human rights impact assessments must be undertaken at all stages, beginning at the conceptualization, design and testing stages of new technologies, including the algorithms and data sets that will be incorporated in them. Potentially discriminatory outcomes should be identified as much as possible in advance, with all necessary steps taken to prevent and mitigate them.

- *Establish clear and transparent protocols for content posted on social media platforms, especially concerning hate speech.* These protocols should be drawn up in close consultation with representatives of minority and indigenous communities and other marginalized groups that may be targeted or otherwise affected. These protocols should also be specific and predictable, clearly informing users in advance, as well as assessed against the legality, necessity and proportionality principles set out in international standards concerning freedom of expression. Content moderation must take into account local contexts, including cultural and linguistic nuances, while remaining coherent and foreseeable. External complaints mechanisms should be established whereby users and others can draw attention to posts that contain hate speech, incite violence or are otherwise in breach of these protocols. Such complaints mechanisms should respond to and address complaints as quickly as possible. Content containing hate speech should be taken down within 24 hours. Platforms should be required to publish the average time between a report of hateful or dangerous speech and its removal at regular intervals, as well as statistics on the proportion of complaints that are upheld and denied.