SOUTHERN ALLIANCE FOR THE GLOBAL DIGITAL COMPACT: CONTRIBUTION FOR THE PROMOTION OF DIGITAL HUMAN RIGHTS

DESCRIPTION

In the beginning of 2023, a new alliance was formed by five NGOs - Data Privacy Brasil (Brazil), Aapti Institute (India), InternetBolivia Foundation (Bolivia), KICTANet (Kenya), and Paradigm Initiative (PIN) (Nigeria). Our main focus is the Global Digital Compact, which seeks to promote and protect human rights in the digital age. We believe that the digital landscape is rapidly evolving and that it is necessary to establish guidelines to ensure that technological advancements are used to benefit society as a whole.

As a group, we are committed to fostering a Global South conversation. We recognize that many of the issues related to digital rights and privacy are unique to countries in the Global South and require a specific approach. Our alliance is dedicated to advocating for policies and regulations that take into account the realities of the Global South and the unique challenges faced by people in these regions. Therefore, we are an alliance united by the vision of advancing digital rights protections for all, within the Global South.

After a few years involved in networks of NGOs from the Global South, we began more systematic efforts for joint advocacy in international spaces. Through these involvements, we engaged in two strategic meetings, in August 2022 and in November 2022, in which we, as a collective, discussed the challenges faced by the Global South in the digital and human rights agenda. We exchanged ideas and information about the most pressing issues faced by our respective communities and developed a plan of action to address them. We are excited about the potential impact that this Southern Alliance can have and are committed to working together to ensure that human rights are respected in the digital age. Each entity brought its expertise in one of the areas of the Compact. The members are from different countries, with representation from the Latin American, Asian and African continents.

THE PROCESS

The Alliance held 3 online meetings, in addition to exchanging asynchronous emails, to work together on this contribution. At the first meeting, each entity opted for an area of greater expertise, to be the responsible rapporteur. Then, each entity chose to be the reviewer of another area, different from the first chosen to report. Deadlines were agreed for the delivery and revision of the texts, to be later collected and submitted in this contribution. It is noteworthy that each area was reported and reviewed by different continents, which brings a true representation of the Global South to the digital cooperation agenda and commitment to the Sustainable Development Goals.

ABOUT THE AUTHORS

DataPrivacyBR
Research

http://dataprivacy.org.br

Data Privacy Brasil Research Association is a non-profit civil society organization that promotes the protection of personal data and other fundamental rights in the face of the emergence of new technologies, social inequalities, and power asymmetries. We work to promote a culture of data protection and to ensure that digital rights are fundamental rights for everyone, carrying out research that is open to the public, guided by a strong social commitment and with ethical funding.

aapti institute

http://aapti.in

Aapti Institute is a public research organisation based in India that works at the intersection of technology and society to build solutions that enhance societal impact, justice and equity. Our work spans many aspects of our digital lives - we conduct research, develop solutions, and embed them in policy and within organisations to achieve scale.

iNTERNET BOLIVIA.ORG

http://Internetbolivia.org

InternetBolivia Foundation is a non-profit organization that was born in the year 2018 from the impulse of a group of activists working at various intersections between technology and the common good. Its mission is to contribute to the promotion of human rights in digital environments and digital inclusion in Bolivia through research, dialogue and public policy discussion.

Paradigm Initiative (PIN) connects underserved young Africans with digital opportunities and ensures the protection of digital rights. Across regional offices in Kenya, Nigeria, Senegal, Zambia, Zimbabwe, Cameroon, the Democratic Republic of Congo (DRC), and beyond, PIN impacts youth with improved livelihoods through digital inclusion and digital rights programs.

KICTANet is a multi-stakeholder Think Tank for ICT policy and regulation. The Think Tank is a catalyst for reform in the Information and Communication Technology sector. Its work is guided by four pillars of Policy Advocacy, Capacity Building, Research, and Stakeholder Engagement. KICTANet's mission is to promote an enabling environment in the ICT sector that is robust, open, accessible, and rights-based through multistakeholder approaches.

CONNECT ALL PEOPLE

Core Principles

- Internet access enables the exercise of several Human Rights such as Freedom of Expression, Access to Information, and Access to Education, that allow a beneficial participation in the digital society.

- Nearly half of the world's population has no Internet access and as a result cannot fully enjoy their Human Rights. We must uphold every person's right to connect to the Internet. and participate in the digital world in an equal way, with meaningful connectivity.

- Connectivity and Digital Inclusion must be looked at as a single, related issue and not two separate issues. Following the reflections of the Alliance for Affordable Internet (A4AI), "look at the users on this network, not just the network's coverage".

- Meaningful Internet access refers to affordability, being able to use the Internet openly and unfiltered, on a daily basis, with an appropriate device, including enough data (when it is a mobile connection), with minimum technical requirements related to speed and latency.

- Ensure that citizens have digital skills to enjoy the digital space, digital security to avoid risks, and without suffering any discrimination based on gender, race, ethnicity, geography, age, or any other discriminating factor.

- Structural conditions for digital inequality, such as discriminatory colonial structures, economic conditions, and cultural norms must be acknowledged and addressed. Vulnerable social groups include women and girls, LGBTIQ+, indigenous peoples, seniors, and people with disabilities. Intersectionalities, being part of two or more vulnerable groups, serve to worsen inequalities.

- Violent online actions against vulnerable groups specified above, such as hate speech, online harassment, online sexual exploitation, diverse types of frauds and cybercrime are rampant and must be addressed on priority.

- There are different models for provision of Internet: private, public and community based and different ways to combine them. Every model should have a regulatory framework and respond to specific characteristics of each country: geographical, social, historical, cultural, etc.

- Internet connectivity should not be provided at the cost of personal data extractivism, predatory practices to the environment or any other conditioning factors that can be harmful to human rights.

- Importance of community networks must be recognised since they can deliver access to underserved areas with infrastructure built, managed and used by local communities.

Key commitments, pledges, or actions

FOR INTERNATIONAL ORGANIZATIONS

- Meaningful connectivity to the Internet must be included as a core and structural policy included in the SDGs.

- International organizations should adopt standards based on meaningful connectivity to promote universal and equal access to the Internet.

- Specific funding should become available for less-developed States to close the digital divide.

FOR GOVERNMENTS AT ALL LEVELS

- States should design and implement public policies to promote universal and equal access to the Internet,

addressing structural discriminatory social conditions and take into account the specific characteristics of the territories.

- Community networks should not be prohibited and legal obstacles should be facilitated to encourage them.

- Develop public policies combining public, private and community based solutions for broadband services and connectivity devices for all. These policies should ensure regulatory and reinforcement mechanisms for community networks and other community based solutions as well as the others.

- Prohibit the arbitrary and deliberate slowing and/or shutting off of the Internet specially during political events and others of public interest.

- Enhance transparency in all actions and promotion of social participation in all phases, such as designing, funding, managing of the spectrum, decisions on the provision, performance indicators, and others.

- States should also ensure enough resources to maintain free wi-fi in schools as well as teachers that facilitate the educational efforts to use digital resources and skills to improve communities' life.

FOR PRIVATE SECTOR

- Complement their efforts of connectivity provision with other community based solutions in the idea of having everybody meaningfully connected.

- Develop applications and other innovations ensuring accessibility for all, including people with physical, sensory, or cognitive disabilities, people who are not literate, and people who speak minority languages.

FOR TECHNICAL AND ACADEMIA ACTORS

- Promote research and improvements to reduce inequalities.

- Assess the government's core Internet usage indicators periodically, in order to identify improvements.

FOR CIVIL SOCIETY

- To develop community networks to solve connectivity gaps of the private and public models of service provision.

- Monitor the development of the public policies and demand information and open data about that.

- Implement capacity building efforts on digital skills and digital security for everybody but specially for vulnerable populations.

PROTECT ALL DATA

Core Principles

- Lawfulness, fairness, and transparency principle: States, organizations and private entities should collect and process personal data in line with the relevant data protection laws in place and in due regard to the principles of justice, human dignity and transparency.

- Purpose Limitation principle: States, organizations and private entities should collect personal data for specific, explicit, and legitimate purposes and not process the said data in a manner that is incompatible with those purposes.

- Data Minimisation principle: States, organizations and private entities should limit personal data collection and processing should be limited to what is strictly necessary and relevant for the purpose for which it is being processed.

- Accuracy principle: States, organizations and private entities should ensure that personal data that is collected and processed by a data controller or processor is kept accurate and up to date. Every reasonable step should be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

- Storage Limitation principle: States, organizations and private entities should ensure that personal data should only be kept for only the period that is necessary for the purposes of processing the said data. Specific time lines should be put in place for erasure or periodic review of the personal data.

- Integrity and Confidentiality principle: States, organizations and private entities should ensure that personal data is processed in a manner that maximizes the security and confidentiality of the personal data in question.

- Accountability principle: All data controller/processor be they States, organizations and private entities have a responsibility to demonstrate that they have complied with all the above listed principles.

Key commitments, pledges, or actions

FOR GOVERNMENTS AT ALL LEVELS

- To promote a multistakeholder approach, collaboration and partnerships to ensure respect for data privacy;

- To conduct data protection impact assessments before embarking on mass data collection and processing activities;

- Work together with civil society to increase awareness of data privacy especially for ordinary citizens to enable them to report privacy violations;

- To develop an accreditation framework for institutions and certification of privacy professionals;

- Work towards developing regulations on Big technology companies and fintechs through the development of a Data Protection Code of Ethics for Big Tech;

- The Global South should adopt a collaborative approach to rein in on harmful practices regarding personal data by Big Tech companies.

FOR CIVIL SOCIETY

- To promote public awareness on gendered as well as non gendered privacy concerns;

- To use joint advocacy efforts and alliances to advocate on common pain points with regards to personal data protection;

- To adopt a collaborative strategy when engaging with government and independent regulators to achieve desired outcomes by mutual agreement.

FOR PRIVATE SECTOR

- To proactively adopt the principles of privacy in their operations as well as privacy by default and design in the technologies they choose to deploy.

REGULATION OF ARTIFICIAL INTELLIGENCE

Core Principles

- Global asymmetry awareness: for the recognition of disparities between the countries of the Global North and Global South, and for the promotion of global best practices in AI to reduce existing asymmetries, especially in the collection and processing of data from the Global South by the Global North, through greater monitoring of international observers, such as UN agencies and secretariats;

- Principle of multistakeholder and networked governance: regulation as a collective undertaking, and not just monopolized by the state, using a responsive regulation framework for it;

- Principle of informational due process: meaningful enforcement of human rights in the scenario of semi or fully-automated decisions to guarantee the adversary proceedings and the right to a fair hearing, especially in the fields of algorithmic management and working conditions, and in databases directly related to the UN Sustainable Development Goals (SDGs), such as about climate development and indigenous peoples;

- Algorithmic fairness principle: algorithms should not unfairly discriminate against individuals or groups, being one of the main aspects of accountability processes;

- Precautionary principle: reduce information asymmetry by having a public scrutiny with regards the risks of AI systems to human rights and fundamental freedoms, and to have regulatory intervention proportionate to these risks;

- Harmonization between risk-based and rights-based approaches: the risk-based approach as a potential enabler of fundamental rights and not as a flexibilization of them.

Key commitments, pledges, or actions

FOR GOVERNMENTS AT ALL LEVELS

- To create a public, open and searchable database on high-risk AI, regularly updated, as well as reports on the impact of personal data protection and human rights.

- To propose Regulatory Sandboxes, subject to an independent oversight entity formed by a diverse and multistakeholder committee.

- To publicize the use of AI in public systems, providing clear and accessible explanations for systems, whose results cannot be explained by their inputs and rules.

- To prohibit the use of AI for social scoring and/or reputational systems that restrict access to social rights.

- To encourage the use of AI to face socioeconomic inequalities and prevent the formation of monopolies involved in the development and implementation of these systems.

- To ensure independent oversight throughout the processes of development, implementation, and accountability of AI systems, linked to the competent regulatory system.

- To ensure legal exceptions, with due legal certainty, so that international commitments (such as international trade agreements) about protecting source code and algorithms do not restrict AI regulation in relation to transparency and accountability.

FOR GOVERNMENTS AT ALL LEVELS
AND THE PRIVATE SECTOR

- To carry out human rights impact assessments, ensuring due participatory process and public scrutiny.

- To provide the right of explainability and review on all

automated or semi-automated decisions that impact human rights, in an accessible and transparent way.

- To encourage the development of systems in native languages, favoring the active participation of all communities in the digital ecosystem.

FOR ACADEMIA AND THE TECHNICAL COMMUNITY

- To expose biases, applications that are discriminatory and have extensive data collection, in addition to monitoring AI implementations.

- To review human rights impact assessments and other documentation supplied by the government and the private sector, regarding the use and application of AI systems.

FOR CIVIL SOCIETY

- To review human rights impact assessments and other documentation suppliedby the government and the private sector, regarding the use and application of AI systems.

FOR CIVIL SOCIETY, ACADEMIA AND THE TECHNICAL COMMUNITY

- To promote awareness and literacy on the public value of AI systems, through public education and civic engagement.

FOR INTERNATIONAL INSTITUTIONS

- Within their respective mandates, supervise and ensure that such guidelines are complied with by all stakeholders, promoting spaces for dialogue and learning.

DIGITAL COMMONS AS A GLOBAL PUBLIC GOOD

Core Principles

- Common understanding of digital commons and enabling infrastructure: While terms such as digital commons, digital public infrastructure and digital public goods have been widely used in the last few years, there exists discrepancy in the way various institutions use these phrases. These are terms borrowed from traditional economic discourse and have been applied to the digital sphere. However, their application does not quite match traditional uses of the terms. For us to recognize digital commons as global public goods, and action them as such, it is essential to have a common understanding of them.

- Recognizing critical infrastructure that support digital commons: In addition to recognizing digital commons and adequately governing them, it is critical that we identify the necessary supporting infrastructure that supports these digital commons and govern them in the nature of public infrastructure / critical infrastructure.

- Embedding inclusion in the design of digital commons: Like most digital technologies, access to and participation in digital commons is not equal, but stymied by structural inequities – based on gender, ethnicity, and wealth among others. These inequities are also aggravated by disparities regarding the digital – be it digital connectivity or digital literacy. The design and implementation of digital commons must take these factors into account to prevent further disenfranchisement and abuse of human rights.

- Promotion of community rights of data: Data is integral to the operation of digital commons. Data either informs the design and implementation of them or flows out of their operation. In both scenarios, data is crucial not only to the

functioning of digital commons but has significant value in the insights it provides about communities. In the age of surveillance capitalism, such data poses a serious threat to communities at large. Given this gravity of data, and seeing as in many cases data is generated by the community themselves, there needs to be a recognition of communities' rights over data with affordances that can help them seek value from it and guard themselves from abuse.

- Democratizing access to digital commons beyond open data: Given existing inequities, there exist only limited actors who can make adequate use of open data. For digital commons to be equitable, there needs to be equitable access to education and technology that allows individuals to make use of open data to further social benefit.

Key commitments, pledges, or actions

FOR GOVERNMENTS AT ALL LEVELS

- To develop data legislation that does not favor data localization, but allows for cross border flow of data, with globally accepted restrictions that ensure data security and safety;

- To adopt a multistakeholder approach in developing the definitions of key terms around digital commons so as to prevent capture of these terms by certain entities, as is the case currently. This can include incentivizing inputs from academic and civil society organizations;

- To incentivize all stakeholder to examine and understand the environmental impact of digital technologies, including those that are deemed to be digital commons. New, promising technologies, such as large language models, have a tremendous impact on the environment, and it is typically marginalized communities that are most affected by climate change;

- As far as possible, States should encourage a system of networked institutions and associations deploying digital commons projects, instead of unifying them into a single national infrastructure;

- States must come together to establish an international treaty to govern the protection of global commons, holding the ideals of equity and justice at its core.

FOR GOVERNMENTS AT ALL LEVELS AND THE PRIVATE SECTOR

- To work together to democratize access to enabling technologies that will allow a greater percentage of the population to harness data for social good.

FOR CIVIL SOCIETY

- To undertake more initiatives to upskill marginalized communities in the use of digital technologies and on data rights. For this, civil society organizations should be adequately incentivized by States and philanthropic funders.

FOR ACADEMIA AND CIVIL SOCIETY

- To develop a common, theoretical foundation for terms such as digital commons, digital public goods, and digital public infrastructure.

FOR INTERNATIONAL INSTITUTIONS AND THE GLOBAL COMMUNITY

- The global community must incentivize the sustainable development of digital commons. Sustainable modes of development are onerous and historical inequities created through unsustainable development over-burden

the Global South. Multilateral forums should therefore provide support to Global South nations for the sustainable development of digital commons and related technologies.