Contribution of the Islamic Republic of Iran to the Global Digital Compact

April 2023

1.

6. It is free from unilateral coercive measures as those measures are major obstacle in the decision-making system based on the sovereignty of the States, as well as an impediment in the way of the digital transformation of nations, or their benefits from global networks and the development of information and communication technologies. Likewise, barrier for the benefit of users from their rights in digital ecosystems;

7. Supporter of the decision-making system based on the national sovereignty of countries, supporter of social justice, driving force of productivity and economic prosperity, facilitator of transparency, public supervision and fight against injustice and corruption in all forms and manifestations;

8. Having responsible, capable users with valid digital identity, literacy and skills necessary for safe living in cyber ecosystems;

9. It has fair distribution of digital resources and benefits resulting from global networks and information and communication technologies;

10. It has Balanced, two-way, and regulated circulation of useful, valid and reliable information, while it has local and context based content moderation systems for harmful and illegal content against individual and society in consistence with national law and values;

11. In this space the fundamental national rights and values are guaranteed, the right of digital self-determination and the right to development of countries are recognized, and all countries have the right to determine their own model of development and governance in this new ecosystem in a fair and equal manner;

12. It has efficient, fair and transparent framework of accountability and responsibility for all the actors (in particular, accountability of powerful and influential actors, including cross-border service providers according to the laws and regulations of the country where they have digital presence, effect and activity);

13. It has safe, trustworthy, flexible and interactive infrastructures within the framework of technical and security standards accepted by all the governments;

14. In the favorable cyber space, the countries respect each other's rights in choosing their own model of development, governance, regulations of cyber space and public policy concerning the internet issues. States have

right to operate own cyber space in line with their national law. They have jurisdiction on infrastructures, data, resources, services and related activities to information and communication technologies in their own territories. Likewise, they have right to protect of their civilians, systems and digital resource against threats, crimes, damages, disruptions, cross-border attacks, subversion and foreign interference to defend their own rights, fundamental values and legitimate interests in cyber space;

15. In the favorable cyber space, no country should seek digital dominance, colonialization and unilateralism. No country should use cyber space, the internet and communication and information technologies for intervention in the domestic affairs of other countries, or should not support or participate in the cyber activities that undermine the security, sovereignty and stability of other countries, by misusing its superiority in the cyberspace;

16. All countries should enjoy necessary capacities and tools for exercising sovereignty in the cyber space in order to manage possible risks and harms caused by the global networks and services provided on their platform, and should protect all societies particularly children, women and families vis-ظvis negative effects and consequences of cross-border illegal, criminal and harmful contents and activities in the internet, digital platforms and emerging virtual environments including Metaverese;

17. The favorable cyber space enables the digital economy in a balanced, safe, comprehensive and multilateral manner;

18. Protecting and expanding cyber space in the favorable one, respect environment and safeguard the environmental assets of the countries;

2. Connecting all people to the internet, including all schools

2-1—Fundamental Principles

1. Regular, Safe, fair, free, reliable and affordable access to all communication resources and cross-border data flows under the national rule and laws;
2. Secure, Sustainable, resilient, stable and regulated global networks consisting of public digital infrastructure and independent and

4. Ensuring necessary political and legal guarantees by key players including dominate States and institutions over global networks and services provided on their platforms for non-abuse of them to realize the illegitimate goals and illegitimate interests including:

   -Non-application of discriminatory policies and unilateral coercive measures by the governments and institutions that have dominance, monopoly and authority over the infrastructure, technology, services and vital resources of global networks and the internet;
   -Inclusive connectivity to global networks and access to services provided in their platforms should not become a tool for systematic violation of national sovereignty and intervention in the internal affairs of States;
   -Inclusive connectivity to global networks and access to services provided in their platforms should not damage national stability and security and undermining security and stability of economic, social and cultural systems of countries;
   -Inclusive connectivity to global networks and access to services provided in their platforms should not be used as a tool for leading and organizing chaos and insecurity, inciting violation through organized dissemination of disinformation and hate speech campaigns against countries and religions;

5. Improving international cooperation in exchanging technology, knowledge and experience in the field of information and communication technology in a non-discriminatory manner, with regard to the effects of digital space on all legal, political, civil, economic, social and cultural aspects;

2-2 - Developing Digital Education based on Justice and Values

1-2-2- **Fundamental principles**

1. Providing safe, fair, free, legal and reliable access to useful and trustworthy educational resources for all ages and languages;
2. Creating global networks of scientific content and knowledge based, consisting of independent sub- networks under the governance and management of governments and interoperable on basis of the rules and protocols agreed by all countries;

3. Empowering, educating and training users in a proper way for a healthy and safe life in cyber space based on principles, values and educational principles governing the official education system of countries;
4.

6.

public policy issues pertaining to the Internet, the enhanced cooperation has yet to realize);

8. Geopolitical neutrality of the internet during international crisis and conflicts and preventing misuse of information and communication technologies and prohibition of using the Internet and cross-border digital platform as a weapon to achieve illegitimate geopolitical goals;
9. Internationalization of the public core of the internet as a global public goods;
10. Shaping fair cyber order and smart, efficient and proper law system to entail all interactions in all layers and main organs;
11. A peaceful goals and application, violence-free cyber space (only peaceful goals and objectives), promotion of stability and security in using ICTs with emphasize on prevention of cyber hostilities and harmful and peace-threatening activities, international stability and security and peaceful settlement of international disputes;
12. Necessity of accountability of cross-border platforms before users, public and the regulatory system of countries and transparency of their processes, performance and digital presence while respecting the laws and values of societies;
13. Not to follow the policy of cultural assimilation and imposing their values and lifestyles on other societies by dominant countries in the cyberspace and supporting cultural diversity and multilingualism on the internet;
14. Observing the concerns and national intergytcio3p.071 Tw 048 0 Td1 (ou)(r)3.nt9s14 Tc

and communication technologies and setting of the comprehensive convention against the use of ICTs for criminal purposes;

3. Collective efforts for creating governance framework for cyber space and internationalization of internet management within the framework of United Nations based on genuine multilateralism and consultation with relevant stakeholders as well as justice, ethic-centered, political neutrality and other principles and norms accepted by all countries, based on considering respect for the legal system and national laws of countries;
4. Providing comprehensive and obligatory framework for the responsible behavior of countries in the cyberspace, taking into account the opinions and concerns of all member countries;
5. Collective and dedicated

11. Creating necessary frameworks for guarantee the ethical, human, cultural and social considerations in the process of designing and developing digital ecosystems, technology, innovations and digital services;
12.

6. Facilitating digital trade while ensuring safe and secure data economy with respect to privacy and protection of data within the framework of domestic laws and regulations of the countries;
7. Increasing trust in the digital economy;
8. In using personal data by providers of services, they should respect fairness and transparency principles, legality of services accordance with national laws of service 's recipient countries and proportional with defined objectives for their services and observing adequate and time limitation of providing services and informing data owners on using their data;
9. Respecting national sovereignty, requirements of countries over their data of users in the area namely, sharing data, transferring data to other countries, national data, hosting and place of storing data, protection of sensitive data and big data;

4-2- Actions and Commitments to realization the Principles

1. Providing international legal frame-.2rnd8.5 (a)3.5 (of)3.7 (us)8 (,)6.2(r)12.2 (vic)15

value from raw data in order to use data as a new economic resource is needed;

7. Data and data flows can support the development of various solutions to

5-2- Actions and Commitments for Realization of Principles

1. Providing necessary frameworks for identifying, pursing and countering against systematic violence of users rights in digital ecosystem including social media and international digital platforms;
2. Developing principles, norms and regulations governing human rights commitments and obligations of technological companies and owners of cross-border digital platforms within the framework of UN.
3. Forming normative frameworks to remove unilateral coercive measures in the cyberspace that prevent countries to access benefits of new communication and information technologies and global networks as a main barrier to achieving national digital development and violation of rights of nations;
4. Developing internationally agreed indicators and reports by all countries regarding the observance of the rights of users in cross-border digital platforms;

6. Introducing Criteria for Accountability for Discriminatory and Misleading Content

6-1- Fundamental Principle

1. Accountability of cross-border platforms before users, public and regulation system of countries and their responsible digital presence while respecting national laws and values;
2. Respecting national fundamental values, cultures and local sensitivities;
3. Striking a balance between the rights and legal freedoms and the protection of society against harm and ensuring safety, health and psychological security of users on the Internet and online environments;
4. Respecting the transparency of procedures, algorithms and functions of cross-border digital platforms (regarding respect for user's rights, public rights, public safety, national security, morality, security of systems, content health, safety of platform, policies of content moderation, cooperation with law enforcement and judicial authorities to prevent and combat ICT-dependent and ICT-enabled crimes);

6-2- Actions and Commitments for Realization of Principles

1. Regulating framework of digital platforms with management and content moderation approach based on local laws, culture and values with the aim to ensure users' safety in online space and protection of societies

the lack of essential cooperation with the competent national authorities regarding countering against criminal and harmful acts and content and criminalizing the misuse of digital tools by the owners of digital platforms for illegal intervention violating national sovereignty and undermining stability, national security, public order and ethics in other countries by leading and organizing insecurity and chaos in other countries by not confronting or helping the organized dissemination of disinformation and hate speech campaigns and incitement to online violence via using algorithms based on artificial intelligence;

9. Criminalization of insulting the sanctities and values of divine religions and publishing defamatory and untrue content with the aim of destroying and tarnishing of divine religions, their leaders and followers on the Internet and digital platforms;
10. Making collective cooperation between governments and owners of technology companies in the field of fighting against organized xenophobia, promoting racism and destroying the image of nations and religions on the Internet and international digital platforms;

7. Improving the Regulation of Artificial Intelligence

7-1- Fundamental Principles

1. Fundamental principles of international laws and principles and objectives, enshrined in the UN Charter in the development and deployment of AI;
2. National sovereignty in providing data required for technologies and artificial intelligence systems;
3. Protecting users ' rights and fundamental national values in the design, development and governance of artificial intelligence;
4. Legal and legitimate purposes and peaceful uses of artificial intelligence;
5. Health and safety in artificial intelligence design and development;
6. Designing and development of artificial intelligence based on values and moral considerations;
7. Accountability and responsibility of designers, developers, organizers of products and services of artificial intelligence;
8. Responsible innovation and non-harm to others, especially in the field of artificial intelligence;
9. Transparency and ability to explain algorithms;
10. Non-bias approach in possesses, outputs and in decision-making of artificial intelligence-based systems;

system in the field of judicial competency of the countries and within the national laws for the safeguard of public rights and interests;

5. Avoiding unilateral coercive measures which prevent the realization of economic and social development for the population of effected countries and prevent them from fully benefiting of the advantages and benefits of communication and information technologies;

6. Confronting technological monopoly as an element which prevent the growth of industry and digital development of all countries, particularly emerging countries in the process of technology;

8-2- Actions and Commitments for Realization of Principles

1. Recognizing and guarantee countries right to development in the cyber space and the necessity of confronting technology sanction and unilateral coercive measures against human rights ((in the fields of investment, infrastructure development, connectivity and access, digital resources, Hardware and software needed for digital development and transformation) adopted by governments and digital platforms;
2. Creating governance framework and regulating digital joint affairs with emphasize on the principle of: safeguarding privacy, data, transparency cultural diversity within the framework of national laws and values and avoiding monopoly;
3. Establishing a governance framework and setting regulations regarding digital commons with an emphasis on the principles of privacy and data protection, transparency and accountability, avoiding concentration and monopoly, cultural diversity within the framework of national laws and values;
4. Designing and implementing of capacity building programs in the cyber field, including through digital commons, should be based on national development goals, national programs and needs of governments and in accordance with the economic, social and cultural situation, and should not use as a tool for interfering in their internal affairs;
5. Removing structural impediments of investment in the development of digital infrastructures and services, access and transfer of technologies and services needed for national digital transformation, as well as including unilateral coercive measures;

6. Creating institutional mechanisms for dialogue and knowledge- sharing, expertise, experiences and digital technologies among countries at the international level;

9. Other Areas:

9-Digital Security and Trust

9-1- Fundamental Principles

1. Respecting sovereignty of governments in cyber space and non-intervention in domestic affairs of governments through cyber space and non-intervention in cyber domestic affairs;
2. Prohibition of threats or use of force against the territorial integrity and political independence of countries, including the prohibition of threats or use of force in and by cyberspace;
3. Mutual respect in international relations, and peaceful coexistence in the digital ecosystem and seeking fair pacifism;
4. Peaceful cyber space free from violence (objectives and uses based on peace), promotion of stability and security in using ICTs based on prevention of cyber conflicts and harmful activities that threaten international peace and stability, and settlement of international disputes through peaceful means;
5. Realization of the principle of cyber security for all (failure to secure oneself by violating the security of others);
6. The right of countries to comprehensively defend their cyber territory against all kinds of cyber threats based on the scale and severity of the effects of cyber operations on the country's critical infrastructures.
7. Geopolitical neutrality of the internet in international crises and conflicts and prevention of misuse of information and communication technology and use of internet and cross-border digital platform as a weapon to achieve illegitimate geopolitical goals;
8. Inclusive protection of societies before threats, crimes, cyber hostilities and harms resulted from illegal activities and content, threatening and weakening security, stability, safety, interest and values of countries;
9. Prohibition of production and use of fully lethal automatic weapons by using artificial intelligence which is contrary to moral principles and rules of international law;

10.

3. Development of commitments, standards and necessary capabilities for ensuring the security of vital national infrastructures vis-ظvis cyber threats and to ensure supply chain security;
4. Development of new principles and norms of current international rights and completing balanced and obligatory framework regarding the moral and behavior of member states in global cyber space, by taking into consideration the views, interests and concerns of all member states;
5. Preventing and countries against the use of information and communication technology for criminal purposes and effective international cooperation in the field of seeking and pursuing cybercrimes, including the exchange of information and digital evidence;
6. Preventing, managing and effectively countering against all verities of criminal and harmful actions and content in the cyber spa n theim

1. Respecting principles, values, interest, national identity, ethical criteria and cultural sensitivities of world religions, by all players who are active in cyber space and ecosystem of internet governance;
2. Empowering users and giving them appropriate training for safe and

and promote cultural and civilizational identity and heritage of the member countries in the platform of cyber space;

11.Digital trade and Economy

11-1- Fundamental Principles

1. Regulated, trusted cross-border data and information flow, respecting sovereignty considerations including data sovereignty, national digital security and economy;
2. Avoiding unilateral coercive measures that prevent the people of targeted countries from full realization of economic and social development and deprive them from fully benefiting from the advantages and benefits of information and communication technologies;
3. Net neutrality with the aims of creating a level and fair playing field for the develop 1 Tf0 ( )TJrTw 0.n (a)3.β43f17o2.3 (s of)3.6 (c)30C - (di)8.4 (ve)3.s(e)3.6 (ne

2. Creating an enabling environment for safe, secure, healthy, trusted digital trade, while respecting the national sovereignty of countries;
3. Legal and responsible activity of cross-border digital platforms in financial, commercial and economic fields in the area of territorial jurisdiction of other countries;
4. Collective collaboration for the setting and developing international principles, norms and rules to counter effectively against anti-competitive practices of big tech companies in the digital ecosystem, and also for abuse