Forum: United Nations Human Rights Council
Main Submitter: The Gambia
Signatories: France, Russian Federation, India, Tunisia, Kenia, Norway
Topic: Protecting the Cyber Privacy and Digital Rights of Citizens from Governments in Times of Crisis

United Nations Human Rights Council,

Recalling the creation of the Cipesa, an organization established in 2004 under the Catalysing Access to Information and Communications Technology in Africa (CATIA) initiative, which was mainly funded by the UK's Department for International Development (DfID) and which works to enable policymakers in the region to understand ICT policy issues, and for various stakeholders to use ICT to improve governance and livelihoods,

Emphasizing the need to modify the law in places where privacy is violated,

Recognizing the need to create new organs, each one with different functions, which will consist of, but not limited to: controlling data-related crime, and judging those accused of having violated the privacy of any citizen,

Aware of the creation of the Small Media, a London-based organization that works to support freedom of expression and access to information globally, as well as, with their global partners, develop strategies and tools that can support human rights defenders, activists and journalists to work safely and effectively in the digital age,

Noting with concern that Technology has proved a useful and necessary tool to help ensure that local and regional governments on the frontline of the emergency continue to provide essential public services during the COVID-19 crisis,

Further recognizing the help of local and regional governments on the frontline of the COVID-19 crisis have resorted to digital technologies to monitor, anticipate, and influence the spread of the disease, as well as to provide education for students,

Believing that all types of transparency that need to be considered when interactions with AI occur, (developer, deployer, and user),

Recalling digital rights including data privacy and ethical digital standards, and they will be taken into consideration even in times of crisis,

1. *Suggests* punishments for companies that have violated a country's laws and regulations regarding the protection of data:
    a. Imposing sanctions in the forms of but not limited to:

i. Increased taxes, and
ii. Fines, and

b. Further limiting monetary sources by ways such as but not limited to:
i. Limiting government revenue including monetary support given by the government and investments provided by the government and related persons, and
ii. Blocking access to methods of further gaining revenue such as the use of public advertisements;

2. *Requests* the creation of the IDAC (International Digital Age Court) which will be in charge of any data-based crime, regarding, but not limited to:
a. Violation of data flow between individual and third party including the distribution of personal data and publication of personal data, and
b. Insufficient methods of securing the safety of data such as the security of company servers;

3. *Calls upon* member states to increase their enforcement on current data protection laws by:
a. Making sure all paperwork regarding such laws are updated,
b. Monitoring companies operating within their country by:
i. Monitoring data safety procedures of a company,
ii. Logging any data related complaints or lawsuits, and
iii. Following through the collection of any fine regarding data breaches,
c. Requests for countries to include previously partial or fully exempted organizations to be included into data protection laws involving:
i. The disclosure of personal data by a third party, and
ii. The publication of any data of an individual or collective;

4. *Pledges* companies that operate in member states to designate at least one Data Protection Officer (DPO) with responsibilities such as but not limited to:
a. Enforcing the data protection laws of the country inside the company,
b. Taking necessary actions when a company breaks the aforementioned laws,
c. Making sure that a company's policies and practices ensure the safety of any data given by any clients,
d. Keeping antivirus programs up to date,
e. Watching out for phishing and scams, and
f. Investigation if any claim regarding the abuse of private data, including claims of identity theft, access to private accounts, and distribution and publication of private data;

5. *Endorses* the increase in government funding in the development of cybersecurity measures, including but not limited to:
    a. Improvement of current security measures such as firewalls, and
    b. Development of new tools to ensure that data can not be taken without consent;

6. *Urges* for member states to include previously partial or fully exempted organizations to be included into data protection laws involving:
    a. The disclosure of personal data by a third party, and
    b. The publication of any data of an individual or collectives;

7. *Asks for* member states governments to be subject to monitoring of:
    a. Data collected by the government, including, and not limited to those from,
        i. National surveys, and
        ii. Immigration paperwork,
    b. Data storage practices, involving:
        i. Server security,
        ii. Worker access to data collected, and
        iii. Firewalls and such technologies, and
    c. Reports regarding:
        i. Data breaches in government departments and subsidiaries, and
        ii. Abuse of private data by government workers;

8. *Recommends* the creation of awareness campaigns that will consist of:
    a. The government and the private sector working together in order to ensure a clear understanding of cybersecurity, and
    b. These campaigns being financed by the government and consider that:
        i. The economic income may vary, and
        ii. They will be supervised by the DPO;

9. *Further requests* that member states follow through the clauses in this resolution and be observed by,
    a. Member states to write reports on,
        i. Any updates in countries regarding, but not limited to: changes in laws and regulations regarding data, policies in data containment, guidelines for companies regarding data distribution, legislations in what constitutes personal data, data breaches, Convictions of companies for violation of data laws,
    b. Asks for said reports to be filed to:
        i. The UN human rights committee for recording and storage, and

ii. Requests that such reports be filed annually to monitor and regulate laws, and

c. Could serve as a model for other efforts;

10. *Encourages* the agility of countries in updating or developing national cybersecurity strategies, as well as legal and regulatory framework regarding cyberspace:
    a. These initiatives must take a multi-stakeholder approach, including paying close attention to the construction of incident response capacities in all sectors, and
    b. Governments cannot act alone, and the participation of the technical community and the private sector are essential to building effective resilience capabilities.