|  |  |
| --- | --- |
|  | No. 1, Johnson Omonire Street Yaba, Lagos State  +2348087878783  contact@techhiveadvisory.org.ng  tech-hive-advisory |

**From: Tech Hive Advisory Limited**

**Date: 27th May 2021**

**Subject: Recommendations to the UN Call for input on the right to privacy in the digital age**

**RE: Call for input: Report on ‘the right to privacy in the digital age**

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference**  **(Section)** | **Issues** | **Comments** | **Recommendations** |
| 1A | Relevant technological developments, the driving economic, political and social factors promoting the use of AI and the main actors in and beneficiaries of deploying and operating AI (developers, marketers, users) | In developing countries, it has been found that its economic benefits drive the race to AI. This is unlike the developed world, where the race to AI is mainly driven by automation, augmentation, robotics, and intelligent weapons system. | Developing countries use AI to tackle fundamental societal challenges like curbing bureaucracy, corruption and improving access to healthcare. Anonymisation of user data should be incorporated into systems to encourage public whistleblowers and preserve the integrity of healthcare data |
| 1B; 3D | Ways in which AI can help promote and protect the right to privacy;  Technology applications that (could) help adequately protect the right to privacy when applying AI and its limits | The last few years have seen the development of new methods for preserving privacy, anonymising data, although they are primarily for commercial use and developed as an alternative to cookies, in light of their phasing out;  New privacy technologies are mainly being developed in separate silos by wealthy corporations. Weaker organisations that lack the financial and professional expertise to build their privacy tools may find themselves unable to apply new privacy standards fully | The UN should tap into the current development of new data anonymisation techniques and issue a set of minimum standards that all new privacy techniques must meet;  The development of an alternative open-source privacy standard should be supported or undertaken by the UN, accessible to weaker organisations. |
| 1D | Discriminatory impacts of the use of AI | The introduction of predictive policing in different parts of the world has been found to create the following risks:   * Increased racial profiling * Interference with privacy * Overreliance on technologies * Risk of targeting people, based on statistical probability, rather than the individual system of wrongdoing   A notable example is the case of WISCONSIN v. LOOMIS in the USA, where the risk assessment system, COMPAS, was found to be biased against African-Americans, recommending harsher sentences and refusing bail for similar crimes committed by other racial groups. Predictive policing systems exacerbate decades of ingrained bias in criminal justice systems. | A ban should be placed on predictive policing systems, pending the development of sufficient safeguards to isolate them from human biases. Precedent for this can be found in the current ban on facial recognition systems by many big tech corporations and authorities in the USA. |
| 2A | Information on relevant existing or proposed national and regional legislative and regulatory frameworks and oversight mechanisms | The problem AI legislation needs to address is not regulating a particular technology but rather the intersection of AI technologies and human interaction at a personal and collective level.  In Nigeria, the National Centre of Artificial Intelligence & Robotics (NCAIR) was set up under the National Information Technology Development Agency (NITDA). The NCAIR is expected to fully independent by the end of 2021.  The telecommunications regulator, Nigerian Communications Commission (NCC), has also published a report on the ethics of artificial intelligence.  At the regional level, the UN Economic Commission for Africa (ECA), in collaboration with the United Nations Industrial Development Organisation (UNIDO) and the International Telecommunications Union (ITU), is supporting the establishment of the African Artificial Intelligence Research Centre (AAIRC) in Congo Brazzaville. The centre is expected to improve the landscape of AI research in Congo and Africa as a whole, to support the use of AI to foster economic and social development, and promote close collaboration of academia and industry. | The trend in AI regulation is domain-specific, with existing government agencies seeking to understand and regulate the use of AI within their sector. Alongside, central hubs for research into AI are taking off.  It is advisable that at the national and regional level, these research hubs should take on the responsibility of ensuring cross-agency collaboration and potential intermediating disputes, especially where AI applications or companies engage in activities that cross the domains of two or more regulators. |
| 2B | Analysis of related human rights protection gaps, ways to bridge those gaps, and barriers to advancing effective, human rights-based regulation of AI | There is an increased proliferation, use, and normalisation of advanced technologies in counter-terrorism, which is not accompanied by human rights guidance, particularly with biometric technologies | A distinct and specialised study of the several use cases of AI in counter-terrorism efforts should be undertaken with the aim of beaming the spotlight on current and potential rights violations. Using this as a guide, recommendations on the next course of action can be proffered. |
| 3A | Self-governance approaches by business enterprises to regulate AI applications, which meet the companies’ responsibilities to respect the right to privacy | Self-regulation efforts by big tech companies, though commendable, tend to be haphazardly implemented and biased based on their ideological inclinations.  Twitter flagging and suspending former President Trump’s account is an example. In comparison, many other users violate the same rules and may not receive the same punishment.  Another example is Facebook which works with a definition of terrorism that is not consistent with international law.  Because of the international spread of many tech companies, attempts by national governments to impose regulations on them can easily take on geo-political and nationalistic undertones. An example is France’s attempt to impose a digital tax on big tech companies, which did not go down well with the Trump administration. | The UN and its agencies must play a more significant role in the cross-continental regulation of AI by providing minimum standards that regional and national authorities can build on but not deviate from. |

**FOR: TECHHIVE ADVISORY LTD**

Akin Agunbiade

Associate (Emerging Technologies)

aa@techhiveadvisory.org.ng