FORUM: Human Rights Council

QUESTION OF: Measures to Prevent Voice Cloning Fraud and AI-Generated Impersonation Scams

MAIN SUBMITTER: Netherlands

CO-SUBMITTERS: Thailand, Slovenia, Republic of Korea, Switzerland, Norway, India, Cuba

THE HUMAN RIGHTS COUNCIL,

Deeply concerned of the increasement of voice cloning fraud and Artificial Intelligence (AI)-Generated impersonation scams,

Acknowledges the need for artificial intelligence companies to strengthen regulations governing the use of AI,

Concerned about AI-enabled frauds and scams,

Hopes Member States to enhance data protection measures and safeguard individual's privac y against AI-related threats,

Recognizing the positive impacts of international cooperation in sharing information and best practices to combat AI-related crimes,

1. Calls upon United Nations-supervised programs aimed at improving education and cooperation among Member States regarding voice-cloning fraud and AI-generated impersonation scams, especially for students and older generations, but not limited to:
    a) Cooperating with the administrative agency, such as the Ministry of Education, to provide annual prevention education on the dangers of voice-cloning for young students:
        i. Offering law education and safety education materials, including fraud prevention,
        ii. Providing creative experience activities about voice scams,
        iii. Demonstrating an educational video of AI generated scam dangers and new wa ys of scamming,

b) Suggesting education that is closely supported by the state and the private sector, focusing on face-to-face education and intuitive experiential programs, especially for older generations, but not limited to:
    i. Visiting field education for seniors,
    ii. Encouraging digital literacy education,
    iii. Providing designated person notification services;

2. Implementing a multi-faceted cooperation strategy to reduce the crime rate that suddenly increased due to AI industry developments, especially AI-generated voice cloning scams, including but not limited to:

a) Actively cooperating with international intelligence and law enforcement organizations, such as the Central Intelligence Agency (CIA) and the International Criminal Police Organization (INTERPOL), to dismantle global fraud networks,
b) Cooperating with legislative and judicial institutions to strengthen the standards of voice-cloning and AI-generated scam punishments,
c) Seeking information networks that have been broken by voice scamming and reinforcing and regenerating new information networks under the support of the Central Intelligence Agency (CIA);

3. Encourages Member States, in cooperation with related United Nations bodies, technology companies and AI companies to strengthen public awareness and prevention of voice-cloning fraud and AI-generated impersonation scams through public education campaigns, including:

a) Encourages Member States to cooperate with United Nations Educational, Scientific and Cultural Organization (UNESCO) in ways such as but not limited to:
    i. Collaborating with UNESCO to develop educational materials and activities that teach people ways to identify voice cloning fraud and AI-generated impersonation scams,
    ii. Working with UNESCO to provide media and digital programs that educate individuals on verifying suspicious communications before responding to them,
b) Using national media and online media platforms to raise public awareness and disseminate educational information on AI-generated scams;

4. Urges Member States to strengthen law enforcement efforts against AI-generated fraud and impersonation scams, improve existing legal frameworks by establishing clear legal definitions, and strengthen oversight and regulation of AI in ways including but not limited to:

a) Strengthening law enforcement efforts against AI-generated fraud and impersonation scams in ways such as:
    i. Establishing specialized AI Fraud Task Forces or AI Fraud Units within existing law enforcement agencies to facilitate cooperation among police forces, cybercrime departments, financial regulatory authorities, and AI regulatory bodies,
    ii. Encouraging Member States to exchange information and successful investigative strategies concerning the prevention and prosecution of AI-generated fraud,
b) Improving legal frameworks concerning AI-generated fraud and impersonation scams by:
    i. Establishing effective penalties for individuals and organizations involved in AI-generated fraud and impersonation scams,
    ii. Identifying and addressing legal loopholes that may allow criminals to evade legal responsibility;

5. Calls upon Member States to establish and strengthen mechanisms to provide compensation and assistance to victims of AI-generated fraud and impersonation scams, to the greatest extent possible, through:

a) Establishing accessible compensation mechanisms to facilitate the recovery of financial losses suffered by victims, including through cooperation with financial institutions and relevant authorities,

b) Providing victims with necessary legal assistance, psychological support, and guidance on reporting fraud and recovering stolen funds,

c) Integrating comprehensive digital literacy programs into school and community curricula, with a focus on:
    i. Developing the capability to critically evaluate online media and independently detect deepfakes,
    ii. Teaching individuals, including students and adults, how to verify the authenticity of communication sources in daily life;

6. Calls Member States to strengthen the protection of personal information and privacy against unauthorized access and misuse in AI-generated fraud and impersonation scams through:

a) Establishing and enforcing stricter regulations on the collection, storage, processing, and sharing of personal information by digital platforms and companies, ensuring that such information is protected against unauthorized access,

b) Promoting the implementation of effective data protection measures to prevent personal information from being leaked or stolen for fraudulent purposes through:

i. Encouraging digital platforms and technology companies to adopt end-to-end encryption and multi-factor authentication to prevent unauthorized access to users' personal information,

ii. Conducting regular security assessments and vulnerability checks on digital platforms to identify and address potential data breaches and cybersecurity risks;

7. Encourages AI companies to develop stronger detection systems such as, but not limited to:

a) Developments in specific detection technologies such as, but not limited to:

i. Detecting acoustic features such as pitch and pronunciation, developing advanced AI detection techniques, and updating the system frequently to respond to emerging voice cloning techniques,

ii. Identifying the digital watermarks in AI-generated voices, so that users can be aware of voices made using AI,

iii. Suggesting real-time detection of suspicious AI-generated voices, and providing immediate warnings to the user to prevent voice cloning scams and impersonations,

b) Promoting joint research on AI detection technologies such as, but not limited to:

i. Research cooperation such as analyzing new voice-cloning techniques and impersonation scams between companies so companies can respond to evolving fraudulent methods,

ii. Sharing the voice detection technologies that each institute possesses and improving reliability and accuracy through the exchange of information between AI companies and research institutes;

8. Calls upon member states for the exchange of knowledge and technical support between different organizations such as, but not limited to:

a) Sharing research results on cases of fraud between countries such as, but not limited to:
    i. Common methods and emerging techniques that are getting developed across border lines,
    ii. Preventing AI fraud by using the methods that each country has already successfully used,
    iii. Exchange on fraudulent organizations that are active in many countries, h owever, complying with each country's personal data protection laws and regulations,
b) Sharing technical proficiency and range for response and among countries such as, but not limited to:
    i. Sharing AI fraud detection methods and system development experience,
    ii. Operating a professional knowledge exchange program that cybersecurity experts and relevant agencies of each member state is joined in so member states can react in an efficient way to AI scams;

9. Encourages all Member States, in cooperation with relevant international organizations such as the UNODC, INTERPOL, and ITU, to strengthen the efforts to prevent AI generated voice cloning fraud and scams while protecting individuals' privacy and human rights, through measures including but not limited to:

a) Having stricter identity verifications for AI voice cloning platforms to prevent people from copying others' voices without permission, including but not limited to:
    i. Strictly checking the identity of individuals who want to use voice cloning technologies,
    ii. Requiring AI developers to create reporting systems that allow individuals to report unauthorized voice cloning,
b) Encourages AI developers and technology companies to build stronger safety measures to identify and prevent the misuse of AI generated audio, including but not limited to:
    i. Adding digital marks to AI generated audio recordings so that people can recognize AI voices,

ii. Developing and improving AI detection systems to help distinguish real human voices from AI-generated voices,

c) Making the protection of personal voice recordings and individuals' privacy safer, through measures including but not limited to:
   i. Establishing clear rules regarding the use of personal voice recordings,
   ii. Requiring technology companies to create secure storage systems to prevent personal voice recordings from being leaked.