

# Law of Ukraine on Regulating Artificial Intelligence Technologies and Addressing the Issue of Deepfakes to Protect Democratic Processes in the Context of Russian Military Aggression

## Section I: General Provisions

### Article 1: Purpose

The purpose of this law is to establish a legal framework for regulating the creation, distribution, and use of deepfakes and artificial intelligence-generated content in Ukraine, particularly in the context of the ongoing Russian military aggression. The law aims to protect democratic processes, including elections, public decision-making, and civil discourse, from malicious manipulation and disinformation campaigns, and to ensure the ethical and responsible use of artificial intelligence technologies during the conflict.

### Article 2: Definitions

- **Deepfake:** Artificial intelligence-generated media, including video, audio, or images, that is manipulated to represent individuals saying or doing things they did not say or do, creating a false or misleading impression.
- **Artificial Intelligence Technologies:** Technologies, including machine learning, natural language processing, and generative models, used to create, enhance, or manipulate content, particularly in the creation of deepfakes.
- **Disinformation:** Deliberate false information designed to deceive or mislead the public, often with the intent to influence political outcomes, social movements, or public perception.
- **Democratic Integrity:** The protection and promotion of democratic institutions, processes, and values, including free and fair elections, informed public discourse, and the preservation of political freedoms and rights.
- **Russian Military Aggression:** The ongoing military actions taken by the Russian Federation against Ukraine, including the use of disinformation, cyber-attacks, and other methods to destabilize Ukraine and its democratic processes.

## Section II: Regulation of Deepfake Creation and Distribution

### Article 3: Prohibition of Malicious Deepfakes

1. **Criminalizing the Creation and Distribution:** The creation or distribution of deepfakes with the intent to deceive the public, manipulate elections, harm individuals or public institutions, or support Russian military aggression is prohibited under this law.
2. **Penalties for Violation:** Individuals or entities found guilty of creating or distributing malicious deepfakes will face criminal penalties, including imprisonment, fines, or both, depending on the severity of the offense.
3. **Public Accountability:** Any deepfake content identified as misleading or harmful to public trust, especially during the conflict with the Russian Federation, must be publicly

labelled as a deepfake by the relevant authorities, and platforms hosting such content must remove it promptly.

### **Section III: Artificial Intelligence Technologies in Political and Public Discourse**

#### **Article 4: Ethical Use of Artificial Intelligence Technologies**

1. **Regulation of Political Campaigns:** Political campaigns and public institutions must adhere to strict guidelines for the use of artificial intelligence-generated content. The use of artificial intelligence for creating misleading or deceptive political advertisements or media content, particularly that could serve the interests of Russian military objectives, is strictly prohibited.
2. **Promotion of Transparency:** Political actors, government bodies, and organizations using artificial intelligence technologies to create content for public consumption must disclose their use of artificial intelligence tools to ensure transparency and accountability.

### **Section IV: Protection of Privacy, Civil Liberties, and Democracy**

#### **Article 5: Safeguarding Personal Data**

**Privacy Protection:** Individuals' personal data must be protected from unauthorized use in the creation of deepfakes. Legal actions can be taken if personal data is exploited for creating harmful artificial intelligence-generated content.

#### **Article 6: Surveillance and Oversight**

**Oversight Body:** An independent body shall be created to oversee the ethical use of artificial intelligence technologies, ensuring that deepfakes and artificial intelligence-generated content are not misused by governmental or private entities. The body will investigate complaints of illegal or unethical use of artificial intelligence technologies, particularly those related to the ongoing Russian aggression.

### **Section V: Combating Disinformation and Strengthening Public Trust**

#### **Article 7: International Cooperation**

1. **Global Standards:** Ukraine will collaborate with international organizations, governments, and tech companies to develop global standards for the responsible use of artificial intelligence technologies, with a particular focus on preventing the creation and

spread of deepfakes that undermine democratic processes, particularly in the context of Russian military aggression.

2. **Cross-Border Information Sharing:** Ukraine will work with other countries to identify and counter artificial intelligence-driven disinformation campaigns that seek to influence elections, political processes, or public opinion across borders, especially those emerging from Russian sources.

## **Section VI: Enforcement and Penalties**

### **Article 8: Penalties for Deepfake-Related Violations**

1. **Criminal Penalties:** Individuals or organizations found guilty of creating or distributing malicious deepfakes or artificial intelligence-generated content designed to deceive the public, manipulate elections, or interfere with democratic processes will be subject to criminal penalties, including imprisonment, fines, or both.
2. **Civil Penalties:** In addition to criminal sanctions, violators may face civil penalties, including compensation for damages caused by the spread of disinformation or the misuse of artificial intelligence technologies.