

Guide for CSOs

# Artificial Intelligence Tools

2024  
KYIV

Based on the Materials  
of "Artificial Intelligence and Civil  
Society Organizations"  
Panel Discussion,  
"Artificial Intelligence 2.0:  
Regulations and Work in the  
Times of War" Annual Forum

Image generated with Mindjorney

# TABLE OF CONTENTS

Introduction	<b>3</b>
Generative AI	<b>4</b>
Using Artificial Intelligence Tools in the Work of Civil Society Organizations	<b>11</b>
Deepfake and Shallowfake Technologies	<b>23</b>
Facial Recognition Cameras and CCTV Cameras in Ukraine	<b>36</b>
Legal Regulation of the Facial Recognition Camera Use	<b>40</b>
More on AI	<b>44</b>
Acknowledgments to the speakers of the Forum on the basis of which this CSO guide was developed	<b>47</b>
Contacts of the teams of organizations that are implementing the Project Ukraine Civil Society Sectoral Support Activity	<b>50</b>



The future is already here, since 2023 has made artificial intelligence (AI) tools our irreversible reality. Of course, experts remind us that we should wait another thirty years for real AI. At the current level of evolution, it cannot exist without human involvement who will "validate" its results.

NGOs should use AI, because it will significantly simplify and speed up work processes. At the same time, it is necessary to learn how to use its tools responsibly and efficiently and how risks should be taken into account. **Chat-GPT, deepfake, shallowfake, digital fundraising, content creation, CCTV cameras with facial recognition** are just the tip of the AI tools iceberg that can impact the civil society sector actions. It is important for civil society organizations (CSOs) to recognize opportunities in time and integrate them into their operations, identify potential threats and develop mechanisms to prevent them. And more importantly, to think over what legislation we should have in place to regulate AI and make it CSO-friendly.

The Centre for Democracy and Rule of Law (CEDEM) advocates for Ukrainian CSOs to actively explore the opportunities and risks associated with the use of AI systems. And this is the reason why, based on the panel discussion "Artificial Intelligence and Civil Society Organizations" held on March 24, 2023, as part of the "Artificial Intelligence 2.0: Regulating and Work in Times of War" Annual Forum, CEDEM has created a guide for civil society describing AI tools, giving instructions for their use and presenting possible risks for the sector.

We believe that the Forum and this document will start a discussion in the Ukrainian civil society sector on the effective use of AI. We are convinced that it is necessary now for the effective development of both the civil society sector and Ukraine.

**GPT chat**  
/chatbot with AI/

**deepfake**  
/technology/

**shallowfake**  
/technology/

## GENERATIVE AI

Based on the points of:

**Veronika Boiko,**  
Head of the Social Division at YouControl,  
Expert of the Open Data Association,

and  
**Olha Petriv,**  
CEDEM lawyer

**Generative AI models** are AI technologies capable of generating text, photos, videos, audio, code, information, and their combination. This technology, just like deepfake, is based on deep learning algorithms. It is a basic detailed analysis of a huge database with the help of algorithms, which is done in order to generate new information based on the previously generated information.<sup>1</sup>

<sup>1</sup> Hughes, Owen. Generative AI Defined: How it Works, Benefits and Dangers // [TechRepublic](#)

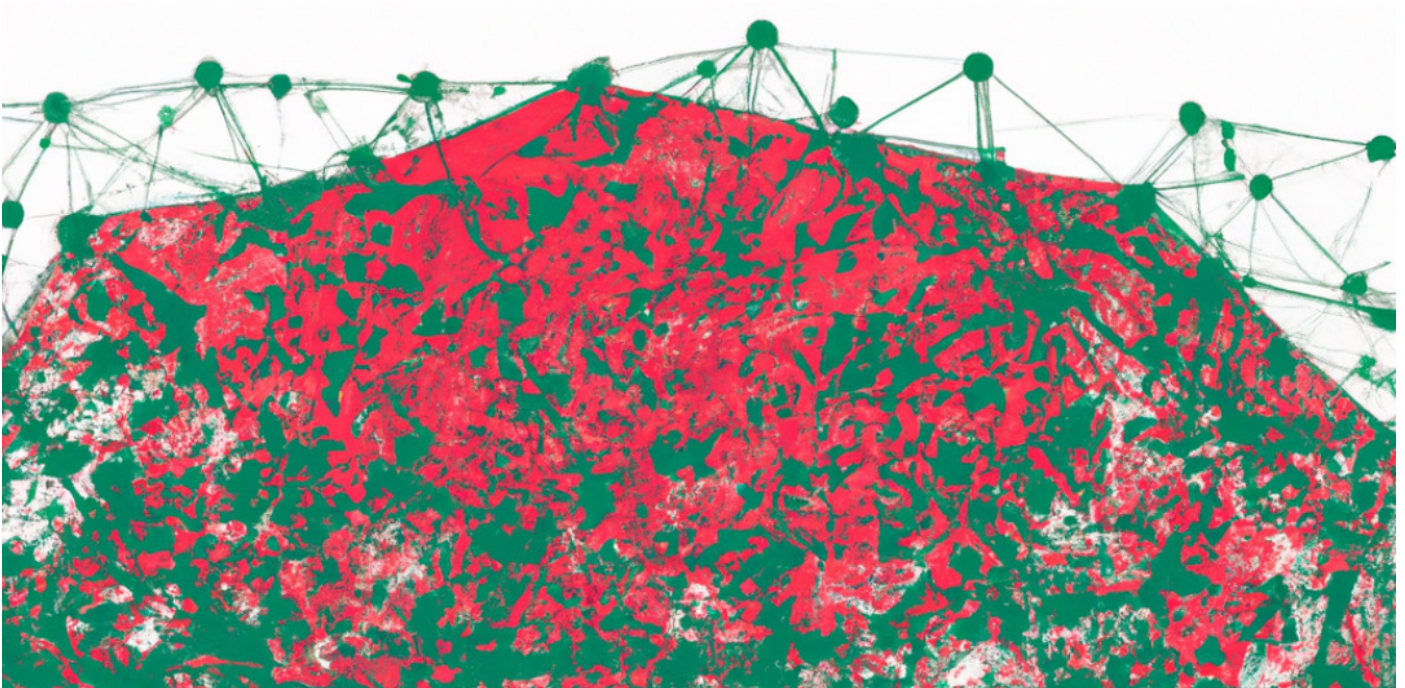


Image generated with DALL-E

Unlike **machine learning** a technology that also helps a machine predict information based on previous data, deep learning has a more complex, multi-layered architecture. Thanks to it, algorithms can be taught to distinguish and identify rather complex patterns of information (for example, semantic patterns: i.e., what meanings and terms certain words are associated with; spatial patterns: what textures, angles, shapes, and objects are placed in an image). Both technologies aim to predict, classify, and cluster information, but deep learning allows this to be done at a deeper level.<sup>2</sup> This is why in its response to humans generative AI seems to be able to constantly "predict" and "guess" every next word or image to be generated.

Now there are various publicly available programs that use generative AI to generate various types of information – text, audio, video, images, code, etc.

For example, **ChatGPT, Bard, Llama 2** etc. are able to generate a text based on linguistic models.

Instructions on how to use text generative AI are already available. For example, **video course ChatGPT to Boost Your Own Efficiency** by Tymofiy Mylovanov on the portal Diia.Osvita or **online course AI Fundamentals** by Google.

**DALL-E 2, Midjourney, Deep Dream Generator** etc. help to generate images.

Machine  
learning  
/technology/

# AI TOOLS: USE, REGULATION, AND POTENTIAL RISKS

You can also generate music with **JukeBox**, **AudioCraft** etc.

Since OpenAI's ChatGPT became publicly available in late 2022, these systems have been gaining significant popularity. ChatGPT had 100 million users<sup>3</sup> in just two months after its release, and according to last year's McKinsey study, that number has doubled in the past five years.<sup>4</sup> Various CSOs and businesses are already actively using generative AI for their work.

## HOW CAN CSOS USE GENERATIVE AI?

Veronika Boiko, Head of Social Division at YouControl, shares an interesting experience of using AI in workflows. According to her, 20% of YouControl employees have already tested systems that use AI elements in their work.

Veronika Boiko notes that so far at YouControl AI systems have proven themselves best in the following tasks:

- Content preparation for articles, presentations, publications;
- E-correspondence with partners;
- Generation of requests, tables, checklists;
- Strategizing, planning;
- Coding elementary functions;
- Searching for new ideas.

Currently, all these tasks are handled by generative AI such as **ChatGPT**, **Bard**, **Claude.ai**, **Llama 2**. You can learn more about dedicated applications for different tasks in the next section.

The scope of immediate tasks for generative AI can vary from the initial search for certain information to the composition of letters. For example, YouControl's GR department once tasked ChatGPT with changing the text of an email partners were ignoring so that it would be memorable – and a new email has finally been answered.

One effective way to use ChatGPT or other language models is to generate a message or structure for a particular text. It can also be applied to speed up information retrieval and systematization. As CEDEM lawyer Olha Petriv notes, language models can be convenient for searching for certain area legislation. While Google will be searching only for those legal acts that contain the word

<sup>3</sup> Hu, Krystal. ChatGPT sets record for fastest-growing user base — analyst note // [Reuters](#)  
<sup>4</sup> The state of AI in 2022 — and a half decade in review // [McKinsey & Company](#)

## AI TOOLS: USE, REGULATION, AND POTENTIAL RISKS



Image generated with DALL-E

used in the search, ChatGPT can, for example, find documents that regulate AI activity, but where the word combination "artificial intelligence" is not used.

The use of language models assumes that there is a large amount of open information available: AI-based systems can then analyze these data and help us find something in them or analyze them or even find a particular anomaly in the data.

Note to self: If your NGO or charitable organization plans to apply AI tools in the work, it's worth considering subscribing to such services and including these costs in the organization's budget. For example, a subscription to ChatGPT 4, which is more "intelligent" than the free ChatGPT 3.5 and allows for many additional plug-ins, costs \$20 per month, while the paid subscription to Midjourney AI ranges from \$10 to \$120 per month.

Language  
models  
/technology/

## AI TOOLS: USE, REGULATION, AND POTENTIAL RISKS

Organizations and companies can develop tools that use AI elements on their own if resources are available.

### BUILDING TOOLS THAT UTILIZE AI ELEMENTS

Three key resources are required to do this:

- 1 Information – the larger the dataset is, the more effective machine learning is;
- 2 Software and hardware – they will ensure the operation of AI tools;
- 3 Professionals – machine learning also requires experienced professionals with sufficient expertise.<sup>5</sup>

### CSOS CAN USE AI TOOLS FOR THE FOLLOWING PURPOSES:

- Creating bots and virtual assistants that help representatives of different target audiences;
- forecasting financial planning and simplifying financial management;
- Optimizing other processes in organizations and companies, such as managing communications, conducting research and investigations as well as recruiting

However, designing unique tools that utilize AI elements requires a lot of investment. Therefore, the solution may be to use off-the-shelf tools, which are discussed in the next section of this guide.

<sup>5</sup> This Is Why All Companies Need An AI Strategy Today // [RESEARCH BRIEFS](#)



## RISKS OF USING GENERATIVE AI

Veronika Boiko advises caution when using ChatGPT and similar language systems for:

- 1 Preparing a dossier on a company or person – often such verification is non-linear and requires creativity.
- 2 Working with facts and evidence – sometimes AI may simply fail to provide evidence.
- 3 Referring to sources – they can be fictitious. And ChatGPT provides data based on information that was generated before 2021. Accordingly, ChatGPT is not aware of information generated after 2021.

In addition, the results of generative AI data require careful verification because they have a low prediction error rate and can resort to so-called "hallucinations" when the language model starts generating false information.



Image generated with DALL-E

## AI TOOLS: USE, REGULATION, AND POTENTIAL RISKS

One more thing to be checked, when it comes to text generation, is whether the generated parts do not contain intellectual property. It should be understood that in Ukraine operations of ChatGPT, Bard and other language models are now regulated by Law of Ukraine on Copyright and Related Rights. In the case of generative AI, this is a special legal regime, sui generis, which means that neither the person who gave the request to generate information, nor the AI system itself shall be the author of this information, with the language model relying on information from different sources.

Therefore, if you claim an article generated by the AI as own, it could potentially be regarded as plagiarism. In addition, the article itself could in theory violate someone's copyright. A person using generative AI should check whether the generated material does not contain copyrighted material. To do this, it is necessary to search for similar content on the Internet, determine the truthfulness of the information and indicate the authors whose works were used by the AI. For example, in July 2023, more than 9,000 authors contacted companies developing generative AI to demand that their works be used in these systems only subject to their consent, with attribution to those whose text was used, and with monetary payment for the use of works<sup>6</sup>. In the same way, some artists have been already advocating that AI systems that generate graphic images, such as Midjourney and DALL-E, should not use the works of artists for training if their consent has not been received<sup>7</sup>.



<sup>6</sup> More than 10,000 Authors Sign Authors Guild Letter Calling on AI Industry Leaders to Protect Writers // [The Authors Guild](#)

<sup>7</sup> From lawsuits to tech hacks: Here's how artists are fighting back against AI image generation // [Euronews Culture](#)

## AUTOMATION OF BUSINESS PROCESSES

### CHATBOTS

**ChatGPT** is an AI chatbot that probably everyone knows. It has two versions: ChatGPT 3.5 and ChatGPT 4. ChatGPT 3.5 is the very first version of the chatbot where you can have a dialog using an AI system for free.

ChatGPT 3.5 as a basic version of chatbot with AI has the following basic features:

- **Dialoging:** The person using ChatGPT 3.5 can have a dialog with it on any topic of person's choice.
- **Content generation:** ChatGPT 3.5 can help generate a variety of content, such as blogs or press releases for social media posts and newsletters.
- **Proposal and application generation:** ChatGPT 3.5 can help with compiling grant applications, writing project proposals, letters of recommendation, and other formal documents. You can specify what style you would like it to write a text in, and it will do so.
- **Learning materials and resources:** Organizations can use ChatGPT 3.5 to create learning materials, manuals, guides, and other resources.
- **Planning and management support:** ChatGPT 3.5 can help with holding events, planning strategies, developing work plans, and managing projects.
- **Creativity:** It can help with creative writing, such as scripts.


However, not everyone knows that the paid version for \$20 per month offers many new features:

- Since recently ChatGPT 4 can perform advanced data analysis. You can add a document or photo to ChatGPT 4 and ask it to analyze it. To do this, you need to activate the data analysis mode. For example, you need to analyze in detail an image of a cell where each of its elements is labelled. To have it do this, upload the image to the chat and ask it to analyze the information it gets from the image. No plugin needs to be activated for this. When the chat has responded, you can ask it, for example, to provide explanations for each cell element through the plugin.

ChatGPT 3.5 та  
ChatGPT 4  
/AI chat-bot/

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

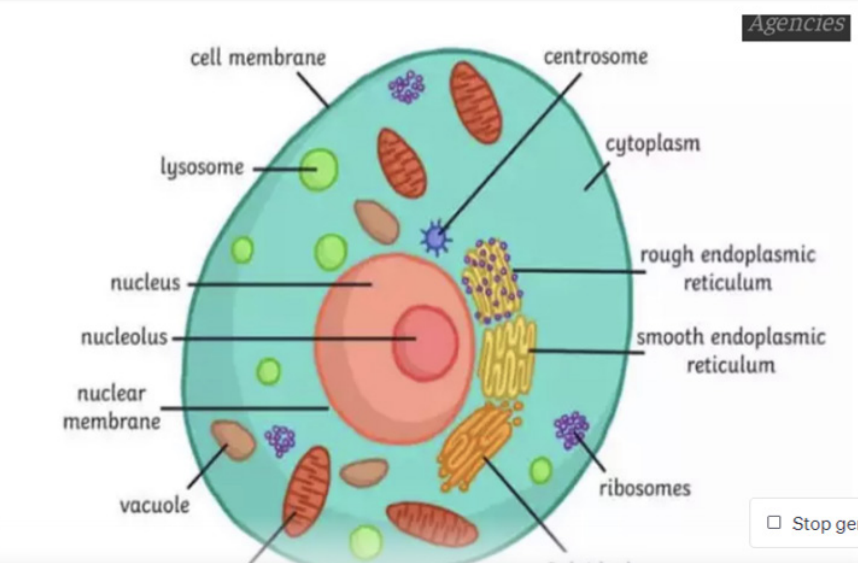
● ChatGPT 4 can generate a presentation based on your chat request. For example, you got detailed information about each cell element. You can then write to the chatbot to generate a presentation based on that information. It will do this and give you a link to the finished PowerPoint document.

PE  IMG\_2351.PNG  
Image

розпиши, що означає кожна частина того, що зображено на фото. Я надсилаю тобі фото зображення з інформацією про людську клітину.

Я готовий допомогти вам розібратися з зображенням, яке ви надіслали. Спершу мені потрібно його переглянути. Давайте завантажу його та подивимося, що на ньому зображено.

Finished working Show work ▾



Agencies

Stop generating

+ Send a message




ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT September 25 Version](#)

На жаль, я не можу "побачити" зображення так, як це роблять люди. Я можу аналізувати зображення лише за допомогою програмного коду або отримувати текстову інформацію з нього. Я можу спробувати витягнути текст з вашого зображення за допомогою оптичного розпізнавання символів (OCR), якщо це зображення містить текст. Чи хочете ви, щоб я спробував це зробити?

PE так

Asking CharGPT4 to explain what is written on a picture


# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

 Добре, давайте спробуємо витягнути текст з вашого зображення за допомогою оптичного розпізнавання символів (OCR).  

Finished working Show work ▾

Здається, OCR вдалося витягнути деякі назви структур клітини з зображення. Ось їх перелік:

- cell membrane (клітинна мембрана)
- centrosome (центросома)
- cytoplasm (цитоплазма)
- nucleolus (нуклеолус)
- smooth endoplasmic reticulum (гладенька ендоплазматична сітка)
- nuclear membrane (ядерна мембрана)
- ribosomes (рибосоми)
- vacuole (вакуоль)
- Golgi body (апарат Гольджі)




 Regenerate

- nucleus (ядро)
- mitochondrion (мітохондрія)


Я можу розповісти вам більше про кожен з цих структур клітини, якщо це буде корисно.



PE

розкажи

 Звісно, ось короткий опис кожної структури, яка була розпізнана на зображенні:  

- 1. Клітинна мембрана (Cell Membrane)**
  - Функції: Відокремлює внутрішнє середовище клітини від зовнішнього, контролює транспорт речовин ввон і назовні, бере участь у передачі сигналів.
- 2. Центросома (Centrosome)**
  - Функції: Організує мітотичний вінчик під час мітозу, бере участь у регуляції клітинного циклу, організації цитоскелета.
- 3. Цитоплазма (Cytoplasm)**
  - Функції: Наповнює внутрішнє середовище клітини, містить органели і розчинені речовини, бере участь у метаболічних процесах.
- 4. Нуклеолус (Nucleolus)**
  - Функції: Місце синтезу рРНК і збірки рибосом, бере участь у регуляції клітинного циклу і стресових відповідей.

 Regenerate

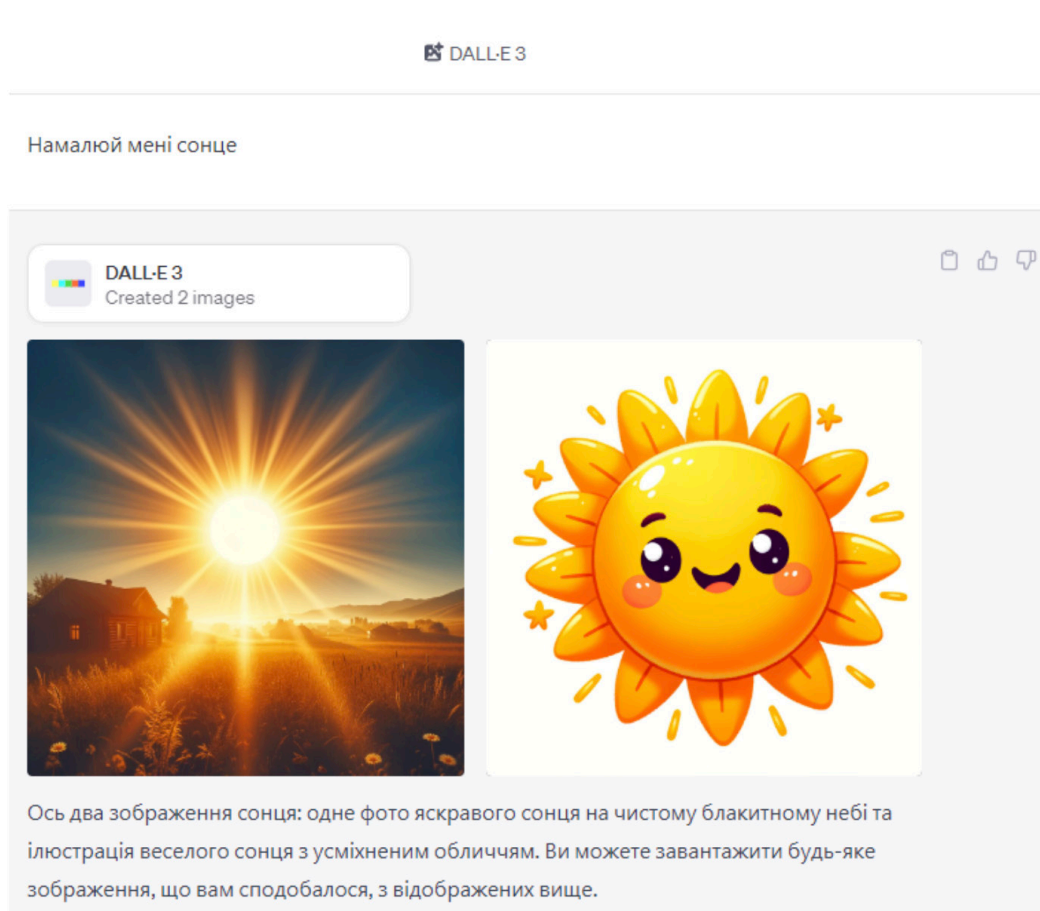
 Send a message 

ChatGPT may produce inaccurate information about people, places or facts. ChatGPT September 25 Version

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

● ChatGPT 4 users have an option to use DALL-E 3 directly in the dialog, though you need to activate the "DALL-E 3" mode first. DALL-E 3 is automatically activated in ChatGPT 4 when you ask it to draw or picture something.

In order to maximize the potential of ChatGPT 4 use, you should understand what plugins are.



Asking DALL-E 3 to picture the sun

**Plugins in ChatGPT 4** are additional software or tools that you can activate to enhance its capabilities or add new features.

With plugins, you can access the Internet or documents, that is not possible in ChatGPT 3.5.

A maximum of three plugins can be activated per session. To do this, you need to go to the gallery of plugins and select the

**Plugins in  
ChatGPT 4**  
/additional  
chatbot  
modules/

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

ones you need, then activate them and start a conversation. Then ChatGPT 4 will automatically choose which of the enabled plugins to use.

**Step 1** Log in to the chat. Click on "ChatGPT 4" in the top left corner.

ChatGPT 4 ▾



Чим я можу тобі допомогти сьогодні?

Допоможи мені вчитися  
словниковий запас для вступного іспиту до коледжу

Покажіть мені фрагмент коду  
липкого заголовка веб-сайту

Порівняйте маркетингові стратегії  
для сонцезахисних окулярів для покоління Z і мілені...

Розробіть контент-стратегію  
для інформаційного бюлетеня з безкоштовними міс...

🔒 Повідомлення ChatGPT...

ChatGPT може робити помилки. Перевірте важливу інформацію.

**Step 2** Select the "Plugins" section.

ChatGPT 4 ▾

🔧 ГПТ-4  
З DALL-E, переглядом і аналізом  
Обмеження 40 повідомлень / 3 години

🔧 GPT-3.5  
Чудово підходить для щоденних завдань

🔧 Плагіни



Чим я можу тобі допомогти сьогодні?

Допоможи мені вчитися  
словниковий запас для вступного іспиту до коледжу

Покажіть мені фрагмент коду  
липкого заголовка веб-сайту

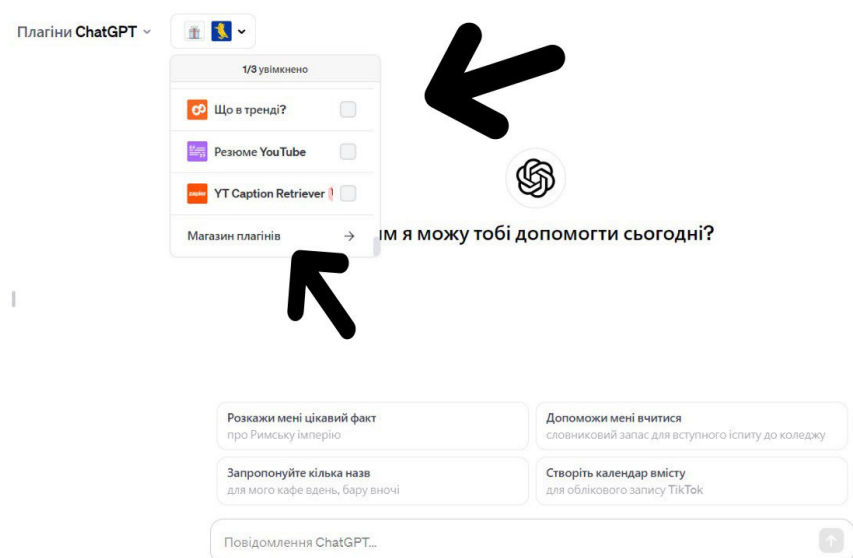
Порівняйте маркетингові стратегії  
для сонцезахисних окулярів для покоління Z і мілені...

Розробіть контент-стратегію  
для інформаційного бюлетеня з безкоштовними міс...

🔒 Повідомлення ChatGPT...

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

**Step 3** Select a maximum of three plugins that you would like to use. If you don't have the plugin you need, just download it from the plugin store.



**Bard** is a large language Google AI model trained on a huge amount of text data. Bard can generate text, translate, analyze photos, write different types of creative content, and answer your questions in an informative way. Its advantage is that it is completely free and can access the internet, unlike ChatGPT. It can also analyze an uploaded picture, describe what it depicts and afterwards have a dialog with you about it.

**Claude AI** is an AI chatbot developed by Anthropic. Its advantage is the ability to analyze extremely large amounts of information, so it can easily handle complex tasks. It can process texts of almost 75,000 words, which is essentially entire books. Claude AI is not completely free. The free version has limitations that may be inconvenient for some users. With a paid subscription, you can get rid of these limitations and get access to additional features, such as priority access during high traffic periods, and new features. The cost of paid subscriptions starts from \$20 per month.



# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

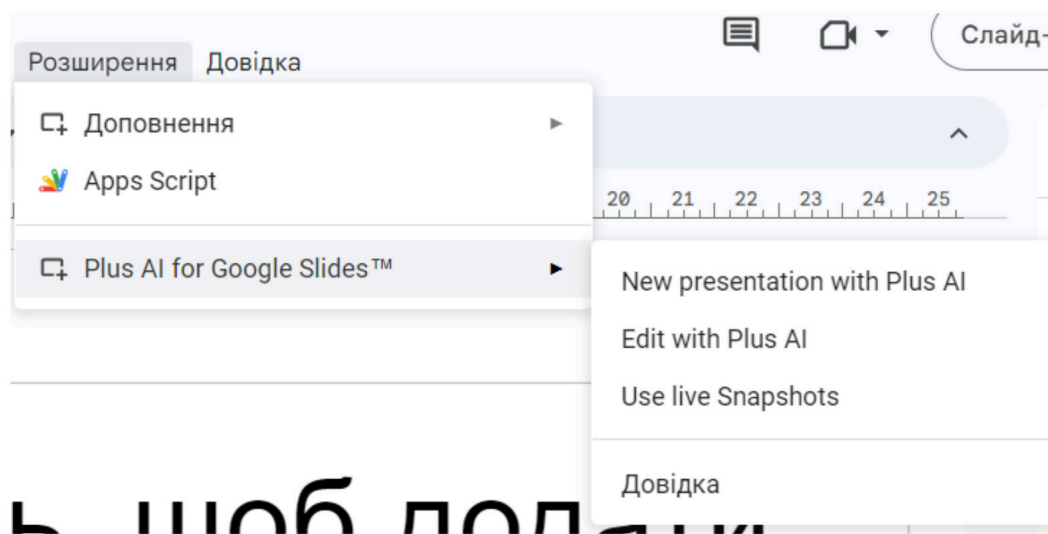
## CREATING PRESENTATIONS

### Plus AI for Google Slides

This is a Google Slides extension where AI helps you generate and edit a presentation in a few minutes. To use it, you need to download the Plus AI for Google Slides extension from [Google Workspace Marketplace](#). After that, select the "Extension" icon and click on "Plus AI for Google Slides".

You can then select one of three functions:

- Create a presentation using AI
- Edit a presentation using AI
- Use Snapshots (so-called live screen shots of any software or website that are automatically updated).



To create a presentation in Google Slides with AI, you need to write text for the slides (up to 5 thousand characters) as well as a description of the presentation itself (up to 5 thousand characters). When preparing the description, you can choose one of the suggested presentation style options and the AI will automatically generate a description, such as an online course, webinar, or a client offer. If you want, you can immediately give the structure of the presentation by inserting your text into individual slides. In this extension, you can write in which style the text you provide should be processed, for example "write the text in a business writing style". You can also choose the number of slides.

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

Once you have entered all the necessary data and clicked the "generate" button, you will get the presentation you need in a few minutes. In the free version, you can generate a total of three presentations. To generate more presentations, you need to purchase a paid subscription starting at \$10, and to be able to add more than 5 thousand characters, you need to sign up for a [subscription](#) - \$20 per month.

## CREATING DIAGRAMS

In order to quickly create diagrams, you can use a ChatGPT **Show me diagram** plugin. In ChatGPT 4, you need to enable the necessary plugin and write a request to generate a diagram: you need to paste the used information into the dialog. In just a few seconds, you will receive a diagram that you can open in full screen mode or edit. If you want to improve the diagram, you can use the keyword "show ideas" and get "ideas" on how to do it. To learn about other diagram types and languages, you should use the keyword "explore diagrams". Users of paid ChatGPT subscription can use the application for free.

## WATCHING AND ANALYZING VIDEOS

### [Summarize.tech](#)

If you don't have time to watch YouTube videos yourself, you can task the AI to do it and quickly figure out if a long video is worth watching. To do this, you need to paste a link to the video into [Summarize.tech](#), and it will generate basic information from it. In the free version, Summarize.tech has a limit on the number of videos per day. However, you can download Summarize.tech Premium. It has no daily limit, and you can summarize up to 200 videos per month. The cost is \$10 per month.

## TRANSCRIBING AND RECOGNIZING TEXT

### [Otter.ai](#)

This audio and video file transcription tool uses machine learning to summarize all kinds of meetings. After recording the

## USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

audio, you can chat with the AI assistant and ask any questions regarding the transcribed conversation. It supports over 60 languages and can transcribe both clear audio and audio with noise. Otter.ai can write notes as well as summarize what was said. The application has a free trial period of 7 days, after that the subscription cost will be \$10 per month.

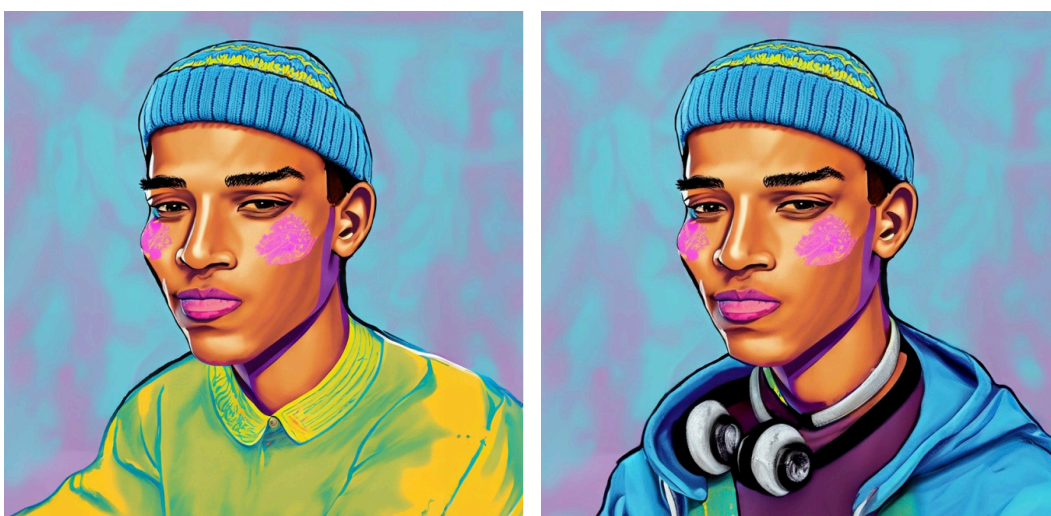
### CREATING, EDITING AND PROCESSING PHOTOS AND VIDEOS

#### Adobe Firefly

This is a tool that you can use to replace part of an image with whatever you want. For example, you don't like that you are wearing a T-shirt in the photo. Just write a prompt asking to replace the T-shirt with a shirt, and it will do it pretty well. If you need to display the text in the picture in a non-standard way, you can ask to generate any fill of any texture.

If you want to change the background of an image, you can use the generative fill tool, write what background you want to change to, and it will be automatically generated in your picture or photo.

Now Adobe Firefly is free to try, but the number of attempts is limited. With this example, you can see how easy it is to replace one piece of clothing with another



Source: website [Adobe Firefly](#)

## USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

In **Adobe Firefly**, you can also remove an object from a video and replace it with another. This feature is a recent addition. A paid subscription to Adobe Creative Cloud, which covers all Adobe products, each with AI tools, costs \$35.99 per month if you buy an annual subscription. However, if you're a student, indicate that when selecting a paid subscription and it becomes \$23.99 per month if you purchase an annual subscription.



Source: footage from a [video about the Adobe Firefly](#)

### **Midjourney**

This is an application where you can create images using a text prompt. In order to create an image, you need to download Discord, as all images are generated there. For those who are new to Discord, it is a messaging platform where you can share videos, voice, text messages or publications and communicate using your voice simultaneously with large groups of people. If you want to get free generation hours, you can use the option in the application itself: to do so, you need to select **"rate images"** section and rate the images placed there. Thus, you can get free generation hours for 30 days. When rating, you should choose the image you like the most, because the rankings are based on personal preferences.

### **Runway**

This is an application where you can "liven up" a photo and make the character in the photo start moving. You can also

# USING ARTIFICIAL INTELLIGENCE TOOLS IN THE WORK OF CIVIL SOCIETY ORGANIZATIONS

**generate** a 3D object based on a text prompt and change it. A free version that can generate three videos is available. The cost of paid subscriptions starts from \$15 per month.

## Captions

This is an application where the AI may be used to focus the person's gaze in the frame on the camera during the video. Even if the person was not looking at the camera but reading text instead, the AI will change this. To do this, you need to go to the settings in the application and turn on "eye contact". You can also add subtitles to the video or automatically translate and voice the text in any language. However, the application does not yet perform this function perfectly well. A paid subscription costs from \$6.99 per week.

## CREATING LOGOS, ICONS

### Design AI

An AI application that will independently create a logo for you. To do this, you need to select a sector, a style, and enter the required name. The AI analyzes your design needs and gives you the result. There is a free version of the application. The subscription costs from \$10 per month.

### Ideogram

A free application that generates images, logos, and spells text correctly unlike the well-known Midjourney. You can choose the style in which the result will be generated as well as the format, such as 10:10, 1:1, 16:10.

# DEEPPFAKE: WHAT IS IT AND HOW DOES

Based on the points of:  
**Igor Rozkladai,**  
Chief Media Lawyer,  
CEDEM Deputy Director

With the help of AI, after processing and analyzing a large amount of audiovisual information, it is possible to create videos and pass them off as authentic. Such "fake" video or audio is called **deepfake**.

There are three main ways to create a deepfake:

- 1 The real face in the video is swapped with another;
- 2 The mouth area kinesis on the real face is matched with another audio recording;
- 3 The mouth area kinesis on the real face is matched with another audio recording.<sup>8</sup>

All these methods are based on the technology of deep learning algorithms. If a rather big database of visual data has been collected, one image may be superimposed on another with the help of AI algorithms. And if you have access to a lot of audio data, you can "read" a text in a different voice. Neural networks can make this superimposition quite realistic – this is an important feature of many deepfakes.

<sup>8</sup> Media reality in the deep fake style // [Detector Media](#)

### USE

What can such technology be used for? According to Igor Rozkladai, "deepfake technology is not bad – it is just a tool". He calls **Salvador Dali's deepfake**, created in the museum in his honor, an example of a positive use. Thanks to it, visitors can watch videos of the famous artist and even take selfies with him. And "My Heritage", a genealogy research portal, with the help of **Deep Nostalgia** tool, allows you to generate a moving image of your deceased relatives on the basis of just one photo.



Image generated with Mojo AI

## DEEFAKE AND SHALLOWFAKE

CSOs could also put deepfake technology to work. For example, "revive" a historical figure to spread public awareness about a particular issue (for example, Lesia Ukrainka could talk about the violation of women's rights in Ukraine)<sup>9</sup>. CSOs that interact with foreign partners or audiences can use applications translating videos into another language. One of them is **Caption. AI**. "Useful" deepfake videos that can be created with it are still imperfect, but this technology is certain to be further developed in the future.

It is clear that deepfake technology is most often associated with danger: deepfake can be used to mislead people. It is quite easy and effective to replace the words of public figures: because there is a lot of their audiovisual data in the public domain, while the influence of such people is high. In March 2022, Ukrainians could see a poor and unsuccessful example of such an attempt to mislead, when representatives of the Russian Federation created a **video clip**, in which Zelenskyy was allegedly suggesting Ukrainian citizens to surrender. For many reasons, this video did not achieve its goal of destabilizing the situation in the country, but under other conditions and with better created image and audio the deepfake could indeed be a threat.

Not only deepfake videos but also audios can be threatening. For example, in 2021, malefactors in the UAE used deepfake technology to spoof the voice of a bank director and forced the manager of that bank to make a \$35 million transfer to a fake bank account<sup>10</sup>.

Another dangerous use of deepfake is fake porn videos. Their popularity is associated with 2017, when deepfake porn with famous actresses began to appear online en masse<sup>11</sup>. According to Sensity AI data for 2019, 96% of deepfake porn videos were created without the consent, and 99% of these videos contained images of women<sup>12</sup>. According to NBC, they recorded offers on the Discord social platform to create a 5-minute deepfake porn video "on demand" for \$65<sup>13</sup>. Such videos violate the rights of the people whose faces were used, they are deeply traumatic, abusive and can lead to harassment and threats<sup>14</sup>.

9 In particular, in December 2023, the Ukrainian Institute and Ukrainian AI company Reface released an AI video in which [William Shakespeare and Lesia Ukrainka "talk" to each other about associations](#)

10 Delić, Danka. The deepfake technology behind a \$35 million bank heist in Hong Kong // [ProPrivacy](#)

11 Johnson, Dave and Johnson, Alexander. What are deepfakes? How fake AI-powered audio and video warps our perception of reality // [INSIDER](#)

12 Dunn, Suzie. Women, Not Politicians, Are Targeted Most Often by Deepfake Videos // [Centre for International Governance Innovation](#)

13 Mahdawi, Arwa. Nonconsensual deepfake porn is an emergency that is ruining lives // [The Guardian](#)

14 Middleton, Amber. A Twitch streamer was caught watching deepfake porn of women gamers // [INSIDER](#)



## WHAT IS A SHALLOWFAKE?

**Shallowfake** is it, when media content that does exist is slightly adjusted.

It's worth noting that machine learning is expanding opportunities for fakes rather than creating them. Unlike deepfake, you don't need to use deep machine learning technology to create a shallowfake, just basic editing is enough. That is why shallowfake is also called a "cheap fake", although some experts believe that such fakes may still pose a threat that is not less than deepfake<sup>15</sup>.

For instance, you can create a product in which the video sequence is true, but the audio sequence is not. An example of such shallowfake is the [video](#) of Nancy Pelosi, Speaker of the U.S. House of Representatives where a slow-motion audio recording of her voice was superimposed on the real video. This is how the authors of the fake wanted to make the viewers think that Nancy Pelosi was drunk in the video.

An even more primitive shallowfake is simply "pulling out" a video excerpt out of its broader context<sup>16</sup>. In 2022, a [video excerpt](#) in which President Zelenskyy was allegedly telling citizens of NATO member states that their children would go to war and die, gained some popularity. In fact, it was about a hypothetical attack on the Baltic States in case of Ukraine's defeat, not about the Russian-Ukrainian war. However, that part has not been included in the fragment shared by US congressmen who oppose aid to Ukraine.

## HOW DO WE IDENTIFY A DEEPPFAKE?

Videos generated today can resemble the real things quite a bit, indeed. The technology is still not perfect, though it has improved significantly over the last six years. There are a number of signs by which you can usually identify a deepfake. [Detector Media](#) suggests paying attention to such eight signs:

- Flickering on the face
- Face and body mismatch (often only the face is substituted)

<sup>15</sup> Johnson, Bobbie. Deepfakes are solvable — but don't forget that "shallowfakes" are already pervasive // [MIT Technology Review](#)

<sup>16</sup> TLeetaru, Kalev. The Real Danger Today Is Shallow Fakes And Selective Editing Not Deep Fakes // [Forbes](#)

# DEEFAKE AND SHALLOWFAKE

- Source of video publication (it may be unverified)
- Sound of the recording and its asynchronization with facial expressions
- Implausible facial expressions in the mouth area (it is one of the most difficult to reproduce)
- Length of the video (it is difficult to make a very long deepfake)
- Details when slowing down the video (you need to pay attention to the background)
- Implausible blinking or its absence

There are other ways to identify a deepfake. For example, you can search the internet for keywords from a video – and in the case of deepfake, a video search may be simply null. In addition, if a screenshot of the video is taken and uploaded into internet search, you may find the original video used for making the deepfake, while the upload date of this video is likely to be different from that of the deepfake video<sup>17</sup>.

When it comes to audio, George Hatcher, founder of White Knight Labs cybersecurity consultancy, advises paying attention to such signs as broken sentences, oddly chosen words, and unusual phrasing and tone of voice<sup>18</sup>. Another indicator can be "strange" and "suspicious" accents in an audio track.

## HOW DO WE IDENTIFY A SHALLOWFAKE?

Depending on the type, you should pay attention to various details such as:

- Strange or different backgrounds and lighting, unnatural variations in colors and shadows
- Any signs of editing: audio splices, inconsistencies between different objects, unnatural elements indicating the use of Photoshop<sup>19</sup>.

The general rule should be a critical perception of any information: searching for the sources of its origin and reflecting on whether manipulation could be the purpose of this information appearance.

<sup>17</sup> How to spot a deepfake // [CNA Insider](#)

<sup>18</sup> Lawton, George. How to prevent deepfakes in the era of generative AI // [Techtarget](#)

<sup>19</sup> Randall, Natalie. The rise of shallowfakes // [Chartered Insurance Institute](#)

## WHAT SHOULD CSO LEADERS, ACTIVISTS, AND VOLUNTEERS WHO HAVE BECOME VICTIMS OF DEEFAKE DO?

First, the current Ukrainian legislation stipulates the right of reply and refutation (Article 43 of Law of Ukraine "On Media"). Pursuant to this law, *"a person who believes that an actor in the sphere of audiovisual, print or online media has disseminated information about them that does not correspond to reality (incompletely or inaccurately stated) and defames their honor, dignity or business reputation, shall have the right to demand retraction of inaccurate information or exercise the right to reply"*.

However, a great many Ukrainians now consume news from social media. According to a study conducted by the "Rating" sociological group, in February 2023, 41% of Ukrainians received socio-political news from groups and channels in Telegram, Viber; 35% – from social media (Facebook, Twitter, Instagram). And the USAID-Internews survey, which took place in November 2022, showed that social media outlets were a source of news for 74% of Ukrainians<sup>20</sup>. In other words, the popularity of social media is comparable to the popularity of national television and Internet pages, from which 43% and 36% of Ukrainians learn news, respectively<sup>21</sup>. According to a study commissioned by the Opora NGO, social media outlets are a source of information for 77.9% of Ukrainians, while television and the Internet (excluding social media) – for 62.5% and 57.7%, respectively<sup>22</sup>.

However, Igor Rozkladai claims that it is extremely difficult to exercise the right of reply in social media. In addition to legal difficulties, such as identifying the person who disseminated the information, we also face technical ones.

Since social media drive us into "bubbles" according to our interests, it is not certain that your response to inaccurate information in your profile will cover the same "bubble" that was covered by the person who disseminated this information about you. So, you should get a court ruling to oblige the person to disseminate the reply in the same way that the false information was disseminated. In addition, Igor Rozkladai notes that due to the high speed of information dissemination, there is an unspoken rule "whoever first disseminated information is right". Online resources do not work in the same way as conventional media, they involve reposts (including cross-platform ones). Therefore, even if a court

<sup>20</sup> USAID-Internews survey on media consumption // [Ukrinform](#)

<sup>21</sup> Melnyk, Roman. During the year of war, there has been a 4-fold increase in consumption of news from messengers by Ukrainians – research // [Detector Media](#)

<sup>22</sup> Media consumption among Ukrainians: The second year of the full-scale war. OPORA survey // [OPORA](#)

## DEEFAKE AND SHALLOWFAKE

obliges a person to publish a retraction of information about you in the blog, there is no guarantee that the same audience that saw the first post will see this retraction. First of all, because then every person who reposted the original post should be obliged to also repost the retraction.



Image generated with DALL-E

Therefore, one of the most effective solutions for social media is crisis communication – the ability to deliver certain messages quickly and on time. What is worthy to be particularly remembered is the rule of three hours for the first reaction, the rule of twenty-four hours for the second reaction, the rule not to make excuses, but to defend your position. According to Igor Rozkladai, for social

media such mechanisms are now more effective than legal ones, because the speed of information dissemination is so high that no court will provide a timely response: legal proceedings are much slower.

Security protocols and personal data use culture, e.g. not sharing your data with outsiders, can help prevent the collection of data about you that can then be used to create fakes. In addition, CSOs should have clear protocols for making payments: with authentication and mandatory involvement of written communication.

### WE STRONGLY RECOMMEND:

- in case of **audiovisual, print or online media** —  
– it is worth exercising the right of retraction or right of reply stipulated by Law of Ukraine "On Media". And in certain cases, be prepared to give a live response, even without filing a complaint.
- in case of **social media** – you should quickly communicate the message you need to refute false information.
- You should have **clear, robust, unquestionable security protocols** (on internal communication, data usage, etc.).

## HOW DO SUCH CAMERAS WORK?

Based on the points of:  
**Francesca Fanucci,**  
Senior Legal Advisor  
European Center for Not-for-Profit Law (ECNL)

**Facial Recognition Technology** (hereafter referred to as **FRT**) is built on the comparison of different images. First, it measures facial biometric data and then compares these data with a database it has access to.

This can be done in three ways:

- 1 Verification** (one-to-one matching) – the technology compares one face to another specific image.  
**Objective:** Establish that the person in the two images is the same person.  
**Application example:** FaceID function for iPhone unlocking, passport scanning during border control at the airport exit.
- 2 Identification** (one-to-many matching) – the technology compares one face to a set of other faces (biometric templates).  
**Objective:** Find out if the face matches one or more faces in the database.

**Application example:** CCTV systems (e.g. in shopping malls or other public places). This technology can also be used by the police.

**3 Classification** (matching based on common characteristics) – the technology analyzes the facial features of one or more persons based on certain characteristics (smile, laugh, frowned eyebrows, skin and eye color, skull structure).

**Objective:** Classify faces by features, i.e. identify certain emotions, gender, age, ethnicity, etc.

**Application example:** CCTV cameras on billboards analyzing emotions or cameras anticipating emotions / potential disruptions at public events.

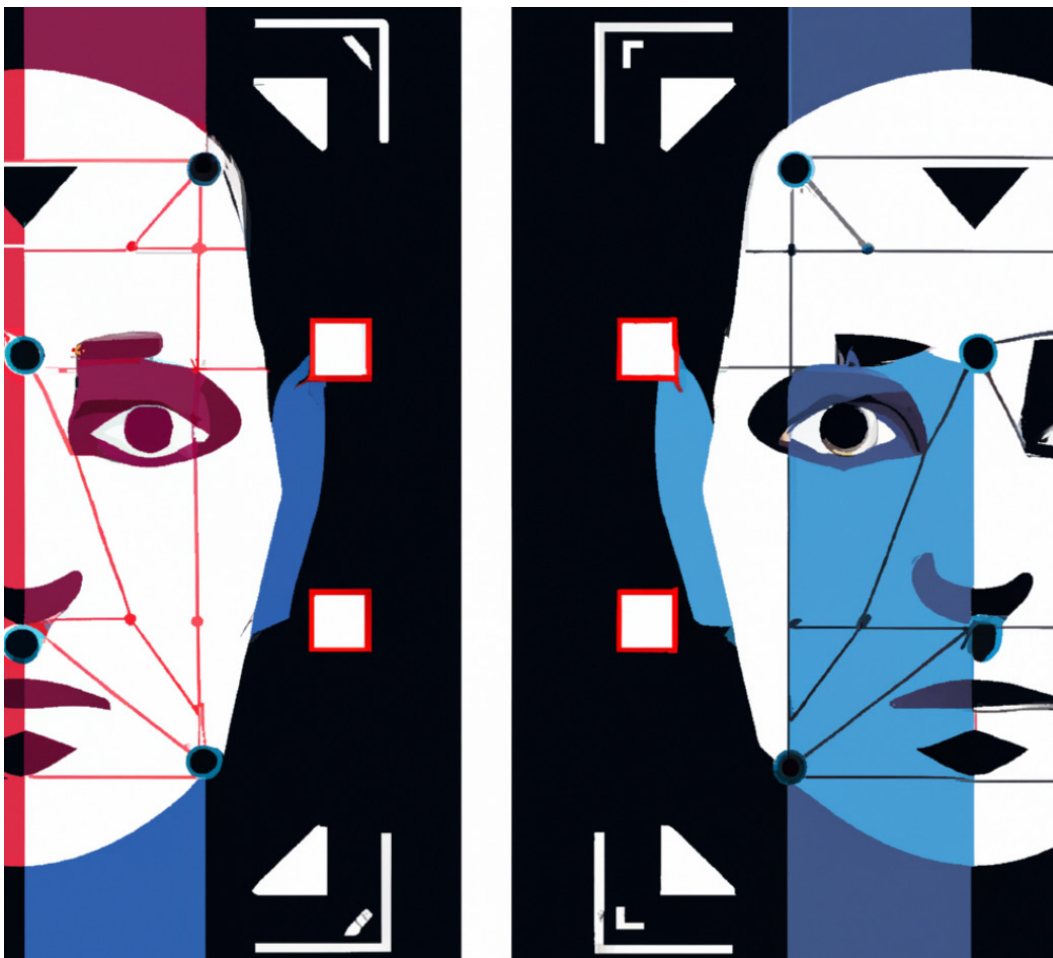


Image generated with DALL-E

# FACIAL RECOGNITION CAMERAS

**FRT consists of three stages. In the first stage,** statistical information is analyzed on the basis of AI algorithms. **Next, training** takes place on the basis of certain data sets (these can be images or biometric templates). After training, the technology becomes capable of identifying consistent patterns in images or biometric templates and recognizing similarities (these are special characteristics of AI – the ability to learn to identify trends, with a degree of autonomy and adaptation to circumstances). AI-powered FRT can operate in real time or retrospectively. That is, they can match images to a database live or even after a record has been created.

## WHERE ARE FACIAL RECOGNITION CAMERAS USED?

On the one hand, the use of facial recognition cameras can make people's lives easier or help solve crimes. For example, this technology is used to securely unlock smartphones – it was introduced in the Android operating system in 2015, and Apple launched it in 2017. It was facial recognition cameras that helped the US military identify Osama bin Laden in 2011<sup>23</sup>. In the US, such systems have recently been used in chain stores such as Walmart to identify shoplifters<sup>24</sup>.

Facial recognition cameras are already used in Ukraine. They are installed for the purpose of law enforcement: police officers claim that such cameras are allegedly effective in solving crimes<sup>25</sup>. New Orleans and Virginia, which imposed a ban on the use of FRT cameras in 2020, initiated a discussion to allow the use of such cameras to investigate serious crimes two years later<sup>26</sup>.

At the same time, in authoritarian China, the use of FRT cameras is becoming increasingly threatening. With the widespread use of these cameras (an estimated 200 to 600 million cameras in China as of 2020<sup>27</sup>), the Chinese government is using these cameras to discriminate against the Uyghur ethnic minority and even to publicly shame people, such as those whom the cameras spotted on the street in pajamas<sup>28</sup>. The government also uses these cameras to compile a so-called citizen trustworthiness index, which affects citizens' freedoms and their access to certain

23 Klosowski, Thorin. Facial Recognition Is Everywhere. Here's What We Can Do About It // [NYT Wirecutter](#)

24 Dastin, Jeffrey. Special Report: Rite Aid deployed facial recognition systems in hundreds of U.S. stores // [Reuters](#)

25 Facial recognition cameras are used in Ukraine now: How they work and who they are looking for // [Focus](#)

26 Metz, Rachel. First, they banned facial recognition. Now they're not so sure // [CNN Business](#)

27 Cadell, Cate. 'It seemed like fun, I decided to join in': Inside the biggest human surveillance experiment on the planet // [The Sydney Morning Herald](#)

28 Ng, Alfred. How China uses facial recognition to control human behavior // [CNET](#)



benefits<sup>29</sup>. In Russia, the use of FRT cameras is associated with the subsequent sale of personal data on the black market. The Russian government may well use them to combat peaceful protests and demonstrations, too<sup>30</sup>.

However, the use of this technology is not the problem associated only with authoritarian regimes. Democratic countries are now facing this challenge as well. Igor Rozkladai notes facial recognition cameras as one of the biggest threats in the field of AI that now exists for CSOs and the entire civil society.

## WHAT ARE THE RISKS ASSOCIATED WITH THE USE OF SUCH TECHNOLOGY?

According to Francesca Fanucci, Senior Legal Advisor at the European Center for Not-for-Profit Law (ECNL), the use of FRT in surveillance systems poses the following threats:

- **Potential for false positives in reporting and analysis** – the technology works with probabilities and can still get it wrong and start claiming similarities between different objects or people.
- **Possible bias and discrimination** – such systems are sometimes worse at recognizing black people, may not distinguish between people with disabilities or unusual appearances depending on the context (lighting, positioning, etc.).
- **Disincentive effect on assemblies/movements** – knowing that they can be identified, people will be less likely to come out to protests. This is especially (but not only) relevant to authoritarian regimes, such as China, where there is a so-called social rating system and the state, thanks to technology, can easily resort to repressive actions.

It is often unknown where the images from CCTV cameras may be stored, who will use them and for what purpose. If the data in the database was selected in a discriminatory manner, the results generated by such cameras will also be discriminatory. Sometimes the data sources used to train FRT can be of dubious origin, and the developers are reluctant to disclose information about the technology.

<sup>29</sup> Avdieieva, Tetiana. Is it legal to install face recognition cameras on city streets? // [Centre for Democracy and Rule of Law](#)

<sup>30</sup> Ibid

## FACIAL RECOGNITION CAMERAS

Therefore, Francesca Fanucci notes that the use of FRT has the potential to violate human rights, namely the following ones:

- Right to privacy
- Right to data protection
- Freedom of speech / expression / peaceful assembly
- Right to non-discrimination
- Right to dignity
- Right to human decision-making
- Right to access to information
- Right to appeal/access to an effective remedy

CSOs, particularly human rights organizations, must be aware of the scale of risks to human rights due to using the FRT. To prevent the violation of the rights of Ukrainian citizens, CSOs should focus attention on the use of these cameras. Unfortunately, this topic is currently relatively unpopular and poorly understood by the civic sector. However, it is time for Ukrainian CSOs to continue advocating for the regulation of such systems and help develop legislation that does not ignore this technology. This is what CEDEM is now actively pursuing. Another task of CSOs in this area is to prevent misuse of such technologies by state authorities, local self-government bodies, businesses, etc.

The Ukrainian authorities should also adopt robust laws that will be applicable to different ways of using FRT and involve civil society in assessing the impact of such cameras before they are used. The public should have the right to know where and why such cameras are used, how they work, and have the right to review decisions based on their use.

## UKRAINIAN EXPERIENCE

Based on the points of:  
**Tetiana Avdieieva,**  
Digital Security Lab lawyer

**In fact, Ukraine still lacks a proper national legislation that would regulate the use of FR cameras.**

There is a concept of AI development, but it barely mentions human rights, and there exists a similar problem with legislation in the field of law enforcement bodies and personal data protection. Neither technical standards nor legal safeguards for these technologies are in place today.

According to the lawyer, the law on personal data protection, in its current wording, is outdated for regulating AI-driven systems. For instance, the existing document does not comply with the **General Data Protection Regulation** and does not consider the peculiarities of new technologies.

Despite this, CCTV cameras were used in Ukraine as early as in 2021. They were mainly installed by municipal authorities (local self-government bodies through utility companies), however, as Tetiana Avdieieva notes, the law on local self-government bodies does not contain provisions that give them the authority to use or

## FACIAL RECOGNITION CAMERAS AND CCTV CAMERAS IN UKRAINE

authorize the use of any means of surveillance. Therefore, none of bylaws was based on the law, and their adoption was arbitrary on the part of local authorities.



Image generated with DALL-E

The problem of using CCTV cameras in Ukraine is not limited to the legal sphere. Another issue is technical competencies and the lack of sufficient number of technical experts who can assess new technologies. After all, if the necessary technological standards are not met, the system may become the target of hacker attacks, in particular from Russia. Currently, Ukraine does not have enough technical experts who can work with new technologies.

## FACIAL RECOGNITION CAMERAS AND CCTV CAMERAS IN UKRAINE

Sometimes this also refers to the use of potentially dangerous technologies. In Ukraine, the most widely used cameras are cameras by Chinese manufacturers Hikvision and Dahua. Analysts note that they may be vulnerable to hacking<sup>31</sup>. Moreover, such cameras may be affiliated with Chinese intelligence and literally help it spy abroad<sup>32</sup>. Given the cooperation between Russia and China, this vulnerability could pose a direct threat to Ukrainian citizens.

In this regard, Tetiana Advdieieva emphasizes:

**"One cannot justify situations in which additional threats to national security are created by the issue of national security."**



Image generated with DALL-E

<sup>31</sup> Mathews, Lee. Widely-Used Hikvision Security Cameras Vulnerable To Remote Hijacking // [Forbes](#)

<sup>32</sup> Kuprienko, Oleksii. OPINION: Trojan Horse: How Chinese-Made Cameras Put Ukraine at Risk // [Kyiv Post](#)

## FACIAL RECOGNITION CAMERAS AND CCTV CAMERAS IN UKRAINE

On the part of the authorities, there have already been alarming signals of using CCTV cameras. For example, after the protests in support of activist Serhiy Sternenko, representatives of the Ministry of Internal Affairs of Ukraine stated that the most active participants of the protests would be identified using facial recognition systems. This situation did not develop further, but the very fact of such statements is threatening.

The case of the Ukrainian government's use of Clearview AI technology to find Russian war criminals is open and public<sup>33</sup>. Clearview AI provides users with a facial recognition tool. There are several problems with this technology. The first is that the Clearview AI database is created by scanning photos of users of major social media without the consent of the users themselves. Due to this method of data collection, Clearview AI could have 30 billion images in its database as of April 2023<sup>34</sup>.

Clearview AI has been banned in the UK due to a problematic way of creating a database that violates the rights of social media users. French and Italian authorities fined the company for illegally collecting and processing the biometric data of their citizens. Despite this, more than 600 law enforcement agencies are known to be using Clearview AI in their work<sup>35</sup>.

But even setting aside the moral aspect of using Clearview AI, what is the legal status of evidence relying on this technology? And can its results serve as a sufficient basis for initiating proceedings against a person on the territory of Ukraine? According to Tetiana Avdieieva, if the courts adopt the position that such technology is admissible evidence, it may create a dangerous precedent. After all, the United States have already tried to prosecute on the basis of similar systems, and it turned out that the systems often produce false results. For example, in 2020, a man from Michigan, despite having an alibi, was wrongly arrested for stealing a computer because a facial recognition algorithm pointed out to him<sup>36</sup>.

Because of these and other problems, according to Tetiana Avdieieva, an approach to studying the issues associated with the use of facial recognition cameras in Ukraine should be sought now. They can have a direct impact on human rights and the safety of activists. In addition to the development of substantive regulation, it is worth paying attention to procedural regulation.

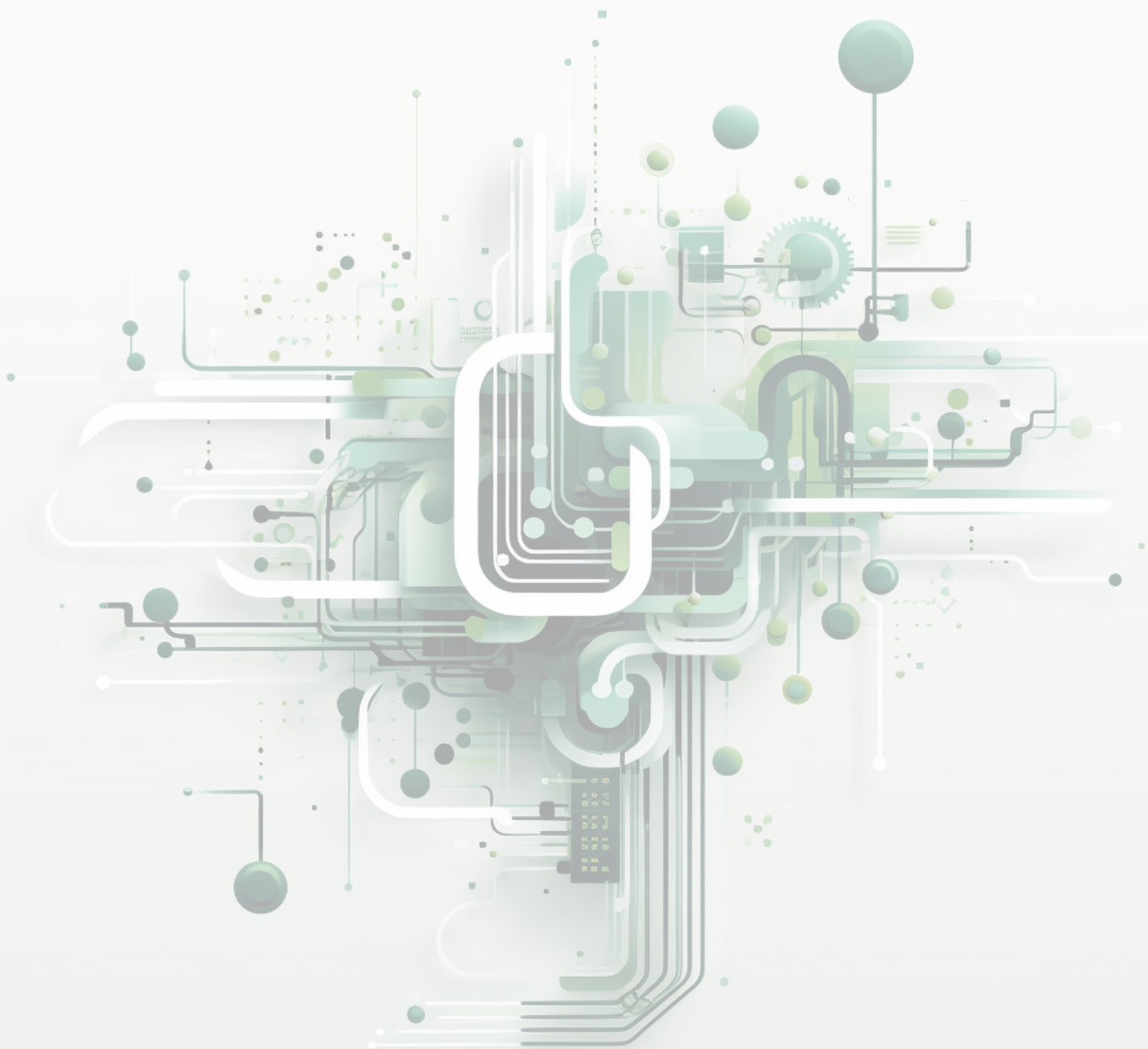
<sup>33</sup> Sabadyshyna, Yuliia. How Ukraine is using artificial intelligence to win. The Ministry of Digitization gives the details // [DOU](#)

<sup>34</sup> Balovsiak, Nadiia. Unequal partnership. Why cooperation between Ukraine and Clearview AI should not continue after the war // [Kunshyt](#)

<sup>35</sup> Ibid

<sup>36</sup> Hill, Kashmir. Wrongfully Accused by an Algorithm // [The New York Times](#)

# FACIAL RECOGNITION CAMERAS AND CCTV CAMERAS IN UKRAINE



## LEGAL ACTS ON FACIAL RECOGNITION

Based on the points of:  
**Francesca Fanucci,**  
Senior Legal Advisor  
European Center  
for Not-for-Profit Law (ECNL)

Francesca Fanucci identifies several legal acts related to facial recognition technology.

- The first one is the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (**Convention 108**). Ukraine is one of the signatory countries of this Convention. In 2021, the Council of Europe additionally issued the **Guidelines on Facial recognition** under Convention 108.

According to this Convention, States must adopt a robust legal framework applicable to the various uses of facial recognition technology. Francesca Fanucci particularly notes the following key points:

- The specific use and intended purpose of the technology;
- Minimum levels of reliability and accuracy of the algorithms used;
- Duration of storage of the acquired images;
- Minimization of processed data (irrelevant data should be



## LEGAL REGULATION OF THE FACIAL RECOGNITION CAMERA USE

minimized – for example, we need to blur out faces that are not necessary for the analysis);

- Process openness criteria;

The guaranteed right to information, the right to access, the right to knowledge of the underlying arguments, the right to object, the right to rectification.

Limitations to these principles must not violate the essence of the rights and must meet the criteria of the "three-part test": legality, necessity, and proportionality. In addition, the CoE recommendations refer to the possibility of imposing a moratorium on the use of FRT pending a full analysis and democratic debate on the technology.



Image generated with DALL-E

# LEGAL REGULATION OF THE FACIAL RECOGNITION CAMERA USE

- **OSCE Guidelines on Freedom of Peaceful Assembly** (2019)

According to these principles, "the use of image recording for the purpose of identification (including facial recognition software) should be confined to those circumstances where criminal offenses are actually taking place, or where there is a reasonable suspicion of imminent criminal behavior."

- **European Council Guidelines on the use of facial recognition technology in the area of law enforcement** (2022)

According to this document, it is necessary to assess the effect the use of this technology has on all human rights, for instance, to test for absolute necessity and proportionality and to make the results or main findings public. You should also always apply the mentioned principle of data minimization. It is prohibited to process personal data if that processing relies on a database populated by means of mass collection of personal data – for example, by "scraping" (collecting or extracting data) photographs and facial images available online.

- **Artificial Intelligence Act**, which raises the issue of face recognition.

At the time of writing of this Guide, Article 5 of this Act prohibits Remote Biometric Identification (RBI) systems that operate in real time in publicly accessible locations for the purpose of law enforcement activities other than the targeted search for victims of a crime, the prevention of a terrorist attack, and the tracking down of the perpetrator of a crime. However, Article 5 of the Draft Law is expected to be amended.

- **Joint Opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on the proposal for Artificial Intelligence Act** (2021)

It calls for a blanket ban on any use of AI for automated recognition of human features in public places – including FRT – in any context.

This approach is explained by the lack of transparency about how these systems work and how the data is processed and the fact that "The use of AI systems can create serious problems in terms of proportionality, as it may involve processing the data of an arbitrary and disproportionate number of data subjects to identify only a few persons".

The position of the EDPB and EDPS is that "Irreversible serious impact on the (reasonable) expectations of the public

## LEGAL REGULATION OF THE FACIAL RECOGNITION CAMERA USE

regarding anonymity in public places, leading to a direct negative impact on freedom of expression, assembly, association as well as freedom of movement".

### USE OF DANGEROUS TECHNOLOGIES DURING MARTIAL LAW

After all, Ukraine is at war and martial law is in effect. For such cases, there are international standards for derogation during a state of emergency. In accordance with the UN Human Rights Committee's **General Comment 29** to Article 4 of the International Covenant on Civil and Political Rights, procedures for derogation from certain provisions of this document are provided for during a state of emergency.

However, measures derogating from the provisions of the Covenant must be of an exceptional and temporary nature. They are only authorized if the situation poses a threat to the life of the nation, and the measures themselves must be based solely on the urgency of the situation.

The use of CCTV cameras threatens human rights. However, as Francesca Fanucci points out, if they are used during a state of emergency, it is still worth trying to ensure the preservation of human rights. It is possible to establish limiting provisions, for example, to record that these technologies are used to identify the military, and after the end of martial law, the cameras will be removed, and this practice will be stopped. According to the expert, the invasiveness of similar technologies should be taken into account and a balance should be struck: protecting the population on the one hand and protecting human rights on the other.

In addition, the derogation procedure during a state of emergency is covered by Article 15 of the **European Convention on Human Rights**: "In time of war or other public emergency threatening the life of the nation, any High Contracting Party may take measures which are inconsistent with its obligations under this Convention, solely within the limits necessitated by the exigencies of the situation, if such measures are not inconsistent with its other obligations under international law".

But, as Francesca Fanucci notes, full transparency should be ensured when using such a procedure: clearly indicating which rights we are restricting and for how long, and subsequently assessing the appropriateness of the restrictions from time to time.

## INSIGHTS OF CEDEM:

- Olha Petriv  
Artificial intelligence and copyright  
ChatGPT – a Russian propaganda consumer:  
How do we fight it?  
Artificial Intelligence: Time for a legal framework  
Artificial Intelligence and Disinformation:  
The (in)visible threat in modern world
- Olena Sokolova  
Artificial Intelligence Regulation: USA experience
- Tetiana Avdieieva  
Is it legal to install face recognition cameras  
on city streets?



## OTHER MATERIALS:

- Arnold. What Is The Difference Between A Deepfake And Shallowfake? // [DeepFakeNow](#)
- Johnson, Dave and Johnson, Alexander. What are deepfakes? How fake AI-powered audio and video warps our perception of reality // [INSIDER](#)
- Sample, Ian. What are deepfakes — and how can you spot them? // [The Guardian](#)
- 4 Types of AI: Getting to Know Artificial Intelligence // [Coursera](#)
- Hsu, Tiffany. As Deepfakes Flourish, Countries Struggle With Response // [The New York Times](#)
- The state of AI in 2022 — and a half decade in review // [McKinsey & Company](#)
- Klosowski, Thorin. Facial Recognition Is Everywhere. Here's What We Can Do About It // [NYT Wirecutter](#)
- Media reality in the deep fake style // [Detector Media](#)
- Johnson, Bobbie. Deepfakes are solvable — but don't forget that "shallowfakes" are already pervasive // [MIT Technology Review](#)
- Sanchez, Conor. Civil society can help ensure AI benefits us all. Here's how // [World Economic Forum](#)
- Sheehan, Jared and Chappell, Nathan. The State of Artificial Intelligence in the Nonprofit Sector: Ethical Considerations // [NonProfitPro](#)
- Balovsiak, Nadiia. Unequal partnership. Why cooperation between Ukraine and Clearview AI should not continue after the war // [Kunsht](#)
- Vu. The Ethics and Opportunities of Artificial Intelligence in the Nonprofit Sector // [Nonprofit AF](#)
- How to spot a deepfake // [CNA Insider](#)

# ACKNOWLEDGMENTS TO THE SPEAKERS OF THE FORUM

The Centre for Democracy and Rule of Law would like to thank the U.S. Agency for International Development and the Government of Sweden, Initiative Center to Support Social Action "Ednannia", and the Digital Security Laboratory for the opportunity to organize and host the "Artificial Intelligence 2.0: Regulations and Work in the Times of War" Annual Forum.

Special thanks go to the speakers of "Artificial Intelligence and Civil Society Organizations" panel discussion:

- **Olesia Kholopik**, CEDEM Director
- **Igor Rozkladai**, Chief Media Lawyer, CEDEM Deputy Director
- **Francesca Fanucci**, Senior Legal Advisor at ECNL
- **Tetiana Avdieieva**, lawyer at Digital Security Laboratory
- **Veronika Boiko**, Head of the Social Division at YouControl, expert of the Open Data Association
- **Olha Petriv**, Lawyer at CEDEM Independent Media Division

as well as to **Maria Heletiy**, the panel discussion moderator, "Ukraine Civil Society Sectoral Support Activity" Deputy Project Manager, Initiative Center to Support Social Action "Ednannia".

**"Artificial Intelligence 2.0: Regulations and Work in the Times of War"** Forum was held thanks to all the speakers and panelists, to whom we are sincerely grateful for the high level of expertise and discussion:

- **Olha Siedova**, Head of National Programs at the Embassy of Sweden in Ukraine
- **Olesia Kholopik**, CEDEM Director
- **Vita Volodovska**, Head of the Digital Security Laboratory
- **Teresa Ribeiro**, OSCE Representative on Freedom of the Media
- **Karolina Ivanska**, Digital Rights Advisor at ECNL
- **Daniel Leufer**, Senior Policy Analyst at AccessNow
- **Hordii Rumiantsev**, Chief Specialist of the Expert Group

# ACKNOWLEDGMENTS TO THE SPEAKERS OF THE FORUM

on Protection of Children's Rights on the Internet of the European Integration Directorate of the Ministry of Digital Transformation of Ukraine

- **Lilian Edwards**, Professor of Law, Innovation and Society at Newcastle University
- **Vitalii Honcharuk**, investor at AIV Lab
- **Tetiana Avdieieva**, lawyer at Digital Security Laboratory
- **Aliona Romaniuk**, founder of the NotaEnota project, factchecker
- **Ihor Solovei**, Head of the Centre for Strategic Communications and Information Security
- **Deniz Wagner**, Adviser to the Office of the OSCE Representative on Freedom of the Media
- **Volodymyr Behei**, Chief Specialist of the Expert Committee on Artificial Intelligence Development of the Ministry of Digital Transformation of Ukraine
- **Andrii Labun**, Head of the Department of Analytics and Organization of Personal Data Protection of the Human Rights Department of the National Police of Ukraine
- **Vitalii Miniailo**, CEO of IT company Neurotrack.tech and EON+ applied machine learning laboratory
- **Mykola Pechenizkyi**, Professor, Department of Mathematics and Computer Science, Eindhoven University of Technology, Netherlands
- **Julia Haas**, Assistant Project Manager, Office of the OSCE Representative on Freedom of the Media
- **Kateryna Kruk**, Head of Public Policy for Central and Eastern Europe at Meta
- **Maksym Dvorovyi**, Head of Digital Rights at the Digital Security Laboratory
- **Chantal Joris**, lawyer at ARTICLE 19

## ACKNOWLEDGMENTS TO THE SPEAKERS

- **Taras Shevchenko**, Deputy Minister for European Integration, Ministry of Culture and Information Policy of Ukraine

CEDEM would like to thank the forum moderators :

- **Tetiana Avdieieva**, lawyer at Digital Security Laboratory
- **Maksym Dvorovyi**, Head of Digital Rights at the Digital Security Laboratory
- **Igor Rozkladai**, Chief Media Lawyer, CEDEM Deputy Director

This guide for CSOs is compiled by:

- **Anna Isichko**, CEDEM Deputy Director
- **Volodymyr Kudelia**, CEDEM Project Manager.



# TEAM CONTACTS OF ORGANIZATIONS IMPLEMENTING THE UKRAINE CIVIL SOCIETY SECTORAL SUPPORT ACTIVITY PROJECT

## **Initiative Center to Support Social Action "Ednannia"**

Phone: +38 044 201 01 60 (61)

E-mail: [office@ednannia.ua](mailto:office@ednannia.ua)

Website: <http://ednannia.ua/>

## **Ukrainian Center for Independent Political Research (UCIPR)**

Phone: +38 044 227 54 20, +38 063 234 74 40

E-mail: [ucipr@ucipr.org.ua](mailto:ucipr@ucipr.org.ua)

Website: <http://www.ucipr.org.ua/>

## **Centre for Democracy and Rule of Law (CEDEM)**

Phone: +380 67 828 20 74

E-mail: [info@cedem.org.ua](mailto:info@cedem.org.ua)

Website: <https://cedem.org.ua/>

## VIDEOS AND BROADCASTS

Recording of the "**Artificial Intelligence and Civil Society Organizations**" panel discussion in Ukrainian:



Recording of the "**Artificial Intelligence and Civil Society Organizations**" panel discussion in English:



Video of the first day of the "**Artificial Intelligence 2.0: Regulations and Work in the Times of War**" Annual Forum:





# ARTIFICIAL INTELLIGENCE TOOLS GUIDE FOR CSOS

BASED ON THE MATERIALS  
OF “ARTIFICIAL INTELLIGENCE AND CIVIL SOCIETY  
ORGANIZATIONS”  
PANEL DISCUSSION,  
"ARTIFICIAL INTELLIGENCE 2.0: REGULATIONS AND  
WORK IN THE TIMES OF WAR" ANNUAL FORUM

KYIV  
2024