UKRAINE La Strada

GOVERNMENT COMMISSIONER for Gender Equality Policy of Ukraine

STOP RAPE NOW UN ACTION AGAINST SEXUAL VIOLENCE IN CONFLICT

UN WOMEN

FOR ALL WOMEN AND GIRLS

# ANALYTICAL REPORT

# TRAFFICKING IN PERSONS FOR THE PURPOSE OF SEXUAL EXPLOITATION IN UKRAINE

## increased vulnerability of women and girls associated with Russia's war against Ukraine and the use of cyberspace by human traffickers

# ANALYTICAL REPORT

# TRAFFICKING IN PERSONS FOR THE PURPOSE OF SEXUAL EXPLOITATION IN UKRAINE

## increased vulnerability of women and girls associated with Russia's war against Ukraine and the use of cyberspace by human traffickers

**Kyiv 2025**

Prepared by UN Women Ukraine and the civil society organization “La Strada-Ukraine” with the support of UN Action Against Sexual Violence in Conflict (https://www.stoprapenow.org/). UN Action supports implementation of the UN Interagency Project ‘Strengthening national and community-based CRSV prevention and response mechanisms in Ukraine through a survivor-centred multi-sectoral approach’ (UNited Action to Empower Survivors of CRSV). The project is implemented by UNFPA, UN Women, IOM, UNDP, WHO, and UNODC, in cooperation with the Government Commissioner for Gender Policy of Ukraine (beneficiary of the international technical assistance) and the Office of the Deputy Prime Minister for European and Euro-Atlantic Integration of Ukraine.

Recommended for publication by the decision of the Scientific and Methodological Council of the CSO “La Strada-Ukraine” (protocol No. 13 dated 18.04.2025)

ISBN 978-966-137-177-3

**AUTHORS:**

***Borozdina, K.A.***, Vice-President of the CSO “La Strada-Ukraine”;
***Bulavin, V.O.***, expert on cybersecurity and cyberintelligence;
***Zhukovska, H.H.***, Candidate of Sciences in Public Administration, Senior Referent at the Office of the Government Commissioner on Gender Policy;
***Rykun O.V.***, expert of Ukrainian Prosecutor Training Centre.

**REVIEWERS:**

***Germán Vega Cortes,*** Women Protection Adviser, UN Women
***Iryna Mykhailovska Pavlyk,*** CRSV Project Coordination Analyst, UN Women.

**EDITED BY:**

***Levchenko, K.B.***, Doctor of Law, Candidate of Philosophical Sciences, Professor, Honored Lawyer of Ukraine, Government Commissioner of Gender Policy of Ukraine.

**Civil Society Organization “La Strada-Ukraine”**

UKRAINE La Strada

03113, Kyiv, PO Box 26
Tel./fax: +38 (044) 205 36 95
E-mail: info@la-strada.org.ua
www.la-strada.org.ua, www.facebook.com/lastradaukraine

ISBN 978-966-137-177-3

# CONTENT

# ABBREVIATIONS

**Directive 2024/1385** - Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence.

**Directive 2024/1712** - Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking and protecting its victims.

**Directive 2011/36** - Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

**Directive 2011/92** - Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

**Istanbul Convention** - The Council of Europe Convention on preventing and combating violence against women and domestic violence of 11 May 2011, ratified by Ukraine on 20 June 2022.

**Budapest Convention** – The Council of Europe Convention on Cybercrime of 23 November 2001, ratified by Ukraine with reservations and statements on 7 September 2005.

**CCU** – Criminal Code of Ukraine.

**TiP** – trafficking in persons.

**CRSV** – conflict-related sexual violence.

**URPTI** - Unified Register of Pre-Trial Investigations.

**IDP** – internally displaced persons.

# INTRODUCTION

Global digitalization is an integral part of modern society, affecting all aspects of human life. Digital platforms, social media, online services and virtual communities create new opportunities for communication, self-expression, professional development and economic growth. At the same time, technological progress, which is designed to promote well-being and improve the quality of life, paves the way for perpetrators to use innovative methods of committing crimes. This is of particular concern in the context of the ongoing war of the Russian Federation against Ukraine, which is leading to increased social, economic, and psychological stress, making people more vulnerable to trafficking in persons and other types of criminal activity.

According to analytical platforms, a significant number of Ukrainians have access to the Internet. As of early 2024, according to DataReportal[1], there were about 29.64 million Internet users in Ukraine, which was approximately 79.2% of the total population. The statistics presented in the report reflect the gender distribution of Ukraine's total population, which in January 2024 was 37.42 million people – 54.3% women and 45.7% men. While the report does not provide a gender breakdown of Internet users, it does present the age distribution of Ukraine's population:

- 3.5% - aged 0 to 4 years;
- 9.0% - aged 5 to 12 years;
- 5.9% - aged 13 to 17 years;
- 4.4% - aged 18 to 24 years;
- 9.7% - aged 25 to 34 years;
- 17.0% - aged 35 to 44 years;
- 15.4% - aged 45 to 54 years;
- 15.0% - aged 55 to 64 years;
- 20.1% - aged 65 and older.

1 https://datareportal.com/reports/digital-2024-ukraine#:~:text=The%20state%20of%20digital%20in,penetration%20stood%20at%2079.2%20percent.

The level of digitalization recorded in the DataReportal report shows a significant increase in recent years, despite military and economic challenges. The majority of users actively interact with social networks, online media, and communication platforms, making the Internet a multidimensional space of interaction – from entertainment and education to doing business and finding employment opportunities. At the same time, the accessibility and popularity of digital services create a favourable environment for criminals that seek to exploit the openness and anonymity of the network for their own illegal purposes.

The realities of armed conflicts, accompanied by socio-economic crises, migration flows, and instability, create the basis for the rise of perpetrators seeking to profit from vulnerable groups.

The full-scale war of the Russian Federation against Ukraine increases the risks of trafficking and exploitation faced by Ukrainian women and girls, further heightening their vulnerability. Vulnerability factors that contribute to this include:

- loss of employment and the risk of being below the poverty line;
- internal displacement, which for an individual (or family) may occur multiple times, increasing the risk of being trafficked;
- traveling abroad for temporary asylum;
- residing in the territory of Ukraine that was or is temporarily occupied by the Russian Federation;
- unsuitability of accommodation at the place of permanent residence due to destruction caused by hostilities;
- other social factors (retirement age, disability, single parenthood, large families, etc.).

As the role of digital technologies grows, the forms and methods of exploitation are transforming and adapting to new conditions. Potential perpetrators are increasingly using the anonymity and global nature of the Internet to recruit, control, spread disinformation, manipulate data and search for potential targets. In this context, special attention should be given to the impact of cybercrime on women and girls, who are often at increased risk. Trafficking in persons in the online space for the purpose of sexual exploitation today is not only a matter of human rights violation, but also poses a serious problem of security, social development and personal protection. Perpetrators use online platforms and resources to recruit, blackmail, and distribute sexual photos and videos without the victims' consent, creating new forms of digital violence. Such activities take on particular significance in the context of a full-scale war, when traditional protection mechanisms may be weakened and vulnerable groups of people – internally displaced persons, women seeking means of survival – become even more exposed to criminal schemes.

Trafficking in persons for sexual exploitation in conflict can be one of the manifestations of conflict-related sexual violence (CRSV). It is closely related to other forms of CRSV, such as war-related rape, forced marriage, sexual slavery and exploitation under occupation. Women and girls in the temporarily occupied territories or in situations of forced displacement are the most vulnerable to these crimes. The use of digital technologies increases the risks for women in cyberspace, in particular through recruitment, blackmail and the spread of disinformation.

Trafficking for sexual exploitation in armed conflict as a form of CRSV is also mentioned in the UN Secretary-General's annual reports on sexual violence in conflict[2], who "urge the authorities in countries in the region hosting refugees to ensure quality multisectoral assistance to survivors and to adopt measures to mitigate the risk of conflict-driven trafficking."

The risks for women to be sexually exploited during displacement abroad are also often discussed at international events.

In order to effectively respond to CRSV cases and provide assistance to survivors, in May 2022, the Government of Ukraine and the UN signed the Framework of Cooperation on the Prevention and Response to CRSV.

On May 25, 2022, to ensure coordination of the activities of government authorities, local governments, international and civil society organizations aimed at implementing the tasks and activities of the Framework of Cooperation, the Commission for Coordination of Interaction of Executive Authorities on Ensuring Equal Rights and Opportunities for Women and Men[3], chaired by the Deputy Prime Minister for European and Euro-Atlantic Integration, established an Inter-Agency Working Group on Combating CRSV and Providing Assistance to Survivors (IWG). The IWG consists of five subgroups, one of which is focused on trafficking in persons for the purpose of sexual exploitation in the conflict setting.

2 https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2024/05/SG-2023-annual-reportsmallFINAL.pdf
3 https://www.kmu.gov.ua/npas/pro-utvorennya-komisiyi-z-pitan-koo-784

In response to the challenges faced by the global community in combating trafficking in persons, international organizations, governments, and human rights organizations are developing new legal frameworks, tools, strategies, and initiatives. In particular, the European Union is introducing directives that expand the conceptual framework and jurisdiction over sexual exploitation and related technology-driven crimes.

The Council of Europe Convention on preventing and combating violence against women and domestic violence emphasizes the importance of combating violence against women, including violence in the digital space.

The Budapest Convention on Cybercrime establishes a legal framework for international cooperation in the investigation and prosecution of crimes committed through computer systems.

However, despite the international norms and instruments being at place, such as EU Directives and Council of Europe conventions, their effective application requires a deep understanding of current threats and trends in the digital environment. Developing effective mechanisms to detect and prevent the recruitment of potential victims of trafficking in persons in the digital environment remains a challenge. Countries face the problem of insufficient coordination between law enforcement agencies, the absence or ineffectiveness of specialized units, lack of knowledge and competencies among specialists, imperfect legal frameworks and shortcomings in the protection infrastructure, and lack of cooperation with social services designed to provide comprehensive assistance to survivors. At the same time, both government agencies and non-governmental organizations, IT companies and social media are now facing the need to reconsider their own approaches to creating a safe online environment. Only an integrated approach based on a thorough analysis of risks and challenges can ensure the effectiveness of awareness-raising activities, the development of recommendations and the implementation of innovative technological solutions aimed at preventing trafficking in persons and providing appropriate assistance to those who have already been affected.

This study aims to address the existing gaps in knowledge about the cybercrime mechanisms used by perpetrators to traffic persons for sexual exploitation, particularly in the context of the ongoing war of the Russian Federation against Ukraine, identify key platforms and resources that pose increased risks, and offer recommendations for actors working to combat trafficking in persons and cybercrime to strengthen response in this area. Particular focus is on women and girls, who suffer most from technology-facilitated violence. In this regard, the scope of analysis includes both legal aspects and international standards, as well as practical tools for monitoring, data collection and analysis, principles of best practices, experience of interaction between the public and private sectors, the role of social media, mechanisms for combating cybercrime, providing assistance to survivors of those crimes, and opportunities for improving the competencies of law enforcement officials and other stakeholders.

The international rules and standards, such as Directive 2024/1712[4], amending Directive 2011/36/EU[5], strengthen measures against trafficking in persons in the online environment. The use of information and communication technologies to commit or facilitate trafficking in persons is now considered an aggravating circumstance, which may lead to stricter penalties. In addition, Member States are obliged to take measures to prevent the use of online platforms for trafficking purposes and to raise awareness of such risks.

Ukraine seeks to determine the limits and potential of these documents in the specific context of war and increased risks for groups in precarious situations, especially women and girls. This research will also be informed by the Istanbul Convention[6], which covers various aspects of digital violence, and the Budapest Convention on Cybercrime, which is an important benchmark for developing common approaches to combating computer crime.

An important aspect of the work is the identification of gaps that exist both in national policies and in the practice of law enforcement agencies, social services, IT companies, Internet service providers and social media. At the same time, it is emphasized that there is a need to develop comprehensive, multidisciplinary approaches to combating trafficking in persons, which will include training law enforcement officers, social workers, improving the legal framework, developing social programs that will help raise awareness and trust of survivors in protection mechanisms, developing standards for assistance to survivors.

Thus, this study is intended to become a conceptual, methodological and practical foundation for all stakeholders – from state and local authorities, international organizations to the private sector, civil society and the media. It will help understand current trends in the use of cyberspace for trafficking in persons for

4 https://eur-lex.europa.eu/eli/dir/2024/1712/oj/eng
5 https://eur-lex.europa.eu/eli/dir/2011/36/oj/eng
6 https://zakon.rada.gov.ua/laws/show/994_001-11#Text

the purpose of sexual exploitation, in particular as a form of CRSV, identify gaps in the protection system, and develop strategic recommendations and innovative solutions to improve the security of online space. Only a comprehensive assessment of the situation, with attention to the gender dimensions of trafficking in persons in digital environment, taking into account the impact of the risks of trafficking on women and girls in wartime, along with the application of international best practices, will create conditions for effective prevention, detection, prosecution and punishment of perpetrators, and most importantly, protect the rights and interests of survivors and vulnerable groups, especially women and girls, from the risks of trafficking for sexual exploitation in times of military conflict, challenges, and insecurity.

## PURPOSE AND METHODOLOGY OF THE RESEARCH

The main objective of this research is to contribute to the formation of a safer and more secure online environment that minimizes the risks of trafficking in persons for sexual exploitation during the full-scale war of the Russian Federation against Ukraine, and to ensure the effective protection of the rights and interests of trafficking survivors, primarily women and girls.

Given the current challenges and trends resulting from the rapid development of information and communication technologies, the international legal context, and relevant data on Internet usage, the study aims to provide a comprehensive analysis of the situation, identify gaps, and develop practical recommendations for the involved stakeholders.

In particular, the research objective includes the following key tasks:

- Research of existing procedures, legislative frameworks, and institutional practices to identify shortcomings and create conditions for enhancing their effectiveness;
- Identification of gaps and challenges in addressing the needs of survivors of trafficking in persons in the cyberspace: analysing mechanisms for detecting, identifying, and protecting survivors of trafficking for sexual exploitation in the digital environment;
- Analysis of cyberspace to identify risk points and exploitation schemes: determining online platforms, websites, social media, and communication tools most commonly used for recruitment and exploitation, particularly of women and girls affected by military conflict or in vulnerable positions. Analysing perpetrators' modus operandi, channels for distributing illegal content, and mechanisms for avoiding responsibility;
- Increasing awareness and capacity of stakeholders: providing an information baseline for all actors – human rights organizations, law enforcement bodies (including cyber police units), representatives of government authorities and local self-government, social workers, IT companies, social media, civil society, and media – to enhance their ability to identify, prevent, and effectively respond to threats of trafficking in persons in the digital environment;
- Identification of gaps in the response of state and local authorities and development of recommendations for their strengthening: assessing the effectiveness of existing state mechanisms to combat online trafficking in persons, identifying weaknesses in interaction among law enforcement, regulators, support services, and international partners. Based on the obtained data, developing recommendations aimed at strengthening institutional capacities and enhancing the protection of survivors;
- Development of recommendations for the technology sector and anti-trafficking actors: developing the set of proposals for state authorities and social media, IT companies, and other technological platforms to reduce the risks of their services being used for recruitment and exploitation. Developing guidelines and best practices to strengthen technical, organizational, and legal mechanisms aimed at complicating perpetrators' operations and improving cooperation between private and public sectors;
- Improving the protection of individuals, particularly women and girls, in the online space: providing recommendations to improve legal, institutional, educational, and social initiatives aimed at protecting rights and freedoms, raising awareness of cyber risks, and strengthening the ability to resist recruitment in the digital environment. Creating conditions for closer interaction with civil society, media, and educational institutions to foster a zero-tolerance attitude towards cyberviolence.

The research methodology includes the following methods:

- Desk research to analyse international standards in combating trafficking in persons, particularly in cyberspace, and national legislative and regulatory documents on trafficking in persons, particularly in cyberspace, as well as the practice of their application;
- Focus group discussions with women and girls at risk for trafficking in persons, and with representatives of actors implementing anti-trafficking measures at national and regional levels, to identify risks and gaps in developing and implementing state anti-trafficking policies, particularly in cyberspace. Quantitative results of focus groups are attached as Annex 1;
- Cyberspace analysis to identify existing threats and risks of situations of trafficking in persons to determine online platforms that may potentially pose trafficking risks, and to analyse the methods used by cybercriminals.

Thus, the study is aimed at building a systematic and comprehensive approach to identifying, preventing, and combating trafficking in persons in cyberspace, enhancing the capacities of all involved stakeholders, and developing comprehensive strategies for response and survivor protection. This will lay the foundation for more effective and consistent policies adapted to modern digital challenges, increase safety levels, and reduce the vulnerability of the population, especially women and girls, to violence in online space and technology-facilitated violence, exploitation, and violations of their rights.

The general methodology for this research is attached as Annex 2.

# OVERVIEW OF CASES OF TRAFFICKING IN PERSONS

Trafficking in persons remains an urgent problem for Ukraine. Modern forms of human exploitation and new challenges experienced worldwide create risks of trafficking for almost all social groups.

The armed aggression of the Russian Federation against Ukraine has increased internal displacement among the population. According to Ekonomichna Pravda Journal, in May 2024 Ukraine had 4.6 million internally displaced persons (IDPs)[7], and people who left the country seeking temporary protection. Most of them were women and girls, who represent a potentially vulnerable group and can be at risk of trafficking at persons. According to the Centre for Economic Strategy, by early 2025, the number reached 5.6 million people[8]. The war has particularly increased the risks of labour and sexual exploitation of women and girls, both within Ukraine and abroad.

> Discussion of the new challenges concerning trafficking in persons affecting women and girls in particular, both inside and outside Ukraine, must consider that the nature of these challenges has changed as a result of the 11-year-long war. To counter them, it is important to analyse the evolvement of the forms of trafficking in persons, recruitment methods, exploitation purposes, and the use of information and communication technologies (ICT) at all stages of this crime.
>
> Representative of tne Office of the Government Commissioner for Gender Policy

According to statistical data from the National Police, in 2020-2023 and in the first 11 months of 2024, law enforcement registered 828 criminal cases under Article 149 (Trafficking in persons) of the Criminal Code of Ukraine in the Unified Register of Pre-Trial Investigations (URPTI):

7 https://epravda.com.ua/news/2024/06/13/715107/
8 https://ces.org.ua/5-2-mln-abroad-how-do-they-live-will-they-return/ /

| CCU article | 2020 | 2021 | 2022 | 2023 | 11 months of 2024 |
|---|---|---|---|---|---|
| 149 | 212 | 232 | 134 | 148 | 102 |

These figures indicate that since the full-scale Russian invasion of Ukraine in 2022, the number of identified cases of trafficking in persons decreased by 57.8% compared to 2021.

However, the actual number of survivors may be significantly higher than suggested by the official records. Survivors may not be seeking help for a number of reasons: lack of communication channels, shame if there is a risk of being recognized, fear of worsening the situation, lack of trust in the assistance system, lack of awareness to identify the crime of trafficking in persons, etc.

The decline of identified criminal cases may also be attributed to:

- armed aggression of the Russian Federation against Ukraine;
- operation of the National Police at the territories under Ukrainian control and limitation on police operations at the temporarily occupied territories;
- law enforcement prioritizing national security tasks;
- a number of criminal proceedings under Art. 149 (Trafficking in Persons) of the CCU were investigated as a part of proceedings registered in the URPTI under Art. 438 (War crimes) of the CCU, which also covers cases of conflict-related sexual violence.

> Loss of housing, employment, change of the place of residence prompt people to search for opportunities to earn money through the Internet. Many job advertisements online do not have full information about the job offered (nature of the work, responsibilities, pay rates, working hours, etc.). Some ask to send the copies of identity documents via email.
>
> Women who fled abroad due to the full-scale war often face language barriers in accessing information. This affects their ability to recognize situations of trafficking in persons. Sadly, not every woman who has been trafficked and sexually exploited is ready to approach law enforcement.
>
> (results of the focus group discussion with representatives of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights)

Since the full-scale war began, the Unified State Register of Court Decisions records 183 verdicts and rulings under Article 438 of the Criminal Code of Ukraine “War Crimes”. However, under Ukrainian law, “trafficking in persons” and “war crimes” are treated as separate offenses. Article 438 of the CCU (“Violations of the Laws and Customs of War”) covers a wide range of crimes – including murders, torture, civilian abuse, forced displacement, and prohibited warfare methods – but does not explicitly mention trafficking in persons.

Meanwhile, Article 149 of the CCU “Trafficking in Persons” defines trafficking based on recruitment, movement, harbouring, or transfer of a person for the purpose of exploitation. If the criminal proceedings record the fact of conflict-related sexual violence or forced labour but without proven intent of exploitation (e.g., for profit), such actions most likely will not be classified as trafficking.

Thus, in order to clearly link the crime of trafficking in persons and CRSV, the recommendation is to amend Article 438 of the CCU to explicitly include “sexual violence and trafficking in persons as war crimes” and expand Article 149 of the CCU to introduce a specific offense: “trafficking in persons related to armed conflict.”

The available data on forms of exploitation identified by the National Police in 2020-2023 and in the first 11 months of 2024 show the following disaggregation of the cases of trafficking in persons under Art. 149 of the CCU:

| No. | Form of trafficking in persons | 2020 | 2021 | 2022 | 2023 | 11 months of 2024 |
|---|---|---|---|---|---|---|
| 1. | Sexual exploitation | 87 | 85 | 42 | 51 | 43 |
| 2. | Labour exploitation | 68 | 83 | 44 | 61 | 23 |
| 3. | Involvement in criminal activity | 36 | 54 | 23 | 13 | 8 |
| 4. | Surrogacy exploitation | 2 | 6 | 12 | 10 | 9 |
| 5. | Organs harvesting | - | - | - | - | - |
| 6. | Begging exploitation | 12 | - | 1 | 6 | 14 |
| 7. | Trafficking in children | 7 | 4 | 12 | 7 | 5 |
| | Total | 212 | 232 | 134 | 148 | 102 |

It should be noted that prior to the full-scale military invasion of Ukraine by the Russian Federation, cases of trafficking in persons for the purpose of sexual exploitation were detected more frequently than other forms of exploitation. In 2022-2023, the National Police recorded more cases related to labour exploitation. However, during the first 11 months of 2024, the number of cases of trafficking in persons for sexual exploitation again doubled compared to the number of cases of trafficking for labour exploitation.

At the same time, no statistical data were found on trafficking in persons involving the use of information and communication technologies for the period 2020-2023 and for the first 11 months of 2024.

According to the information received from the National Police of Ukraine, countries of destination and exploitation for cases of trafficking in persons detected in 2020-2023 and in the first 11 months of 2024 were the following:

| Year | Sexual exploitation (country of exploitation) | Labour exploitation (country of exploitation) | Trafficking in children (country of exploitation) | Involvement in criminal activity (country of exploitation) | Begging exploitation (country of exploitation) | Surrogacy exploitation (country of exploitation) |
|---|---|---|---|---|---|---|
| 2020 | Turkey, France, Germany, Malta, Israel, Cyprus, Slovakia, Italy, Denmark, Ukraine, UAE, Hungary, Greece, Czech Republic, China, Denmark, Malta, Russia | Ukraine, EU, Belarus, Brazil, Turkey, China | Austria, Ukraine | Russia, Turkey, France, Greece | Turkey, France, Germany, Malta, Israel, Cyprus, Slovakia, Italy, Denmark, Ukraine, UAE, Hungary, Greece, Czech Republic, China, Denmark, Malta, Russia | Ukraine, EU, Belarus, Brazil, Turkey, China |
| 2021 | Germany. Poland, Iraq, Greece, UAE, Italy, Ukraine, Hungary, Sweden, Maldives, Portugal, Bahrain | Ukraine, Iraq | Ukraine | Greece, Turkey, Brazil, Russia, France, Ukraine | | China, Ukraine |
| 2022 | Austria, Turkey, Czech Republic, Lithuania, Croatia, EU, Morocco, Cyprus, Germany, Romania, Sweden, Bulgaria, UAE | Ukraine | Ukraine, France, China | Ukraine, Turkey, France | Ukraine | France, China |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2023 | Czech Republic, Ukraine, Germany, Turkey, Lithuania, Israel, England, France, Sweden, Poland | Ukraine, Romania | Slovakia, Germany, France, Ukraine | Russia, Ukraine, France, Poland, Bulgaria, Turkey | Poland, Ukraine | France, Italy, Turkey, Germany, Ukraine |
| 11 Months of 2024 | Ukraine, Italy, UAE, Czech Republic, Spain, Cambodia, England, Poland, Turkey, Singapore, Denmark | Ukraine | Ukraine, France | Ukraine | Ukraine | France, Italy, Germany, Ukraine |

Main findings of the analysis of the countries of destination show that sexual exploitation occurs predominantly abroad, primarily in the EU countries, Asia, and the Middle East.

After the start of Russia's full-scale war against Ukraine in 2022, the number of countries where persons subjected to trafficking end up has increased significantly. New destinations have emerged, including Morocco, the UAE, Cambodia, Singapore, Spain, and England, although these countries were not in the list in previous years. Poland and Lithuania have become more frequent places of exploitation, which may be linked to the mass influx of Ukrainian women seeking temporary asylum there.

At the same time, there is no official statistics on trafficking in persons in the online space, in particular on cases related to sexual exploitation, as such data are not covered by statistical reporting of law enforcement agencies. Such information can be gathered only through the analysis of all criminal proceedings registered in the URPI under Article 149 of the CCU.

According to the statistical data of the National Police in 2020-2023 and in the first 11 months of 2024, **785 persons** were identified as victims under criminal proceeding under Article 149 of the CCU: **402** men, **323** women, and **60** children, **41** of them under the age of 14.

| Article 149 of the CCU | 2020 | 2021 | 2022 | 2023 | 11 months of 2024 |
|---|---|---|---|---|---|
| Men | 83 | 117 | 78 | 80 | 44 |
| Women | 51 | 94 | 50 | 78 | 50 |
| Children/including under age of 14 | - | 25/17 | 11/8 | 13/10 | 11/6 |
| Total number | 134 | 236 | 139 | 171 | 105 |

At the same time, according to the information published on the official webpage[9] of the National Social Service of Ukraine, which is responsible for prevention and combating trafficking in persons, the number of persons identified as survivors of TiP within the last three years is as follows:

**2022**

47 persons identified: 25 men, 19 women, 3 minors.

Forms of exploitation: labour – 14, sexual – 2, begging – 8, involvement into criminal activity – 11, exploitation in armed conflicts – 12.

**2023**

118 persons identified: 53 men, 47 women, 18 minors.

Forms of exploitation: labour – 22, sexual – 11, child trafficking – 2, begging – 1, involvement into criminal activity – 17, exploitation in armed conflicts – 55, other forms – 10.

9 https://nssu.gov.ua/protidiya-torgivli-lyudmi/kilkist-osib-yakim-nacsocsluzhboyu-vstanovleno-status-osobi-yaka-postrazhdala-vid-torgivli-lyudmi

**2024**

182 persons identified:105 men, 67 women, 10 children (5 boys and 5 girls). Destination: internal – 105 cases, cross-border – 74 cases, mixed – 3 cases.

Forms of exploitation: labour – 15, sexual – 13, child trafficking – 1, begging – 7, involvement into criminal activity – 4, exploitation in armed conflicts – 19, mixed forms – 123.

The statistics of the National Police of Ukraine and the National Social Service of Ukraine on persons who have been identified as victims in criminal proceedings initiated under Article 149 of the Criminal Code of Ukraine and persons who were granted the status of a survivor of trafficking in persons differ.

In particular, in 2022, the police initiated 139 criminal cases of trafficking in persons, while the National Social Service granted the status of survivors to only 47 persons.

In 2023, the police initiated 171 criminal cases of trafficking in persons, while the National Social Service granted the status of survivors to 118 persons.

Such a difference in statistical data is attributed to a number of factors:

**1.** Difference in procedures: According to the Article 55(1) of the Criminal Procedure Code (CPC) of Ukraine, a victim in criminal proceedings is an individual who has suffered moral, physical or property damage as a result of a criminal offense. The Article 55(2) of the CPC of Ukraine clearly establishes, that the rights and obligations of the victim (as defined in Articles 56 and 57 of the CPC of Ukraine) arise after a statement has been filed regarding a criminal offense committed against him or her or regarding his/her involvement in the proceedings as a victim. Whereas, the status of a survivor of trafficking in persons is established after a person personally submits a relevant statement to the local state administration;

**2.** According to Article 16 of the Law of Ukraine "On Combating Trafficking in Persons",[10] assistance to a survivor of trafficking in persons does not depend on whether that person contacted the law enforcement agencies or participated in criminal proceedings. In other words, in order to obtain the status of a survivor of trafficking in persons, it is not mandatory for them to report the crime to the police. Therefore, there are cases when law enforcement agencies are not aware of such persons;

**3.** When a survivor of trafficking in persons has been identified in accordance with paragraph 4 of the CMU Resolution "On Approval of the Procedure for Interaction of Entities Implementing Measures to Combat Trafficking in Persons" of August 22, 2012, No. 783[11], law enforcement agencies, with the consent of such a person or his or her legal representative, refer the survivor to the relevant structural unit of the local state administration at their place of residence. However, in order to avoid retraumatization, such persons may not apply for the status of a trafficking survivor;

**4.** Over the past three years of Russia's full-scale military invasion of Ukraine, the National Social Service has granted 66 survivor statuses to the survivors of trafficking in persons exploited in armed conflicts. In the vast majority of cases, the persons who were granted this status were held in captivity and subjected to any kind of exploitation[12]. Some of those persons are victims in criminal proceedings registered in the URPI under Article 438 of the Criminal Code of Ukraine, which may include Article 149 of the Criminal Code of Ukraine, as well as other articles of the Criminal Code of Ukraine covering criminal offenses related to conflict-related sexual violence. Hence, it is possible that such persons are not included in the official statistics of the National Police as victims of trafficking in persons, but are listed as victims of war crimes. A similar situation can be observed in the statistical data of the National Police cited above regarding forms of exploitation, where there is no such form as exploitation in armed conflicts.

The analysis above shows that among all the recorded cases of trafficking in persons, there are no cases related to the commission of this crime in cyberspace.

At the same time, recognizing that trafficking in persons, which has historically been associated mainly with illegal migration, exploitation of physical labour and sexual violence in the offline dimension, is now taking on new forms in cyberspace, the state and society must face the task of comprehensively rethinking the concept of security. If earlier attention was focused primarily on strengthening borders, developing justice systems and cooperation between law enforcement agencies of different countries, now the ability to effectively respond to crimes on the Internet should come to the fore. This is especially true in the context

10 https://zakon.rada.gov.ua/laws/show/3739-17#Text
11 https://zakon.rada.gov.ua/laws/show/783-2012-%D0%BF#Text
12 Exploitation in armed conflicts is the coercion of a person in a state of servitude to perform combat missions related to the overthrow of state power or violation of the sovereignty and territorial integrity of the state.

of a full-scale war, when the vulnerability of the population increases and military operations contribute to the spread of criminal schemes related to sexual and labour exploitation, child abduction and recruitment of women through social media. At the same time, the development of a national system to combat cybercrime should be a key priority, as modern technologies allow perpetrators to act even more sophisticatedly using the darknet and anonymous platforms. It is necessary not only to identify the platforms that pose the highest risk but also to gain a deeper understanding of the ways used to involve women in exploitation, to design methods for collecting information on current trends, and to develop systematic approaches to monitoring and analysing global search queries.

# SECTION I

# IMPLEMENTATION OF THE INTERNATIONAL STANDARDS ON COMBATING TRAFFICKING IN PERSONS, IN PARTICULAR IN CYBERSPACE, INTO UKRAINIAN NATIONAL LEGISLATION

This chapter examines international standards on combating trafficking in persons, in particular with the use of information and communication technologies, in order to identify gaps and challenges, to meet the needs of persons affected by trafficking in the digital environment and to raise awareness and capacities of actors to identify and respond to such cases, and assist survivors and vulnerable groups.

The following legal acts were studied:

- Directive 2024/1385[13];
- Directive 2024/1712[14];
- Directive 2011/36/EU[15]
- Directive 2011/92/EU[16];
- Istanbul Convention[17];
- Budapest Convention[18];
- Council of Europe Convention on Action Against Trafficking in Human Beings of 16 May 2005[19];
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime adopted by the UN Resolution 55/25 of the General Assembly of 15 November 2000[20];
- Law of Ukraine on Combating Trafficking in Persons of 20 September 2011[21];
- Law of Ukraine on Domestic Violence Prevention and Response of 07 December 2017[22];
- Criminal Code of Ukraine[23].

EU Directive 2024/1385 introduces new approaches to the definition of sexual violence, including its manifestations in armed conflict. It provides for liability for intentional acts related to sexual exploitation, forced marriage and cyberviolence that can be used as an instrument of a war crime or crime against humanity.

International law classifies the sexual violence in conflict as a war crime (Articles 7 and 8 of the Rome Statute of the International Criminal Court). According to the Geneva Conventions (1949) and Additional Protocols, in particular the Geneva Convention relative to the Protection of Civilian Persons in Time of War[24], any acts of rape, forced prostitution, sexual slavery or other forms of sexual exploitation against civilians may be considered a serious violation of international humanitarian law. Accordingly, the legal mechanisms of the EU and Ukraine should ensure the effective prosecution of such crimes.

Directive 2024/1385 also regulates the issue of liability for intentional acts related to crimes of sexual exploitation of women and children and technology-facilitated crimes.

Ukrainian legislation is gradually adapting to international standards on combating sexual violence, including the CRSV. The Criminal Code of Ukraine states the key norms on criminalization of sexual violence, in particular:

- Article 149 – trafficking in persons, which may include sexual slavery and forced prostitution.

- Article 152 – rape, which in wartime can be considered a war crime.

- Article 438 – violations of the laws and customs of war, including sexual violence as a method of warfare.

The Law of Ukraine “On Combating Trafficking in Persons” of September 20, 2011 is the key regulatory legal act of Ukraine that regulates combating trafficking in persons. This regulatory document currently does not contain a definition of technology-facilitated sexual violence.

At the same time, Article 173-7 of the Code of

13 https://jurfem.com.ua/wp-content/uploads/2024/11/Dyrektyva.pdf
14 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401712
15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0036
16 https://jurfem.com.ua/wp-content/uploads/2023/09/%D0%94%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B0-2011-92.pdf
17 https://zakon.rada.gov.ua/laws/show/994_001-11#Text
18 https://zakon.rada.gov.ua/laws/show/994_575#Text
19 https://zakon.rada.gov.ua/laws/show/994_858#Text
20 https://zakon.rada.gov.ua/laws/show/995_791#Text
21 https://zakon.rada.gov.ua/laws/show/3739-17#Text
22 https://zakon.rada.gov.ua/laws/show/2229-19#Text
23 https://zakon.rada.gov.ua/laws/show/2341-14#Text
24 https://zakon.rada.gov.ua/laws/show/995_154#Text

Ukraine on Administrative Offenses[25] stipulates that sexual harassment, i.e. the intentional commission of offensive, degrading acts of a sexual nature against the will of a person, expressed verbally or non-verbally (words, gestures, body movements), may occur also through the use of electronic communications.

EU Directive 2024/1385 defines cyberviolence as a method of committing sexual violence and exploitation of women, including its use in situations of armed conflict. The most common forms of cyberviolence related to trafficking in persons and CRSV include:

- online recruitment through social media, messengers, dating platforms;
- cyber blackmail - extortion of intimate materials under the threat of publicity;
- distribution of materials of a sexual nature for the purpose of manipulation and control over the victim.

The directive obliges EU member states to criminalize such actions and ensure their effective investigation, which is especially relevant for Ukraine in the context of armed conflict.

Currently, the national legislation of Ukraine provides for liability for the following offenses specified in EU Directive 2024/1385:

- genital mutilation, covered by Article 121 (Intentional grievous bodily harm) of the Criminal Code of Ukraine;
- invasion of privacy, Article 182 of the Criminal Code of Ukraine, which covers unlawful acts related to the unlawful collection, storage, use, destruction, dissemination of confidential information about a person or unlawful alteration of such information;
- forced marriage (Article 151-2 of the Criminal Code of Ukraine).

As well as sexual harassment, which is provided for by Article 173-7 of the Code of Ukraine on Administrative Offenses, including using electronic communications, as well as sexual harassment of a child, including using information and telecommunications systems, which is covered by Article 156-1 of the Criminal Code of Ukraine.

The Verkhovna Rada of Ukraine is currently considering the draft Law of Ukraine on Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine “On Domestic Violence Prevention and Response” to establish liability for stalking, No. 12088 of 02.10.2024[26], which introduces the term cyberstalking – a type of criminal stalking that involves constant surveillance of the victim without his or her consent or legal permission through information and communication technologies. It can be carried out by processing the victim’s personal data, in particular as a result of identity theft or spying on the victim through their social media or messaging platforms, email and phone, stealing passwords or hacking their devices to access their private space by installing geolocation applications, including spyware, or by stealing their devices.

According to the Criminal Code of Ukraine, an attempted criminal offence is an act (action or inaction) committed by a person with direct intent, directly aimed at committing a criminal offence under Article 15 of the Special Part of the Criminal Code of Ukraine, if the criminal offence was not completed for reasons beyond the person’s control. In accordance with Article 16 (Criminal Liability for an Uncompleted Criminal Offence) of the Criminal Code of Ukraine, liability for an attempted criminal offence is the same as for a completed criminal offence.

EU Directive 2024/1385 also contains important sections on the protection and assistance to victims, in particular:

- Chapter 3. Protection of victims and access to justice;
- Chapter 4. Victim support.

The legal act harmoniously combines and implements international standards for the protection of victims of sexual and other types of violence. Thus, the Directive reflects the basic principles of assistance and protection of victims:

- avoiding secondary and repeat victimisation;
- applying a victim-centred approach;
- individual needs assessment;
- providing medical and psychological assistance;
- rehabilitation and social and economic integration services;
- access to justice;
- reporting violence online;
- referral of victims;
- protection of privacy;
- removal of online materials;
- compensation from offenders;
- involvement of support services, crisis centres,

25 https://zakon.rada.gov.ua/laws/show/80731-10#Text
26 https://itd.rada.gov.ua/billInfo/Bills/searchResults

shelters, assistance centres, counselling centres.

In addition, sufficient attention is paid to training "[...] officials likely to come into contact with victims, such as police and court staff, receive both general and specialised training and targeted information at a level appropriate to their contact with victims to enable them to identify, prevent and address instances of violence against women or domestic violence and to treat victims in a trauma-, gender- and child-sensitive manner. [...]" (Part 1, Art. 36, Ch. 5)

Chapter 6 also highlights issues related to coordination and cooperation, namely:

- coordinated policy and a coordinating body;
- national action plans to prevent and combat violence against women and domestic violence;
- multi-agency coordination and cooperation;
- cooperation with non-governmental organisations;
- data collection and research.

Thus, in general, Ukrainian legislation is in line with the provisions of EU Directive 2024/1385 on survivor protection and access to justice.

In particular, these rules are regulated by the following legal acts:

- Law of Ukraine of 20 September 2011 No. 3739-VI "On Combating Trafficking in Persons";
- Law of Ukraine No. 2229-VIII of 07 December 2017 "On Domestic Violence Prevention and Response";
- Resolution of the Cabinet of Ministers of Ukraine of 18 January 2012 No. 29 "On the National Coordinator for Combating Trafficking in Persons";[27]
- Resolution of the Cabinet of Ministers of Ukraine of 22 August 2012 No. 783 "On Approval of the Procedure for Interaction of Entities Carrying Out Measures in the Field of Combating Trafficking in Persons";
- Resolution of the Cabinet of Ministers of Ukraine of 23 May 2012, No. 417 "On Approval of the Procedure for Establishing the Status of a Survivor of Trafficking in Persons" ;[28]
- Resolution of the Cabinet of Ministers of Ukraine of 25 July 2012, No. 660 "On Approval of the Procedure for Payment of One-Time Financial Assistance to Survivors of Trafficking in Persons" ;[29]
- Joint Order of the Ministry of Social Policy of Ukraine and the Ministry of Internal Affairs of Ukraine of 11 January 2016 No. 4/5 "On Approval of the Instruction on Collection and Monitoring of Statistical Information on Survivors of Trafficking in Persons" ;[30]
- Order of the Cabinet of Ministers of Ukraine of 02 June 2023 No. 496-p "On Approval of the State Targeted Social Programme for Combating Trafficking in Persons for the Period up to 2025"[31].

Another important European Union Directive regulating the issue of combating trafficking in persons is Directive (EU) 2024/1712, which amended Directive 2011/36[32].

Directive 2011/36/EU is the main EU legal instrument to prevent and combat trafficking in human beings and to protect victims of this crime. The Directive establishes a comprehensive framework for combating trafficking in human beings, setting minimum rules on the definition of criminal offences and sanctions. It also contains general provisions on strengthening the prevention of trafficking in human beings, assistance provided to survivors and their protection, taking into account gender, disability and children's interests, as well as a survivor-centred approach.

EU Directive 2024/1712 introduces major novelties regarding the forms of exploitation of trafficking in human beings, in particular, in order to tackle the steady increase in the number and relevance of offences concerning trafficking in human beings committed for purposes other than sexual or labour exploitation. According to them, the exploitation of surrogacy, of forced marriage or of illegal adoption should be included as forms of exploitation in that Directive, in so far as they fulfil the constitutive elements of trafficking in human beings, including the means criterion.

As of today, Article 149 of the Criminal Code of Ukraine provides in note 1 a non-exhaustive list of types of human exploitation within the framework of trafficking in persons, which include:

- all forms of sexual exploitation;
- use in the porn business;
- forced labour or forced services;
- slavery or practices similar to slavery;
- servitude;
- involvement in debt bondage;

27 https://zakon.rada.gov.ua/laws/show/306/2020#Text
28 https://zakon.rada.gov.ua/laws/show/417-2012-%D0%BF#Text
29 https://zakon.rada.gov.ua/laws/show/660-2012-%D0%BF#Text
30 https://zakon.rada.gov.ua/laws/show/z0169-16#Text
31 https://zakon.rada.gov.ua/laws/show/496-2023-%D1%80#Text
32 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401712

- removal of organs;
- conducting experiments on humans without their consent;
- adoption for profit;
- forced pregnancy or forced termination of pregnancy;
- forced marriage;
- forced involvement in begging;
- involvement in criminal activity;
- use in armed conflicts, etc.

Evidently, among the types of exploitation listed in Directive 2024/1712, Ukrainian legislation recognized adoption for profit and forced marriage, while surrogacy exploitation is not included into the list.

However, according to statistics provided by the National Police, 39 cases of trafficking in persons under the guise of surrogacy were identified in 2020-2023 and in the first 11 months of 2024.

As sexual violence crimes are increasingly committed in the digital environment, the Directive clearly defines the cases to be addressed.

Thus, paragraph 8 of the Directive states: "An increasing number of offences concerning trafficking in human beings are committed or facilitated **by means of information or communication technologies**. Traffickers frequently use the internet and social media, inter alia to recruit, advertise or exploit victims, to exercise control over them and organise their transport. The internet and social media are also used to distribute exploitative materials. Information technology also hampers the timely detection of the crime and the identification of the victims and perpetrators."

Paragraph 9 of the Directive includes the following crimes committed with the use of information and communication technologies within the scope of the definition of trafficking in human beings:

- recruitment and exploitation of victims;
- organisation of their transport and accommodation;
- advertising victims online and reaching out to potential clients;
- controlling victims;
- communication between perpetrators;
- financial transactions related to trafficking in human beings.

The Law of Ukraine of 20 September 2011 No. 3739-VI "On Combating Trafficking in Persons" defines trafficking in persons as "settlement of an illegal agreement, the object of which is a human being, as well as recruitment, transportation, harbouring, transfer or receipt of a human being for purpose of his/her exploitation, including sexual exploitation, by means of deception, fraud, blackmail, abuse of a person's position of vulnerability or by use of force or threat of use of force, with abuse of power or economic or other dependence of the victim on another person, which is considered a crime under the Criminal Code of Ukraine."

However, the national definition of trafficking in persons does not include such an act as an activity committed through information and communication technologies. The Criminal Code of Ukraine, in particular Article 149, also does not provide for such an act.

In addition, an important novelty of the Directive is the obligation of Member States to take the necessary measures to ensure that in cases of offences related to trafficking in human beings, the facts that the offender facilitated or committed, by means of information and communication technologies, the dissemination of images or videos or similar materials of a sexual nature involving the victim are considered as aggravating circumstances (Art. 4, para. 3(b)).

"The level of penalties for trafficking should reflect higher opprobrium for more serious types of conduct, and for the more harmful and longer-lasting impact that they have on the victims. This includes the amplifying effect of the dissemination of exploitative material, including dissemination in closed groups accessible to a limited number of participants. Therefore, it is necessary to provide for, as an aggravating circumstance, the dissemination, by means of information and communication technologies, of images or videos or similar material of a sexual nature involving the victim." (para. 10)

The aggravating circumstances in the Ukrainian legislation are set out in Article 67 of the Special Part of the Criminal Code, however, there is no provision that recognizes the use of information and communication technologies in the commission of a criminal offense as an aggravating circumstance.

In order to ensure the effective investigation of criminal offences related to trafficking in persons by means of information or communication technologies, the Directive obliges Member States to ensure that persons, units or services investigating offences in this category have sufficient experience and technological capacities. It also encourages the establishment of specialised units within law enforcement and prosecution services, where appropriate and in accordance with their national legal systems.

Currently, there are such units within the structure of the National Police of Ukraine. The Migration Police Department is responsible for combating trafficking in persons, and the Cyber Police Department is responsible for combating cybercrime. These departments have well established cooperation in the area of pre-trial investigation of criminal offences related to trafficking in persons.

The Directive also addresses the following:

- the response of the criminal justice system to trafficking-related crimes committed in the interests of legal entities and the prevention of such crimes;
- establishing the possibility of not prosecuting and not applying punishment to victims of trafficking in human beings in connection with criminal offences they were forced to commit as a direct consequence of being trafficked;
- referring victims to the relevant services to provide the necessary assistance, establishing the necessary mechanisms at the national level;
- criminalising the use of services where the victim is exploited to provide such services;
- raising awareness of prosecutors and law enforcement agencies that may come into contact with victims or potential victims of trafficking in human beings;
- establishing national coordinators for combating trafficking in human beings;
- developing national action plans to combat trafficking in human beings.

At present, Ukrainian legislation does not include provisions regulating the liability of legal entities for trafficking in persons, establishing the possibility of non-prosecution and non-punishment of victims of trafficking in persons, or criminalising the use of services.

These norms have been adopted by Ukraine through the ratification of the Council of Europe Convention on Action against Trafficking in Human Beings of 16 May 2005 and the United Nations Convention against Transnational Organised Crime adopted by General Assembly Resolution 55/25 with the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children. The domestic legislation of Ukraine does not regulate these norms.

At the same time, the Verkhovna Rada of Ukraine was considering a draft law on amendments to the Criminal Code of Ukraine to strengthen criminal liability for trafficking in persons, No. 5134 of 22.02.2021[33], which provides for the introduction of criminal liability of legal entities for trafficking in persons.

In Ukraine, the Ministry of Social Policy of Ukraine is responsible for developing the state policy on combating trafficking in persons and gender-based violence, including domestic violence[34], while the implementation of this policy is entrusted to the National Social Service, in accordance with the Resolution of the Cabinet of Ministers of Ukraine of 26 August 2020 No. 783[35].

To fulfil its tasks of preventing and combating trafficking in persons, the National Social Service:

- ensures the implementation of the State Social Programme for Combating Trafficking in Persons;
- inspects and monitors the activities of actors engaged in trafficking response;
- coordinates and monitors the activities of institutions providing assistance to survivors of trafficking in persons, in particular by referring those who have been trafficked abroad and are returning to Ukraine to such institutions, if they require temporary shelter;
- decides on the establishment/refusal to establish, extension/refusal to extend, or denial of the status of a survivor of trafficking in persons;
- participates in the preparation of an annual report on the state of implementation of measures to combat trafficking in persons;
- takes measures to eliminate the root causes of trafficking in persons;

As for the State Social Programme for Combating Trafficking in Persons until 2025[36], it contains tasks and measures aimed at combating trafficking in persons in the context of Russia's armed aggression against Ukraine. However, the tasks and measures to combat trafficking in persons using information and communication technologies are not covered.

> "The legislation currently does not address challenges in the field of combating trafficking in persons related to the development of information and communication technologies, for example, the State Targeted Social Programme for Combating Trafficking in Persons until 2025 does not contain tasks and measures aimed at combating trafficking in persons in the online space using information and communication technologies."
>
> Office of the Government Commissioner for Gender Policy

Hence, analysing the current challenges in combating trafficking in persons, especially in the context of global digitalisation and the full-scale war in Ukraine, which has increased the vulnerability of women and children to trafficking, including sexual exploitation, the approach to ensuring the safety of survivors of

33 https://itd.rada.gov.ua/billInfo/Bills/Card/25646
34 https://zakon.rada.gov.ua/laws/show/423-2015-%D0%BF#Text
35 https://zakon.rada.gov.ua/laws/show/783-2020-%D0%BF#Text
36 https://zakon.rada.gov.ua/laws/show/496-2023-%D1%80#Text

trafficking in persons should be comprehensive and survivor-centred, taking into account the needs of women and men, boys and girls. An important area is the adaptation of Ukrainian legislation to international standards, in particular the EU Directives on combating cyberviolence and exploitation in the digital environment, covering legal, technological and social aspects, as well as close interagency and international cooperation and coordination.

# JUDICIAL PRACTICE

The scope of the analysis of judicial practice included court decisions in criminal proceedings on criminal offences of trafficking in persons related to sexual exploitation with the use of information and communication technologies in the period from 2014 to 2024, posted on the portal of the Unified State Register of Court Decisions.

The analysis of the narrative part of court rulings shows that perpetrators use information and communication technologies to commit trafficking in persons, in particular for the purpose of sexual exploitation, which indicates the relevance of the issue under study.

The analysis of court rulings has shown that perpetrators employ information and communication technologies at different stages of the commission of criminal offences.

**Examples:**

***Case category No. 607/14020/13-к***

***Date of entry into force: 03.11.2014***

Due to her adverse financial situation, due to her difficult life situation, she, PERSON_11, decided to look for a high-paying job abroad and, for this purpose, placed an advertisement on a dating website on the Internet stating that she urgently needed a job and left her mobile phone number, on which she received a call the following day and was offered to meet regarding her employment.

***Case category No. 591/7967/13-к***

***Date of entry into force: 17.10.2014***

She also met PERSON_10 through an Internet website and, during their conversation, she learned about her marital status, difficult financial situation, bank loan debts and offered her work in the Republic of Turkey as a sex worker, and told her about the conditions of work, payment for this work, accommodation, and meals.

***Case category No. 751/3191/17***

***Date of entry into force: 19.03.2018***

Thus, PERSON_7, performing actions related to the recruitment of girls among the population of Chernihiv region, offered employment in the People's Republic of China through the profile of PERSON_14 on the VK website.

***Case category No. 727/9754/18***

***Date of entry into force: 19.03.2019***

In order to obtain detailed information about possible employment abroad, PERSON_9 and PERSON_7, using the VIBER messenger, began to communicate and the latter said that in order to travel abroad, she needed a passport of a citizen of Ukraine for travelling abroad, and if she had one, a visa in this passport, which, if necessary, could be issued by his acquaintance, who, as it later became known, was PERSON_11.

# RECOMMENDATIONS FOR SECTION I

Following the analysis of the results of the desk study of existing practices of cyberspace audit(s) and the state of their implementation in order to reduce the vulnerability of women and girls in Ukraine to trafficking in persons in the online space for the purpose of sexual exploitation and other forms of exploitation using information and communication technologies, a number of recommendations were prepared for public authorities, in particular for actors involved in countering trafficking in persons.

Overall, in line with recommendations below, the actions of all actors should be focused on addressing the gender-sensitive aspects of cybercrime. In particular, it is essential to introduce specialised algorithms to monitor online platforms used for recruitment, including the targeting of women and girls for sexual exploitation. Special attention should also be given to detecting digital traces of CRSV offences.

# RECOMMENDATIONS FOR THE OFFICE OF THE PROSECUTOR GENERAL OF UKRAINE, THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE, AND THE NATIONAL POLICE OF UKRAINE

1. To strengthen liability for crimes of trafficking in persons for the purpose of sexual exploitation, including when committed as a form of CRSV through the use of digital technologies, by amending Article 67 of the Criminal Code of Ukraine (Aggravating circumstances) to include "committing the crime in the context of armed conflict" and "using digital technologies for recruitment or sexual exploitation of women".

2. To improve the mechanism for recording war crimes of a sexual nature, including trafficking in persons for the purpose of sexual exploitation, in the context of CRSV, including through training for police and prosecutors working with affected women and girls.

3. To amend Article 153 (Sexual violence) of the Criminal Code of Ukraine by adding the words "including through the use of information and communication technologies" after the words "victim" in part one of the article.

4. To amend Article 182 (Violation of privacy) of the Criminal Code of Ukraine by adding the words "including through the use of information and communication technologies" after the words "such information" in part one of the article.

5. To amend Article 149 (Trafficking in Persons) of the Criminal Code of Ukraine to criminalise the act of advertising victims on the Internet and to add the use of surrogacy to the list of types of exploitation in Note 1;

6. To develop a draft law to amend the Criminal Code of Ukraine to criminalise the use of services provided by victims of trafficking in persons;

7. To initiate further consideration of the draft law of Ukraine "On Amendments to the Criminal Code of Ukraine on Strengthening Criminal Liability for Trafficking in Persons" No. 5134 of 22.02.2021, which provides for the introduction of criminal liability of legal entities for trafficking in persons, before the Verkhovna Rada Committee on Law Enforcement;

8. To hold consultations with Internet service providers and develop algorithms to block websites that advertise the provision of sexual services, promote sexual violence, and remove advertisements offering work related to the provision of sexual services. To develop a mechanism for bringing the owners of those websites to justice;

9. To develop and institutionalize trainings and learning for prosecutors, investigators, police officers responsible for investigating criminal offences related to trafficking in persons and cybercrime on detection and pre-trial investigation of criminal offences and crimes related to CRSV, in particular on:

- the impact of the conflict on the growing risk of trafficking for sexual exploitation;
- use of information technologies to recruit women;
- work with CRSV survivors.

10. To develop a mechanism for collecting and recording sex-disaggregated statistics on criminal offences, pre-trial investigations of which have been initiated on the grounds of trafficking in persons, including trafficking for the purpose of sexual exploitation with the use of information technologies, including those investigated under Article 438 (War Crimes) of the Criminal Code of Ukraine;

11. To amend the statistical reporting of criminal offences, pre-trial investigation of which have been initiated on the grounds of trafficking in persons, including as a form of CRSV, in order to collect sex-disaggregated information on trafficking in persons committed with the use of information and communication technologies;

12. To develop methodological recommendations for law enforcement agencies on the detection, pre-trial investigation and procedural guidance of trafficking in persons, including for the purpose of sexual exploitation in the context of Russia's armed aggression against Ukraine, committed with the use of information and communication technologies;

13. To develop algorithms for to identify survivors in high-risk areas (IDPs, those abroad, people from the temporarily occupied territories), taking into account their vulnerability to recruitment and exploitation.

14. To establish cooperation with international organisations and civil society organisations to more effectively respond to cases of trafficking in persons, including for the purpose of sexual exploitation with the use of information technologies, and to assist survivors, as well as to document war crimes of a sexual nature, in particular those committed through digital platforms and social media.

# RECOMMENDATIONS FOR THE MINISTRY OF SOCIAL POLICY OF UKRAINE AND THE NATIONAL SOCIAL SERVICE OF UKRAINE

1. To initiate an amendment to the Law of Ukraine "On Domestic Violence Prevention and Response" of 07 December 2017 to expand the term "sexual violence" by adding the words "including through the use of information and communication technologies";

2. To initiate an amendment to the Law of Ukraine "On Combating Trafficking in Persons" to expand the definition of "trafficking in persons" to include "Trafficking in persons as a form of conflict-related sexual violence shall mean any actions aimed at recruiting, moving, harbouring, transferring or exploiting a person (especially women and girls) during or as a result of an armed conflict";

3. When developing the State Targeted Social Programme for Combating Trafficking in Persons for the period after 2025, to include tasks and measures to combat trafficking in persons in the online space, focusing on women and girls as the primary vulnerable group;

4. To initiate amendments to Article 438 of the CCU to add a provision on sexual violence and trafficking in persons as a war crime, and to Article 149 of the CCU to add a separate crime of trafficking in persons for the purpose of sexual exploitation in relation to the conflict;

5. To amend the joint order of the Ministry of Social Policy of Ukraine and the Ministry of Internal Affairs of Ukraine of 11 January 2016 No. 4/5 "On Approval of the Instruction on Collection and Monitoring of Statistical Information on Survivors of Trafficking in Persons" to include the National Social Service of Ukraine. Given that the National Social Service is the main holder of statistical information on survivors of trafficking in persons and performs key functions in making decisions on establishing, extending or revoking the relevant status, its main tasks should officially include prevention and combating gender-based violence, including domestic violence and trafficking in persons;

6. To organise and conduct trainings and learning for actors at the regional level involved in anti-trafficking activities to improve protection, in particular for women and girls, against the risks of trafficking in cyberspace and technology-facilitated violence, including sexual exploitation as a form of CRSV;

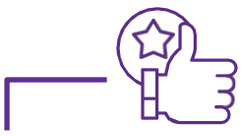
7. To conduct information campaigns for actors involved in anti-trafficking activities to improve the identification of survivors of trafficking in persons, especially women and girls at risk (IDPs, those residing in temporarily occupied territories, those living abroad, etc.), and survivors of sexual exploitation, including through the use of information and communication technologies;

8. In order to prevent re-traumatisation of trafficking survivors during their interview, survey and needs assessment, to develop a unified interview form that can be used at all stages of providing assistance to the survivor and establishing the appropriate status;

7. To amend the Procedure for granting the status of a survivor of trafficking in persons, approved by the Cabinet of Ministers of Ukraine on 23 May 2012, No. 417, in order to strengthen the prevention and response to trafficking in persons with regard to the possibility of submitting an electronic application for the status of a survivor of trafficking in persons;

8. To establish cooperation with international and civil society organisations to better respond to cases of trafficking in persons, especially for the purpose of sexual exploitation, as a form of CRSV, and provide assistance to survivors;

9. To strengthen public awareness of cases of trafficking in persons and the risks of becoming involved in situations related to trafficking in persons for sexual exploitation through the use of information and communication technologies, including risks during the war.



## RECOMMENDATIONS FOR DIGITAL PLATFORMS (WEBSITES, APPLICATIONS, ETC.) AND SOCIAL MEDIA

- To implement mechanisms for monitoring and removing content related to CRSV and trafficking for sexual exploitation, including recruitment advertisements, fake job postings, and coercion to provide sexual services.
- To introduce a system of warnings for people, in particular for women and girls at risk (IDPs, those living abroad) in the form of notifications about potential recruitment and exploitation risks.
- To expand cooperation between social media and law enforcement agencies to quickly block accounts used for criminal activities (recruitment, blackmail, online intimidation).
- To provide confidential mechanisms to report suspicious activities for women who suspect they have been recruited or blackmailed.

## RECOMMENDATIONS FOR THE DEVELOPMENT OF INFORMATION POLICY AND STRATEGIC COMMUNICATIONS TO COMBAT TRAFFICKING IN WOMEN USING INFORMATION AND COMMUNICATION TECHNOLOGIES

1. When developing state targeted programmes, action plans and implementation plans, to include the issue of strengthening information policy on combating trafficking in persons, especially women, with the use of information and communication technologies for the purpose of sexual exploitation, in particular with regard to:

- conducting information campaigns on the risks of online recruitment and exploitation, especially among vulnerable groups (youth, women);
- creating and promoting digital literacy training tools, including methods for recognising recruitment and exploitation schemes;
- promoting the rules of safe use of social media and job search platforms.

# SECTION II

# TRAFFICKING IN PERSONS IN THE ONLINE SPACE: KEY THREATS, PLATFORMS, AND ANALYTICAL TOOLS

The process of global digitalization is creating large-scale challenges: along with new opportunities for economic growth, democratisation of knowledge and expansion of rights and freedoms, network resources are becoming a tool for illegal activities. Criminal activity in the digital environment ranges from subtle recruitment and disinformation tactics to complex multi-stage schemes that leverage the use of private communication channels, anonymous platforms and cross-border interaction. The Internet provides perpetrators with opportunities to disseminate information quickly, target vulnerable groups, disguise their intentions and, most importantly, avoid direct physical contact with both their targets and justice.

People facing difficult life circumstances, particularly in relation to the war, often look for new opportunities to earn money, evacuate or start a new life in another country. In such moments, it is particularly easy for them to fall into the traps of cybercriminals. In addition, the popularity of social media, communication platforms and online labour exchanges, as well as the general trend towards the digitalisation of services and resources, create conditions for more covert recruitment that is difficult to track.

## KEY THREATS AND CHALLENGES IN THE ONLINE ENVIRONMENT

According to the Report on Trafficking in Persons[37] for 2023, released in February 2024, there is a further upward trend in the number of cases of trafficking in persons related to the use of digital platforms. The report states that "traffickers reportedly kidnapped women and girls from conflict-affected areas for sex and labour trafficking in Ukraine and Russia. Traffickers targeted IDPs and subjected some Ukrainians to forced labour, forced conscription, and sexual exploitation in Russia-occupied areas, often via kidnapping, torture, and extortion" and " Ukrainian women and girls being recruited for sex trafficking abroad." Online searches for "Ukrainian escorts" and other search terms related to the sexual exploitation of Ukrainian women and girls increased. Traffickers targeted displaced Ukrainians via information posted online or on social media. Across Europe, Ukrainian refugees were at risk of forced labour including in domestic work, childcare, and seasonal agriculture, although there are only a few confirmed trafficking cases."

In some regions of Europe, the European Commission estimates in its 2024 Annual Review of Combating Trafficking in Human Beings in the EU[38] that up to 50% of newly identified cases of recruitment for sexual exploitation occurred via online channels. This figure demonstrates the extreme flexibility of criminal networks, which are rapidly adopting new technical opportunities. Global instability also has a significant impact on the growth of risks. The International Organisation for Migration's (IOM) World Migration Report 2024 states that the vulnerability of populations experiencing socio-economic hardship, conflict and internal displacement is increasing[39]. At the same time, according to the Rapid Gender Analysis conducted by UN Women and CARE International in May 2022, 90 per cent of those who left Ukraine are women and children[40]. During times of crisis, women may be more inclined to trust dubious offers of employment or relocation, without being able to thoroughly verify the sources of information. This allows perpetrators to exploit the crisis situation as a cover for manipulation and dissemination of false advertisements.

The technical component of the problem is not standing still either. A special analysis by Europol[41], published in April 2024, indicates that perpetrators are increasingly using encrypted messengers, anonymous networks (such as Tor), and cryptocurrency transactions. Such technologies make it much more difficult to identify the real people

37 https://ua.usembassy.gov/wp-content/uploads/sites/151/2023_TIPR_UKR.pdf
38 https://ec.europa.eu/anti-trafficking
39 https://ua.usembassy.gov/wp-content/uploads/sites/151/2023_TIPR_UKR.pdf
40 https://news.un.org/en/story/2022/03/1114592
41 https://www.europol.europa.eu

behind the illegal activities. The lack of unified data exchange protocols and differences in the laws of different countries complicate international law enforcement cooperation. A review published by the OSCE Office for Democratic Institutions and Human Rights in August 2024[42] highlights the problem of insufficient digital literacy among vulnerable groups and low awareness of online protection mechanisms. This factor, combined with an imperfect content moderation system and slow response from some online platforms, allows perpetrators to operate undetected for a long time. The European Commission, in its Interim Report on the Implementation of the EU Strategy to Combat Trafficking in Human Beings (2021-2025) of October 2024, emphasises the need to harmonise legislative approaches, increase the efficiency of the public and private sectors, and introduce the latest tools for analysing large amounts of data. Without such coherence, it will be difficult to build an effective international mechanism for early detection of threats and timely response.

Thus, the key threats and challenges in the online environment for Ukrainian women and girls lie in the ability of perpetrators to quickly use technological opportunities, anonymity and the cross-border nature of the Internet to recruit and control their victims. At the same time, government agencies, law enforcement, civil society and international organisations need to find new approaches to legal and regulatory frameworks, join forces, improve monitoring and analysis tools, and raise awareness and digital literacy among the population. Only a systematic, multi-level approach, reinforced by adequate resources, will effectively deter and reduce the threats associated with the use of online space for criminal purposes.

## ANALYSIS OF HIGH-RISK ONLINE PLATFORMS, OVERVIEW AND PRACTICAL CASES

The Ukrainian online community is characterised by widespread and active use of social media. According to analytical platforms, in 2023-2024, the share of users who regularly accessed social media was over 65% of all Internet users in the country. The most active users were those aged 18 to 44, with particular activity in the 25-34 and 35-44 age groups.

In the context of war and economic instability, many women and young girls use social media to search information about opportunities to travel abroad, part-time work or educational programmes, and not always they have the time and resources to carefully verify sources. This creates risks of labour or sexual exploitation. In addition, many women who have stayed in Ukraine face challenges in providing for their families on their own due to the loss of the primary breadwinner and difficulties in finding employment. After all, the full-scale Russian military aggression has provoked an increase in unemployment and poverty, often leaving women as the sole earners in their households.[43]

The war also has a significant impact on the psychological and emotional wellbeing of women and girls: they struggle to cope with forced displacement, loss of loved ones, continuous attacks, etc. Social media are becoming not only a means to seek assistance, but also a platform to express pain and hope for support. However, the risk of cyberviolence – including recruitment, manipulation, and threats – is also increasing.

Therefore, it is important to develop digital literacy initiatives and support for women to help them avoid dangers, as well as to promote their safety and social inclusion.

### Facebook

This platform in Ukraine has a fairly wide audience of users aged 25-45. Although Facebook's popularity has been declining among young people in recent years, it remains a tool for professional networking, job search, and discussions in numerous thematic groups. Perpetrators post fake job offers in groups focused on work abroad, presenting members "legitimate" job opportunities in the service, hospitality, modelling or entertainment sectors. Since Facebook groups can have thousands of members, recruiters gain access to a large and engaged audience.

42 https://www.osce.org/odihr
43 https://ukraine.unwomen.org/sites/default/files/2023-08/best_practice_analysis_private_sector.pdf

As of the beginning of 2024, there were 13.85 million Facebook users in Ukraine, which is approximately 37% of the total population. Of these users, 52.9% were women and 47.1% were men[44]. The largest age group is 25-34 years old (NapoleonCat[45] data, December 2024). This data indicates that women constitute a larger share of social media users in Ukraine.

***Case:*** In the group "Jobs for women in Europe without intermediaries", fake accounts periodically post advertisements for vacancies such as "an assistant in an elite hotel", "an assistant in a holiday home" and others. The contact person insists on moving the conversation to private messages or Telegram for a more detailed discussion. Candidates are asked to provide passport details for "visa processing" and make an "advance payment" for the agency's services, and then they are blackmailed or their personal details are used for recruitment for coercion into sexual exploitation.

"As soon as I moved abroad, at the beginning of the full-scale war, I constantly received messages on Facebook offering work in clubs or escorting rich people. The messages always emphasized that the work was easy. To get a job, you had to write in messenger."

(from the response of a focus group participant)

"When I was looking for a job, I saw an offer advertised on Facebook. The advert did not contain full information about the vacancy and the working conditions. They demanded money from me to get this information."

(from the response of a focus group participant, an unemployed woman, IDP, resided in the temporarily occupied territory, 30 years old)

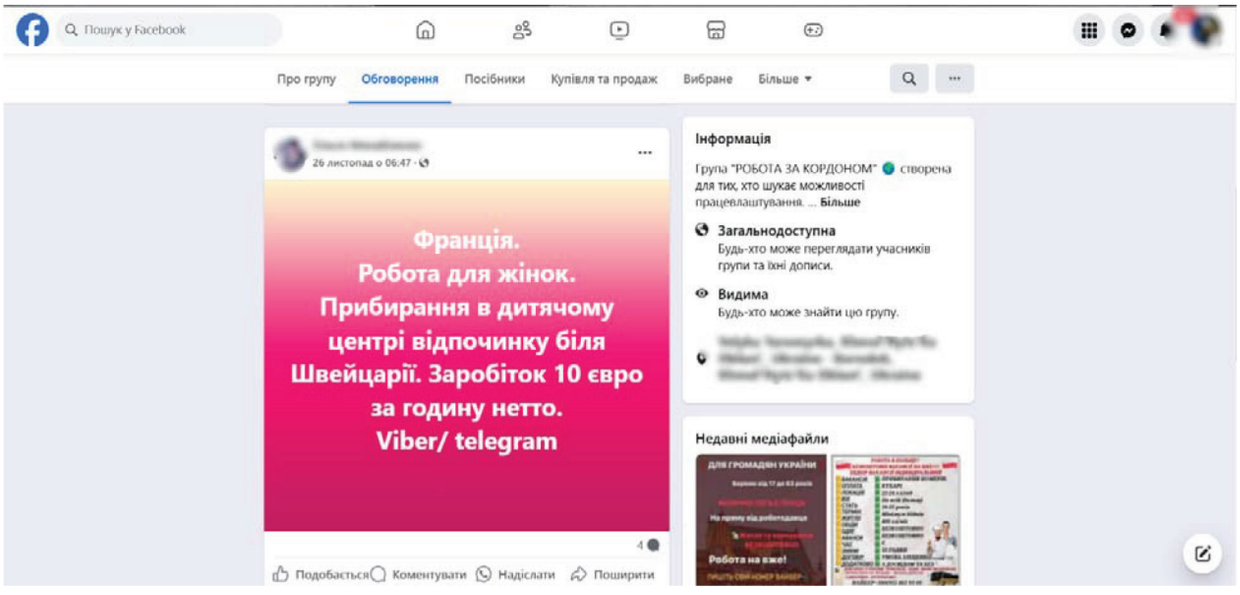



**Fig. 1. Example of a potentially harmful publication**

44 https://ms.detector.media/internet/post/34670/2024-04-15-kilkist-korystuvachiv-sotsmerezh-v-ukraini-za-rik-zmenshylasya-na-10/?utm_source=chatgpt.com

45 https://napoleoncat.com/

**Instagram**

The Instagram social network in Ukraine is actively used by women aged 18 to 35. According to NapoleonCat, among Instagram users in Ukraine, 63.4% are women and 36.6% are men. The visual component stimulates trust in profiles that demonstrate a "beautiful life", attractive working conditions, and allegedly successful stories of those who have already moved abroad. Recruiters can create profiles of modelling agencies, beauty salons, "international recruitment companies", publish success stories, photos of "happy girls" in luxurious settings. Through direct messages, they establish individual contact and create a sense of perspective and security in their target.

***Case:*** A profile with hundreds of followers posts photos of "clients" who have allegedly achieved success in Milan or Paris. In private messages, the interested person is invited to an online interview, asked to send a full-length photos, copies of documents, and sometimes even intimate photos under the pretext of "assessing their appearance". Once such materials are received, perpetrators use them to blackmail or coerce the person into traveling abroad, where they maintain full control over the person.

**TikTok**

According to DataReportal, TikTok had 17 million users aged 18 and above in Ukraine in late 2024. The platform's advertisement reach was equivalent to 53.6 percent of the country's adult population.

According to data from the Start.io platform , TikTok's audience in Ukraine is distributed as follows:

- 18–24 years old: 50.7%
- 25–34 years old: 28.3%
- 35–44 years old: 11.8%
- 45–54 years old: 4.8%
- over 55 years old: 4.4%

Among TikTok users in Ukraine, 50.9% are women and 49.1% are men.

This platform is especially popular among young people (approximately 16-25 years old), who spend a significant amount of time there watching short videos. A lot of content is consumed without in-depth analysis. Recruiters create videos with tips on how to make quick money, life hacks for travelling abroad without bureaucracy, using trending hashtags.

***Case:*** A short video with the hashtag #workEurope, where an anonymous author claims to help find a high-paying job without language skills. The description includes a contact on Telegram. The user, who is looking for travel opportunities, texts them and receives "Instructions" that require personal data and promise a quick trip. As a result, she falls into the trap of exploitation.

**YouTube**

Ukrainian women often watch longer videos, entertaining, educational and motivational content on this platform. Perpetrators post stories of "successful migration", interviews with alleged employment experts, and leave contact details in the description or comments.

***Case:*** A video in which a "manager of an international recruitment agency" talks about incredible opportunities for Ukrainian women in Switzerland. Those interested follow the link in the description, get into a private chat, where they are prompted to provide personal information, photos, and transfer money for "paperwork". This leads to blackmail, isolation and coercion.

**Messengers: Telegram, Viber, WhatsApp**

Messengers are extremely popular among Ukrainian users due to their ease of use, mobility, and the possibility to create channels and groups. Telegram and Viber are one of the key means of communication, especially in times of crisis and conflict, when users are looking for up-to-the-minute news and offers. According to various estimates, more than 50% of Ukrainian Internet users use Telegram channels and chats.

Unfortunately, there is no sex-disaggregated statistics on the number of Telegram, Viber and WhatsApp users in Ukraine. However, a survey conducted by AIN.UA in 2023 revealed that 50.6% of respondents chose Telegram as their main messenger for communication, while Viber was used by 18.5% and WhatsApp by only 6% .

**Telegram**

This messenger allows you to create hidden groups, channels, using pseudonyms, and chatbots. The lack of strict moderation contributes to the spread of fake "work channels" and "labour exchanges abroad". Recruiters send messages in bulk, organise communication anonymously, and have wide access to the audience.

***Example:*** Closed channel "Jobs for women in the EU". Users are admitted upon requests, and the administrator shares messages about "vacancies" with high salaries. Those interested are asked to fill out an application through a bot, provide contact details and send a photo. Subsequently, the information is used for recruitment and blackmail.

46 https://www.start.io/audience/tiktok-users-in-ukraine?utm_source=chatgpt.com
47 https://ain.ua/2023/03/09/telegram-osnovnyj-mesendzher-opytuvannya/

**Viber**

Interest groups are created on Viber: “Work in Poland”, “Moving to the Czech Republic”, etc. Perpetrators can join and contact potential victims directly. Although Viber is not as open as Telegram, some groups post unverified ads, creating a favourable environment for recruitment.

***Example:*** The Job in Prague group publishes a vacancy for a maid in a hotel with a “sky-high” salary. The potential candidate is asked to contact them via private messages, where perpetrators demand to send personal data or pay a “processing deposit”. After that, the candidate falls under the control of the perpetrators.

**WhatsApp**

It is less popular and is often used as a supplement after initial contact on another platform. Perpetrators can transfer communication to WhatsApp to send “official” documents, photos of the premises where their target is supposed to work.

***Example:*** After meeting on Facebook, the “recruiter” asks to switch to WhatsApp, where they send fake official contract forms and photos of beautiful apartments. This creates an illusion of legitimacy and convinces the victim to comply with the perpetrators’ demands.

**Job search platforms and freelance websites**

Job search websites are popular among Ukrainians, especially in the context of the unstable economic situation. Statistics from leading websites shows millions of monthly visits. In this environment, perpetrators gain access to an audience that is already interested in new opportunities.

**Work.ua, Rabota.ua, Jooble**

They are widely used to find work, particularly abroad. Perpetrators post fictitious vacancies with attractive conditions, often without clear qualification requirements. The candidate is asked to continue the conversation off the platform, in a messenger or by email.

***Example:*** A job posting for a “holiday home assistant in Spain, no experience required” sparks interest. The recruiter asks the applicant to send passport details and a small cash payment for “paperwork” via bank transfer, after which they cut off any contact or use the information to subsequent blackmail.

**Upwork**

This international freelance platform is also popular among Ukrainian users. Cybercriminals can post projects looking for “online models”, “personal assistants”, “translators with special conditions”. The requirement to send additional materials (photos, videos) or go to private channels has been identified as a standard recruitment procedure.

***Example:*** An Upwork project: “ A European agency needs an online model, $500 per photo shoot”. The candidate sends a photo, and is offered a “higher fee” if she provides more explicit material. After receiving the intimate materials, the perpetrator resorts to blackmail, coercing her to “cooperate” and ultimately trapping her in a situation of trafficking in persons.

**Dating platforms: Tinder, Badoo, Mamba**

Online dating is actively used to find romantic relationships. Recruiters use the emotional aspect, offering not just a job, but a “new life” with a loved one abroad. Many users do a poor job of verifying the authenticity of profiles, driven by emotions and trust.

***Example:*** A man with a profile of an attractive foreigner communicates with a woman from Ukraine for several weeks, sends romantic messages, and “supports” her in difficult time. Later, he offers to come to him: he promises to pay for the trip and help with the documents. In fact, upon her arrival, he takes away her documents and forces her to engage in sex work.

**Darknet and anonymous forums**

The darknet is a special part of the Internet where perpetrators can anonymously exchange contacts, sell databases, recruitment instructions, and information about vulnerable women looking for work. Access to the darknet is more difficult, but for organised groups it serves as a space to coordinate activities without the risk of being quickly exposed.

***Example:*** On a closed forum, perpetrators offer “partnership programmes”: if another recruiter provides a certain number of women, they will be paid in cryptocurrency. There you can also find tips on how to disguise fake Facebook and Instagram profiles and avoid being detected by moderators.

**Classifieds platforms: OLX**

OLX and similar platforms sometimes become a source of contacts for those looking for cheap accommodation or urgent work without experience of international travel. Perpetrators may post an advertisement with an attractive offer and then invite their target to a private chat.

***Example:*** The advertisement “Housekeeper in Germany, free accommodation “actually leads to a scheme where the target is asked to send money for alleged “paperwork” or provide photos of documents. Subsequently, they are blackmailed, coerced into providing sexual services, or forced to travel to another country.

> "While on maternity leave, I needed some money. So I posted an advert on OLX that I could work as a nanny on an hourly basis. I received a reply about a job as a nanny in the evening from 6 to 10 pm. Then, in messages, I was asked to provide sexual services."
>
> (from the response of a focus group participant)

## TYPES OF PLATFORMS IN THE CONTEXT OF RECRUITMENT

Quantitative indicators of recruitment by platform are difficult to determine due to the shadowy nature of criminal activity. According to a 2023 report by the International Organisation for Migration, social media, messengers and other digital platforms remain one of the key channels through which trafficking survivors are recruited, among other things.[48] Other platforms, such as job search, dating and classifieds websites, also play a significant role in this process. Darknet in this context is not a public platform for contacting victims, but rather a tool for coordination between perpetrators, so its role is particularly difficult to measure. According to the independent research of the Ukrainian digital market, Telegram is the most popular platform as a news and information messenger, while Instagram and TikTok are actively growing their audience among young people, and Facebook, although losing ground in some segments, remains an important means of communication for a large part of the population. From the perspective of perpetrators, each of these platforms has its own advantages: Facebook and YouTube for building trust and narratives, Instagram and TikTok for emotional engagement of young people, and Telegram and Viber for quickly transferring contact to a private, less regulated area.

Women and girls are a particularly vulnerable group in this process, often becoming targets of sexual and labour exploitation. Russia's full-scale war against Ukraine has significantly exacerbated this problem, as millions of women are displaced or look for work or support, often without the opportunity to carefully verify information. Perpetrators take advantage of the insecurity by offering allegedly legitimate jobs and assistance programmes. Dating websites and social media can be particularly dangerous for young girls, who are forced into communication through psychological coercion or blackmail, which can ultimately lead to exploitation.

The danger of dating websites and social networks for young girls is confirmed by global research: according to NSPCC data[49] in the United Kingdom, 83% of online grooming victims are underage girls; according to a study by Thorn[50], 18% of teenage girls aged 13-17 in the United States fall into the high-risk group for online exploitation.

The potential increase in the number of female users on Instagram and TikTok makes these platforms attractive to perpetrators who create fake accounts and recruit women and girls with promises of quick money or safe relocation abroad.

It is also worth noting that in messengers such as Telegram and Viber, women may face more direct forms of cyberviolence: harassment, receiving explicit photos or extortion of sexual content. A particular danger is posed by groups that discuss and sell women's personal data, as well as disseminate manipulation instructions, such as how to coerce a person to travel abroad under the pretext of work or romantic relationships.

An analysis of the responses of women and girls participating in the focus groups revealed that that they most frequently use the following online platforms: Facebook (33% of women and girls surveyed), Instagram (28%), Telegram (28%), YouTube (9%), Viber (26%), Messenger (3%), Signal (5%), Tik Tok (4%). For all participants of the focus groups, the use of online platforms and messengers is about communicating with their families, friends, and acquaintances, as well as finding important and useful information and raising their awareness.

Each of the platforms in question offers its own unique online environment with specific technical characteristics, audience and style of communication. This allows perpetrators to select the most effective tactics targeting specific groups of women, taking into account their social and economic status, cultural and age characteristics. Experience shows that even platforms with

48 https://www.iom.int/msite/annual-report-2023/

49 https://www.nspcc.org.uk/about-us/news-opinion/2023/2023-08-14-82-rise-in-online-grooming-crimes-against-children-in-the-last-5-years/?utm_source=chatgpt.com

50 https://www.thorn.org/press-releases/online-grooming-report-young-peoples-online-encounters-growing-riskier/?utm_source=chatgpt.com

advanced moderation systems do not guarantee full protection against fake offers, as fraudsters are constantly improving their methods of circumventing the rules. This analysis underscores the need for a comprehensive approach to counteracting fake advertisements: strengthening technological tools to detect threats, raising user awareness, developing special educational programmes on digital security, and improving cooperation between public and private entities. This will ensure more effective counteraction to the use of online space for recruitment in trafficking situations.

Below is a list of the main platforms with a description of their type, specifics of criminal misuse and an indicative level of risk for potential victims. The assessment of "low", "medium" or "high" is approximate and is based on the platform's popularity, the possibility of establishing individual contact with victims, the anonymity of communications, as well as the available data on documented cases of these resources being used for trafficking in persons.

| Platform | Platform type | Features of criminal misuse | Estimated level of risk for women and girls |
|---|---|---|---|
| Facebook | Social network | Use of open/closed groups and pages to publish fake vacancies, recruitment through personal messages, creation of fake "recruiter" accounts | Medium |
| Instagram | Social network (visual) | Eye-catching visual content, fake modelling agencies or career opportunities, direct messages for individual impact | High |
| TikTok | Social network (short videos) | Use of trends, hashtags, offers of quick money without formalities, targeted at young people, low level of critical thinking of the audience | High |
| YouTube | Video platform | Sharing "success" stories, motivational stories, providing contacts of "recruiters" in descriptions or comments, longer content to build trust | Medium |
| Telegram | Messenger (channels, groups) | Private groups, channels, bots for collecting information, anonymity, quick access to a large number of users, use of pseudo-employment agencies | High |
| Viber | Messenger (local groups) | Smaller scale of open communities, but possible recruitment through private messages in groups for employment abroad | Medium |
| WhatsApp | Messenger (less popular in Ukraine) | Used mainly after establishing contact on other platforms, sending instructions, documents, "supplementing" the main communication | Low - medium |

| | | | |
|---|---|---|---|
| Work.ua, Rabota.ua, Jooble | Job search platforms | Posting fake vacancies with attractive terms and conditions, communication quickly moves to private channels, extortion of personal data or “contributions” | High |
| Upwork | Freelance platform | Creation of fake projects for “models” or “assistants”, gradual transition to a private channel, collection of personal data and materials for blackmail | Medium - high |
| Tinder, Badoo, Mamba | Dating platforms | Emotional connection, romantic aspect, creating an image of a reliable partner, offers of relocation, work or “living together” with further coercion to exploitation | High |
| Darknet (anonymous forums) | Anonymous shadow resources | Exchange of instructions, sale of information about potential victims, coordination of criminal networks, difficult access for law enforcement | High |
| OLX | Ads platform | Fake job advertisements, housing abroad, transfer to private channels, collection of personal data or advance payments, subsequent blackmail | Medium - high |

## MANIPULATIVE METHODS OF RECRUITING WOMEN

Criminal groups specialising in trafficking in persons are constantly improving their methods of influence and manipulation. Whereas previously they relied primarily on deception about the nature of the work or the field of activity, today their approaches have become much more flexible and sophisticated. Using an arsenal of psychological, social and technological techniques, recruiters focus on the specific traits and needs of potential victims, choosing the most effective means to keep their attention and build trust.

Firstly, a fairly common method is to create an idea of “the only chance” or “exceptional opportunity”. Women are offered unique vacancies that allegedly do not require any experience, language skills or special abilities, but promise high pay and comfortable working conditions. Often, such offers can be accompanied by “success” stories, supported by allegedly real feedback from “clients” who have already used the services of intermediaries and successfully found work abroad. This creates the impression that the victim has stumbled upon a very profitable, but rare option that should not be missed.

> “I kept receiving messages on Instagram that appeared to be professional requests for employment abroad. They contained success stories of other women who had found employment through this agency. But over time, all of those requests turned out to be well-disguised and contained sexual overtones. Now I just block such requests.”
>
> (from an anonymous response of a focus group participant)

Secondly, recruiters actively use the interests and values of their victims. If they manage to find out about a

woman's desires – for example, to find a stable job, leave the danger zone, provide better living conditions for her family, or realise her talents in art or modelling – they will build communication in such a way that their offer seems to be the perfect answer to those needs. They may emphasise that they know how difficult it is to find a job abroad on your own and offer to take care of all the difficulties: preparing documents, arranging accommodation, finding an employer.

These trends are confirmed by the responses of women and girls participating in the focus groups. 77% of the women and girls interviewed confidently said that during the full-scale war they had often encountered similar suspicious offers on the Internet.

> "When I moved to Germany because of the war in Ukraine, a lot of strangers wrote to me in all the messengers I had, offering me a job, promising me housing and money. This continued until I blocked everyone."
>
> (from an anonymous response of a focus group participant)

The third aspect is a gradual emotional attachment. In addition to formal proposals, perpetrators often try to establish more personal contact: they ask questions about a woman's life, her dreams and fears, and demonstrate understanding and sympathy. This approach is especially typical in cases where the perpetrator poses as a romantic partner or a friendly assistant. In the course of correspondence or conversations, the recruiter creates an impression of safety and empathy. The victim may feel that she has found a person who listens carefully, understands the situation and sincerely wants to help. Emotional connection reduces wariness and makes it more likely that the victim will agree to take further steps, such as relocating, providing personal data, or fulfilling the recruiter's "small requests".

> "I constantly receive friend requests on Facebook and message requests on Messenger. Most of those requests are from men from other countries, as indicated in their profiles. They ask me about my personal life and work. I have never accepted such requests or replied to their messages."
>
> (from the response of a focus group participant who lived in the temporarily occupied territory, a mother of many children, raising a child with a disability, 38 years old, Lviv

> "At first, I could not understand the purpose of such private messages. Initially, I even found the attention pleasant, but then, when he began to ask me more questions about my life, with whom I lived, my income, who lived with me, and my relationships, I refused to answer. The following messages were manipulative and threatening. I could only stop them by blocking this profile."
>
> (from the response of a focus group participant, Khmelnytskyi region

The fourth method is to use gradualism and small steps. Perpetrators do not ask for everything at once. At first, they may ask for a CV or photos, allegedly necessary for "pre-selection" or "registration". Then they may ask to pay a small "service fee" or "insurance premium", justifying it with bureaucratic requirements of the employer or migration services. Over time, the demands become more and more stringent: send copies of documents, provide addresses of relatives, confirm readiness to leave on a specific date. Such small steps make the victim feel that they have already invested their resources and that it will be more difficult to refuse.

The fifth factor is the use of time and urgency. Recruiters often emphasise that the offer is valid for only a few days or even hours, and if a woman does not make up her mind now, she will miss her chance for a better life. Such time pressure reduces the ability to think critically, check information, and consult with family or friends. It creates an artificial sense of scarcity and urgency, which pushes for hasty decisions.

> “While looking for a job, I visited a lot of relevant websites. Then I started receiving job offers in messengers. One day, I think it was on Viber, I received a message about a “hot” vacancy that would be relevant for only a few days, and they immediately sent me a CV form. In the education section, I indicated that I had a university degree. A few hours later, I received a reply that the vacancy did not require a university degree.”
>
> (from the response of a focus group participant)

> “While looking for a job, I encountered a persistent employer who sent me private messages and urged me to make a positive decision about the job I was offered abroad.”
>
> (from the response of a focus group participant)

The sixth technique is the use of language and cultural codes. Perpetrators may adopt the manner of communication of a particular group, use local slang, or make references to specific events, news or realities that are familiar to their victim. This helps with building trust, as it makes it seem that that person really understands the context of the woman’s life, reducing suspicion that they might be a fraudster from another country. This adaptation to the victim’s culture and language is particularly effective when perpetrators carefully study social media profiles, comments and posts to understand what might be emotionally affecting.

> “I notice in local groups in Italy that, when someone is looking for work or help, some inadequate offers pop up. But those who respond to such offers are pressured with their position, feelings, while perpetrators create a false sense of positivity.”
>
> (from the response of a focus group participant)

The seventh method is the use of positive associations and brands. Sometimes perpetrators hide behind well-known international organisations, agencies or companies that the victim may have heard of in the news or advertising. For example, they may mention the name of a well-known modelling agency, refer to a non-existent “deal” with a well-known hotel brand, or claim to be acting on the recommendation of an international charity. Such associations automatically inspire trust and a desire to use an “exclusive channel” that is supposedly available only to the chosen few.

> “I came across an advert for a photo shoot on fairly favourable terms with the possibility of sending the photos to a well-known agency. At first, everything was fine and looked like a real photo shoot. But at the end of it, I was offered all sorts of additional “perks” if I agreed to an additional photo shoot on their terms after the main one.”
>
> (from the response of a 26-year-old focus group participant)

The eighth technique is switching communication channels to enhance the effect. After initiating recruitment on one platform (for example, a social network), the perpetrator suggests moving to a more “private” and supposedly secure channel (messenger, email) where “confidential information” can be shared. This change of medium creates the illusion of closer and more personal contact. It also makes it difficult for the administration of the platform where the contact originally took place to track the dialogue.

The ninth aspect is forcing the victim to perform a certain “preliminary” action, which will later become a lever of pressure. This can be a photo taken in a compromising pose, a copy of documents, or a recording of an intimate conversation. Once such material is obtained, the perpetrator can easily turn the initial trusting interaction into a blackmail tool, compelling the woman to continue cooperation or to travel abroad to a place where she will be subjected to control.

Focus group participants noted that online contacts, in particular during the job search, pressured them to disclose personal information: hobbies, education, employment, information about relatives and children, and asked them to send photos and videos.

> "When asked about my personal data, I always answered that I do not talk about these topics with strangers. Once I received a shocking response: "I already know a lot about you, just go to my page and see for yourself." I immediately replied that I was contacting the cyber police. I never received any more messages like that."
>
> (from the response of a focus group participant)

The tenth factor is the manipulation with fears. If the victim expresses doubts or asks for too many details, the perpetrator can switch to intimidation: if she refuses right now, she will lose the money she has already transferred or her photos will become public. This turns recruitment into a form of psychological terror, where a woman no longer acts out of hope, but out of fear and a sense of hopelessness.

All these methods can be combined. For example, perpetrators can first create the illusion of an exceptional opportunity, then establish an emotional connection, gradually push the woman to share personal data, and when she has doubts, switch to soft blackmail or urgency. Their main goal is to deprive the victim of the ability to objectively assess the situation, to create conditions in which the woman either sees no alternatives or is too involved to refuse.

Thus, the methods of recruiting women are based on a thorough study of the needs, fears, aspirations and context of each individual victim. Recruiters are skilled psychologists who use a variety of influence, manipulation and deception techniques to gradually make women dependent on the promised prospects. This allows perpetrators to successfully disguise their true intentions, making their offers as attractive and believable as possible.

It is worth paying attention to some other aspects mentioned by the focus group participants.

For example, 48% of focus group participants have taken media literacy courses or attended lectures, which helped them understand the threats they may face online. 52% of participants had not heard of such training.

At the same time, 80% of participants have personal data protection settings on social media, messengers, and other online platforms. But only a few percent of the respondents use two-factor authentication.

90% of focus group participants have encountered online offers that may be part of a fraudulent scheme, including: offers without specific details but with promises of significant income; promises of convenient and flexible working hours; many promises of easy work; offers only for young girls.

## SELECTION OF TOOLS AND METHODS TO MONITOR, COLLECT AND ANALYSE INFORMATION IN CYBER-SPACE IN ORDER TO IDENTIFY THREATS RELATED TO THE CRIMES OF TRAFFICKING IN PERSONS

In the field of combating trafficking in persons online, it is important not only to understand the specifics of recruitment platforms and methods, but also to use effective tools to collect, analyse and monitor information. In particular, such tools include open source intelligence (OSINT), social analytics, monitoring of darknet resources and analysis of search queries. The combination of these approaches helps quickly detect new trends in recruitment schemes, identify key risk platforms and common patterns of criminal activity, and respond to identified threats in a timely manner. In turn, this, helps increase the effectiveness of preventive measures, develop targeted education and awareness campaigns, and improve cooperation mechanisms between government agencies, CSOs and the private sector.

# TOOLS FOR COLLECTING AND ANALYSING INFORMATION FROM OPEN SOURCES

Open-source intelligence, commonly abbreviated as OSINT, is a methodology for "intelligence" or the search and analysis of information from publicly available sources. It is now possible to collect huge amounts of data on the Internet without using methods that accumulate information in an illegal way.[51] The tools that are widely used within the OSINT methodology to monitor and analyse threats related to trafficking in persons in the online space include the following software and services:

**Maltego** is a powerful tool designed to analyse data and visualise the relations between different objects such as websites, domain names, email addresses, IP addresses, social media profiles and other digital identifiers. With Maltego, you can quickly transform disparate information collected from open sources into visual graphs and charts that reveal hidden patterns, chains of related resources, or common intersections between different elements.

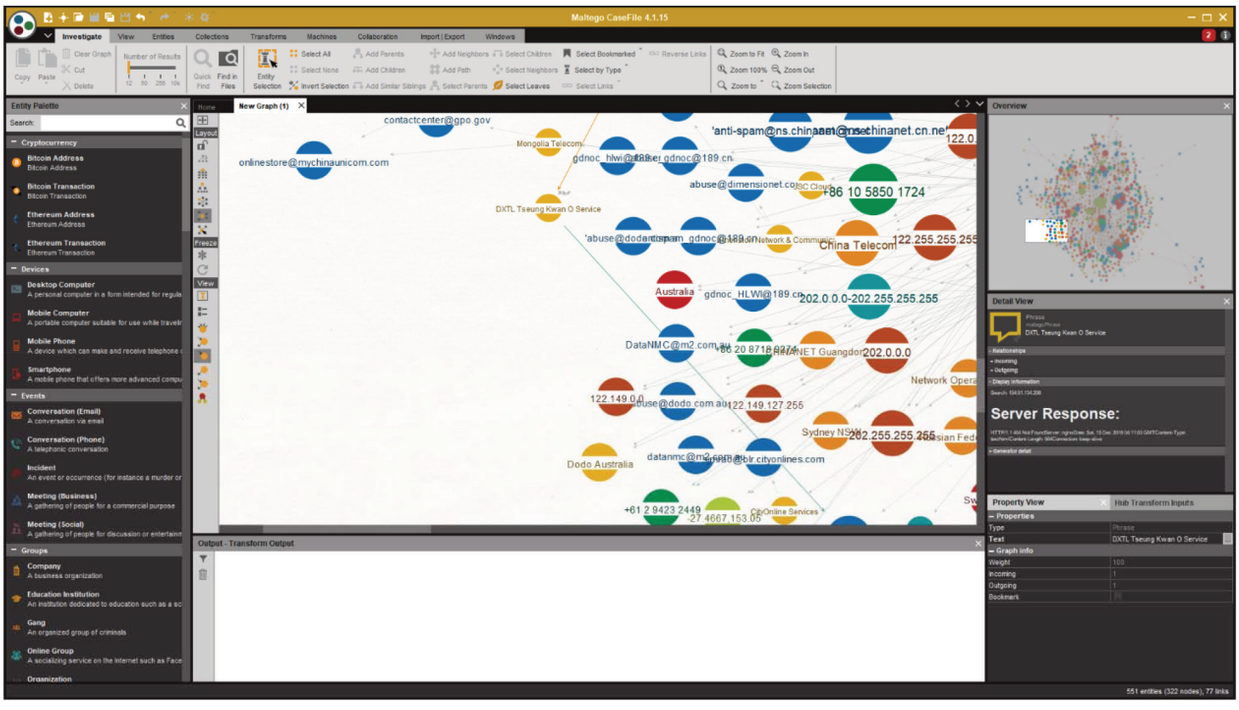



**Fig. 2 Maltego application interface (based on the materials from**
https://docs.maltego.com/support/solutions/articles/15000018948-what-is-maltego-casefile-

In the context of monitoring and analysing threats related to trafficking in persons, Maltego can perform the following tasks:

- Establishing links between suspicious social media accounts and domains hosting fake job postings;
- Identifying common indicators (e.g., repeated contact details or similar agency names) across different "attractive work abroad" advertisements;
- Uncovering a network of interconnected accounts that may belong to the same criminal group by identifying infrastructure connections and other related elements (IP addresses, hosting servers, email addresses).

In this way, Maltego enables analysts to gain a comprehensive view of potential criminal networks, creating a visually comprehensible map of interactions and supporting the development of more targeted and effective countermeasures.

**Artellence** is a Ukrainian IT company that develops unique AI technologies and works on OSINT projects. In particular, it offers BigDataPeople 2, a tool for solving OSINT tasks based on big data that comprehensively analyses the public information space and digital footprints using the latest advances in generative artificial intelligence. The product analyses data from social media, messengers, marketplaces and other open sources based on search queries, while machine learning algorithms help to structure and unify it.

51 https://www.issp.training/post/osint-chomu-tsey-napryam-takyy-perspektyvnyy-i-komu-vin-mozhe-znadobytysya

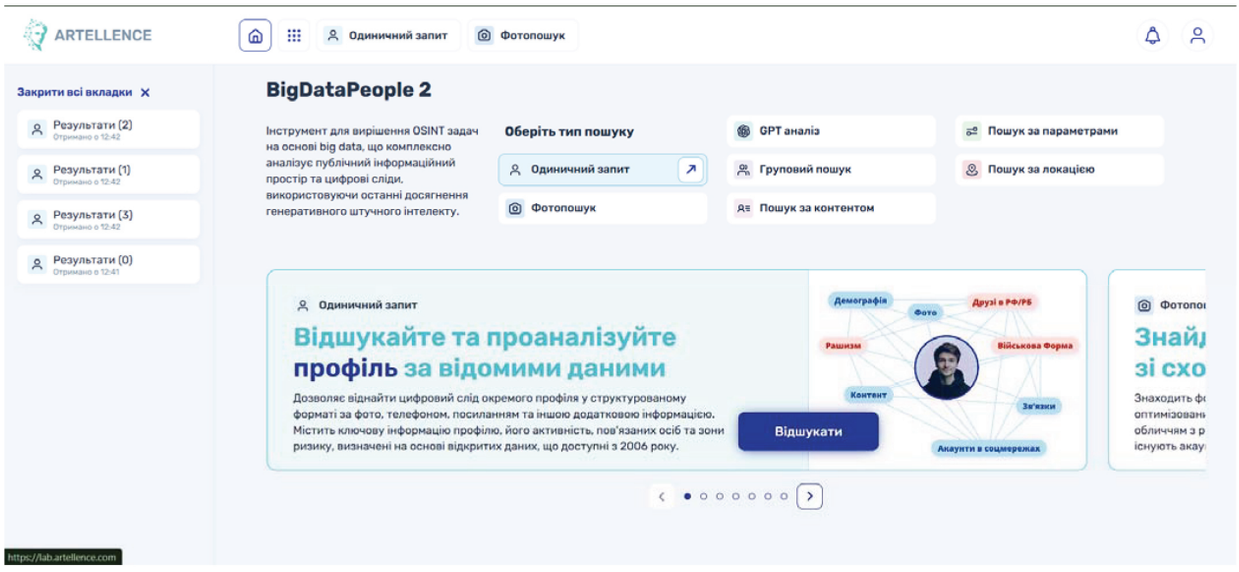



**Fig. 3 Artellence application interface**

**IntelligenceX** is a search and analytical tool focused on working with open data (OSINT) and closed sources of information, such as the darknet, public and private databases, forums, social media, etc. Its main purpose is to provide access to historical and up-to-date data for investigations related to cybercrime, fraud, security breaches, as well as to ensure transparency and protection.

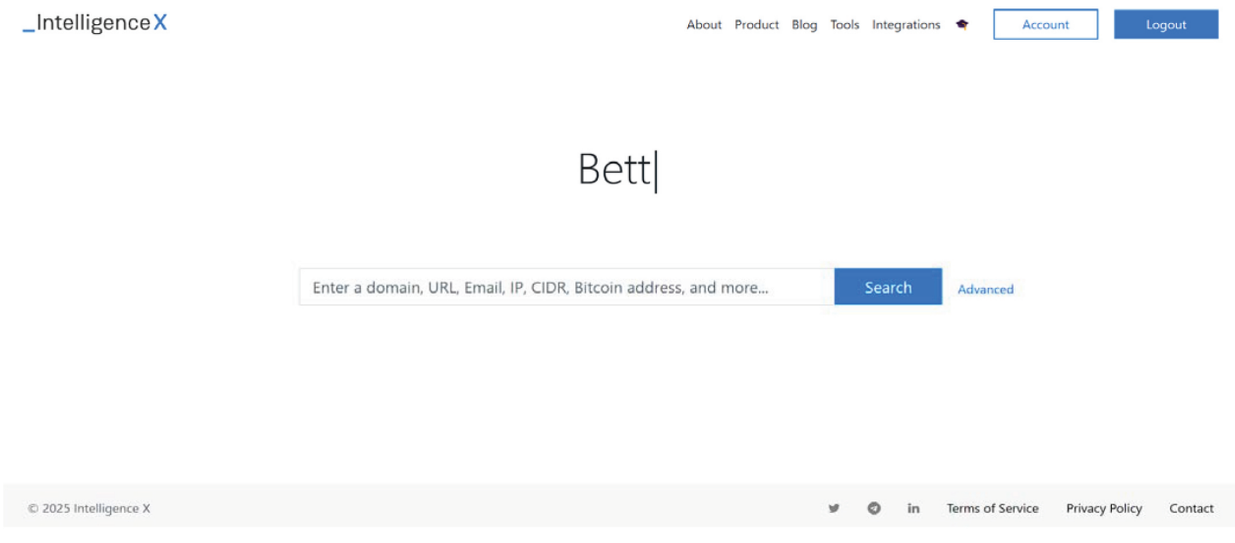



**Fig. 4 IntelligenceX application interface**

# METHODS FOR MONITORING ONLINE RESOURCES

Monitoring information resources and analysing data related to the recruitment of people for sexual exploitation and trafficking is overall a complex and multifaceted task that requires a comprehensive approach. This process involves the systematic tracking, study and analysis of a large amount of information that may be related to illegal activities. Given the specifics of this type of crime, special attention should be given to both publicly available sources of information and hidden platforms often used by perpetrators.

When monitoring territorial information resources, it is important to focus on identifying key signs of criminal activity. This can include specific vocabulary typical of recruitment advertisements, certain keywords or phrases that indicate a search for “work abroad”, “high-paying jobs” without requirements for experience or special skills. Such advertisements usually provide a minimum of specifics, which can serve as a signal for further analysis. Effective monitoring requires knowledge of the information space in the region, in particular popular online platforms used by locals to find work or communicate. In addition, it should be borne in mind that perpetrators can disguise their activities by creating fake profiles, groups or pages, making careful attention to detail essential during monitoring.

It is equally important to take into account the geographical features of the region of the search. This may include analysing language differences specific to certain areas or the use of words from the regional dialect to help narrow down the search. The territorial aspect also involves understanding the local infrastructure, such as Internet service providers, popular local platforms and forums that perpetrators may use for their activities.

One of the key elements of analysis is the ability to identify not only the content itself but also its source. This requires consideration of technical aspects, such as the pool of IP addresses that can be associated with regional providers or networks. This makes it possible to determine whether the information originates from a certain territory. Analysing the technical characteristics of the content, including its metadata, can also provide important clues as to the time, place and conditions of the information creation. The issue of a dynamic nature of the information space requires special attention. Recruitment-related content is often modified or deleted. Therefore, monitoring should be continuous, and the data collected should be analysed promptly to identify trends. It is important to record even the slightest changes, as they may indicate the activity of perpetrators, including a change in strategy or the relocation of their activities to another region or platform.

At the same time, monitoring cannot be effective without proper coordination between different law enforcement units or other stakeholders. Well-established communication allows for the exchange of analysis results and joint efforts to detect and stop criminal activity. This also includes cooperation with platform providers and administrators who can provide additional data for analysis.

To ensure effective monitoring and analysis of territorial information resources, especially in the context of combating recruitment for sexual exploitation and trafficking in persons, the use of specialized software tools is essential. These tools make it possible to automate the processes of collecting, processing and analysing large amounts of data, identify hidden connections between different actors and respond quickly to new threats. The use of such technologies improves the efficiency of law enforcement agencies and allows them to more accurately identify potential sources of criminal activity.

One of the simplest tools for content monitoring is Google Alerts. This is a free service from Google that allows you to automatically receive notifications about new content on the Internet that matches your search criteria. Its functionality is based on the Google search engine, enabling it to cover a wide range of sources: news, blogs, forums, websites, videos, etc. Users set keywords or phrases, and the tool tracks the appearance of new material related to these queries and sends relevant email notifications.

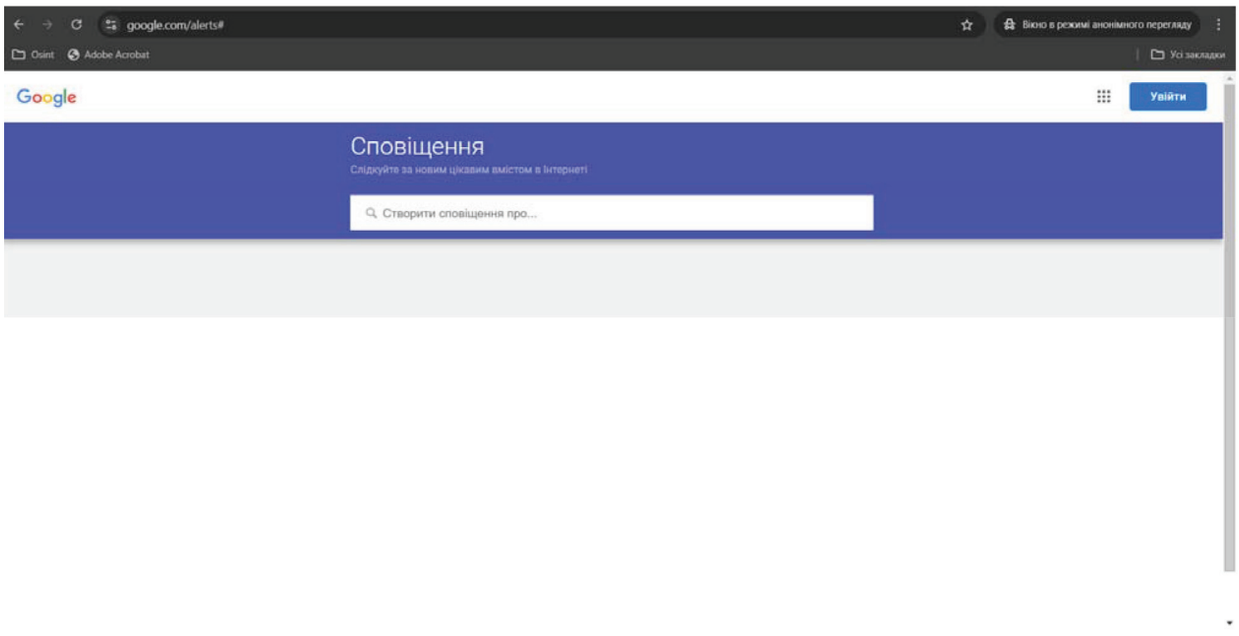



**Fig. 5 Google Alerts application interface**

Google Alerts allows you to create alerts for a variety of topics, from a person or brand to broad concepts or issues. For example, if you are interested in the topic of trafficking in persons in Ukraine, the tool will automatically find all new posts that mention those keywords and send them to your email address. The frequency of notifications is customisable: you can receive results instantly, once a day or once a week. This automation is convenient for long-term monitoring as it saves time and effort. The tool does not require you to constantly enter queries in the search engine, instead providing updates in a convenient format.

The tool also allows you to use search operators that significantly improve the accuracy and relevance of results. Here are the most popular operators, their properties, and examples of how to use them:

1. “ “ (quotation marks) operator

- Purpose: Search for an exact phrase;
- How it works: it returns only those results where the words appear in the specified order.

**Example:**

Request: “work abroad without experience”

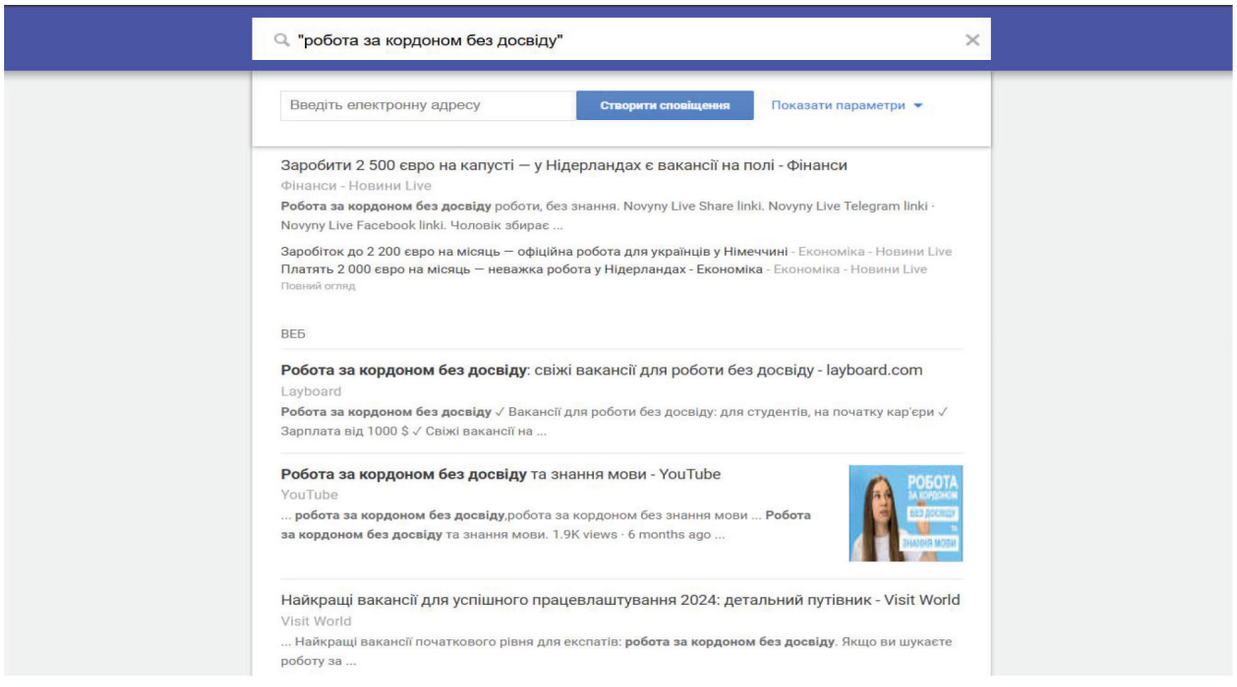



**Fig. 6 Example of using the “ “ operator (quotation marks)**

The result: displaying search results that contain only the exact wording, not variations of it.

2. OR operator

- Purpose: Search by one of several terms.
- How it works: Returns results that contain at least one of the specified words.

**Example:**

- Request: job OR vacancy.

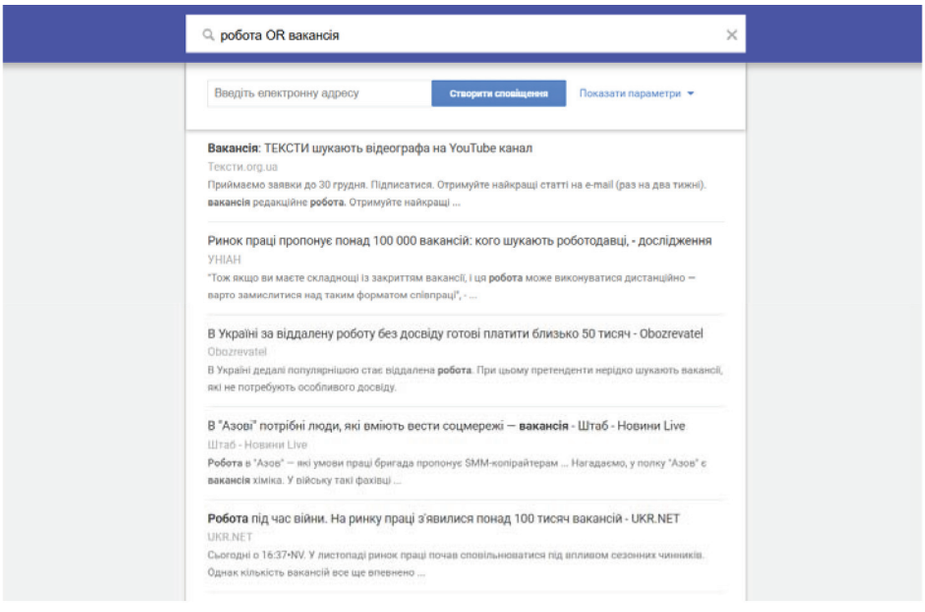



**Fig. 7 An example of using the OR operator**

Result: displaying search results that contain either the word “job” or “vacancy”.

3. AND operator

- Purpose: Search that combines multiple terms.
- How it works: Returns results that contain all the specified terms.

**Example:**

- Request: work AND web model

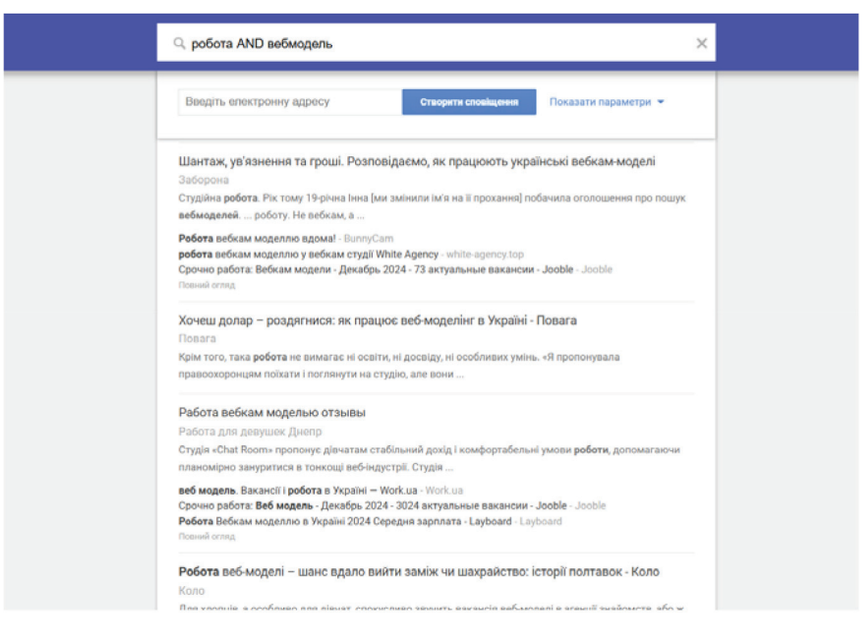



**Fig. 8 An example of using the AND operator**

Result: Displaying search results where both the words “job” and “model” are present.

4. - (minus) operator

- Purpose: Exclude certain terms from the search.
- How it works: Does not show results containing the specified word.

**Example:**

- Request: job - teacher

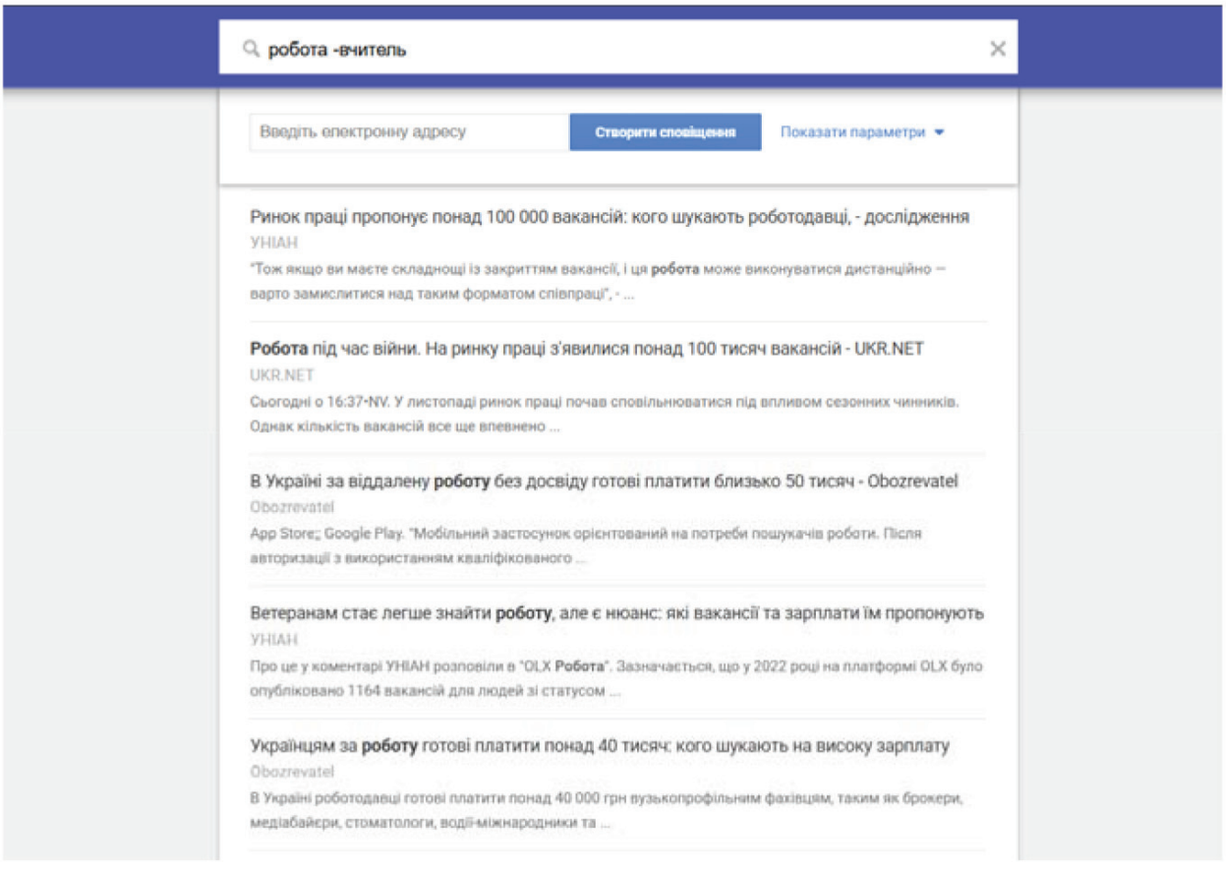



**Fig. 9 Example of using the - (minus) operator**

Result: displays search results that contain the word “work” without the word “teacher” in the text.

5. site operator

- Purpose: Search for results only on a specific website.
- How it works: Returns results limited to the specified domain name.

**Example:**

Request: work site:olx.ua

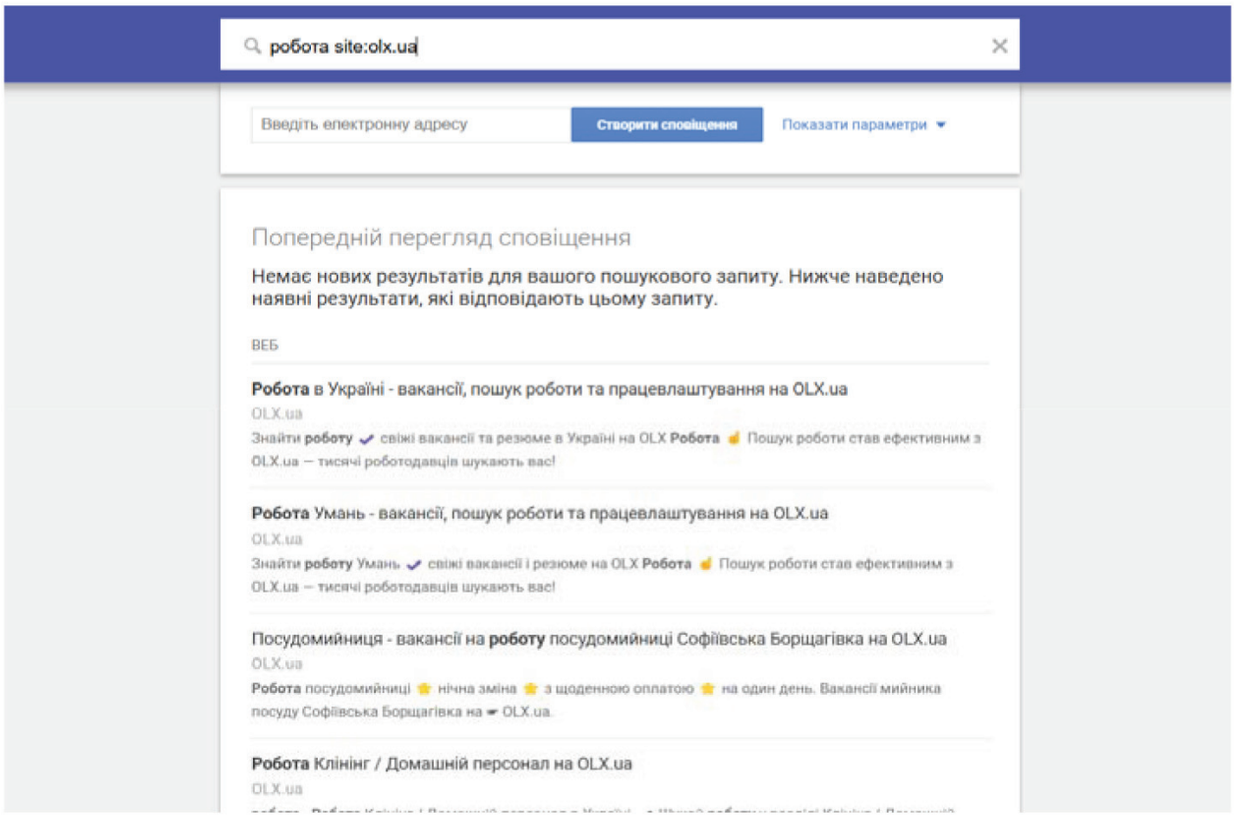



**Fig. 10 An example of using the site operator**

Result: displaying search results only from the olx.ua website.

6. 6. intitle operator:

- Purpose: Search for words in page titles.
- How it works: Returns results where the specified term is present in the titles.

**Example:**

Request: intitle:work

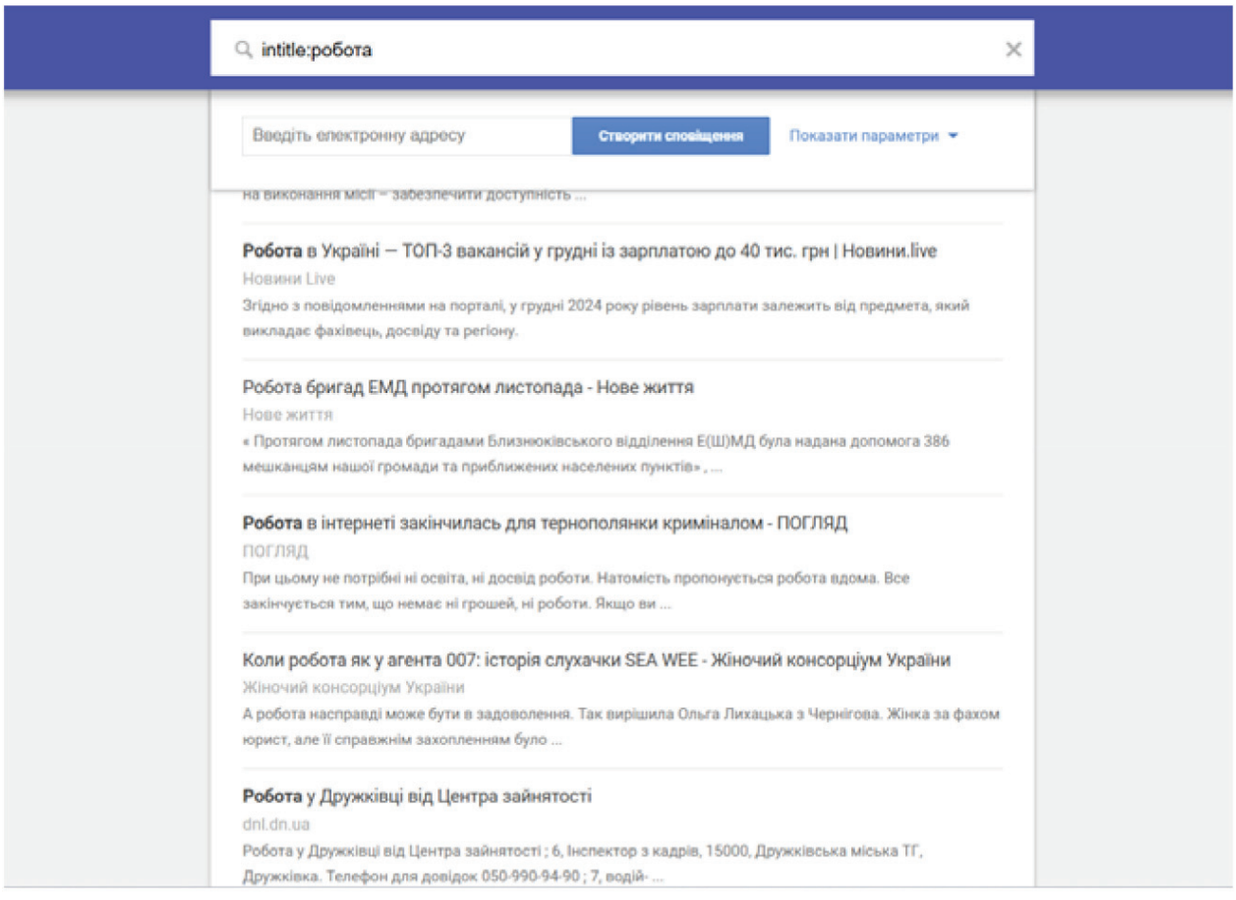



**Fig. 11 An example of using the intitle operator**

Results: Displaying search results with titles containing the word “job”.

**Situation analysis**

Imagine that an analyst investigating the recruitment of people through social media for sexual exploitation has received information about preparations for a crime through the free classifieds service OLX. The analyst will use the Google Alerts tool to monitor the advertisements that the perpetrator will publish to recruit a potential victim. He or she sets several search queries, for example:

- “work abroad without experience” site:olx.ua;
- “model vacancies, quick earnings” site:olx.ua;
- “free travel to Europe” site:olx.ua.

The analyst sets the frequency of notifications to “no more than once a day” to receive updates at the end of the day. In addition, the analyst limits the geographic region to Ukraine and sets the language to Ukrainian to ensure that the results are as relevant as possible. Over the course of a month, the analyst receives a series of messages containing links to suspicious advertisements on a given website. Some of them are a cover for recruitment, as evidenced by details such as offers of “guaranteed confidentiality” or “job without paperwork”. Using the collected materials, the analyst prepares a report that can be used to initiate an investigation.

Alongside the well-known OSINT methods and social analytics tools, there are more highly specialised systems that focus specifically on tracking and documenting potentially illegal activities related to sexual abuse and exploitation. Among them, the following ones stand out:

- ICACCOPS (Internet Crimes Against Children Child Online Protective System) is a platform primarily designed to detect and investigate crimes against children. While its core functionality is focused on combating child pornography and exploitation, the tool can also be used effectively for a wider range of trafficking crimes, as it allows monitoring of various online resources and the collection of evidence for further investigation.

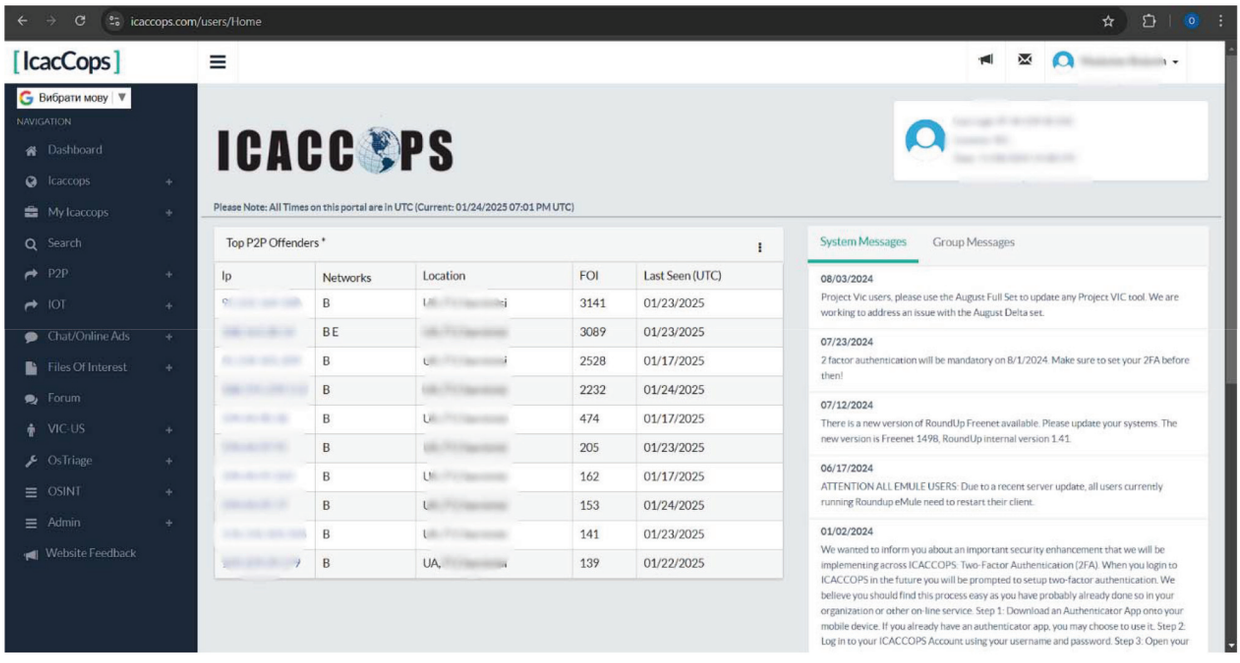



**Fig. 12. Dashboard of the ICACCOPS tool**

- GRID COP is another specialised platform that enables law enforcement agencies and authorised specialists to quickly track illegal activity in cyberspace. It provides access to data analytics tools and automated algorithms that can identify specific patterns of recruitment, distribution of compromising content, and coordination between perpetrators.


**Fig. 13. Dashboard the GRID COP tool**

Such systems are often integrated into the workflows of specialised units that investigate online crimes in relation to trafficking in persons. They allow for a quick response to new threats, the collection of digital evidence, and the establishment of links between potential perpetrators and victims. Subsequently, the accumulated information contributes to more effective cooperation between law enforcement agencies at both the national and international levels, as crimes of trafficking in persons almost always have a cross-border dimension. At the same time, the proper implementation and use of such tools requires proper skills and an understanding of the ethical and legal aspects of working with personal data.

# CONCLUSIONS

# CONCLUSIONS

The analysis of the state of trafficking in persons in cyberspace and the identification of key challenges faced by potential victims showed that modern digital technologies, despite their many advantages, also pose serious challenges related to trafficking in persons, cybercrime and online violence. The full-scale war in Ukraine has significantly increased the risks of sexual exploitation and cyberviolence, in particular against women and girls. Particular attention should be given to women and girls who are the most vulnerable to sexual violence, which is used as a tool of war and has long-term consequences for survivors and society as a whole.

The previous stages of the study found that the high level of anonymity and global accessibility of the Internet create favourable conditions for recruitment, while technological platforms do not always have sufficient mechanisms to prevent abuse. At the same time, the role of law enforcement agencies and organisations specialising in the protection of women and girls is still underestimated, as they often face limited resources or lack expertise in digital communication channels. Despite the general increase in awareness of the risks of being trafficked and the active role of state and civil society institutions, the effectiveness of the response is hampered by the rapid change in recruitment tactics and methods. Therefore, cooperation between IT companies, law enforcement and survivor rights organisations are becoming a crucial factor for successful crime prevention and survivor assistance.

Therefore, the set of recommendations covers three areas: first, comprehensive measures for the technology sector to reduce the risks of exploiting digital platforms for recruitment purposes; second, effective mechanisms for improving the skills and tools of law enforcement agencies; and third, strengthening the protection of women and girls as the most vulnerable group that is most often affected by trafficking in persons. The combination of these three dimensions allows us to cover the entire chain of issues – from creating technical barriers against criminal activity to shaping a sensitive environment in which the interests of vulnerable groups are protected systematically.

The technology sector includes a wide range of companies and organisations that develop and maintain digital services and infrastructures. This sector includes social networks (e.g., Facebook, Instagram), messengers (Telegram, WhatsApp), job search platforms (OLX, Work.ua), cloud services (AWS, Azure), as well as companies specialising in the development of machine learning algorithms, analytical tools and cybersecurity solutions. Since perpetrators most frequently use these platforms, it is necessary to continuously implement and systematically update algorithms for automatic monitoring and detection of content that may pose a threat to user safety, including content related to trafficking in persons. It is important to introduce tools that enable the rapid detection and blocking of dangerous content, including machine learning and artificial intelligence.

The algorithms proposed in the recommendations should be based on sensitivity thresholds that will allow detecting potentially dangerous content without violating users' rights. For example, algorithms can find posts using specific keywords ("work for women", "paid photo shoot"), analyse the text for criminal recruitment patterns and automatically flag the content for additional processing by moderators.

The most common behavioural patterns of criminal recruitment are as follows:

- **"Pseudo-legal" vacancies:** advertisements promising "easy work abroad", often with no experience requirements but with high pay. For example, "work as an assistant in Europe", "modelling business without contracts".
- **Emotional component:** publications that use emotionally charged phrases to create a sense of unique opportunity, for example, "only one chance to change your life";
- **Requirements to provide personal data:** request to provide copies of documents, full-length photos or intimate photos under the pretext of registration or "pre-selection";
- **Transferring to private messages:** an invitation to switch to messengers such as Telegram or WhatsApp for "more information";
- **Urgency to make a decision and subsequent pressure:** indications of a limited time frame for the offer, e.g. "last places", "register today only";
- **Advance payment offers:** demands to pay an "insurance deposit" or "fee for documents" that indicate fraudulent intent;

Particular focus should be on the projects of cooperation between IT companies and law enforcement agencies, including the creation of joint databases of potentially dangerous activities and joint platforms for collecting and analysing evidence of crimes. Such initiatives can provide a basis for creating focused analytical studies, developing risk forecasting tools and monitoring the situation in real time. For example, the use of cloud technologies to integrate databases will allow for the rapid exchange of information between government agencies and private entities.

With regard to moderation, existing mechanisms do not always meet modern challenges. Successful moderation requires not only technological solutions, but also a strategic approach based on proven data and research, which includes the following:

**Integration of innovative technologies:**

Use of machine learning algorithms based on specific patterns of criminal content. For example, text analysis systems can identify risk based on keywords, context, or profile history.

Use of computer vision technologies to identify suspicious visual materials, including those related to recruitment through fake advertisements.

**Transparency of moderation processes:**

Establishing a system of regular reporting for users, where each complaint receives a status and an explanation of the outcome of its review

Publication of statistical data on moderation activities, including the number of content removed, reasons for removal, and response time.

**Training of qualified moderators:**

Organising training programmes for moderators that include consideration of real cases of trafficking in persons and methods of identifying hidden risks.

Ensuring intercultural competence of moderators to work with content from different countries, taking into account language and cultural differences.

**Active participation of users:**

Developing simple tools for filing complaints, such as interactive forms or hot buttons to report suspicious content.

Conducting information campaigns that raise awareness of recruitment methods and teach users how to recognise fraudulent schemes.

**Cooperation with independent experts:**

Involving researchers and organisations specialising in cybersecurity and trafficking response to assess the effectiveness of moderation processes.

Organising joint initiatives between platforms, law enforcement agencies and civil society to develop interdisciplinary solutions.

All these measures are aimed at building a sustainable moderation system that takes into account the dynamic nature of criminal content. An approach focused on researching and deploying new technologies can significantly improve the quality of moderation, while ensuring user trust and protection against exploitation. Priority should be given to adaptive and interdisciplinary methods that integrate technological innovation, research and social interaction.

The use of fake accounts for criminal purposes, including trafficking in persons and sexual exploitation, highlighted in the recommendations, is also highly relevant, as perpetrators create fake profiles to disguise their true identities, making it difficult to identify and prosecute. To effectively tackle this problem, a multi-component strategy that combines technological innovation, cross-sectoral cooperation, and enhanced user authentication is needed. The first and most important task is to implement multi-level authentication. Authentication systems should include mandatory verification of users through official identity documents, combined with biometric data such as fingerprints or facial recognition. To protect the privacy of these processes, cryptographic protocols can be used to allow authentication without storing personal data in an accessible form. Technologies such as Zero Knowledge Proof can be used to verify an identity without disclosing its details. In addition, platforms should ensure that user activity is regularly checked to ensure that the profile matches the declared information.

Automated fake account detection systems should consider not only technical features, such as IP addresses or registration patterns, but also user behavioural analysis. For example, platforms can use machine learning algorithms to analyse anomalous activity, such as the simultaneous registration of a large number of accounts with similar characteristics, the lack of real activity on a profile, or the use of similar patterns in messages. This analysis can be done in collaboration with research institutions and companies that have the relevant expertise and tools.

The importance of cooperation between technology platforms, government agencies and NGOs cannot be underestimated. For example, the creation of a centralised database of fake accounts used for criminal purposes would allow for rapid information sharing between platforms and alerting other organisations to the threat. Such a mechanism could be based on international initiatives, such as Interpol or Europol, which coordinate efforts to combat cybercrime.

Particular focus should be paid on identifying accounts that use photos or personal data of real people without their consent. Such actions are a violation of human rights and should be addressed through both technical and legal means. For example, automated image recognition systems can help identify the use of stolen photos, allowing for a quick response to such violations. Public awareness is another important element of the strategy. Awareness-raising campaigns should focus on the risks of interacting with unreliable accounts. At the same time, complaint processes should be simplified for users by creating intuitive tools for reporting suspicious activity. For example, hot buttons for reporting fraud can be an effective tool in the fight against violations.

In addition, effective counteraction to trafficking in persons in the digital space is impossible without the continuous development of professional competencies of law enforcement officers and specialists involved in digital investigations. Expanding knowledge and skills in cybersecurity, data analytics and open source intelligence (OSINT) is a priority to ensure a quick and accurate response to new challenges.

First and foremost, it is necessary to implement systematic training programs that cover various aspects of digital investigations. Such programmes should include:

- Methods of collecting and analysing digital evidence. This includes learning how to work with data obtained from social media, messengers, and cloud services, as well as analysing metadata and identifying hidden connections between the perpetrators of a crime.
- Use of specialised software. Law enforcement officers should master tools for monitoring, analysing and visualising data, such as Maltego, i2 Analyst's Notebook, Cellebrite, etc.
- Techniques for working with OSINT tools. The training should cover the use of platforms for automated monitoring of open sources, image and video analysis, geolocation and information verification.
- Legal aspects of digital investigations. The course should include international norms and regional legislation governing the collection, storage and use of digital evidence to ensure that human rights are respected.

It is also necessary to introduce a certification system for law enforcement officers to confirm their qualifications in digital investigations. For example, international certifications such as the Certified Ethical Hacker (CEH) or GIAC Certified Forensic Examiner (GCFE) could become the standard for specialised units.

In addition to training programmes, it is important to create conditions for continuous improvement of skills. This includes regular practical exercises, participation in international exercises and simulations such as Capture the Flag (CTF), which simulate real-life cyber threats. In addition, law enforcement agencies should have access to the latest research in cybersecurity and data analytics to keep abreast of new trends and techniques. An essential component of competence development is the introduction of mentoring systems. Experienced professionals can pass on their knowledge and skills to younger employees, thus contributing to the creation of a talent pool with a high level of professionalism. Integration of these approaches into the daily activities of law enforcement agencies will ensure a rapid response to the challenges posed by online trafficking. Combined with technological innovations, the development of professional competencies will be the basis for increasing the effectiveness of combating this type of crime.

Additionally, it is important to note the effective identification and monitoring of online platforms that can be used for trafficking in persons, as this requires the introduction of modern technical tools and the development of a comprehensive approach to working with digital data. The main components of such tools are automated analysis systems, specialised monitoring software and machine learning algorithms. One of the key components is automated monitoring systems that allow for real-time tracking of activity on social media, message boards and other online platforms. These systems should include functionality for collecting metadata, analysing textual and visual content, and identifying patterns that are typical of trafficking recruitment. For example, the use of tools such as Hunchly or WebHarvy can help automate the process of data collection and subsequent data processing. Hunchly automatically collects URLs, timestamps, and hashes of every page you visit and takes full snapshots of websites, search inquiries, and social media.

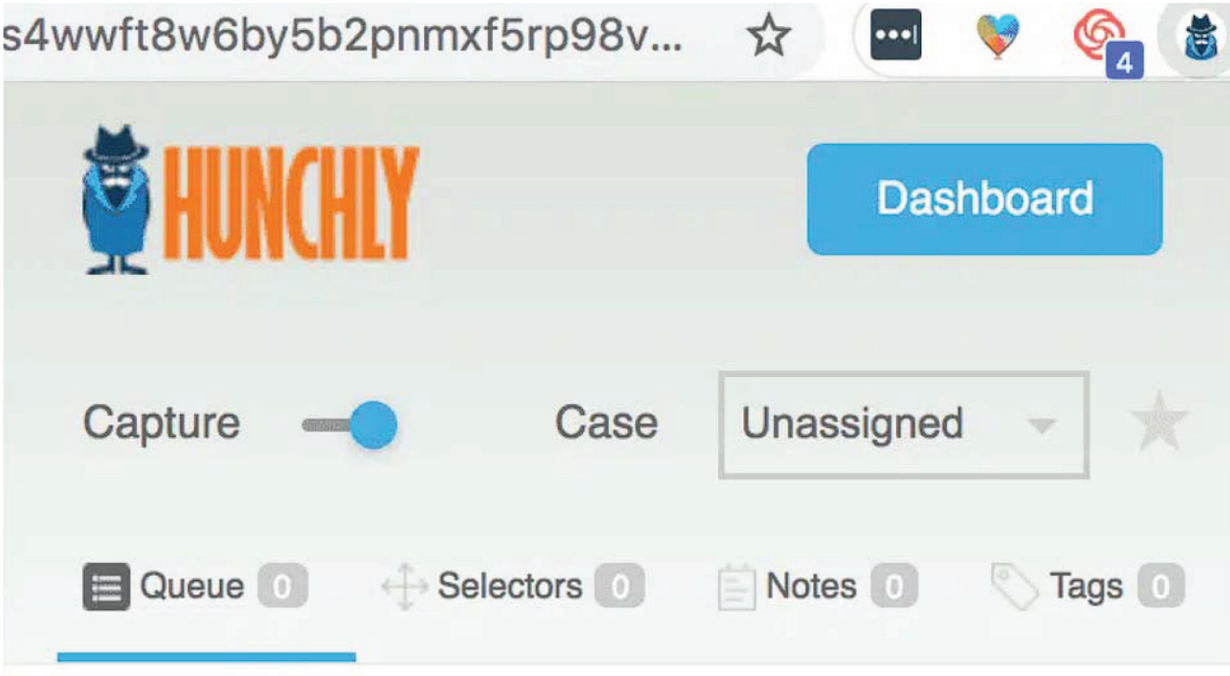



**Fig. 14 The dashboard of the HUNCHLY tool**

WebHarvy is a commercial web scraping tool[52] that automates the process of collecting data from websites without the need for programming. It is suitable for collecting structured information such as text, images, tables, prices, product lists, contact details, etc. The software has an intuitive graphical interface enabling users to easily configure scraping tasks.

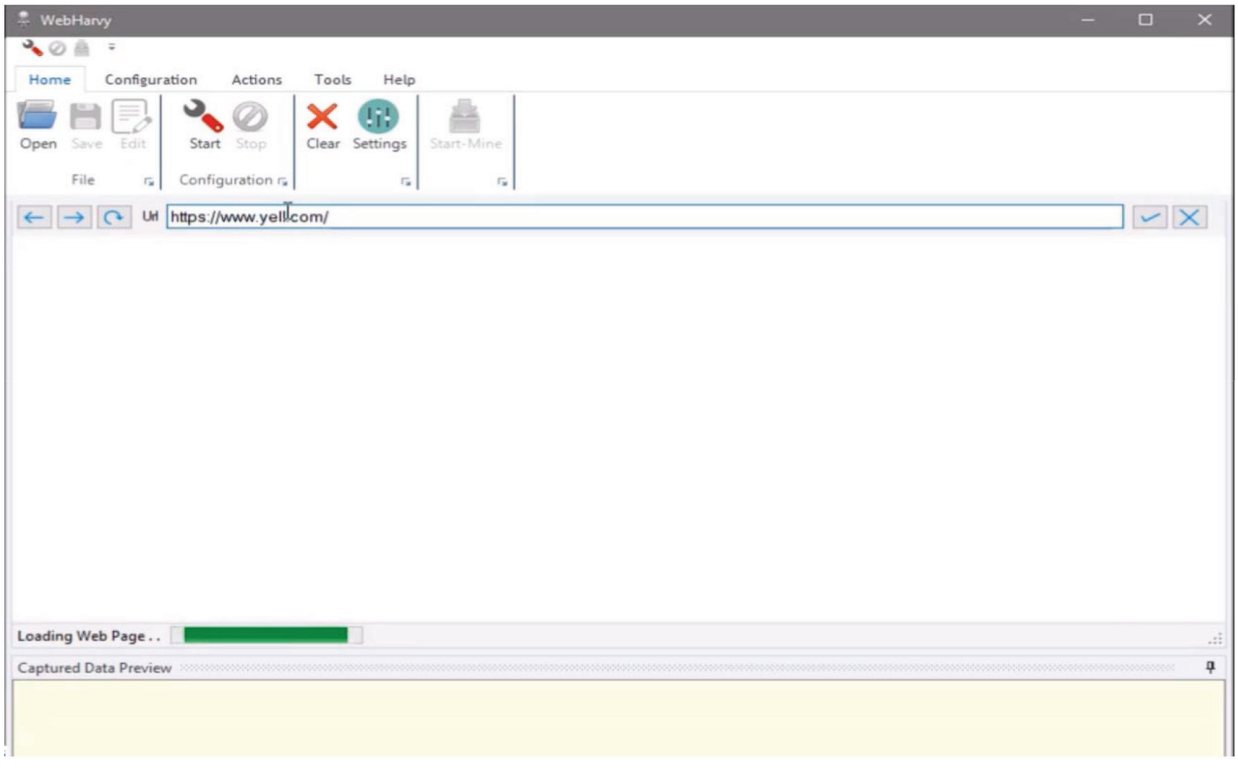



**Fig. 15 Example of using the WebHarvy tool**

52 https://www.webharvy.com/

Another important tool is analytical platforms that enable the consolidation of data into a single information environment for analysis. Solutions such as IBM i2 Analyst's Notebook make it possible to visualise connections between objects, such as suspicious profiles, contact details or geolocations, which can help identify trafficking networks. Such systems should also be capable of integrating with databases of law enforcement agencies and international organisations to share information. Machine learning algorithms play an important role in improving monitoring systems. They can be used to analyse large amounts of data and identify hidden patterns that indicate potentially criminal activity. For example, algorithms can identify specific keywords, communication patterns, or geographic trends that are typical of recruitment for trafficking in persons.

An important aspect is the cooperation between law enforcement agencies and IT companies that can provide access to monitoring tools and technical support. For example, joint projects with companies such as Google or Meta allow for the development of platform-specific solutions. In addition to technical tools, it is necessary to implement clear protocols for specialists working with monitoring. These protocols should include mechanisms to verify the information received, process signals of suspicious activity, and further transfer data for investigation. It is also important to ensure that such actions comply with legal and privacy standards.

The use of detection and monitoring tools should be integrated into the overall anti-trafficking strategy. Regular evaluation of the effectiveness of these tools, their improvement and adaptation to new threats will contribute to the creation of a safer online environment.

# RECOMMENDATIONS TO REDUCE THE RISKS OF ONLINE RECRUITMENT, STRENGTHEN THE CAPACITIES OF ANTI-TRAFFICKING ACTORS, AND IMPROVE THE PROTECTION OF WOMEN AND GIRLS

**1. Developing professional competencies in digital investigations through the introduction of specialised training programmes for law enforcement agencies, including investigators, field officers and cyber police analysts.** Today, perpetrators are actively using digital platforms and technologies to recruit people for trafficking in persons, therefore law enforcement officers must have a high level of competence in analysing digital evidence, conducting OSINT investigations, working with large amounts of data and identifying criminal networks in the Darknet.

In particular, it is recommended to introduce:

- Training programmes on the use of digital forensics tools and OSINT methods;
- Creating interagency training platforms to share experience and improve skills in working with modern analytical systems;
- Cooperation with international organisations and training centres, such as Europol, Interpol, and the OSCE, to provide courses and certification in the field of combating cybercrime and trafficking in persons.

**2. Developing and implementing tools to identify and monitor potentially dangerous online platforms by creating specialised analysis systems that will identify digital resources used for trafficking in persons and other forms of exploitation.** Trafficking in persons is increasingly facilitated through online platforms, social media, forums, dating sites and the Darknet. Existing monitoring mechanisms do not always ensure the detection of criminal activity, therefore law enforcement agencies require access to modern analytical tools and automated tracking systems.

In particular, the following is recommended:

- Using artificial intelligence to analyse large amounts of digital data and detect abnormal behaviour;
- Integrating OSINT tools for automatic collection of information from open sources;
- Introducing machine learning algorithms to recognise criminal activity patterns;
- Collaborating with IT companies and providers to identify and block resources that facilitate trafficking in persons.

3. **Strengthening interagency and international coordination by creating a single operational platform for the exchange of information between national law enforcement agencies, international entities, IT companies and NGOs involved in combating trafficking in persons.** Joint interagency think tanks should ensure rapid processing of digital data, coordinated response to threats and prompt detection of new criminal schemes. In addition, it is necessary to integrate automated systems for analysing large amounts of data to identify cross-border criminal activity.

In particular, the following is recommended:

- Creating interagency think tanks to collect, analyse and disseminate information on digital threats.
- Establishing effective data exchange with international partners (Europol, Interpol, the Council of Europe Group of Experts on Action against Trafficking in Human Beings).
- Concluding cooperation agreements with IT companies to quickly block recruitment-related accounts and content.
- Participating in joint international operations to eliminate criminal networks in the Darknet and on open digital platforms.

4. **Improving mechanisms for identifying survivors and documenting digital evidence by developing standardised protocols for working with survivors that take into account the specifics of cybercrime and online exploitation.** Identifying survivors of trafficking in persons in the digital environment is a complex process that requires the integration of various techniques, including analysing behavioural patterns, monitoring suspicious online activities and using digital traces to establish links between recruiters and survivors.

In particular, the following is recommended:

- Introducing a unified digital evidence database with automated analysis of transactions, profiles and interactions;
- Integrating mechanisms for analysing large amounts of data to identify potential survivors who have left traces of their exploitation in the online space;
- Establishing enhanced cooperation between government agencies, NGOs and the private sector to ensure effective information sharing and survivor identification;
- Expanding the authorities of law enforcement agencies to collect and analyse digital evidence, in line with international standards on personal data protection..

## RECOMMENDATIONS FOR IMPROVING THE PROTECTION OF WOMEN AND GIRLS IN CYBERSPACE

1. Introducing and implementing awareness-raising campaigns and educational programmes aimed at improving digital literacy, in particular among women and girls, and raising awareness of risks in cyberspace. Educational initiatives should cover topics such as digital security, privacy, and recognising online manipulation and recruitment techniques. It is important to involve government agencies, NGOs, educational institutions and IT companies in the campaigns. A special focus should be placed on integrating digital security programmes into the education system, as well as on creating educational materials for different age groups.
2. Supporting and developing partnerships with civil society organisations for the effective implementation of protection measures, particularly for women and girls in the digital space. Cooperation between government agencies, the private sector and civil society organisations will increase the effectiveness of prevention and intervention measures. Civil society organisations play a key role in providing support to survivors of cyberviolence, offering counselling, and implementing prevention programmes. Therefore, it is necessary to expand existing initiatives and develop joint projects to protect human rights in the digital environment.
3. Developing specialised support and safety tools for individuals, particularly women and girls, who are survivors of cybercrime and online crime. For effective protection and rapid response to threats, it is necessary to implement technological solutions that will provide timely assistance and prevent digital exploitation.

In particular, the following is recommended::

- **Developing mobile applications and online**

**platforms** for prompt assistance, including emergency call functionality, consulting chatbots and support resource databases;

- **Implementing a threat reporting system** on social media and messengers that will enable users to anonymously report potential cases of online violence or exploitation;
- **Expanding access to online psychological and legal assistance**, including advice on cybersecurity and digital self-defence;
- **Developing artificial intelligence algorithms for monitoring and automatic detection of dangerous content** aimed at exploiting women and girls.

# RECOMMENDATIONS FOR IT SECTOR

**1. Developing algorithms for detecting and blocking suspicious content and implementing them in the work of entities involved in preventing and combating trafficking in persons.** This will increase the effectiveness of response to potential threats in the online space, including the identification and blocking of content that contains signs of recruitment, fraud and exploitation. The existing moderation mechanism does not take into account all the peculiarities and risks associated with the use of digital platforms for trafficking in persons, so separate algorithms to automatically detect and respond to such threats need to be developed. These algorithms should be integrated into the activities of online platforms, law enforcement agencies and other actors involved in combating human exploitation.

**2. Increasing the effectiveness of content moderation and prompt response to complaints by improving mechanisms for checking and removing harmful content used for recruitment, intimidation or exploitation.** This includes improving moderation algorithms, engaging independent experts, and establishing clearer rules for digital platforms to combat online crime. A significant number of cases of recruitment and trafficking in persons are carried out through social media, messengers and other digital platforms, where content moderation remains ineffective. Current moderation mechanisms require significant improvements as perpetrators continue to find ways to bypass existing rules. Therefore, it is necessary to strengthen control over verification algorithms, integrate mechanisms for analysing potentially threatening interactions, and implement a system for prompt response to user complaints.

**3. Enhancing user authentication and combating fake accounts by introducing mandatory identity verification for users posting advertisements or communicating on digital platforms.** Fake accounts are widely used by criminal groups to recruit people for trafficking in persons, disguise their activities and bypass the security measures of online platforms. The introduction of mandatory multi-level authentication (for example, through document verification or video verification) will significantly complicate the operations of perpetrators and reduce the risks to potential victims. It is also necessary to introduce automated algorithms to detect and block mass-created accounts used for fraud and recruitment.

**4. Ensuring an ethical approach and protection of personal data by implementing transparent policies on collection, processing and storage of personal information of online platform users, especially in the context of combating trafficking in persons.** Existing mechanisms for processing personal data often do not provide an adequate level of protection against the misuse of information. This creates additional risks for survivors, including the possibility of secondary victimisation. It is necessary to introduce unified standards for the secure storage of personal data, increase the responsibility of platforms for data breaches, and guarantee the right of users to privacy.

# ANNEX

# ANNEX No. 1
# RESEARCH METHODOLOGY

## I. Introduction

The global digitalization of almost all areas of social life has led to the infiltration of many crimes into cyberspace. Since the beginning of Russia's full-scale military invasion of Ukraine, the risk of Ukrainian women falling into situations of trafficking in persons and exploitation (both labour and sexual), including online, has increased dramatically.

At the end of 2022, the CSO "La Strada-Ukraine" conducted a survey through the National Hotline for the Prevention of Domestic Violence, Trafficking in Persons and Gender Discrimination to identify the risks of being exposed to trafficking in persons, labour or sexual exploitation and violence during the war in Ukraine[53]. In particular, only 34 per cent of respondents indicated that they were aware of the risks of trafficking in persons and exploitation. 18.3 per cent of respondents said they would agree even to illegal employment. One of the general conclusions of the survey is that the full-scale war increases the risks of Ukrainian women and men being exposed to trafficking in persons and exploitation, exacerbating their vulnerability. Vulnerability factors that contribute to this include:

- loss of employment and the risk of being below the poverty line;
- internal displacement, which for an individual (or family) may occur multiple times, increasing the risk of being trafficked;
- traveling abroad for temporary asylum;
- residing in the territory that was or is temporarily occupied;
- unsuitability of accommodation at the place of permanent residence due to destruction caused by hostilities;
- other social factors (retirement age, disability, single parenthood, large families, etc.).

The main risk group is women and girls, both those who have gone abroad in search of safety and those who have stayed in Ukraine. Thus, in 2023, the CSO "La Strada-Ukraine" provided consultations via the National Hotline for the Prevention of Domestic Violence, Trafficking in Persons and Gender Discrimination (116-123). In 2023, the National Hotline received 1,590 calls on the prevention of trafficking in persons, with 83.2% of calls on the prevention of trafficking in persons coming from women and 16.8% coming from men.

One of the negative consequences of the use of information technologies for illegal purposes is trafficking in persons: prostitution, production of pornographic content, trafficking in children, including for sexual exploitation. The online space enables perpetrators to remain completely or partially anonymous, which can make it difficult to track and identify them, or to use fake profiles on social media, dating websites, online marketplaces etc. By exploiting the Internet, traffickers gain access to a wide pool of potential targets in different regions and countries.

A potential increase in trafficking in persons and sexual exploitation of Ukrainian women who have travelled abroad due to Russia's aggression against Ukraine was discussed at a session in the European Parliament in November 2023.[54] There is also information indicating that an analysis of search traffic revealed a rise in interest in Ukrainian pornography following Russia's invasion of Ukraine.[55]

Trafficking for sexual exploitation in conflict can be a form of conflict-related sexual violence (CRSV), according to the definition of CRSV used in the UN Secretary-General's annual reports on conflict-related sexual violence.[56]

According to UN Women's study "The Dark Side of Digitalisation: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia", women most often report that Facebook and Instagram are the platforms where they feel most at risk. TikTok, Skype, Messenger, Viber, WhatsApp, Telegram, and dating platforms are less mentioned[57]. According to the study, 76.8% of Ukrainian women surveyed reported experiencing some form of technology-facilitated violence during their lifetime, which indicates that this form of violence against women is widespread in Ukraine.

Article 149 of the Criminal Code of Ukraine defines trafficking in persons as recruitment, transportation, harbouring, transfer or receipt of a person committed for the purpose of exploitation, using coercion,

53 https://la-strada.org.ua/download/rezultaty-opytuvannya-shhodo-vyyavlennya-ryzykiv-potraplyannya-do-sytuatsiyi-torgivli-lyudmy
54 https://www.euractiv.com/section/europe-s-east/news/trafficking-and-sexual-exploitation-of-ukrainian-refugees-on-the-rise/
55 https://www.theguardian.com/world/2023/mar/26/ukrainian-refugees-increasingly-targeted-for-sexual-exploitation-research-finds
56 https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2024/05/SG-2023-annual-reportsmallFINAL.pdf
57 https://eca.unwomen.org/sites/default/files/2024-01/research-tf-vaw_full-report_24-january2.pdf

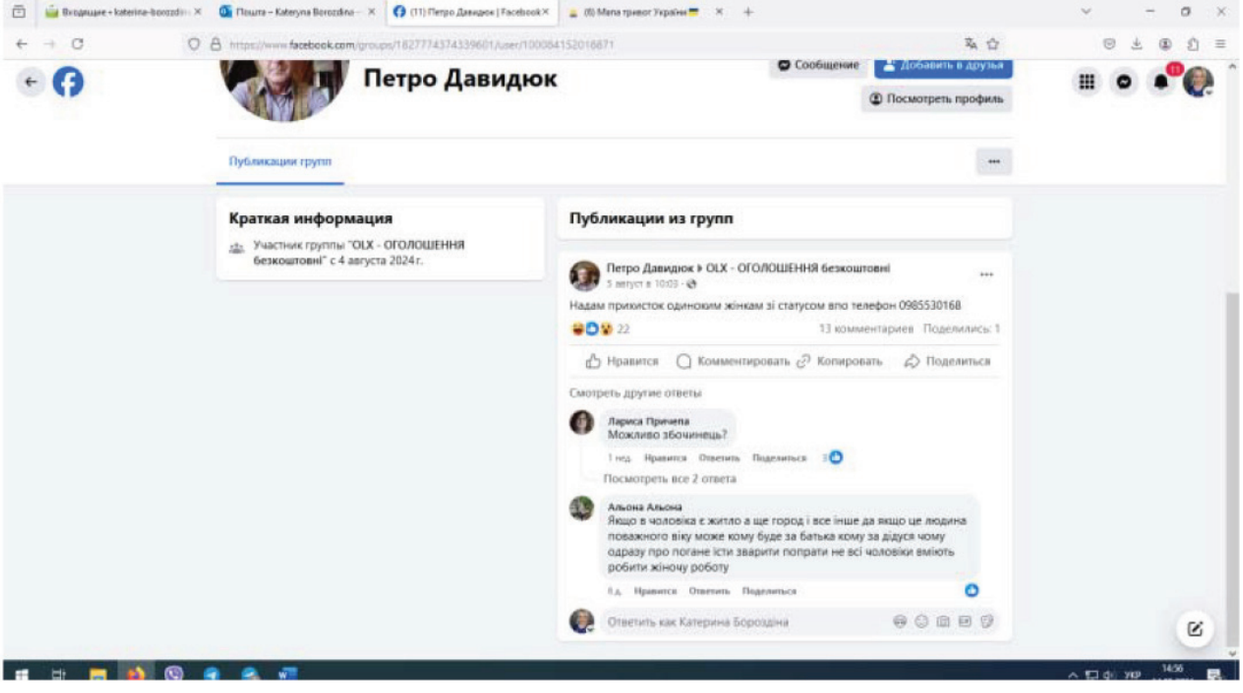
abduction, fraud, blackmail, material or other dependence of the victim, his or her vulnerable condition, or through bribery of a third party who has control over the victim to obtain consent to his or her exploitation.

Online trafficking in persons can include:

- recruitment through social media and classifieds websites, where “attractive” job or dating offers are posted that are, in fact, traps. These may include promises of high salaries or easy work, often abroad, which can encourage people to undertake risky journeys or engage in illegal arrangements;
- sexual exploitation on online dating platforms using online cameras;
- use of social media and/or messengers not only for recruitment, but also for controlling victims, blackmailing them, monitoring their activities and restricting their freedom of movement and communication. This includes threatening to disclose the victim’s personal data, photos (e.g. intimate ones) if he or she refuses to comply with perpetrators’ demands.

**II. Issues that increase the risk of trafficking in persons online for the purpose of sexual exploitation and technology-facilitated violence, in for particular women and girls.**

1. Since the outbreak of the full-scale war, crimes of trafficking in persons facilitated by information and communication technologies have become more widespread.
2. Innovative online technologies, products, platforms and services are used both as a means of recruiting potential victims and as a means of committing crimes of trafficking in persons.
3. The most common forms of trafficking in persons online are sexual and/or labour exploitation.
4. Recruitment of potential victims often takes place through online platforms and dating sites.
5. Exploitation takes place via web cameras and online dating platforms with the subsequent monetisation of content or its sale on dark web markets.
6. Internet users are often unaware of the protection of personal data, which makes them vulnerable to exploitation.
7. An example of potentially dangerous posts on social media:




https://www.facebook.com/groups/1827774374339601/user/100084152018871

**III. The purpose of the study**

- Identifying gaps and challenges in addressing the needs of survivors of trafficking in persons in the online space and with the use of technologies through cyberspace analysis, including identifying places in the online space with high risks of trafficking in women for sexual exploitation in conflict settings. Identification of modus operandi of women's involvement in exploitation.
- Increasing the awareness and capacities of stakeholders to identify and respond, and provide assistance to survivors and vulnerable groups.
- Identifying problematic areas in the counteraction and response to trafficking in persons in cyberspace by state authorities, and providing recommendations to strengthen them.
- Preparing a report on the identified problematic aspects in both the legal framework and practical implementation, and developing recommendations for improving the protection of women and girls from the risks of trafficking in cyberspace and technology-facilitated violence, including sexual exploitation.

**IV. Methods and tools for achieving the purpose**

I. Analysis of international standards on combating trafficking in persons, including in cyberspace.

When analysing international instruments, the following should be considered:

1. The EU Directive on combating violence against women and domestic violence, taking into account the requirements of the Directive on the definition of criminal offences in the field of sexual exploitation of women and children, computer-related offences and penalties for their commission. The Directive emphasises the impact of violence in the digital space:

- information and communication technologies increase the negative impact of the violation, thereby changing the properties of the offence;
- cyberviolence particularly targets women;
- cyberviolence can silence women and hinder their societal participation on an equal footing with men.

2. Directive (EU) 2024/1712 of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.

3. The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention), which is the main legal instrument in the European region that addresses the issue of violence against women. The scope of the Convention, as defined in Article 2, covers violence committed online and through the use of information and communication technologies. The analysis of the applicability of the Istanbul Convention to technology-facilitated violence against women shows that several articles of the Istanbul Convention may be applicable to the digital context, in particular the articles on sexual harassment and stalking.

4. The Council of Europe Convention on Cybercrime (Budapest Convention), which is the first and most important legally binding regional treaty addressing cybercrime and electronic evidence. Ukraine ratified the Convention in 2005.

II. Desk research to analyse existing national regulations in the field of combating trafficking in persons, including in cyberspace, and practices of their application, as well as analysis of existing studies and surveys. Analysis of available cyberspace audit practices, their findings and implementation at both national and international levels.

In order to assess the risks and factors contributing to the involvement of Ukrainian women in situations of trafficking for sexual exploitation, in particular in the neighbouring countries of Ukraine, through the use of online tools and technologies, CSO "La Strada-Ukraine" will cooperate with La Strada International. Relevant information requests will be shared with partners to learn about their activities in the field of combating trafficking in persons for sexual exploitation, including in cyberspace, and technology-facilitated violence against women and girls, as well as providing assistance to women and girls (data from local hotlines, research data, etc.).

3. Stakeholder capacity analysis (Office of the Prosecutor General of Ukraine; National Police of Ukraine, in particular the Cyber Police Department and the Migration Police Department; State Border Guard Service; Ministry of Social Policy of Ukraine): conducting online/offline focus groups at the national and regional levels to identify risks and gaps in the development and implementation of state policy on combating trafficking in persons, including in cyberspace (to cover approximately 8 regions of Ukraine: Cherkasy, Vinnytsia, Sumy, Kharkiv, Odesa, Khmelnytskyi, Ivano-Frankivsk regions, and the city of Kyiv, where at least 16 focus groups will be held). The focus groups will be conducted based on the developed questionnaire. The results of the focus groups will be used to analyse the mechanisms and approaches to combating cybercrime implemented by anti-trafficking actors.

An essential element of the desk study is an audit of cyberspace for existing threats and risks of trafficking in persons, which will include:

a. identifying online platforms that could potentially pose a risk of trafficking;

b. analysis of existing approaches used by perpetrators in cyberspace;

c. monitoring of technical tools and systems operating in cyberspace and used to commit the crime of trafficking in persons.

III. Preparing a report based on the findings of the desk research, focus groups and cyberspace audit.

IV. Preparing a report with the identified problematic aspects both in the legal framework and in practice, and recommendations for improving the protection of women and girls from the risks of trafficking in persons in cyberspace, including for sexual exploitation.

**VI. Expected results**

It is expected to provide comprehensive results: assessment, research, and information support. The long-term impact will be ensured through the public presentation of the research results and the publication of the final report on the research results, which will allow the results and recommendations to be applied in practice.

# ANNEX No. 2
# ANALYSIS OF FOCUS GROUPS TO IDENTIFY THE RISKS OF SEXUAL EXPLOITATION IN CYBERSPACE, RISKS AND GAPS IN THE FIELD OF COMBATING TRAFFICKING IN PERSONS, INCLUDING SEXUAL EXPLOITATION IN CYBERSPACE IN THE CONTEXT OF ARMED CONFLICT

One of the research methods employed was focus groups with women and girls, as well as representatives of bodies involved in combating trafficking in persons and related institutions. This approach allowed for the collection of perspectives on the subject under study. The primary objective was to gather in-depth answers and understand the participants' needs and attitudes regarding the research topic.

**The purpose of focus groups:**

1. Identifying the level of awareness, experience and attitudes among women and girls on the issue of combating trafficking in persons in cyberspace for the purpose of sexual exploitation;
2. Identifying existing risks of women and girls being trafficked and/or exploited in the online space;
3. Assessing the effectiveness of existing legislative norms and measures, risks and gaps in combating trafficking in persons for sexual exploitation, including in cyberspace;
4. Analysing the capacities of anti-trafficking actors and other relevant bodies and institutions to protect women and girls from the risks of being trafficked for sexual exploitation in cyberspace;
5. Analysing the interaction and coordination between anti-trafficking actors and other relevant bodies in preventing the risks of trafficking in persons and providing assistance to survivors;
6. Identifying typical shortcomings in the implementation of the state on combating trafficking in persons by local executive authorities.

**Target audience of the focus groups:**

1. Representatives of anti-trafficking actors and related bodies and institutions.
2. Women and girls who are at risk of being trafficked, including sexual exploitation online.

Between November 2024 and January 2025, 26 focus groups were held, including 12 focus groups with women and girls, 9 with local-level actors and stakeholders, and 5 with central-level actors and stakeholders. 8 focus groups were held offline and 4 online.

# FOCUS GROUPS WITH WOMEN AND GIRLS

Focus groups with women and girls were held in Kharkiv region (2 groups), Lviv region (2 groups), Ivano-Frankivsk region (1 group), Vinnytsia region (1 group), Cherkasy region (2 groups), and Khmelnytskyi region (2 groups). In addition, 2 focus groups were held with women and girls who had fled abroad due to Russia's full-scale invasion and received temporary asylum in Switzerland, Germany, Poland, Hungary, and Israel. A total of 86 women and girls took part in the focus groups.

**Social status of participants** (4 participants did not disclose their social status):

- 36 internally displaced women, including 12 women who were displaced several times;
- 13 women who received temporary asylum, including 3 women who were displaced several times;
- 3 women with disabilities;
- 18 unemployed, including 10 women abroad;
- 7 women who resided in the temporarily occupied territories, including 3 women currently living in Lviv region, 2 persons in Khmelnytskyi region, 1 person in Cherkasy region, and 1 person in Poland;
- 13 women who lost their accommodation due to hostilities;
- 29 women who travelled abroad to seek asylum, including 13 women who are still abroad;
- 21 single mothers, including 9 abroad;
- 11 women who have many children;
- 8 pensioners;
- 1 woman raising a child with a disability.

**The age distribution of the participants was as follows:**

- 18-25 years old - 20 women;
- 26-30 years old - 4 women;
- 30-35 years old - 8 women;
- 35-40 years old - 20 women;
- over 40 years old - 34 women.

**General awareness**

85% of women and girls surveyed had previously heard about cases of sexual exploitation or trafficking in persons on the Internet, most often from their friends or from social media such as Facebook, Telegram and Tik Tok, as well as other Internet sources.

48% of the focus group participants had taken media literacy courses or listened to lectures, which helped them understand the threats they may face and how to respond to different types of attacks or dangers online. 52% of the participants had not heard of such training and had not taken it.

Focus group participants indicated that they could disclose such personal information on the Internet:

- first name and surname - 75%;
- contact details - 37%;
- age - 35%;
- place of residence - 27%.

5% of participants said that their personal information was already public because their professional activities required it.

**As for the experience of communication on the Internet**, all participants use the following online networks: Facebook, Instagram, Telegram, YouTube, Viber, Messenger, Signal, Tik Tok. For all participants, it is about communicating with their families, friends, and acquaintances, as well as finding important and useful information and raising their awareness.

At the same time, 77% of respondents have at least once encountered suspicious offers or messages on the Internet (for example, from strangers). Most often, such messages were ignored.

25% of respondents noted that there were cases when someone on the Internet pressured them to send their own photos, videos and to disclose details about their hobbies, occupation, information about relatives. In such situations, all participants stopped the conversation and blocked the individual.

When asked about seeking assistance from the police regarding dangerous situations on the Internet, 86% of participants indicated that they had not reported it and did not plan to report because they did not trust the law enforcement system or did not believe that their case would be accepted because they thought that such a crime was simply impossible to prove.

At the same time, more than 70% of respondents know where to seek help in case of trafficking, including online: the police and hotlines. 50% of the participants indicated that they would contact the National Hotline for the Prevention of Domestic Violence, Trafficking in Persons and Gender Discrimination (116 123).

**What risks do women and girls see on the Internet?**

78% of respondents have encountered job offers on the Internet. Participants considered the following offers to be suspicious: no specific details, notices of flexible working hours, excessive promises, offers requiring small investments, offers only for young girls, promises of earning large amounts of money, significant income with minimal effort, and a small description of responsibilities.

More than 90% of respondents shared that risky offers are most often received on Telegram, Instagram, and job search platforms. Most often, perpetrators can disguise their advertisements with phrases such as: “Join a modelling agency with no prior experience”, “Work abroad, high pay, accommodation and meals at the expense of the employer are guaranteed”.

**What measures do women and girls take to protect themselves online?**

79% of participants have personal data protection measures in place. At the same time, 21% of respondents never use specially configured security measures, such as unique passwords for different accounts.

Less than 10% of respondents use system-generated passwords and/or two-factor authentication.

**Awareness of women and girls on how to receive assistance for survivors of trafficking in persons, including online.**

50% of respondents know where to seek assistance in case of trafficking for sexual exploitation, including online.

The respondents were not able to assess the accessibility of institutions providing assistance to survivors of trafficking in persons (whether there are convenient channels for informing about them, whether there is confidential access to assistance, whether it is possible to get advice/assistance at a convenient time, etc.), since they have never faced such situations.

When asked whether online platforms sufficiently protect users from the risks of online sexual exploitation, only 18% responded that they do. 82% of the respondents believe that online platforms do not protect users sufficiently, especially with regard to uncontrolled advertising and other offers to involve people to sexual exploitation.

**General conclusions based on the results of the focus groups with women and girls on preventing the risks of trafficking in persons online**

The vast majority of focus group participants are aware of cases of sexual exploitation or trafficking in persons on the Internet, but have never been involved in such situations themselves. The participants learned about such cases from TV news, read about them on social media, Instagram, TikTok, Telegram channels, YouTube, and Facebook.

Due to the lack of information about the risks of being trafficked online, women and girls are unable to predict the risks of communicating with suspicious persons on the Internet. Women and girls do not have a clear distinction between online fraud (e.g., money luring) and online recruitment for sexual exploitation.

Unfortunately, women and girls have a rather low awareness of protecting themselves and their personal data on the Internet.

The focus group participants demonstrated that they are only interested in the information on the Internet that they need here and now, that is interesting to watch and easy to understand. In search of such content, participants actively use all available social media, but singled out TikTok as the most dangerous network of all, as it has a huge range of online job offers, and when they tried to view the offers in more detail, the link redirects them to other communication channels, where they are asked to provide their personal data.

A clear understanding of the risks is demonstrated only about job advertisements for “easy” work with inflated wages.

Women with IDP status noted that, being in a difficult financial situation, they often pay attention to such “attractive” offers.

**Recommendations based on the results of focus groups with women and girls on preventing the risks of trafficking in persons online**

1. Intensifying activities to inform women and girls about the dangers associated with trafficking for sexual exploitation in the online space while searching for a job.

2. Developing and implementing training programmes on the risks of trafficking in persons online.

3. Improving access to information about risks on the Internet and about the possibility of receiving assistance: distribution of information products through retail outlets, supermarkets, beauty salons, cosmetics stores, hospitals, etc.

## FOCUS GROUPS WITH REPRESENTATIVES OF ANTI-TRAFFICKING ACTORS AND RELEVANT AUTHORITIES AND INSTITUTIONS

9 focus groups were held at the regional level: in Kharkiv region (2 groups), Ivano-Frankivsk region (2 groups), Vinnytsia region (1 group), and Khmelnytskyi region (2 groups). In addition, 2 focus groups were held with representatives of the Consulates of Ukraine in Germany, Poland, Greece, and Slovakia. A total of 56 specialists took part in the focus groups.

At the regional level, the focus groups included representatives of the police (5 persons); prosecutors (1 person); social service centres (33 persons); teachers (10 persons); and representatives of HR departments (7 persons).

At the central level, five focus groups were held: with representatives of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights; the Office of the Government Commissioner for Gender Policy; the Office of the Prosecutor General of Ukraine; the National Social Service; and the State Migration Service.

All representatives of state institutions who participated in the focus groups noted that the full-scale war has created new challenges for combating trafficking in persons, including in the online space. In particular, the loss of housing, work, change of residence due to internal displacement or travelling abroad encourages people to look for income opportunities, including through the Internet. It is in such situations that perpetrators can take advantage of the vulnerable state of Ukrainian women and recruit them for further exploitation.

80% of focus group participants said that the current state of combating trafficking in persons in cyberspace is rather insufficient. More than 50% of focus group participants believe that there are not enough specialists among all actors involved in combating trafficking in persons to conduct high-quality monitoring and analysis of online activity.

> “In times of crisis, perpetrators actively use various online platforms to find vulnerable people. The full-scale invasion and internal and external displacement have created unique conditions for the rise of trafficking in persons, especially in the online space. In search of solutions to financial problems through online resources, women and girls are at risk of being recruited by perpetrators.”
>
> Focus group with representatives of social service centres

70 per cent of the interviewed representatives of social service centres noted that they lacked the knowledge and skills to identify survivors.

Stereotypes that affect the self-identification of survivors, such as shame, self-blame for the situation, fear of being blamed for what happened, and fear of social condemnation, were also voiced as problematic aspects.

With regard to the adequacy of available resources to work with survivors of trafficking, the responses of representatives of social service centres were as follows:

- 18.2% believe that there are sufficient resources available to work with survivors of trafficking in persons;
- 63.7% believe that there are not enough resources;
- 18.1% do not know whether there are not enough resources.

In assessing the situation and challenges in the field of combating trafficking in persons, including online, focus group participants identified certain vulnerable groups of women and girls, particularly during the

full-scale war: women and girls in general; single mothers; adolescent girls; women who sought temporary asylum abroad due to the war in Ukraine. More than 90% of focus group participants believe that the number of vulnerable groups among women has increased significantly due to the full-scale war and, accordingly, the risks of sexual exploitation have increased. All these factors have created conditions where perpetrators have begun to use various online platforms to search for and recruit women and girls.

> "Women face risks at all stages of moving abroad - from crossing the border to seeking help. Many do not even know that their rights are being or may be violated. This happened because of the war. More women began to seek support. There are many cases when women are deceived, involved in exploitation through fake job advertisements in Europe."
>
> Focus group with representatives of Ukrainian consulates abroad

> "Women and girls who have left Ukraine because of the war, single mothers, adolescent girls. Risks are higher for those who have left Ukraine for the first time, and people from small towns, villages and settlements who do not have access to quality information about potential threats."
>
> Focus group with representatives of Ukrainian consulates abroad

Focus group participants noted changes in trafficking situations over the past few years, including the impact of the full-scale war, especially in terms of the use of online platforms to recruit potentially affected women. However, representatives of anti-trafficking actors and related agencies and institutions lack the knowledge and experience to identify potentially affected women and provide them with quality assistance.

> "Perpetrators use sophisticated online technologies, they use the Internet, while the specialists who can identify survivors lack knowledge and experience. Online platforms are not always helpful with investigations."
>
> Focus group with representatives of Ukrainian consulates abroad

> "It is difficult to identify a survivor, there is a lack of knowledge and skills. Training is needed for all those who can identify possible survivors of trafficking."
>
> Focus group with representatives of Ukrainian consulates abroad

> "Due to the full-scale war, the number of women using online platforms has increased. Women looking for work fall for online fraudsters who recruit them."
>
> Focus group with representatives of Ukrainian consulates abroad

Sexual exploitation, forced labour, and forced begging were cited as among the most common forms and types of trafficking in persons in cyberspace.

> "Recruitment for sexual exploitation and fraudulent job advertisements have become more frequent. Here in Greece, it is covered up by massage services."
>
> Focus group with representatives of Ukrainian consulates abroad

As for the general awareness of the focus group participants about the risks of falling into a situation of trafficking in persons in the online space, all participants rated their awareness as high. At the same time, only 50 per cent of the focus group participants had taken media literacy courses or attended lectures on this topic on their own initiative, which helped them understand the threats they could face and how to respond to different types of cyberattacks or dangers on the Internet, and made them more cautious online, acquiring skills in recognising cyberfakes.

In general, 100% of focus group participants believe that it is necessary to raise awareness among Ukrainian women, including those who have left abroad, about the risks of trafficking in persons online. Immediate attention should be paid to the development of new tools to identify individuals online and their activities without violating privacy rights and to improve support for survivors of online trafficking.

**General conclusions from the focus groups with representatives of anti-trafficking actors and relevant authorities and institutions**

1. The war has created new challenges in combating trafficking in persons, especially in the online space.
2. Women are the most vulnerable group.
3. There are barriers to self-identification and identification of survivors by relevant actors.
4. Sexual exploitation and forced labour are the most common types of exploitation of women in cyberspace.
5. Representatives of anti-trafficking actors and relevant authorities and institutions lack the knowledge and skills to identify and assist survivors.

**Recommendations based on the results of focus groups with representatives of stakeholders and relevant authorities and institutions**

The findings indicate the need to strengthen the anti-trafficking system, with a focus on the online space, and to extend protection to the most vulnerable categories – women and girls. To achieve results, it is necessary to:

1. Expand measures to combat trafficking in persons in the online space, including improved monitoring and cooperation with online platforms.
2. Increase the number of specialists on combating trafficking in persons, in particular those involved in analysing online activity.
3. Strengthen the training of social workers and law enforcement officers through specialised training.
4. Conduct information campaigns for women and girls about the risks of being trafficked via the Internet.

# ANALYTICAL REPORT

# TRAFFICKING IN PERSONS FOR THE PURPOSE OF SEXUAL EXPLOITATION IN UKRAINE

## increased vulnerability of women and girls associated with Russia's war against Ukraine and the use of cyberspace by human traffickers

**EDITED BY:**
Levchenko, K.B., Doctor of Law, Candidate of Philosophical Sciences, Professor, Honored Lawyer of Ukraine, Government Commissioner of Gender Policy of Ukraine.