INTERNATIONAL RESCUE COMMITTEE

# Behind the scam: How fraud messages are linked to forced criminality

**November 2026**




TIES

Co-funded by the European Union

## Author

**Filip Mitrovski**
Senior Officer Safety and Legal Protection
IRC Deutschland
Filip.Mitrovski@rescue.org

© 2026
International Rescue Committee IRC Deutschland gGmbH
Wattstraße 11, 13355 Berlin
Commercial Register: Amtsgericht Berlin-Charlottenburg
Registration Number: 181447 B
Tax Number: 27/614/04217
Managing Director: Madlin Sadler
Supervisory Board: Kathrin Jungehülsing (Chair), Dr Kara Preedy (Vice-Chair)
Cover Photo and Layout: Filip Mitrovski

https://de.rescue.org
https://antitraffickingresponse.org

The author would like to thank Marija Todorovska and Open Gate/La Strada North Macedonia for their valuable collaboration within the TIES Community of Practice and for providing additional context on the case from Skopje discussed in this article.

This article was written within the framework of the TIES project. TIES is co-funded by the European Union. Views and opinions expressed are, however, those of the author only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

Co-funded by
the European Union

# Behind the scam: How fraud messages are linked to forced criminality

Scam messages have become a common part of today's digital communication. They may appear to come from a bank, a parcel service or a family member using a new phone number. They are often designed to persuade people to transfer money or share personal information. Advice on how to recognise and avoid such scams is widely available. Much less attention, however, is paid to the people on the other end of these messages.

In some cases, the people sending these messages have themselves been deceived and trafficked. They responded to job offers that appeared legitimate, travelled to start a new job abroad and later found themselves forced to commit online fraud under coercive conditions. This article looks at this less visible side of online fraud: trafficking for the purpose of forced criminality.

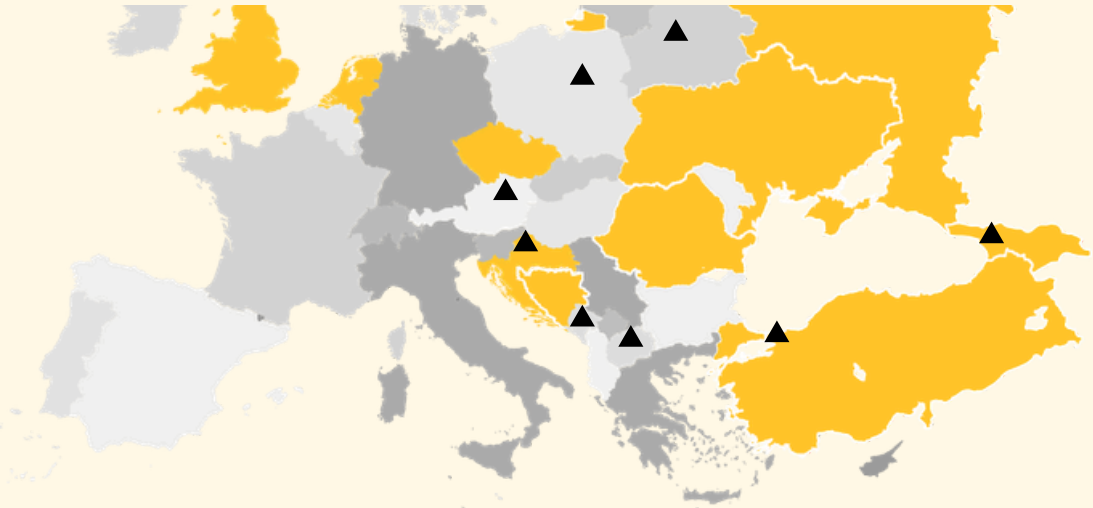
## From Southeast Asia to Europe

Cyber scam centres are places where trafficked people are forced to commit online fraud. UNODC has identified people from at least 56 countries and territories in Southeast Asian scam compounds. The UN agency describes multilingual workforces numbering in the hundreds of thousands. These include both trafficking victims and people who knowingly take part in the operations.[1]

Survivors of this form of trafficking, known as trafficking for the purpose of forced criminality, describe working shifts of 12 to 18 hours a day and being forced to repay debts of 5,000 USD to 30,000 USD.[2] Survivors interviewed between 2023 and 2025 described severe psychological and physical violence in Cambodian scam centres. This included the systematic use of 'dark rooms' to punish people who failed to meet daily fraud targets. Other reported human rights abuses included sexual violence, debt bondage, torture and other ill-treatment.[3] Escaping from these scam centres was often impossible. Victims were held behind prison-like security measures, including walls and razor wire, guarded gates and security personnel. Attempts to escape could result in severe violence or torture.[4]

According to the OSCE, the model associated with Southeast Asian scam centres is now also being seen in Europe.[5] As of April 2026, forced cyber scam operations had been identified in Austria, Belarus, Croatia, Georgia, Montenegro, North Macedonia, Poland and Türkiye. Other European countries are affected as well through their nationals being trafficked into such operations. These include Bosnia and Herzegovina, Croatia, Czechia, Georgia, the Netherlands, Romania, Russia, Türkiye, Ukraine and the United Kingdom.[6] Among the recruitment adverts analysed by the OSCE, those offering jobs in Eastern and South-Eastern Europe showed the highest proportion of high-risk adverts linked to recruitment for scam centres.[7]

**EUROPEAN COUNTRIES AFFECTED BY FORCED CYBER SCAM OPERATIONS**



▲ Country where forced cyber scam operations have been identified*

Country whose nationals have been reported as trafficked into cyber scam operations

Map: Author's own visualisation based on OSCE data. As of April 2026.
* The position of the triangle does not represent an exact location.

## A case example from North Macedonia

In May 2021, a police investigation in North Macedonia uncovered scam call centres in two houses in the Skopje area. The authorities acted on a request for legal assistance from Taiwan. During the police search, the North Macedonian authorities found 48 people from Taiwan. Nine were organisers of a criminal group, while the remaining 39 were later identified as potential victims of human trafficking for the purpose of labour exploitation.[8]

The traffickers had recruited these people with the promise of better jobs and a better life in Europe. All 39 individuals were young adults and they had entered North Macedonia legally. At the airport, their travel documents were taken away from them on the pretext of administrative formalities. Once they arrived at the houses, their mobile phones were also taken away. With one of the organisers always present, they could not contact anyone outside to ask for help.[9]

The organisers forced them to commit fraud by phone and on the internet, targeting people in China and Taiwan. The scheme was organised in three groups. The first group posed as employees of banks, postal services or insurance companies. The second acted as police officers and demanded proof that a fictitious fine had been paid, using the exchange to obtain personal data. The third acted as prosecutors and judges and threatened serious criminal charges unless money was transferred. If the victims failed to complete their tasks on time, the organisers used physical violence and intimidation, threatening that the lives of their families would be in danger.[10]

After the police operation all 48 persons were temporarily accommodated at the same reception centre and later transferred to Taiwan. During their time in the reception centre, Open Gate, a specialised anti-trafficking organisation based in Skopje, provided the victims of trafficking with an interpreter and information on assistance organisations in Taiwan.[11]

In August 2021, Taiwanese prosecutors charged 42 people with fraud in connection with the operation, accusing them of having caused total financial damage of 2.04 million USD in 124 cases. As only nine had been identified as organisers, up to 33 persons of those charged might have been among the 39 trafficking victims. The outcomes of these court proceedings could not be definitively determined at the time of publication.[12]

## Cases in other European countries

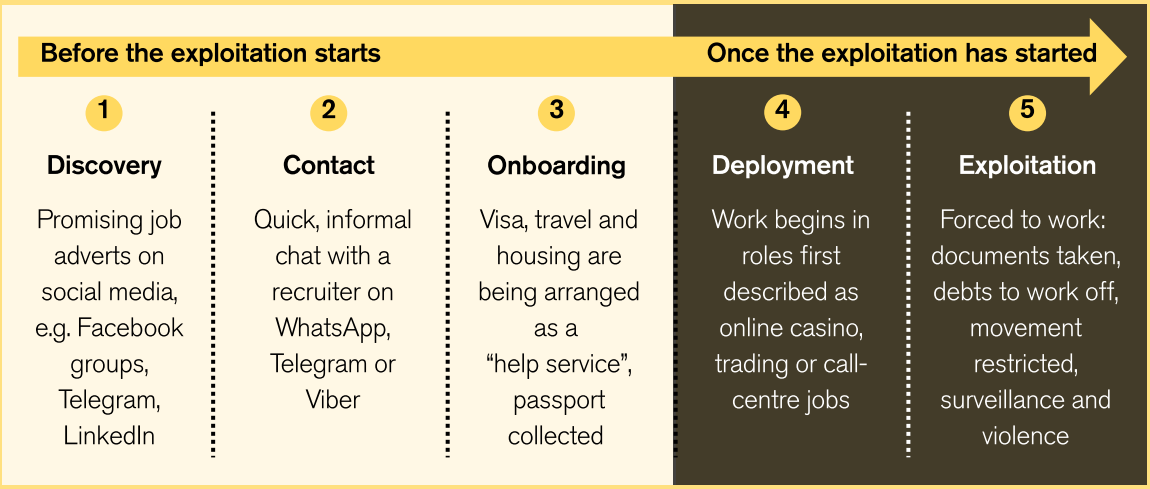
59 Taiwanese citizens were also exploited in a cyber scam centre near Zagreb, Croatia in 2018.[13] In 2020, the Montenegrin police found 84 people who were accommodated in different locations in Podgorica and forced to defraud Chinese citizens.[14] In January 2026, a 22-year-old Ukrainian managed to call the police after being threatened and held against his will in a building in Warsaw by a criminal network to commit online fraud. The subsequent police operation led to the arrest of 22 people. Six Ukrainian men and three Ukrainian women were identified as victims of trafficking for the purpose of forced labour.[15]

This classification is not unusual in Europe. According to the OSCE, in several cases it assessed, people were formally identified as victims of trafficking for the purpose of forced labour rather than forced criminality. This was because the relevant national law did not recognise forced criminality as a separate form of trafficking.[16]

## From job advert to exploitation

The path into this form of exploitation often begins with social media and the job adverts posted there. The OSCE describes a sequence of five stages. The early stages can also be part of an ordinary job search, which can make them appear less suspicious.[17]

**THE FIVE TYPICAL STAGES FROM RECRUITMENT TO EXPLOITATION**




Author's own visualisation based on the OSCE assessment. See endnotes 17–28.

### Discovery

The OSCE calls the first stage discovery: the moment when a person comes across a promising job opportunity. This can be a job in online gaming, casino platforms, customer service, call centres or sales.[18] The advert can also be gender-specific. In one advert reviewed during the OSCE assessment, a game presenter job in Bucharest was posted in an Italian-speaking Facebook group. The text of the job advert was directed at 'girls' who were 'good-looking and with a sunny personality'.[19] The adverts typically provide ways of contacting recruiters, most commonly via Telegram or WhatsApp, followed by email, direct messages on social media platforms and phone calls.[20]

### Contact

Once someone responds to the job advert, the contact stage begins. A recruiter replies quickly and informally and then moves the conversation to private messaging apps such as Telegram or WhatsApp.[21] Suspicious recruiter profiles may have little verifiable history, use stock photos or appear to be based in a different country from the one in which the job is located.[22]

### Onboarding

During onboarding, recruiters offer to arrange visas, flights, airport transfers and accommodation, and ask applicants to provide a passport or ID card. What looks like support, however, can make applicants dependent on the employer from the beginning, as they no longer organise their journey or accommodation themselves.[23] Requests for fees in advance are another warning sign. So are indications that visa, travel or accommodation costs will have to be repaid through work, which can create conditions of debt bondage.[24]

It is important to note that legitimate employers in some sectors may also use some of these recruitment practices, such as offering relocation packages or establishing contact through messaging apps. Therefore, these signs do not automatically indicate trafficking for the purpose of forced criminality. The more of these signs occur together, however, the more reason there is for caution.[25]

### Deployment

At the deployment stage, people may begin working in roles that were previously described to them as jobs in online casinos, currency or crypto trading, or call centres. According to the OSCE, these job categories are linked to specific forms of fraud: fake gambling platforms designed to take victims' money, investment fraud and telephone scams such as the three-tier scheme described in the North Macedonia case study above.[26] The Telegram recruitment channels analysed often requested language skills such as English, French, German, Dutch and Portuguese. Based on this, the OSCE assessment identifies citizens of Western European countries as particular targets of online fraud.[27]

### Exploitation

The final stage is exploitation. It can begin as early as the deployment stage, as the stages are not always clearly separated. People subjected to exploitation may face debt bondage, restrictions on their movement, surveillance and psychological pressure. Their contact with the outside world may be controlled and, in some cases, they may also experience physical abuse.[28]

**Example of a suspicious job advert from the TIES project**

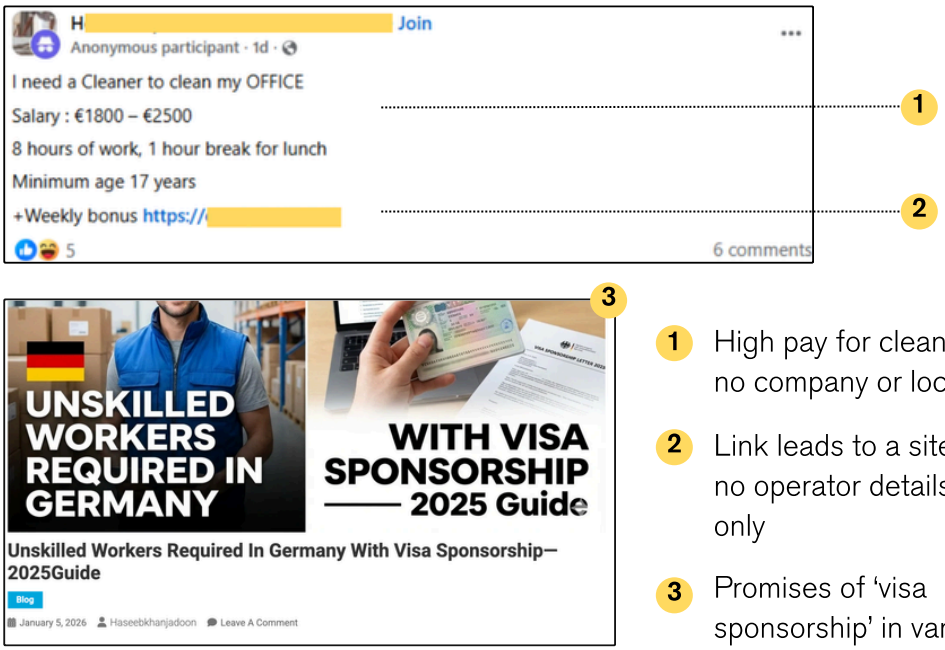
TIES is a joint victim-support project implemented by IRC Deutschland and specialised counselling centres in Germany, Italy and Greece. The project focuses on two forms of exploitation in particular: forced criminality and labour exploitation. One distinctive feature of TIES is digital streetwork. It is being piloted in all three countries. As part of this work, trained digital streetworkers regularly come across suspicious job adverts in online forums and social media groups whose members appear to include many migrants and jobseekers from third countries.

The following example is a suspicious job advert identified by a TIES digital streetworker in a Facebook group for people interested in housekeeping and nanny positions in Greece. As the salary offered was unusually high for this type of work, a digital streetworker from the Greek project partner ARSIS examined the job offer more closely.

The advert linked to a website offering visa support and employment opportunities for unskilled workers in several EU countries, including Denmark, Germany and Italy. No reliable information about the company behind the website could be found online. The website did not say who operated it and provided no legal or company details. Instead, the only way to contact the recruiters was through a contact form.

Within the TIES project, both the website and the associated Facebook post were classified as highly suspicious. The digital streetworker from ARSIS warned all Facebook users who expressed interest in the advert in the comments section about the potential risks associated with the offer.

**WARNING SIGNS IN A JOB ADVERT FOUND THROUGH DIGITAL STREETWORK**




1. High pay for cleaning, no company or location
2. Link leads to a site with no operator details, form only
3. Promises of 'visa sponsorship' in various EU countries

Screenshots: TIES digital streetwork. Group name and link removed.

**BEYOND ONLINE FRAUD:**
**A CASE STUDY ON FORCED CRIMINALITY IN THE TIES PROJECT**

While the TIES project has not encountered any cases of forced online fraud in Germany, Greece or Italy to date, other forms of forced criminality do occur. The following anonymised case from JADWIGA, a specialist counselling centre for victims of trafficking in Bavaria and a TIES project partner, was closed in 2026 and illustrates one such form of exploitation:

Sergei is a man from Moldova who wanted to start a new chapter in life after serving a prison sentence. In his village, an acquaintance approached him and said that he was looking for workers in Germany. He offered Sergei a job, a lift to Germany by car and lent him 100 EUR to obtain a passport for the journey. Once in Germany, the acquaintance told Sergei that he was expected to commit burglaries in Bavaria together with two other men. Intimidated by the three men, Sergei agreed to be driven to the intended target. By chance, a police patrol car passed by. In a split-second reaction, Sergei ran towards the car and attracted the officers' attention.

At the police station, Sergei was identified as a victim of trafficking and referred to JADWIGA's victim support services under the TIES project. A counsellor helped him find safe accommodation and provided psychosocial counselling and legal information. With JADWIGA's psychosocial support, Sergei gave evidence in court, contributing to the conviction of all the defendants. At his own request, JADWIGA referred him to a trusted Moldovan victim support centre, which helped him to return to Moldova, where he now lives.

## The non-punishment principle

People who are forced to defraud others commit criminal offences while they are being exploited. Whether authorities recognise that they are acting against their will and have no real alternative often depends on what happens at first contact. If they are treated primarily as suspects, detained or quickly deported, the trafficking behind the fraud may not be identified. Instead, the victims themselves may end up being prosecuted.[29]

The non-punishment principle is intended to prevent this. It allows authorities not to prosecute or punish victims of trafficking for offences or other unlawful acts they were forced to commit. However, it does not grant general immunity. It only applies to offences that a person was made to commit as a direct consequence of being trafficked.[30] The principle is established in an EU directive, but member states have implemented it in national law in different ways.[31]

### The situation in Germany

In Germany, the non-punishment principle is currently reflected in section 154c (2) of the Code of Criminal Procedure. If a victim reports the trafficking to the authorities and this leads to the discovery of an offence they committed themselves, the public prosecutor may decide not to prosecute that offence, unless it is considered too serious. However, the provision has clear limits: the prosecutor is not required to drop the case, only less serious

offences are covered, and it only applies if a victim reports the crime themselves.[32]

Germany's implementation of the non-punishment principle has therefore been criticised. In its most recent report on Germany, the Council of Europe's Group of Experts on Action against Trafficking in Human Beings (GRETA), for example, concluded: 'section 154c(2) of the CPC leaves too much discretion to prosecutors and does not apply to victims of crimes related to THB [...] Moreover, the non-punishment provision should be applicable to all offences that victims of THB were compelled to commit. It should also be noted that the non-punishment principle can only be applied by prosecutors and not by judges.'[33]

Germany is currently reforming its criminal law on trafficking and exploitation. In May 2026, the Federal Cabinet adopted a government bill, which is now before parliament. The proposed reform would broaden the application of the non-punishment principle in several ways. A new section in the Code of Criminal Procedure would cover victims of both trafficking and related forms of exploitation. Victims would no longer have to report the crime themselves, and courts would also be able to discontinue proceedings after charges have been brought.[34]

However, important limitations would remain. The non-punishment principle would still be an option available to prosecutors and courts, but not a rule applied as standard. It would also continue to cover only less serious offences (Vergehen), but not serious criminal offences (Verbrechen).[35]

## What needs to happen now

While the consulted reports document and contextualise the rise of forced scam operations in Europe, findings from TIES provide examples of how digital streetworkers can respond to suspicious recruitment practices and how counselling services support people forced to commit other criminal offences. European institutions and national authorities will need to address this form of exploitation more systematically in the years ahead.

Based on the findings presented, the following recommendations can be made to policymakers and other relevant actors across the European Union:

1. **Recognise forced criminality as a form of trafficking in national legislation**, strategies and policy documents, and ensure that protection frameworks address people exploited through criminal activities.
2. **Train police officers, labour inspectors, migration authorities, consular staff and other frontline professionals** to recognise indicators such as restrictions on movement, debt bondage, psychological coercion and control over communication. Where there are indicators of trafficking, potential victims should be referred to specialised protection and support services rather than automatically prosecuted, detained or deported.
3. **Apply the non-punishment principle consistently.** Police officers, prosecutors and judges need clear guidance and practical training on identifying situations in which offences may have been committed as a direct consequence of trafficking and exploitation.

4. **Cooperate with social media and messaging platforms**, including Facebook, LinkedIn, Instagram, TikTok and Telegram, to improve the identification, reporting and removal of recruitment content that shows multiple indicators of potentially exploitative or fraudulent recruitment.
5. **Develop multilingual awareness campaigns**, particularly for young people, multilingual communities and people who are unemployed or experience economic insecurity. Wherever possible, these initiatives should include peer-to-peer approaches and involve people with relevant lived experience.[36]
6. **Enable survivor-centred, specialised counselling services** to build expertise in digital streetwork, forced criminality and exploitation in scam operations. Services need adequate funding and trained staff to support this emerging group of clients both digitally and in person. This includes training staff to reach people at risk online as well as setting up rehabilitation programmes that address the specific psychological consequences of being forced to participate in fraud and other criminal activities.
7. **Provide debt relief and financial recovery support.** Debts incurred by victims of trafficking, or by their families, as a result of deceptive recruitment and exploitation should not become a lasting consequence of the trafficking situation. Victims should have access to financial assistance, safe return and reintegration support where appropriate, as well as longer-term measures that enable them to rebuild a stable life after exploitation.

## Conclusion

Online fraud linked to human trafficking has mainly been known as a human rights violation in Southeast Asia. However, this article shows that this form of exploitation has also spread across Europe in recent years. The victims are not only Europeans or others who lose money to fraudsters. Those sending fraudulent messages and making scam calls may themselves be victims – specifically, victims of human trafficking for the purpose of forced criminality.

The case study from the TIES project illustrates that forced criminality can also take other forms. Experiences from the project, consistent with the other reports presented here, also show that recruitment for these forms of trafficking is visible on social media and online users reply to job adverts that are highly suspicious.

One way for anti-trafficking organisations to respond is through digital streetwork, which means reaching out to people online to offer information and support. This approach can help organisations identify and respond to suspicious recruitment at an early stage. It can also help victims of human trafficking access information and support through their smartphones.

The policy recommendations set out further measures. They include recognising forced criminality as a form of trafficking in national legislation, applying the non-punishment principle consistently, and cooperating with social media and messaging platforms to improve the identification, reporting and removal of suspicious recruitment content.

**ANTI-TRAFFICKING AT IRC DEUTSCHLAND**

IRC Deutschland has been running anti-trafficking projects nationally and across Europe since January 2022. Its work follows the 4P framework of prevention, protection, prosecution and partnership. IRC's European projects focus on prevention and provide protection through partnerships with specialised counselling services. Three projects are currently being implemented: TIES, REACH and Lichtblicke.

Detailed information on all current and previous projects is available at: rescue.org/de/land/deutschland/schutz-rechtsberatung.

Further publications from the TIES project are available on the dedicated TIES project page: mehr-teilhabe.de/TIES.

# Endnotes

1 United Nations Office on Drugs and Crime (UNODC), Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia, April 2025, pp. 5, 7, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

2 Organization for Security and Co-operation in Europe (OSCE), Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Trafficking into Cyber Scam Operations: Implications for the OSCE Region. Exploratory Assessment, April 2026, pp. 15, 26, https://cthb.osce.org/sites/default/files/documents/publications/2026/04/Cyber%20Scam_Screen_260429.pdf.

3 Amnesty International, "I Was Someone Else's Property": Slavery, Human Trafficking and Torture in Cambodia's Scamming Compounds, June 2025, pp. 76–80, 86–87, https://www.amnesty.org/en/documents/asa23/9447/2025/en/.

4 Ibid., pp. 10, 38–54.

5 OSCE, Trafficking into Cyber Scam Operations, p. 15.

6 Ibid., p. 8.
The report lists the affected countries for the whole OSCE region. Only the European entries are given here.

7 Ibid., p. 17.

8 Ibid., p. 10.
On the number of organisers and victims and their classification, see United Nations Office on Drugs and Crime (UNODC), Analysis of Cases of Trafficking in Human Beings and Child Trafficking in the Republic of North Macedonia: Challenges for Effective Prosecution and Sanctioning of Perpetrators, April 2022, p. 56; https://www.unodc.org/documents/human-trafficking/2023/New_publications/Publication_Macedonian_Verion_EN_v.2.0.pdf;
Government of the Republic of North Macedonia, National Commission for Combatting Trafficking in Human Beings and Illegal Migration, 2021 Annual Report of the National Commission for Combatting Trafficking in Human Beings and Illegal Migration, 2022, pp. 28, 31–32, http://nacionalnakomisija.gov.mk/wp-content/uploads/2016/12/ANNUAL-REPORT-OF-THE-NC-THB-AND-IM-2021.pdf.

9 OSCE, Trafficking into Cyber Scam Operations, p. 10.
On the victims' age, see UNODC, Analysis of Cases, p. 56; National Commission, 2021 Annual Report, p. 28.

10 OSCE, Trafficking into Cyber Scam Operations, p. 10.
On the use of violence, see UNODC, Analysis of Cases, p. 56.

11 OSCE, Trafficking into Cyber Scam Operations, p. 10.
On Open Gate's support, see UNODC, Analysis of Cases, p. 57.

12 UNODC, Analysis of Cases, pp. 56–57.

**13** Council of Europe, Group of Experts on Action against Trafficking in Human Beings (GRETA), Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Croatia: Third Evaluation Round, 3 December 2020, para. 91, https://rm.coe.int/report-on-the-implementation-of-the-council-of-europe-convention-on-ac/1680a09509.

**14** OSCE, Trafficking into Cyber Scam Operations, p. 11.

**15** Komenda Stołeczna Policji, 'Policyjne uderzenie w zorganizowaną grupę przestępczą' ['Police strike against an organised criminal group'], press release, 28 January 2026, https://mokotow.policja.gov.pl/r2/aktualnosci/146745,Policyjne-uderzenie-w-zorganizowana-grupe-przestepcza.html.

**16** OSCE, Trafficking into Cyber Scam Operations, p. 9.

**17** Ibid., p. 11.

**18** Ibid., pp. 9, 11.

**19** Ibid., p. 27.

**20** Ibid., p. 23.

**21** Ibid., pp. 11, 23.

**22** Ibid., p. 31.

**23** Ibid., p. 23.

**24** Ibid., p. 31.

**25** Ibid., p. 32.

**26** Ibid., pp. 11, 21.

**27** Ibid., p. 20.

**28** Ibid., p. 11.

**29** Inter-Agency Coordination Group against Trafficking in Persons (ICAT), 'Joint Statement of the Inter-Agency Coordination Group against Trafficking in Persons (ICAT) on the World Day against Trafficking in Persons', 30 July 2026, https://violenceagainstchildren.un.org/en/news/joint-statement-inter-agency-coordination-group-against-trafficking-persons-icat-world-day.

**30** European Parliament and Council, Directive 2011/36/EU, recital 14 and Article 8, as amended by Directive (EU) 2024/1712, https://eur-lex.europa.eu/eli/dir/2024/1712/oj/eng.

**31** European Commission, Commission Staff Working Document: Evaluation of Directive 2011/36/EU, SWD(2022) 427, 19 December 2022, pp. 41–42, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0427.

**32** German Code of Criminal Procedure (Strafprozessordnung, StPO), section 154c (2), https://www.gesetze-im-internet.de/stpo/__154c.html.

**33** Council of Europe, Group of Experts on Action against Trafficking in Human Beings (GRETA), Access to Justice and Effective Remedies for Victims of Trafficking in Human Beings: Evaluation Report – Germany, Third Evaluation Round, June 2024, p. 31, para. 106. https://rm.coe.int/greta-evaluation-report-on-germany-third-evaluation-round-focus-access/1680b04977.

**34** German Bundestag, Entwurf eines Gesetzes zur Stärkung der strafrechtlichen Verfolgung des Menschenhandels und der sexuellen Ausbeutung sowie zur Umsetzung der Richtlinie (EU) 2024/1712, Bundestagsdrucksache 21/6584, 22 June 2026, pp. 17, 48, https://dserver.bundestag.de/btd/21/065/2106584.pdf.

**35** Ibid.

**36** For an example of peer-to-peer work in the anti-trafficking context, see the article 'When I help her, I also help myself' by Tosin Johnson, a human trafficking survivor and IRC staff member, https://mehr-teilhabe.de/materialien/peer-support-in-anti-trafficking-work/.

All online sources have been accessed on 4 November 2026.


INTERNATIONAL
RESCUE
COMMITTEE