https://www.eeagender.org/the-synergy-network/news/how-can-we-fight-tech-facilitated-violence/

How can we fight tech-facilitated violence?

Awareness-raising campaigns, free and accessible digital information for women and girls, and engaging men and boys in order to reach out to a broader community. These were just three of the many examples and good practices shared in an online conference.

BY VIBEKE HOEM, ADVISER AT KILDEN GENDERRESEARCH.NO PUBLISHED 30 JUNE 2022 LAST UPDATED 1 JUL 2022

Illustration photo: iStockphoto

The suggestions came from the participants of the online conference "The digital dimension of violence against women" on 10 March 2022, on the sub-themes sexual harassment, online stalking and psychological violence.

Building on the first General Recommendation of the Council of Europe's Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), the online conference focused on ways of combating online and technology-facilitated violence.

The three provisions of the Istanbul Convention that are applicable to online and tech-facilitated violence formed a key part of the conference.

"These are psychological violence, stalking and sexual harassment," explains Elif Sariaydin from the Violence Against Women Division of the Secretariat of the Istanbul Convention monitoring mechanism, Council of Europe, at the online conference on digital violence.

"Since the issue is very complex and multi-layered, the general recommendation provides a holistic approach that covers all four pillars of the Istanbul Convention, or 'the 4 Ps'. These are prevention, protection, prosecution and coordinated policies," says Sariaydin.

See also: Calls for a holistic approach to combating digital violence

Tech-facilitated violence is psychological violence

The Istanbul Convention is already applicable to the digital dimensions of violence against women. Article 33 of the Declaration on the Elimination of Violence against Women defines violence against women as:

"any act of gender-based violence against women that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."

All forms of online tech-facilitated violence have an impact on victims' psychological wellbeing and could therefore fall under the definition of psychological violence, underlines Sariaydin.

"Another specific dimension of online and tech-facilitated psychological violence is that it is often used by perpetrators in the context of domestic violence."

"Partners and ex-partners use electronic devices and other technology to control and manipulate and psychologically abuse their victims. This can take place during a relationship, but it is unfortunately also the case that it most often continues after the relationship has ended," says Sariaydin.

According to GREVIO's descriptions of different forms of psychological violence, domestic violence can take radical forms when coupled with new technologies. With the aid of the digital domain, it can take on a new dimension where current or former partners are in possession of intimate images of their victims. Abusers can similarly misuse technology to track the whereabouts of their victims, according to the general recommendation.

Online stalking and sexual harassment

Stalking committed in the digital sphere also falls within the scope of the Istanbul Convention. This can include spying on the victim on their various social media

accounts or stealing their passwords or hacking their devices to gain access to their accounts, according to Sariaydin.

The Istanbul Convention also covers online sexual harassment. This can be sexual abuse, which is often referred to in the media as revenge porn.

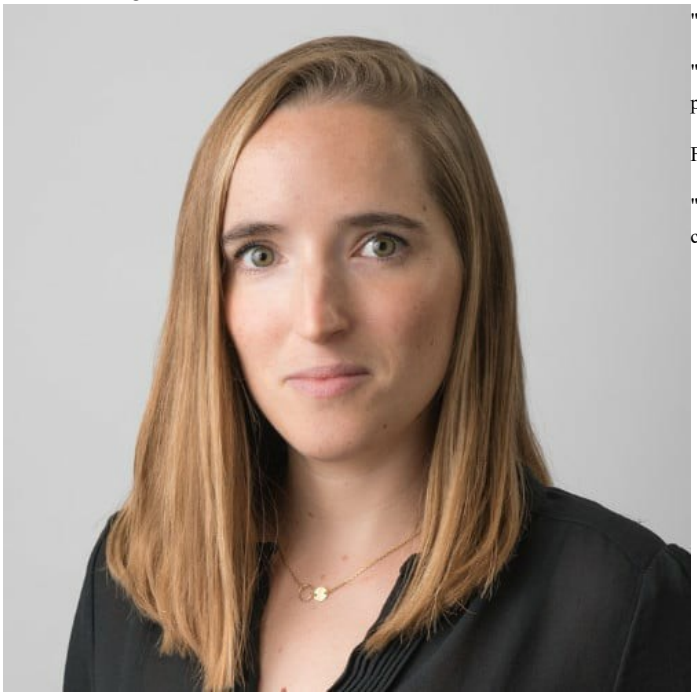
> Sexual harassment is one of the most widespread forms of violence in the digital sphere.

In addition, all other practices related to taking intimate pictures of their victims without consent, such as creepshots or deepfakes, or making rape threats online or sexual bullying, are covered by the Convention.

"Sexual harassment is one of the most widespread forms of violence in the digital sphere, especially among young women and girls who are on online platforms in their daily life," says Sariaydin.

The need for technology solutions

Stalkerware was one of the topics that Kaspersky, a company that has monitored cyber threats for many years, decided to focus on, according to Senior External Relations Manager Olivia Soave.



Olivia Soave, Senior External Relations Manager, Kaspersky

"Technology companies can and should be part of the solution," claims Soave.

"Stalkerware enables a person to spy on another person's life through their mobile phone, without the owner of the phone being at all aware of it," Soave adds.

Further, Soave explains that this software is fairly easy to buy and install.

"You just need physical access to the mobile phone. While its use is illegal in many countries, the software is still available and easily downloadable."

> Another survey concluded that 30 per cent of people had no issue when it came to secretly monitoring their partners.

"What is particularly disturbing is that this software enables the perpetrator to see someone's location, text messages, camera, photos and so on. Studies have shown that this is a gateway to abuse and other forms of violence. There is a direct link to physical violence as well," says Soave.

Almost 1 in 3 have no issue about spying on their partners

In 2021, Kaspersky conducted a survey in 21 countries across the world. The respondents were asked whether they had ever been stalked by means of technology.

"24 per cent of the respondents answered yes to this question," says Soave.

Read more in the report: The State of Stalkerware in 2021.

Another disturbing factor that Soave emphasises is people's behaviour when it comes to stalkerware.

"We conducted another survey which concluded that 30 per cent of people had no issue when it came to secretly monitoring their partners. Even though some of the respondents said that it was only acceptable under certain circumstances, they are still open to the idea," explains Soave.

"On a global basis, 15 per cent of the respondents had been required by their partners to install a monitoring app. Of those 15 per cent, 34 per cent had indicated that they had already experienced abuse by an intimate partner, which, in turn, demonstrates the link between offline and online violence," says Soave.

Important to share expertise

The Coalition Against Stalkerware was founded in 2019 in response to the growing threat of this type of software. Today, the coalition brings together more than 40 organisations from a wide range of sectors.

"These include victims of domestic violence, support organisations and organisations that perform perpetrator work, security organisations such as Kaspersky, and higher education and research organisations," Soave explains.

"We share knowledge and data and discuss terminology. We are also regularly contacted by NGOs that reach out with technical questions and receive support from the tech organisations," Soave continues.

Many NGOs and law enforcement agencies have informed the coalition that it still lacks sufficient technical expertise to help victims or survivors in the best possible

way.

"This is why we have developed technical training on stalkerware within the framework of the EU project Destalk. Collaborating with NGOs also enables us to improve our tools and solutions for supporting victims and survivors," says Soave.

One example is the stalkerware detection tool TinyCheck, which is free open-source software developed by Kaspersky in 2020.

"With this tool, the perpetrators will not be informed or aware of the scan," says Soave.

Last year, Kaspersky also trained more than 200 law enforcement officers in a partnership with Interpol.