



# Cooperating for an Institutional Strategy to Tackle the Digital Dimension of Violence Against Women: **the DeStalk Capacity building and Campaign**

March 6, 2023

Elena Gajotto

*Una Casa per l'Uomo - WWP EN*



## DeStalk

detect and stop stalkerware and  
cyberviolence against women

Supported by the Rights, Equality  
and Citizenship Programme of the  
European Union (2014–2020)



# Project info

Funded by: REC programme

Duration: 2 years – 01/2021 to 01/2023



BLANQUERNA

Academic & research expertise



KASPERSKY LAB SL.

Tech expertise (stalkerware)



UNA CASA PER L'UOMO  
SOCIETÀ COOPERATIVA SOCIALE

Perpetrators programme & victim  
support service providers perspective

**Advisory Board:**  
Coalition Against Stalkerware  
Italian Police  
D.i.Re Network



REGIONE DEL VENETO

Regional Authority, institutional &  
policy makers point of view



WWP EUROPEAN NETWORK

EU wide perspective

Supported by the Rights, Equality  
and Citizenship Programme of the  
European Union (2014–2020)



# The actions



**Awareness raising and capacity building** on recognizing and hindering the use of cyberviolence and stalkerware as new, widespread and hidden form of gender-based violence, through:

**Setting up a e-learning course for public officials and professionals** working with victims and perpetrators of intimate partner violence, on the issue of cyberviolence and stalkerware

**Developing Capacity building actions for professionals** working with victims and perpetrators through:

- Toolkits designed to detect, assess and work on digital violence
- Training workshops on theoretical and practical aspects of digital violence

**Developing a campaign and communication materials** on such a complex issue to raise awareness on the general public, and to empower survivors

# DeStalk's approach



Multi-disciplinary

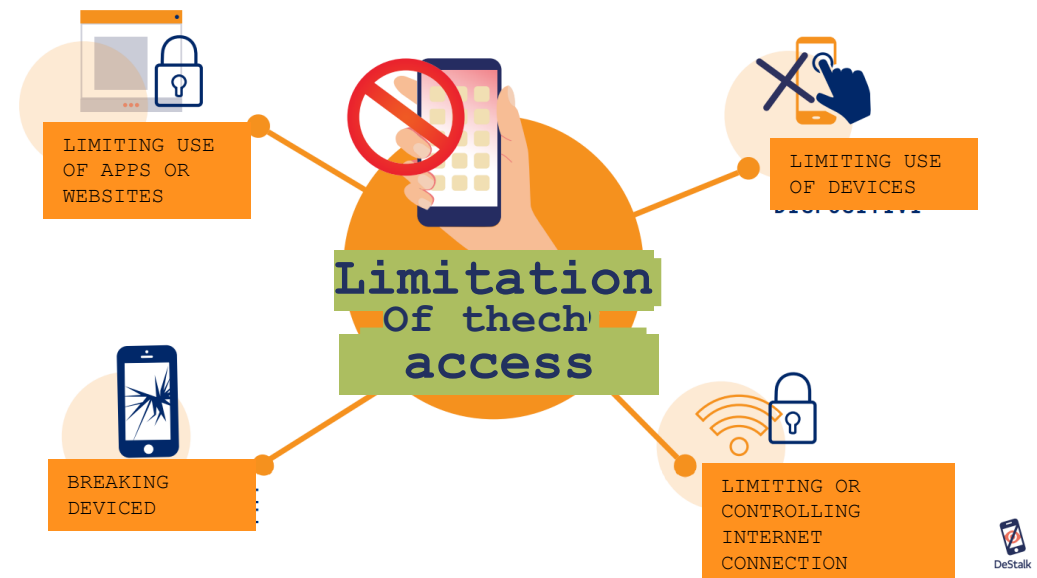
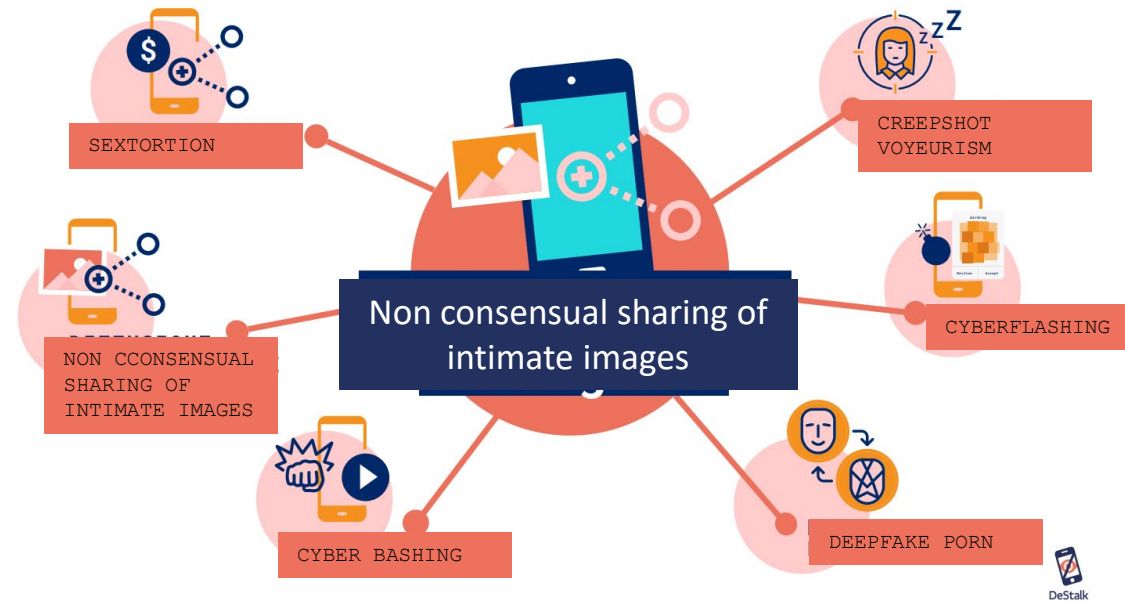
Multi-agency

Bottom up

Practical



# The complexity of digital violence



# The challenges

No common EU framework (at least at the beginning)

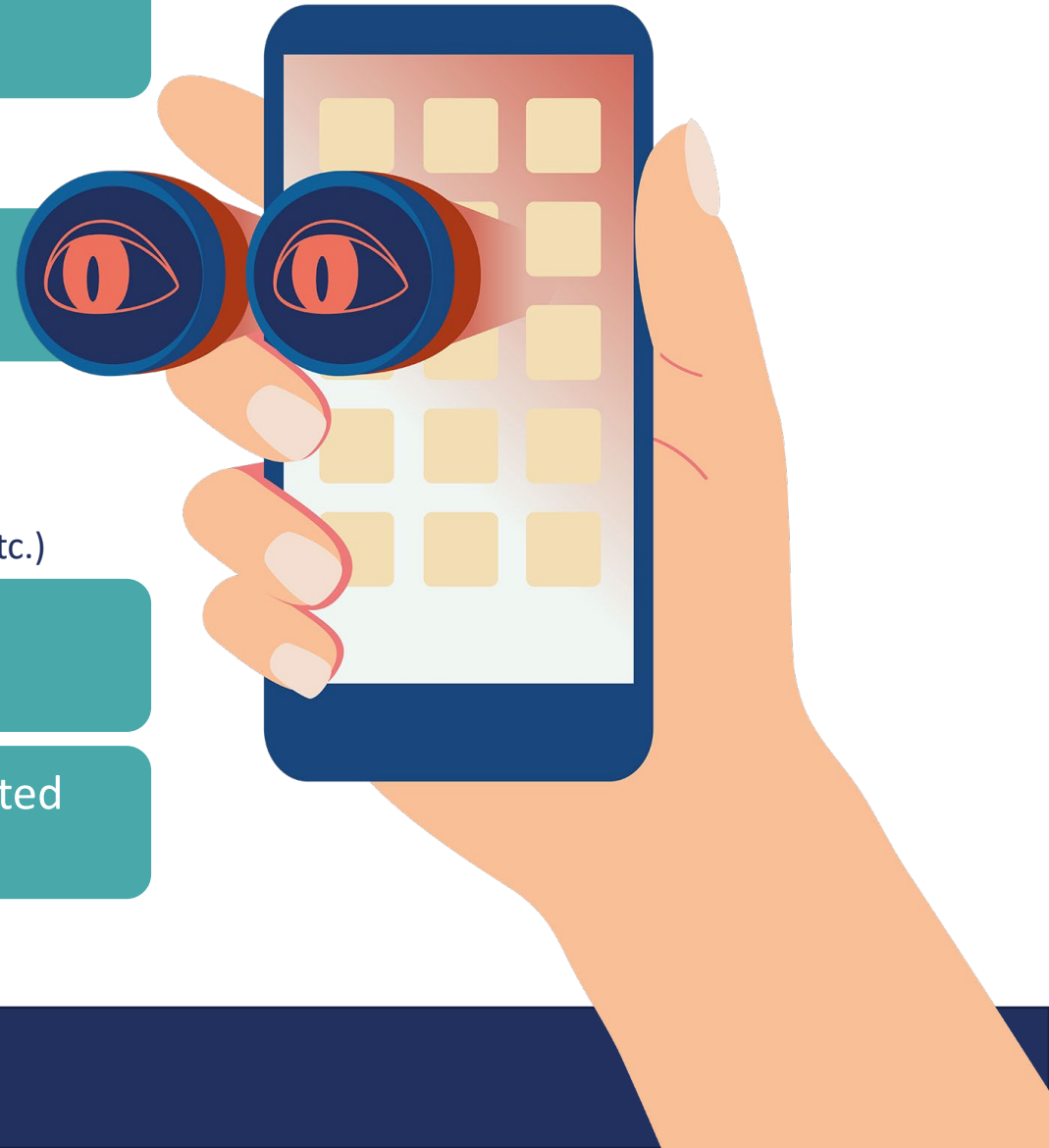
- Definition
- legal

Complexity of cyberviolence

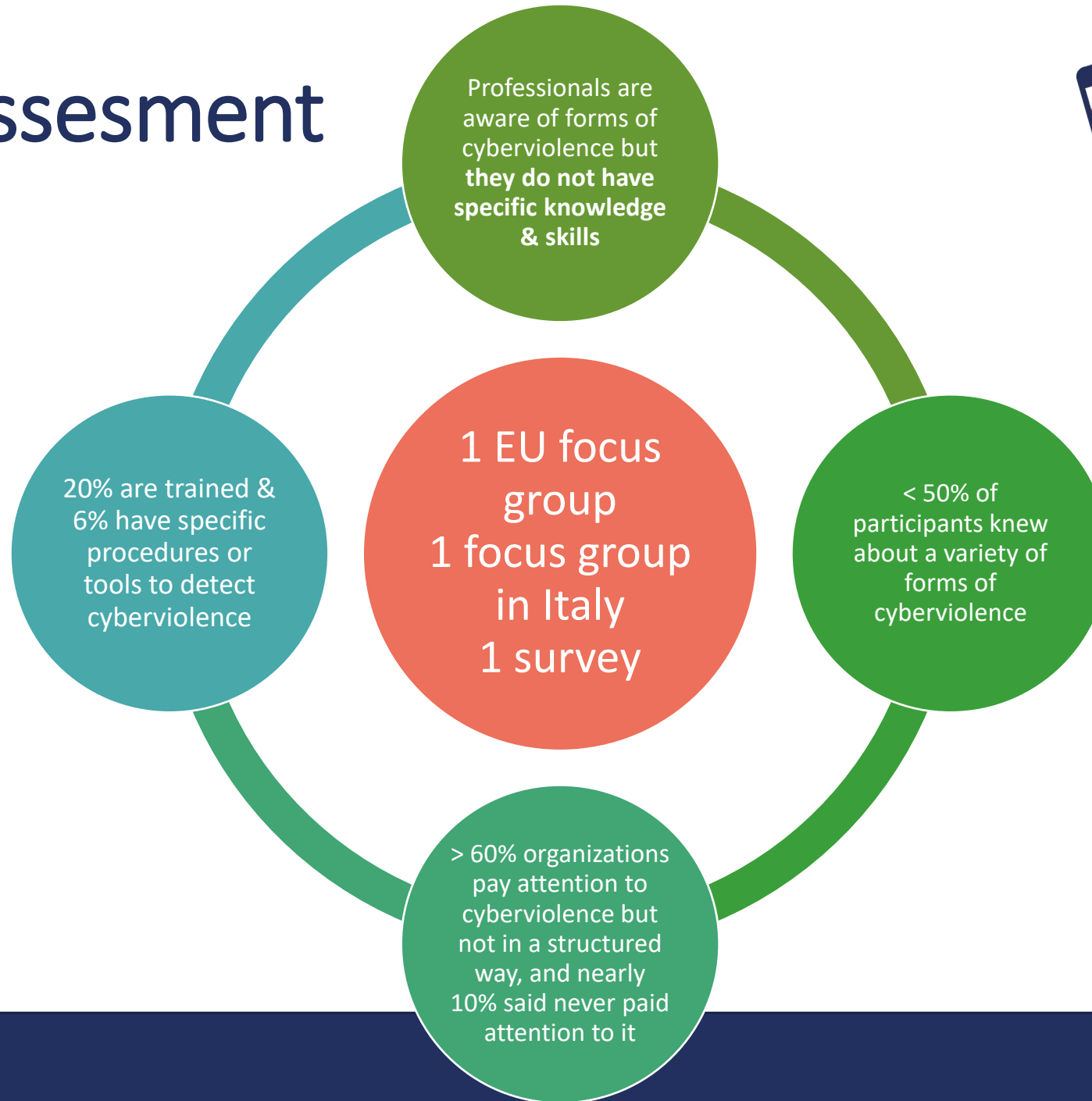
- Many forms
- Different types of perpetrators (known or unknown)
- Different platforms (social media, chats, metaverse, etc.)
- Different devices (smartphones, pcs, GPS, smart home, etc.)

Lack of relevant data

Characteristics of cyberviolence require dedicated skills



# Needs assessment



Enhanced tools and shared  
approach for effective work to address  
cyber violence against women:  
the DeStalk toolkit and training



# The adaptation of existing tools

Materials and tools  
used by PP and VSS  
almost never  
mention  
cyberviolence

As standalone category

In case studies

In examples (ex. "control" is just physical  
or related to relationships)

In risk assessment tools

Multiagency approach requires  
shared definitions

We need to recognize  
warning signs and know how  
to “dig deeper”

How can we tackle this  
topic with perpetrators?

We need to know how to  
assess cyberviolence and  
how to tackle it

We need survivors to know  
how to increase their tech  
safety

we need safety tips for  
every woman

Before taking action, we  
need to recognize warning  
signs and what they mean

We need to have a better  
understanding on the (Italian) laws  
that can be applied to cyberviolence

## Glossary of cyberviolence terms

Checklist of red flags to  
detect digital violence

Group session for  
perpetrators  
programmes

Safety planning guide for  
support services

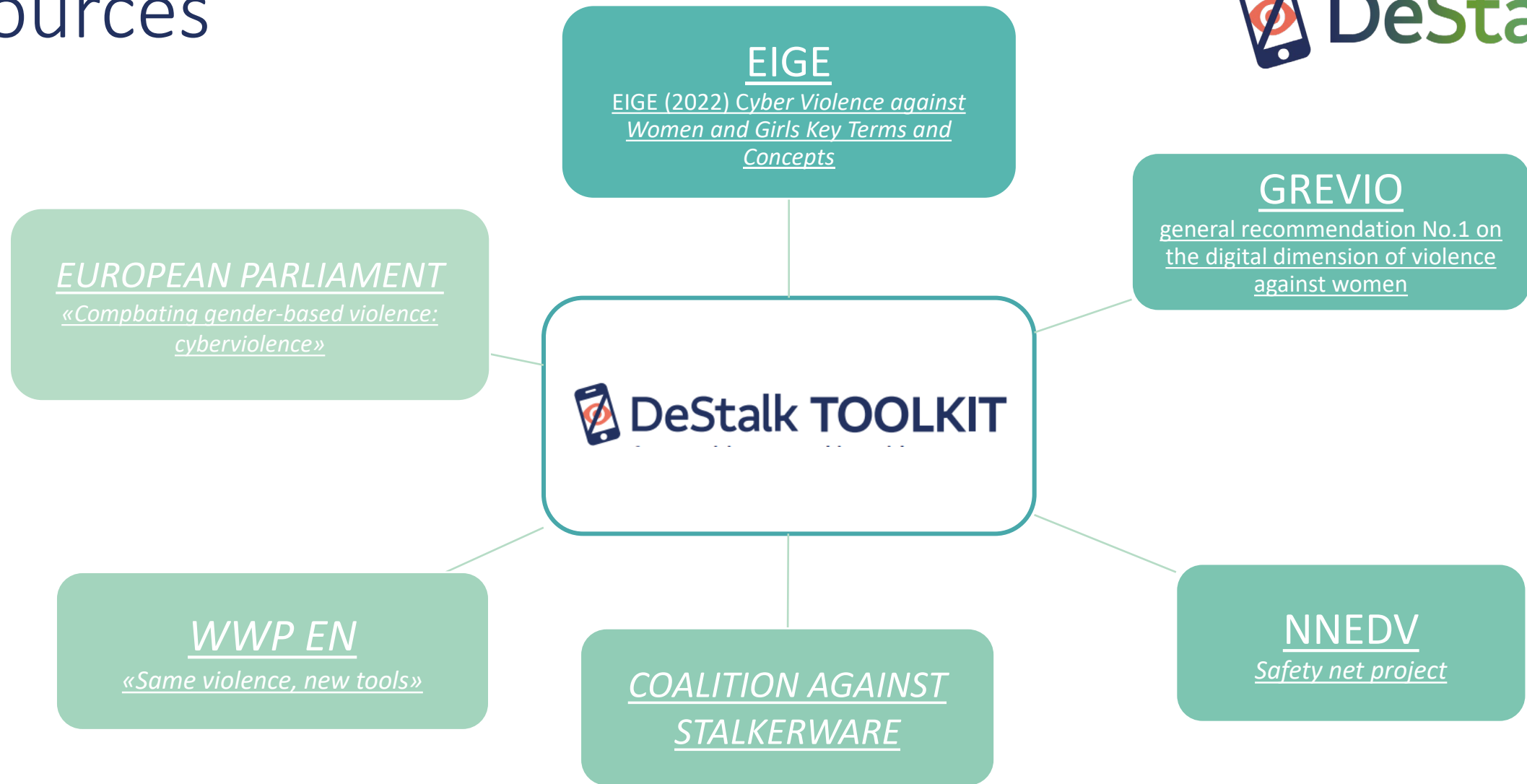
ICT safety guide for  
survivors

**PRACTICAL GUIDE FOR WOMEN  
FREE FROM DIGITAL VIOLENCE**

Red flags checklist for  
support services

## Legal guide (Italy)

# Sources







## DeStalk TOOLKIT

for practitioners working with perpetrators



## DeStalk TOOLKIT

for providers working with victims/survivors

General definition

Cyberstalking & subforms

Cyber harassment & subforms

NCSII

Limiting tech access

Other forms

# The glossary

## Glossary of cyber violence terms

Despite technology having been a fundamental part of our every day life for a long time, cyber violence has only recently come to the attention of professionals and policy makers. A first EU-level definition of cyber violence was given by GREVIO in November 2021

**The digital dimension of violence against women encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is a legitimate and equally harmful manifestation of the gender-based violence experienced by women and girls offline.**

GREVIO General Recommendation No. 1 on the digital dimension of violence against women

According to this definition, cyber violence is called the digital dimension of violence against women and encompasses abuses perpetrated online or through digital devices.

It is important to understand that the following list with forms of cyber violence is not exhaustive because forms of cyber violence change and develop following the constant and rapid evolving of digital technologies. Also, a form of cyber violence may vary a bit in their appearance so that characteristics may overlap. In addition, it happens that the same form of violence may have a different name. As EIGE (2017) pointed out, it would be helpful to have definitions politically agreed as this would facilitate better coordination at inter-organisational level. When cooperating, victim support organizations, perpetrator programmes and law enforcement may overcome as a first hurdle the need to agree on the same definition.

Cyber violence is an umbrella term. That includes all the forms of violence that are perpetrated through ICT. The most common forms are cyberstalking, cyberbullying, harassment and non-consensual sharing of images. As gravity oh. Affirms. In its recommendation, facilitated forms of violence Against women and girls are amplified and facilitated by technology, and this brought to a never seen before escalation of the phenomenon. Violence perpetrated online or through ICT is a continuum of offline forms of violence, and it is not a phenomenon separated from offline violence, because often. It follows the same patterns of offline violence, and it leads to psychological, social and economical consequences for women and girls and can transform into physical, sexual or psychological.

As specified by EIGE<sup>1</sup> Cyber violence against women and girls includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs).

All acts of cyber violence can:

- start online and continue offline such as in the workplace, at school or at home;
- start offline and continue online across different platforms such as social media, emails or instant messaging apps;
- be perpetrated by a person or group of people who are anonymous and/or unknown to the victim;
- be perpetrated by a person or group of people who are known to the victim such as an (ex) intimate partner, a school mate or co-worker

Due to the many possibilities offered by ICT, there is a wide variety of forms to carry out gender based cyber violence. The following is a list with the most relevant methods in which gender based cyber violence is carried out.

<sup>1</sup> EIGE (2022) Cyber Violence against Women and Girls Key Terms and Concepts: Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)

## Glossary of cyber violence terms

### ■ Cyber stalking

involves intentional repeated acts against women. It is committed through the use of ICT means, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the victim feel threatened, distressed or unsafe in any way (EIGE 2022). Online stalking can be carried out in different ways:

- **Stalkerware** are apps secretly installed on the victim/survivor's device to monitor and track her
- **Hacking or cracking** of communication and data stored online (for example on the cloud) or on private computers that are accessed without consent. This includes webcam hacking which often affects women, and the use of smart home devices to listen to conversations.
- **Cybersurveillance** use of ICT to monitor activities, locations and social interactions of the victim/survivor. This can be done through specific devices (GPS trackers, fitness trackers, etc.) or through the access to online accounts (e.g. Google or iCloud, etc.)
- **Following the woman online**, monitoring her social media accounts, replying to all her posts, joining the same groups, tagging her obsessively. This can also be done with fake accounts

### ■ Cyber harassment

is a wider category of threats or other offensive behaviours by an individual or by a group of persons aimed at offending, disparaging, or belittling a person through digital public and private channels. Online harassment encompasses:

- Non requested emails or messages
- Offensive or inappropriate requests on social media or chats
- Threats of physical or sexual violence through emails, messages or chats
- Hate speech, that is the use of offensive, denigratory or threatening language online
- Inappropriate or sexual comments to social media posts or contents

Cyberharassment includes:

- **Slander** refers to damaging someone's reputation by making a false statement about them (e.g. spreading rumours via social media).
- **'Slut-shaming'** is according to CYBERSafe (2020) the online "practice of criticizing people, especially women and girls, who are perceived to violate expectations of behaviour and appearance regarding issues related to sexuality".
- **Online threats** of rape, abuse or death
- **Body shaming.** Messages or comments written with the intent of humiliating someone by making mocking or critical remarks about their body shape or size.
- **Gender trolling.** Malicious acts online involving the sending or submission of provocative emails or social-media posts, including rape and death threats. Similarly to trolling, also gender trolling aspires to foment dispute and cultivate a following, inciting an angry or upsetting response from its intended target (EIGE, 2022)
- **Sexual solicitation.** Receiving unwanted requests to talk about sex or do something sexual in a variety of online contexts, like sending sexually explicit images or engaging in technology-mediated sexual interactions. It can lead to receiving abusive misogynist comments, harassment, and threats, particularly if the victim has rejected the requests in some way (EIGE, 2022)

### ■ Image-based sexual abuse

covers a variety of methods that can be explained by sexual images or videos shared or obtained without a person's consent. This category includes

- **Sextortion.** The act of threatening to publish sexual content (images, videos, deepfakes, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both. The perpetrator can be an ex-partner who obtains images or videos during a prior relationship, and aims to publicly shame and humiliate the victim, often in retaliation for ending a relationship (EIGE 2022)



## Assessment

## Safety planning

## Safety measures

## Stalkerware detection

## Suspect case

## Certain case

## NCSII

## Content removal

# Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

## ■ Assessment and evaluation

Assessment helps us identifying any existing form of digital violence, discussing options with victims/survivors, safety planning and collecting documentation and evidence.

Digital violence can be overwhelming, because it can happen anytime, anywhere and in many different ways. Assessment provides validation that their experience is genuine and harmful, and can give reassurance. When working with victims/survivors, it's important to keep in mind all forms of online violence and to know how to face each of them.

### Digital violence assessment framework

In the assessment of digital violence it is important to:

- **Listen to the woman's experience**
  - What happened, and how often?
  - How does the survivor think it happened?
- **Consider information abuse**
  - What information is needed to cause what happened?
  - Where is that information stored? Who can access it, and how?
- **Make a list of devices, accounts** – Keep the types of information abused in mind
- **Assess for access**
  - What can the survivor access, what can the perpetrator access?
  - How could those accounts or devices be secured?
- **Assess for risk**
  - Think about what can be done safely
- **Plan**
  - What are the survivor's goals?
  - How can she reach them in safety?
  - How can evidence be collected safely?

## ■ IT safety plan

IT safety planning is not different from the safety planning normally carried out by support services, it is useful to concentrate on the woman's immediate and long-term needs and goals, and to understand how digital violence is interfering with her life. Tech knowledge is helpful when safety planning, but it is not needed.

A good safety plan should be individualized, survivor-driven, and empowering. It is important to remember that "safety" can change quickly. When safety planning, survivors should be given tools and strategies so they can manage their risk and safety, taking back some control.

As mentioned before, immediate and long-term needs and goals of the survivor must be taken in consideration when safety planning:

- **Accountability and legal questions:**
  - Collecting documents and evidence for court
  - Perpetrators accountability and protection measures
  - Civil remedies: divorce, children custody
- **Increased privacy and tech safety**
  - Establishing a safe connection with the perpetrator
  - Increasing the safety of existing social media profiles
  - Creating new accounts and profiles
- **Stopping violence**
  - Understanding how violence is abused by the perpetrator
  - Finding a way to mitigate the abuse
  - Understanding how tech can be used to reduce or prevent abuse

# Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

## The pillars of IT safety planning

One of the most crucial aspects that must be considered is documenting the abuse. The survivors should be informed and guided on how to

- Keep a diary of what is happening
- Take screenshots or pictures
- keep originals (emails, messages, voicemails, or apps)
- Store important documents in safe places or dedicated storing apps

Another important aspect concerns the assessment of access and control of devices and accounts:

- How the survivor communicates
- What devices she has
- How she gets around
- Personally Identifying Information (PII) available online

### Elements for risk identification

When assessing possible risk sources, it is important to remember that personal information can be memorized in many different devices, apps and accounts that the abuser may have access to, like for example:

- Social Networks (Facebook, Instagram, Tik Tok, etc.)
- Paypal or other electronic payment systems
- Home banking
- Health apps
- Amazon (Incl. Prime Video)
- Food delivery apps (Foodracer, Glovo, JustEat, Deliveroo, UberEats etc.)

- Spotify
- Streaming apps (Netflix, Discovery+. Disney+, DAZN)
- Workout apps (Garmin, Fitbit, MiFit, Strava, Run Keeper, etc.)
- Travelling (Booking, Trivago, TripAdvisor, etc.)
- Dating apps (Tinder, Bumble, etc.)

The following aspects on connections, information and access need to be considered:

- **Connection**
  - What are devices connected to? (other devices, accounts, apps)
  - How are they connected? (wifi, Bluetooth, wire connection)
  - Who controls the connection?
- **Information**
  - What information is being shared?
  - To whom is this information being shared? (another device, online account, etc.)
  - Does the company have a privacy policy?
  - Can you limit what is shared and to whom?
- **Access**
  - How can the device be accessed? (remote access, physical access)
  - What accounts are associated?
  - Who has access?

To facilitate tech abuse assessment and safety planning, you can use the attached "**DeStalk Digital violence assessment checklist**", which includes warning signs and red flags to detect possible forms of digital violence, indicating connected risks and countermeasures.

## Assessment

## Safety planning

## Safety measures

## Stalkerware detection

## Suspect case

## Certain case

## NCSII

## Content removal

## Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

### ■ Assessment and evaluation

Assessment helps us identifying any existing form of digital violence, discussing options with victims/survivors, safety planning and collecting documentation and evidence.

### ■ IT safety plan

IT safety planning is not different from the safety planning normally carried out by support services, it is useful to concentrate on the woman's immediate and long-term needs and goals, and to understand

## Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

### The pillars of IT safety planning

One of the most crucial aspects that must be considered is documenting the abuse. The survivors should be informed and guided on how to

- Keep a diary of what is happening

- Spotify

- Streaming apps (Netflix, Discovery+, Disney+, DAZN)

- Workout apps (Garmin, Fitbit, MiFit, Strava, Run Keeper, etc.)

### ■ Safety measures

When there is the possibility that the perpetrator is monitoring and tracking the victim/survivor's phone the priority is to develop a clear and thorough IT safety plan with the woman. Always remember that about changes can escalate the nemetator's

Another important aspect in safety planning is checking with the survivor for any safety concerns or limitations they may have with turning off their phone. One thing that should be discussed is the potential reaction of the nemetator if he tries to

### Check the device for stalkerware

If the woman seeking your help has the feeling that her (ex)partner may know too much about her without her sharing information, it will be helpful that you offer the woman assistance to check the device with her.

**REMEMBER:** when checking for unknown apps in the device, please keep in mind that there may be several apps installed by default that are part of the operating system. If you have any doubt, ask a trusted IT tech to help you identify the unknown apps.

### ■ Safety measures when there is the suspicion that the victim/survivor may be monitored and/or tracked

- ☐ Inform her that stalkerware might register her conversations even if it's turned off. Suggest that she should leave it in the car or outside the room during interviews at the Service or with doctors, police, lawyers, etc.

- ☐ Check apps location and camera permissions and revoke them if they are active

- ☐ Disconnect WhatsApp Web and/or Telegram from PCs and other devices that can be accessible to the perpetrator

- ☐ Discuss with the woman the importance of not letting her children use her devices.

- ☐ Change online banking access account

### ■ Safety measures when it is certain that a phone/device is tracked

When it is certain that a device is tracked through a stalkerware app or that the perpetrator is monitoring the victim/survivor through other IT means, it is important to take the necessary steps to ensure the safety of the victim and the collection of evidence against the perpetrator.

**REMEMBER:** creating new Google or iCloud accounts to activate a safe device is a fundamental step in IT safety planning, because these accounts give access to a wide variety of apps and information, like emails, files on cloud storages, maps and locations, photos, contacts, etc.

- ☐ If there is no stalkerware, but the perpetrator is monitoring the woman through other IT means

### ■ What to do in case of cyber-harassment or non-consensual sharing of pictures or information

In case of suspect or certainty about these forms of cyberviolence (that include sextortion and revenge porn), aside from the importance of reporting them to the police (Cyberbullying, revenge porn and non-consensual sharing of explicit sexual images and videos are illegal in Italy, and can be reported

- ☐ Discuss about reporting the harassment/publication of images to the social media (please check each social media's reporting policy [Facebook](#) | [Instagram](#) | [Twitter](#) | [YouTube](#) | [TikTok](#)) or website company. If it violates the site's terms of service or content guidelines, they may remove the content. In this case, it is important to document the abuse first to keep evidence of it. Please check below how to report to adult websites.

- ☐ If content has already been published, it can be removed from search engines: EU residents have the right to request that links to pages containing data that is out of date, irrelevant, excessive or inaccurate must be removed from [Google](#) search results. It does not require those pages to be taken down, only that they not be shown in Google's search results, reducing the chance of people finding it. This can also be requested to [Bing](#) and [Yahoo](#) (there might be a different link

### ■ Removal of content from adult sites

If private content has been published online on adult sites, most websites have a "content removal" policy. Here you can find the "content removal" page for some websites [Pornhub](#) | [Xhamster](#) | [X videos](#) | [XXNX](#) (attention: these links will open the adult sites page)





## Safety tips for survivors living with the abuser

## Cyber violence and stalkerware: Technology and social media safe tips for survivors

**T**echnology is a fundamental part of our lives: it is everywhere, and we use it constantly. It is important to know how we can increase our personal "digital safety" so that we can continue to use technology and stay connected.

Here you can find some tips on how to improve your digital safety while you still live with an abusive partner or after leaving him.

- ☐ **Use a safe device**, that is, a device that your partner can not access. It can be a new device, a public one, or a trusted person's. You should use this device for all the information and communication that your partner must not know. This includes communications with the support service, with the police, with your lawyer, with your doctor, online banking, etc. An old mobile phone without data connection is also a good choice. **Activate a new phone number**: or use a safe number to communicate with the police, the support service, and your lawyer. Share this safe number only with trusted persons.
- ☐ **Add password or PIN to devices**: every device that you have – phone, pc or tablet – should be protected with a password, passcode or PIN that only you know. When you set up these passcodes, do not use birthdates, pet names, or other thing that you like (food, movies, songs) and that can be easily guessed. Do not use the same passcode for every device.
- ☐ **Do not share passwords** and passcodes with other persons, not even with your children (they might share passwords with their father).
- ☐ **Do not save passwords** and passcodes on your computer or phone. Browsers like Chrome, Edge, etc. will ask you if you want to memorize your passwords for future use: say "No". If you are already using saved passwords to log in to your accounts, your partner may be able to access them. You can safely store your passwords in dedicated passwords manager apps.
- ☐ **Set up a new email account** to manage your communications. You will also use this email account to set up other accounts (for banking, health services, insurance, etc.) and when you need another email to verify your identity. If possible, don't use your name/surname for the email, but choose another name (for example *SomethingSomething@email.com* instead of *YourNameSurname@email.com*)
- ☐ **Create a new Google or iCloud account** for your safe device. Remember that Google or iCloud accounts often store information on you and your life, like photos, emails, contacts, files, etc., so it's important that you choose a strong password to protect your new account and that you don't share it with anyone.
- ☐ **Deactivate smart home devices** like "google nest" or Alexa, that may be used to listen to conversations from afar.
- ☐ **Use incognito mode** in your browser when you navigate, so that you leave no trace of the websites you visited.
- ☐ **Sign off and log out** from sites and accounts, especially social media and email. If you just close the window, someone else using the pc may be able to access your accounts.

## Safe online

### Practical guide for women free from digital violence

## Safe online

Digital technology is a fundamental part of our lives: it is everywhere and we use it constantly. It is important to know how we can increase our online security so that we continue browsing feeling free and safe.



If you think it's normal. Or if you have the feeling that it is not but you would not be able to say why.

If you think it won't happen to you. Or if you feel that maybe you might be at risk but you don't know how.

If you want to know more because, it's true,

we live connected. Or if you find yourself in difficulty, for yourself or for your friend, sister, colleague, neighbor, mother, daughter.

This handbook is useful for:

- Knowing how to protect yourself
- Being able to help other women close to you
- Making you think, even if everything is fine

## Forms of digital violence against women

The digital dimension of violence against women<sup>2</sup> includes both abuses that occur online and those that are facilitated by technology, and there is continuity between online and offline. The medium is virtual, but the abuse is real and its effects are concrete.

Cyberviolence against women and girls<sup>3</sup> includes many forms of cyber-based violence on gender related grounds.

Acts of cyberviolence against women and girls can

- start online and continue offline, in physical locations, such as at work, school or home;
- start offline and continue online via different platforms, such as social media, email or messaging apps;
- be acted upon by a person (or group of persons), anonymous or unknown to the woman;
- be acted upon by a person (or group of people) that the woman knows, such as a (former) partner, classmate or colleague.



## Forms of digital violence against women

### RESTRICTING DIGITAL ACCESS

Prevent or limit the use of devices such as phone, PC or tablet, apps or internet connection, with the aim of controlling or isolating a person, or threatening to do so, with the aim of manipulating him.

### CYBERSTALKING AND CYBERSURVEILLANCE

Use of computer tools to harass, intimidate, spy on a person, making them feel threatened and insecure.

This can be done by logging into devices and accounts via

- Device usage request
- Using shared or stolen passwords
- Access to shared or unsecured devices
- Installing spy apps (stalkerware)
- and/or through the use of devices such as
- Car GPS or tracking devices
- Video surveillance systems
- Smart home devices (e.g. Google home or Alexa)

### CYBERHARASSMENT AND CYBERBULLYING AGAINST WOMEN AND GIRLS

Harassment through emails and messages, online profiles and internet pages, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

These are:

- Unsolicited email or message
- Offensive or inappropriate requests on social media or chat rooms
- Threats of physical or sexual violence via email, messages or chat
- Hate speech, or use of disparaging, offensive, threatening language
- Inappropriate or sexual comments on online posts or content

### NON-CONSENSUAL USE OF PERSONAL AND INTIMATE CONTENT

Abuse related to the circulation, or threat to circulate through computer means, of intimate, private and/or manipulated images/videos of a woman or girl without her consent.<sup>4</sup>

Images and videos can be

- obtained in a non-consensual manner
- manipulated in a non-consensual manner
- obtained by consensus but shared in a non-consensual way





- Tech aspects (devices)
- Use of apps and devices
- Behavoir of perpetrator
- Social media

## Checklist for professionals working with victims/survivors

When it comes to online violence and electronic devices, there are a few red flags that can warn the victim/survivor and the professional of the Support Service about the potential presence of stalkerware or of other forms of cyber violence.

Many times, the victim/survivor may not know about the forms and extent of cyber violence. It is important to be active and screen for the possibility of any form of cyber violence even if the woman shows no concern or expresses such suspicions. A woman may not be aware of what is happening, or she may not consider it an issue.

This tool is not to be considered a list of questions to be asked directly to the victim/survivor, but rather as a collection of "red flags" that may signal the presence of stalkerware or of other forms of control perpetrated using digital means. It's important to remember that cyber violence is not limited to cyberstalking, but it includes other forms of violence, like cyber harassment, non-consensual sharing of images (to the extent of sextortion and revenge porn), trafficking, etc.


The tool provides a list of warning signs divided into four groups:

- Technical aspects regarding smartphones (or other devices)
- Use of devices and accounts
- Behaviour of the perpetrator
- Social media

For each warning sign, you will find the related danger, the possible type of cyber violence and a tip on what to do.

**⚠ WARNING:** before taking any countermeasure listed below, the priority is to develop a clear and thorough IT safety plan with the woman (see above) Always remember that abrupt changes can escalate the perpetrator's abusive behaviour

### Technical warning signs related to smartphones or other devices

 RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
The mobile device disappeared for a period of time and then suddenly reappeared			These are signs that a stalkerware app might be installed on the device	Cyberstalking, stalkerware	Check for any stalkerware app installed by the perpetrator. If the presence of stalkerware is confirmed, plan next steps carefully. Please remember all safety issues related to the management of stalkerware
The mobile phone / tablet / pc is also used by the partner					
The phone battery drains faster than before					
There is an app icon that the victim/survivor doesn't recognize					
The phone has a higher consumption of mobile data					
The perpetrator gifted new devices to the victim/survivor or to the children			These apps allow the installation of software bundles on phones	Hacking, cyberstalking, non-consensual sharing of images	Periodically check that permissions are revoked
In the phone there's an app called "Superuser" (Android) or "Cydia" (iOS)					
Some apps have permissions for location and / or camera even if they were not initially set			There may be apps sharing info on location, or using the camera without the woman being aware		Delete all data from old devices
The woman recently changed her mobile phone without deleting the data on the old one			The perpetrator may have access to the old phone, to the data stored there and to apps accounts (email, social media, etc.)		

Tech aspects (devices)

Use of apps and devices

Behaviour of perpetrator

Social media

## Warning signs about social media:

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
The woman has been contacted by strangers on social media			The perpetrator may have created fake profiles to monitor her; her contact info may have been shared online by the perpetrator	Monitoring, on-line harassment, sexting, doxing	Check the unknown profile for pictures, posts, followers, common contacts
She often shares pictures and details on her whereabouts on social media or WhatsApp stories			These details can be used to track and monitor her. WhatsApp stories can be viewed even by someone who's not among her contacts	Monitoring, cyberstalking, non-consensual sharing of images	Talk with the victim/survivor about the importance of evaluating the impact of what she posts
She shared social media accounts passwords with her partner			The partner can access her accounts, monitor conversations, see friends/followers, acquire pictures		Change passwords. Discuss the importance of not sharing them with other persons, not even for "emergency" situations.
The password recovery email address is also accessible to the partner			In this case, if the woman changes a password, the perpetrator will easily find out. He can also change passwords himself, locking her out of her own accounts	Monitoring, cyberstalking, identity theft	Modify the recovery address before changing passwords
The woman noticed strange activity on her social accounts as if someone has accessed them			Someone, not necessarily the partner, may have access to her accounts	Cyberstalking, identity theft, non-consensual sharing of images	Change passwords
The woman has received "appreciation" calls and/or messages from strangers			It is possible that the woman's contact details, and intimate images have been published online	Doxing, sexting, non-consensual sharing of images, cyber harassment, revenge porn	Keep a track of calls/messages, set up "Google Alerts", request removal from search engines
The woman receives phone calls from num-			The perpetrator may be		Keep a log of these calls

## Warning signs about social media:

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
been contacted by strangers			The perpetrator may have created fake profiles to monitor her; her contact info may have been shared online by the perpetrator	Monitoring, on-line harassment, sexting, doxing	Check the unknown profile for pictures, posts, followers, common contacts
on her social media			These details can be used to track and monitor her. WhatsApp stories can be viewed even by someone who's not among her contacts	Monitoring, cyberstalking, non-consensual sharing of images	Talk with the victim/survivor about the importance of evaluating the impact of what she posts
media accounts			The partner can access her accounts, monitor conversations, see friends/followers, acquire pictures		Change passwords. Discuss the importance of not sharing them with other persons, not even for "emergency" situations.
recovery also partner			In this case, if the woman changes a password, the perpetrator will easily find out. He can also change passwords himself, locking her out of her own accounts	Monitoring, cyberstalking, identity theft	Modify the recovery address before changing passwords
ed in her if accessed			Someone, not necessarily the partner, may have access to her accounts	Cyberstalking, identity theft, non-consensual sharing of images	Change passwords
received his from			It is possible that the woman's contact details, and intimate images have been published online	Doxing, sexting, non-consensual sharing of images, cyber harassment, revenge porn	Keep a track of calls/messages, set up "Google Alerts", request removal from search engines
ives numbers, answers the			The perpetrator may be using apps that fake his caller ID	Spoofing, harassment	Keep a log of these calls together with phone records

## General goals

## Case studies

## Activities

## Group session for perpetrators: cyberviolence

## ■ Goals

- Help stop online control and coercion behaviours
- Have perpetrators take responsibility and face the consequences their behaviour has for their (ex-)partner
- Prevent further cyber violence
- Raise awareness on the legal consequences (fines, etc.) connected to cyber violence.

## ■ Case study

Read or role-play the following case:

"Mark and Lucy have been living together for six years and have a one-year-old daughter. Mark has always been very protective of Donna, even more so since their daughter was born. A few months ago, Mark asked Donna to share her phone and PC passwords as he might need them "in case of emergency". Donna was doubtful because she was afraid, she would give up some of her privacy, but she trusted Mark and decided to share her passwords. Since then, weird things have been happening: Mark seems to always know where Donna is or was and he mentioned a conversation she never shared with him. Donna became suspicious and talked to him about it, also mentioning that she would change her password. He got very angry and blamed her because he thought she had something to hide."

## ■ Discussion on Mark and Lucy's story

Divide the group into 3 sub-groups where each of them works on the following questions:

- **Group 1:** Do you think what just happened is violence? If yes, please write on a post-it which one of these behaviours are an indicator of violence.
- **Group 2:** What do you think the effects of this behaviour are on Lucy?
- **Group 3:** Do you think there may be legal consequences for Mark? Which kind?

Discuss the three questions with the whole group

## ■ Read, reflect, answer and discuss with the group: the forms of cyber violence

## Definition and characteristics

Cyberviolence is considered a generic term that indicates all the forms of violence perpetrated through information and communication technologies.

It can be defined as the online access to and distribution of offensive, violent, or dangerous materials with the objective of causing emotional, psychological, or physical damage. The most common kinds are cyber bullying and harassment.

We will talk about online cyber violence within relationships, that is, when someone's former or current partner uses technology to:

- Monitor or track one's partner
- Blackmail or threaten her with the release of intimate pictures or videos
- Release intimate pictures or videos
- Steal her identity, or make debts in her name
- Create fake profiles to monitor or spy on her
- Send threatening or offensive messages

Cyber violence within relationships is not separate from "real world" violence, since it often follows the same patterns as offline violence and is associated to both negative psychological and social consequences, including a poorer quality of life, and, often, to physical, psychological and sexual violence (EIGE, 2017).

In fact, social media, smartphones and other technologies can be used to perpetrate violence and this makes perpetrators partners feel paranoid and anxious.

## Group session for perpetrators: cyberviolence

## Read, reflect, answer, and discuss with the group

Based on what we've seen today, do you think the situations described below can be defined as "violent behaviour"?

Rate each situation on a scale from 0 to 10, where 0 represents a "non-violent" behaviour and 10 a "very violent" behaviour.

The man checks his partner's WhatsApp conversations without her knowing	0	1	2	3	4	5	6	7	8	9	10
The man gets angry because his partner doesn't want him to check her phone; he then accuses her of not loving him enough and of having something to hide	0	1	2	3	4	5	6	7	8	9	10
The man uses technology to monitor her movements, messages, and calls.	0	1	2	3	4	5	6	7	8	9	10
The man creates a fake social media profile to write to his (ex-) partner, pretending to be someone else.	0	1	2	3	4	5	6	7	8	9	10
She sends him intimate pictures or videos, he shows them to his friends or shares them online.	0	1	2	3	4	5	6	7	8	9	10
He threatens his ex-partner that if she doesn't sleep with him, he will post nude images online that she sent him in the past.	0	1	2	3	4	5	6	7	8	9	10
He gets her social media passwords without her knowing.	0	1	2	3	4	5	6	7	8	9	10
He installs the bank app with his partner's data on his phone to check her expenses and earnings.	0	1	2	3	4	5	6	7	8	9	10



## Cyber violence and stalkerware: Checklist of red flags and questions to detect possible episodes of digital violence

When working with perpetrators, both in individual and group settings, you may hear some statements that are in fact red flags that may warn you about the risk of cyber violence being perpetrated.

It's important for you to be able to pinpoint these red flags, to

- Recognize the forms of cyber violence associated
- Further investigate the abusive behaviour connected to cyber violence and assess the risk

In this tool we will specifically refer to cyber violence within a relationship, that is when a man uses technology to

- Control or spy on his partner, using specific apps installed on her device, or accessing her devices and accounts
- Blackmail or threaten her to share intimate images online
- Share or publish online intimate pictures or videos without her consent
- Steal her identity, make debts in her name
- Create fake online profiles to control or spy on her
- Send her threatening and/or offensive messages, also using fake identities/profiles

**⚠ WARNING! We must be very careful when we talk about cyber violence with perpetrators because we don't want to give them too many details on aspects they don't know about. The risk is to suggest them new forms of coercive control, increasing the risks for victims/survivors.**

We recommended to start with general questions and then move to more specific questions about the possible use of violence. This technique is known as funnel questions.

If the program implements "partner contact" activities, or if there's a collaboration protocol with a Support Service for Victims, it's important that all professionals involved in the case share any useful information on possible or actual cyber violence episodes, in order to better focus the work with the perpetrator and to increase the safety of the victim/survivor. Remember that the exchange of information must be compliant with all privacy regulations.

In the following table you will find some of the red flags associated with cyber violence, together with an indication of the possible type of violence connected, and example questions that can help you get a better insight in a safe way.

RED FLAGS	Yes	No	Form of cyber violence	Possible questions
He says her new car has a GPS system			Cyberstalking, Tracking	<ul style="list-style-type: none"> <li>• Do you think GPS is an important feature of the car?</li> <li>• Have you ever checked the destinations on the GPS?</li> </ul>
He bought/ installed smart devices at home (for example, Alexa, Google home, etc.)			Cyberstalking, Monitoring and tracking	<ul style="list-style-type: none"> <li>• What can you do with these devices?</li> <li>• Can you control them from afar?</li> </ul>
He refers information on his (ex) partner that he should not know ("I know for sure that she went to that place/ that she met with that person...")				<ul style="list-style-type: none"> <li>• How did you get this information?</li> </ul>
He knows about his partner's movements, even those not usual ("she said she was going to the doctor, but she went to [another place]")			Cyberstalking, Monitoring and tracking, stalkerware	<ul style="list-style-type: none"> <li>• How do you know she went there? Did she tell you?</li> </ul>
He quotes in detail parts of texts or conversations the (ex) partner had with someone else				<ul style="list-style-type: none"> <li>• How did you get this information?</li> </ul>
He mentions that his (ex) partner's WhatsApp web/Telegram access details are saved on a shared device			Cyberstalking, Monitoring, (acquired pictures can be shared online or used for sextortion, revenge porn), identity theft	<ul style="list-style-type: none"> <li>• Do you ever read your partner's or your children's messages?</li> <li>• Do you look at their pictures or check their contacts?</li> </ul>
He says he uses social media frequently (more than normal); he often mentions things or images his (ex) partner posted online ("I saw her pictures at [place] with", "she blocked me...")				<ul style="list-style-type: none"> <li>• Do you often check your (ex) partner's profiles?</li> <li>• (if she blocked him) Have you ever created a fake profile?</li> </ul>
He mentions that he prefers to have sex always in the same spot of the room or in particular conditions (hidden cameras)				<ul style="list-style-type: none"> <li>• Why is that?</li> <li>• Does your partner share the same preferences?</li> <li>• Does your partner know?</li> </ul>
He mentions sexting with his (ex) partner ("we send each other pictures")			Non-consensual sharing of images, doxing, sexting, sextortion revenge porn	<ul style="list-style-type: none"> <li>• Have you ever shown the pictures to someone else?</li> <li>• (if he "only showed to friends") How? From your phone? Did you share the pictures with them?</li> <li>• Have you ever threatened your (ex) partner to publish the pictures?</li> <li>• Have you ever shared or published them to get revenge (after a breakup)?</li> </ul>




Redflags = things that the perpetrator might say

Yes/no

Form of cyberviolence

Possible questions

## Technical warning signs related to smartphones or other devices

 RED FLAGS	Yes	No	Form of cyberviolence	Possible questions
He talks about a shared use of phones and other devices ( <i>"she uses mine too, I'm not jealous"</i> )			Cyberstalking, stalkerware	<ul style="list-style-type: none"> <li>Do you think that in a relationship it's important to share everything and that there should be no secrets?</li> <li>Do you get angry if your partner doesn't want you to see her phone or pc?</li> </ul>
He says devices or accounts are not password protected, or that he knows the passwords, or that he has access to the password recovery email ( <i>"it is a normal thing, if you have nothing to hide..."</i> )				<ul style="list-style-type: none"> <li>Do you get angry if your partner sets up or changes passwords of accounts and devices without sharing them with you?</li> <li>Have you ever glanced at message notifications on your partner's phone?</li> <li>Have you ever checked your partner's phone or accounts without her knowing?</li> </ul>
He has recently bought a new device for his partner (maybe to replace a device he broke during an episode of violence; <i>"I got angry and crashed her phone, but then I bought her a new one..."</i> )				<ul style="list-style-type: none"> <li>Why did you decide to give her this present?</li> <li>Do you expect your partner to give you free access to the devices you buy her?</li> <li>Do you get angry when she doesn't answer your calls or messages?</li> </ul>
He uses parental control apps ( <i>"I use this app to check where my kids are / what they post online"</i> )				<ul style="list-style-type: none"> <li>Why did you decide to use this app?</li> <li>Does your partner know or agree?</li> <li>Have you ever used this kind of apps for other purposes?</li> </ul>
He says that he is the person in charge of buying/setting up devices in the family ( <i>for example because his "partner doesn't know a thing about technology, I do it all myself"</i> )				<ul style="list-style-type: none"> <li>Why do you have this role in the family?</li> <li>When you deal with these tasks have you ever gotten access to information (on your partner or children) that you didn't have before?</li> </ul>
				<ul style="list-style-type: none"> <li>Do you think it is your right to look at her</li> </ul>



What topics?

Theory of cyberviolence  
Tech aspects  
Legal aspects  
Psychological aspects  
Practical aspects

How long?

Complete: 8 hours  
Short: 4 hours

What method?

Interactive, with many live demos

What speakers?

Cyberviolence experts (PP/VSS)  
ICT experts  
Legal experts

# The DeStalk Training



# DeStalk



**DeStalk**  
detect and stop stalkerware and cyberviolence against women

**"LA DIMENSIONE DIGITALE DELLA VIOLENZA DI GENERE"**  
Workshop formativi dedicati alle operatrici dei Centri Antiviolenza della rete **DuRe**

**1ª giornata – La Dimensione digitale della violenza di genere: definizioni, caratteristiche e aspetti tecnici e legali**  
12 settembre 2022, 15:30-19:30

15:30	<b>Saluti e introduzione</b>	Elena Gajotta – Project Manager Una Casa per l'Uomo
15:40	<b>Il progetto DeStalk</b>	Dimitra Minetsidis – Financial & Project Manager WWP EN
15:50	<b>Perché occuparsi di cyberviolenza?</b>	Elena Gajotta – Project Manager
16:00	<b>Definizioni e caratteristiche e forme di cyberviolenza Q&amp;A</b>	Elena Gajotta – Project Manager Luca Casagrande – Psicologo Una Casa per l'Uomo
17:00	<b>Pausa</b>	
17:10	<b>Sicurezza digitale: Tutelarsi da intrusioni e abusi Q&amp;A</b>	Dott. Luca Cadonici – Consulente informatico forense – Docente European Forensic Institute
18:10	<b>Aspetti legali della cyberviolenza Q&amp;A</b>	Laura Asti – Avvocato penalista Faro di Bologna
19:15	<b>Conclusioni</b>	Una Casa per l'Uomo

Link al modulo di iscrizione: <https://bit.ly/DeStalk-DIRE-1>







Supported by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)





**DeStalk**  
detect and stop stalkerware and  
cyberviolence against women

## Cyber violence and stalkerware online course



Do you work for a European public authority,  
victim support service, or perpetrator programme?  
Do you want to improve your capacity to support  
victims of cyber violence and stalkerware?  
Then the DeStalk project online course is for you!

**What will you learn?**

- 1) What is gender-based cyber-violence
- 2) How to identify different forms of cyber-violence
- 3) What is stalkerware and how to detect and remove the software effectively and safely
- 4) What to do when confronted with cases of cyber-violence and stalkerware

After completing the course you will receive a certificate of completion.

**What will you contribute to?**

The DeStalk online training will have an indirect but very significant impact in helping thousands of victims and those working to combat cyberviolence.

Join our free online course [here](#)  
The course is available in English,  
French, German, Italian and Spanish



**DeStalk**

Level 1 –  
**Gender based  
cyber violence**

9 lessons + test

Level 2 –  
**Forms of  
cyber violence**

6 lessons + test

Level 3 –  
**Cyber  
surveillance:  
Stalkerware**

8 lessons + test

Level 4 –  
**Working with  
a survivor-  
victim and/or  
a perpetrator**

3 x 4 lessons +  
test



# Lessons: content



All content is available in English, French, German, Italian and Spanish.

## Che cos'è lo stalkerware?

Fai clic sulle schede per maggiori informazioni

1 2 3 4



La tecnologia ha consentito alle persone di essere sempre più connesse. Possiamo scegliere di condividere digitalmente le nostre vite con il nostro o la nostra partner, la famiglia e gli amici indipendentemente dalla distanza che ci separa dalle altre persone. Tuttavia, si assiste anche a una diffusione del software che consente agli utenti di spiare a distanza la vita di un'altra persona tramite il proprio dispositivo digitale, senza che quest'ultima dia il proprio consenso o ne sia al corrente.

## Was ist Stalkerware?

Klicken Sie auf die Registerkarten, um mehr zu erfahren

1 2 3 4



Die Technologie ermöglicht es den Menschen, mehr als je zuvor miteinander in Kontakt zu treten. Wir können uns dafür entscheiden, unser Leben digital mit unserem Partner, unserer Familie und unseren Freunden zu teilen, unabhängig davon, wie weit wir räumlich voneinander entfernt sind. Es gibt jedoch auch immer mehr Software, mit der Nutzer andere Personen über ihre digitalen Geräte aus der Ferne ausspionieren können, ohne dass die betroffene Person ihr Einverständnis gibt oder jemals benachrichtigt wird.

## ¿Qué es el stalkerware?

Haga clic en las pestañas para obtener más información

1 2 3 4



La tecnología permite a las personas estar más conectadas que nunca. Podemos compartir digitalmente nuestras vidas con nuestra pareja, familia y amigos, independientemente de la distancia física. Sin embargo, también está aumentando el software que permite a los usuarios espiar de forma remota la vida de otra persona a través de su dispositivo digital, sin que esta dé su consentimiento o se le notifique.

## Qu'est-ce qu'un stalkerware ?

Cliquez sur les onglets pour en savoir plus

1 2 3 4



La technologie permet aux gens de se connecter plus que jamais auparavant. Nous pouvons choisir de partager numériquement nos vies avec notre partenaire, notre famille et nos amis, quelle que soit notre distance physique. Cependant, on constate également une augmentation du nombre de logiciels qui permettent aux utilisateurs d'espionner à distance quelqu'un d'autre via leur appareil numérique sans que la personne concernée ne donne son consentement ou ne soit avertie.

Supported by the Rights, Equality and Citizenship Programme of the European Union (2014–2020)




# Lessons: content



**What is stalkerware?**

Click the tabs for more information

1 2 3 4



Technology has enabled people to connect more than ever before. We can choose to digitally share our lives with our partner, family and friends regardless of how far we are physically. However, there's also a rise in software that let's users remotely spy on someone else via their digital device without the affected person giving their consent or ever being notified.

BACK NEXT

Content is prepared according to micro-learning approach.

# Impact: practical changes

**+ increased  
sensitivity**

**+ improved skills  
to recognize  
digital violence**

**+ check about  
cyberviolence  
with perp.**

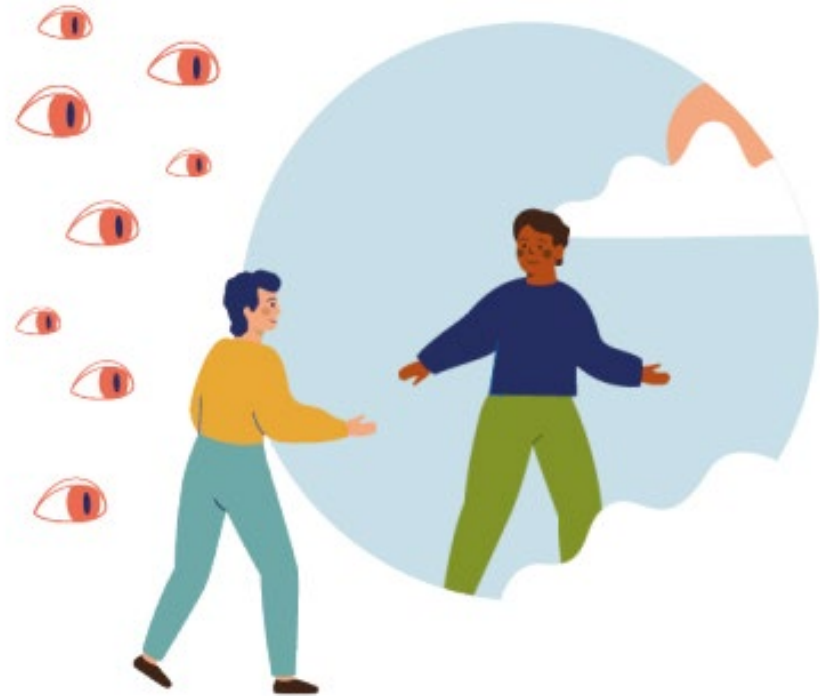
**+ train other  
colleagues**

**+ incorporation  
of safety  
planning**

**+ creation of  
support groups  
on cyberviolence**



Cooperating for an institutional  
strategy against cyber abuse:  
The DeStalk campaign



# DeStalk communication campaign on digital violence



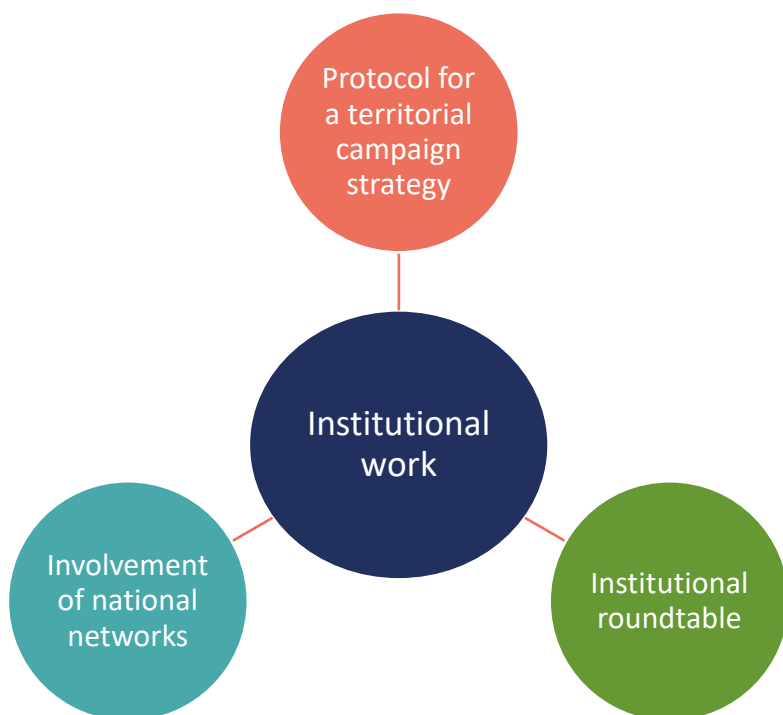
**Engage relevant stakeholders** among institutions, services, NGOs, etc, in a territorial campaign addressing cyber violence and stalkerware

**Raise awareness** among the general public by launching a pilot campaign targeting women, men, and bystanders

**Develop replicable tools and templates** for a cooperation strategy to address the digital dimension of GBV to be scaled up at European Level

**Engage relevant stakeholders**  
among institutions, services,  
NGOs, etc, in a territorial  
campaign addressing cyber  
violence and stalkerware

## PHASE 1



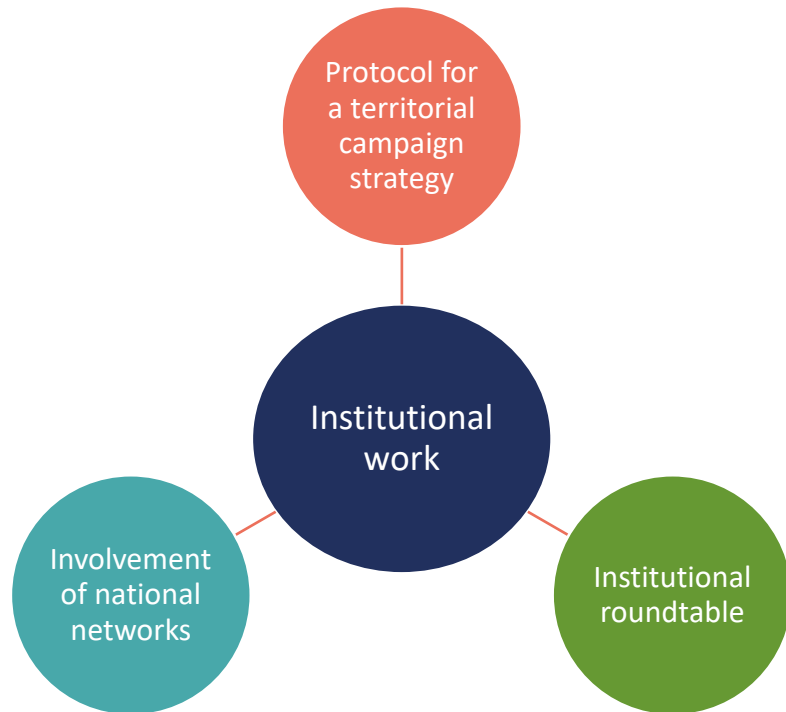
**Raise awareness** among the  
general public by launching a  
pilot campaign targeting  
women, men, and bystanders

**Develop replicable tools and  
templates** for a cooperation  
strategy to address the digital  
dimension of GBV to be scaled  
up at European Level



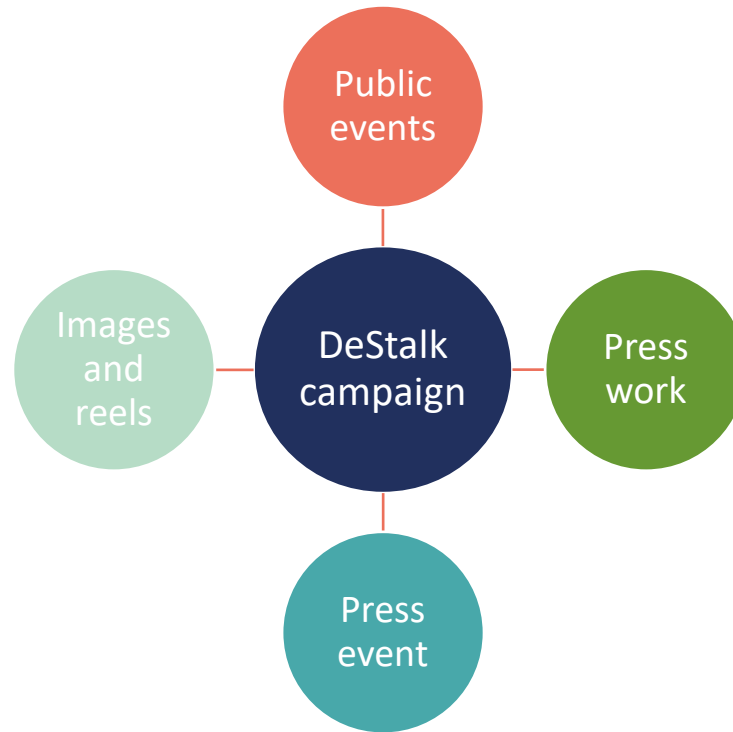
**Engage relevant stakeholders** among institutions, services, NGOs, etc, in a territorial campaign addressing cyber violence and stalkerware

## PHASE 1



**Raise awareness** among the general public by launching a pilot campaign targeting women, men, and bystanders

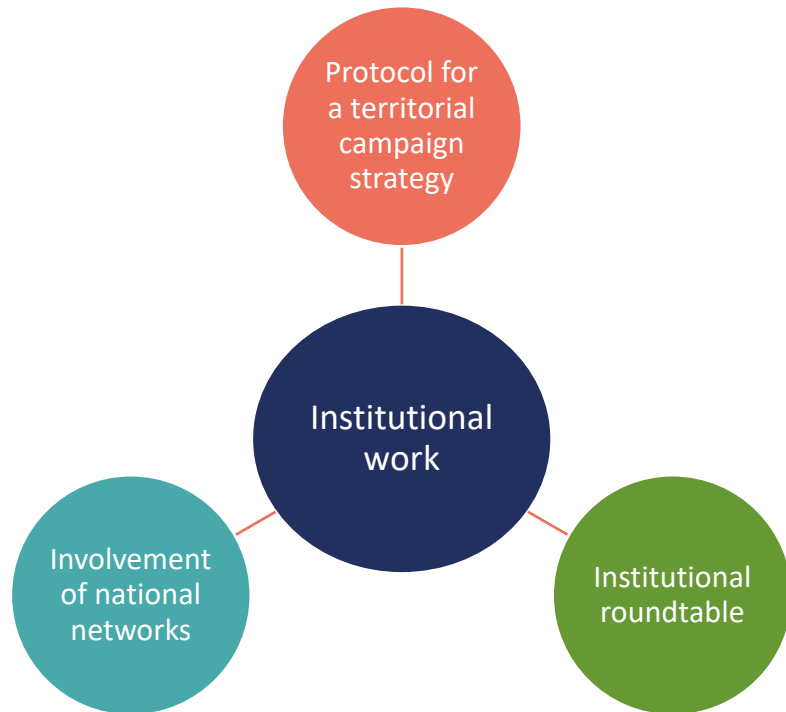
## PHASE 2



**Develop replicable tools and templates** for a cooperation strategy to address the digital dimension of GBV to be scaled up at European Level

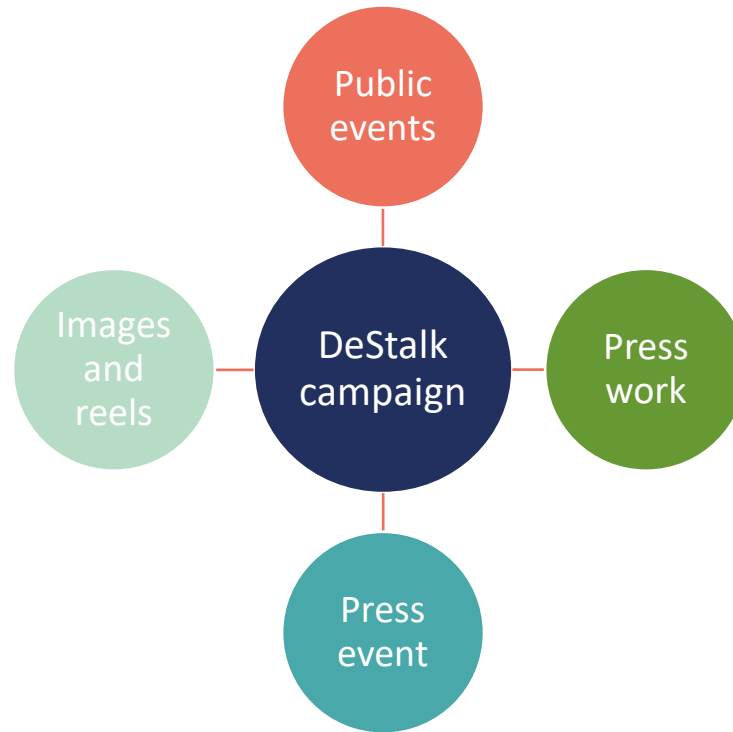
**Engage relevant stakeholders** among institutions, services, NGOs, etc, in a territorial campaign addressing cyber violence and stalkerware

### PHASE 1



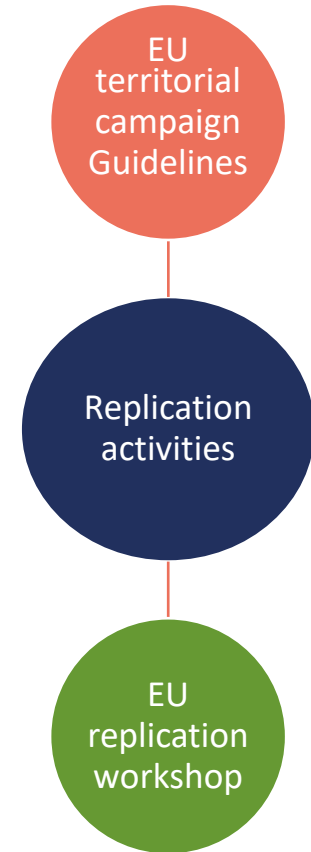
**Raise awareness** among the general public by launching a pilot campaign targeting women, men, and bystanders

### PHASE 2



**Develop replicable tools and templates** for a cooperation strategy to address the digital dimension of GBV to be scaled up at European Level

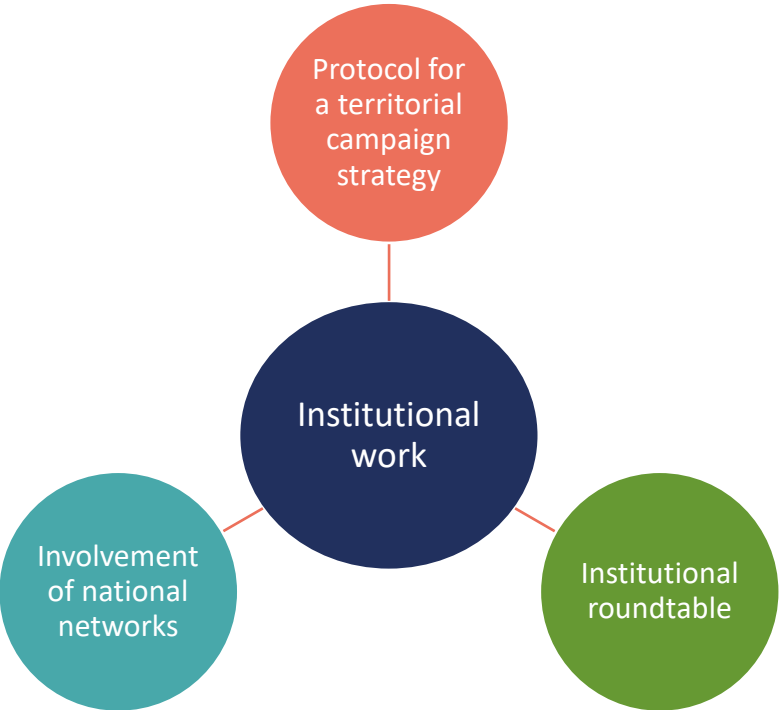
### PHASE 3



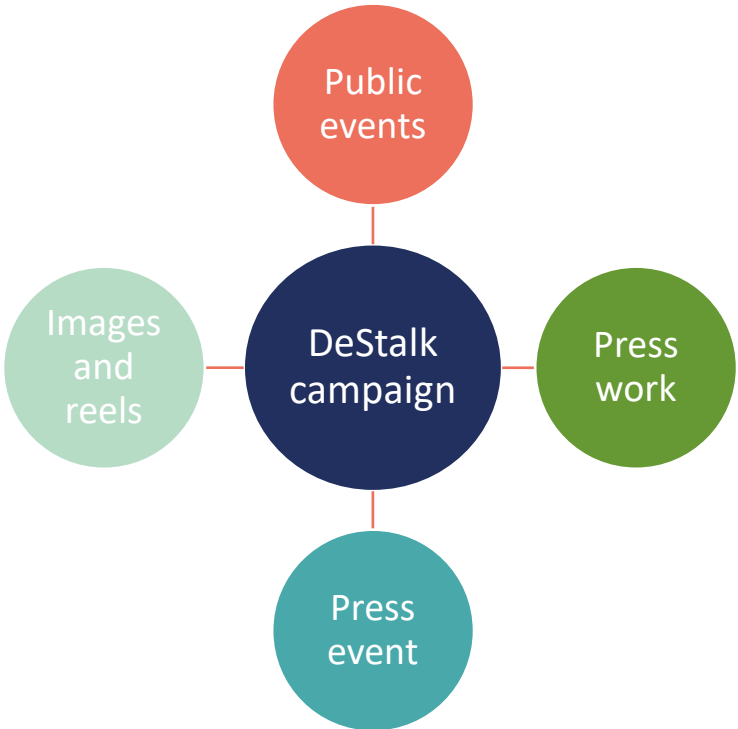
# DeStalk communication campaign on digital violence



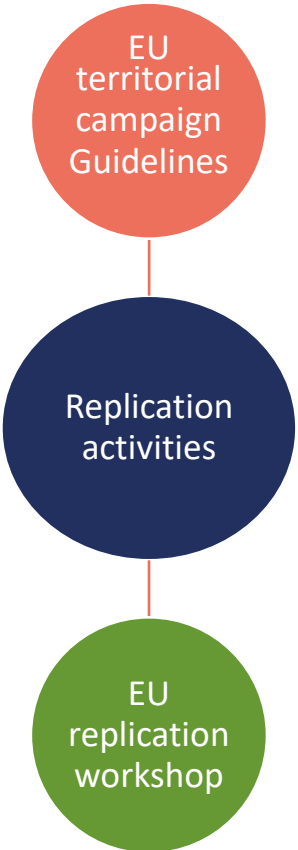
## PHASE 1



## PHASE 2



## PHASE 3



## DeStalk European territorial campaign guidelines to address cyberviolence and stalkerware against women

### Content

Background.....	3
Why DeStalk campaign guidelines .....	5
Campaign outline .....	7
Specific objectives and target groups .....	8
Set of proposed actions and potential outcome .....	8
Content strategy: DOs and DON'Ts .....	10
Lessons learnt .....	11
Success highlights .....	11
Challenges .....	12
Resources and templates .....	13

## Resources and templates

Besides collecting a thorough list of **external resources on the DeStalk webpage**, the consortium developed a comprehensive set of resources for potential multipliers to know more and improve their capacity and reach. The items listed below complement these **Guidelines for a territorial campaign**:

**Safe Online: Practical Guide for Women free from digital violence** to be used as an annex to VSS toolkit or a stand-alone resource



**E-learning course for public and private entities addressing GBV on fundamentals on cyber-violence and stalkerware against women**



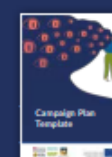
**Protocol of cooperation for public authorities and services to deliver a shared campaign tackling the digital dimension of IPV**



**Toolkit for practitioners of victim support services and of perpetrator programmes to address digital violence against women**



**Campaign plan template** based on DeStalk pilot campaign to be adapted to outline further territorial comms actions



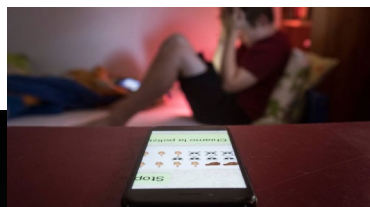
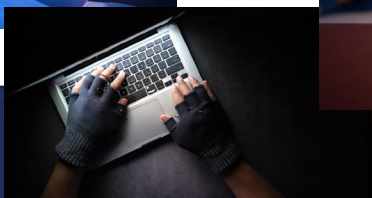
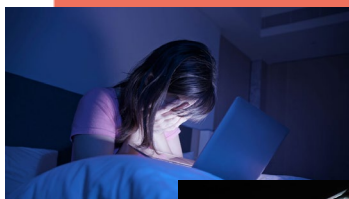
**Comms materials and samples**, such as infographics explaining types of online abusive behaviors, short video reels for women and men in their way out, etc.



# Content strategy: DOs and DON'Ts

## ❌ Based on this, in the content outline the following aspects should be avoided:

- **Victimization of women** (e.g. wording and images with woman depicted as suffering or humiliated)
- **"Monsterification" of men** (e.g. images of dark hooded shadows, too specific examples of violent behaviours)
- **Potentially harmful information** (e.g. name or link to website where stolen intimate pictures are shared, info on how stalkerware can be installed)
- **Morbid titling and easy wording** which could revictimize women, minimize abuse, shift the focus (e.g. sick love, revenge porn)
- **Difficult language**, vague or random information (e.g. too technical language, confusion among glossary, mentioning child sexual abuse data in an article about digital intimate partner violence)



## ✅ Good communication practices include:

- **Using non-stereotyped imagery** and fair wording to allow both men and women to identify and feel the message is for them
- **Keeping the focus on the abusive behavior** and clearly defining what is to be considered as violence
- **Promoting a holistic approach** and direct women to services instead of insisting on tech indicators of abuse
- Sharing an empowering message for women with **focus on the way out** and give practical info on how to get support
- Sharing a **constructive message for men** with a focus on accountability and on the possibility of changing one's behavior through specialized services
- **Stating clear commitment** and offer of the organization(s) running the campaign, and underlining institutional engagement to increase sense of safety and credibility

# DeStalk






# DeStalk campaign Video reels for men and women



All DeStalk materials are available at  
<https://www.work-with-perpetrators.eu/destalk>



Select your language <

ABOUTEVENTSRESOURCESIMPACTPROJECTSTRAININGGRANTS

WWP || EUROPEAN NETWORK

## Destalk Outputs

- ✓ **DeStalk E-learning Course**
- ✓ **Upgraded response of PP and VSS**
- > **Institutional campaigning**

Key stakeholders will cooperate to pilot territorial action and campaign. Guidelines and templates will be produced and tailorable for other territories of the European Union. The innovative outputs of the DeStalk project tackling online violence and stalkerware will be disseminated within strategic channels.

Read the "Protocol for a territorial campaign strategy addressing the topic of cyber violence and stalkerware" in [English](#) and [Italian](#).

Read the "Safe Online - Practical Guide for Women free from digital violence" in [English](#) and [Italian](#).

Watch the awareness raising reel videos for [women](#) and [men](#) made for the Italian campaign (English subtitles).

Have a look at the DeStalk pilot campaign plan ([English](#) and [Italian](#) available).

View the DeStalk campaign illustrations [here](#).

Read the Destalk campaign guidelines in [English](#) and [Italian](#).

Thank you for your attention!

Elena Gajotto

[elena.gajotto@unacasaperluomo.it](mailto:elena.gajotto@unacasaperluomo.it)