Dear readers,

Digitalisation is ubiquitous and changing the way we live. It offers new opportunities and challenges but may also pose dangers for people. This newsletter focuses on one of these dangers, namely the increasing digital violence against women, and presents selected policy approaches, initiatives and studies on the extent and the handling of digital violence against women in Europe: What does digital violence mean? Is digital violence against women a recent phenomenon or the continuation of violence against women and girls in the real world? How does the European Union approach this phenomenon of gender-related digital violence and its effects? Which national approaches and initiatives on detecting and tackling digital violence already exist? And which (digital) means can effectively counter digital violence? You will find answers to these questions in this newsletter.

In the first feature of this newsletter, we present selected approaches at European level. The focal point here is on the Council of Europe Convention on preventing and combating violence against women and domestic violence, the so-called Istanbul-Convention, which constitutes the most far-reaching international, legally binding instrument to date for preventing and combatting violence against women as well as domestic violence.

In the second feature, we take a closer look at Austria. There, a comprehensive legal review of online violence against women and girls was published in 2018. Doctor Dina Nachbaur is the managing director of WEISSER RING, a victim support organisation in Austria, and coauthor of the study. In her contribution, she discusses some current legal cases in Austria dealing with digital violence against women.

In a third feature, Lise Linn Larsen from the Danish Stalking Center and Riccarda Theis from the victim support organisation WEISSER RING Germany report on stalking, the effects of digitalisation and their experiences with the development of two new apps aimed at actively combating stalking.

The team of the Observatory wishes you an exciting read.

Katrin Lange, Project coordinator and research officer of the Observatory
Digital violence against women at European level

By Katrin Lange

Violence against women continues to be a major problem in Europe – and its extent is appalling:

One in three women has experienced some kind of physical and/or sexualised violence since the age of 15.¹ This adds up to about 62 million women in Europe.

The increased use and integration of digital technologies such as computers, the Internet and smartphones into everyday life has added a new dimension to violence against women. When digital technologies, in particular digital media, are used to harm others, we speak of digital violence. This digital violence can take on a multitude of forms: On the one hand, existing forms of violence against women such as harassment, bullying and stalking are being “exported” and extended to find their digital equivalent. On the other hand, the anonymity and reach of the Internet as well as new contact possibilities via social media allow new forms of violence to emerge, such as Doxing, Hate Speech or Revenge Porn. Experiences of digital violence often precede or accompany experiences of psychological, physical or sexualised violence in the real world. The omnipresence of digital media and the indefinite storage capacities of the Internet are particularly burdensome for the affected women.²

European Union

Within the European Union, there are already policies, initiatives and studies dealing with digital violence against women. As a basis, the official definition of genderbased violence by the European Commission includes “cyberviolence and harassment using new technologies”³. In 2012, the European Fundamental Rights Agency conducted a survey among 42,000 women in Europe⁴ and thus for the first time quantified digital violence against women across Europe.

According to the study, eleven percent of women over the age of 15 had already been exposed to cyberharassment, and four percent of 18- to 29-year-old women had been affected by cyber-stalking at least once.

Since 2012, the EU Victim Protection Directive sets minimum standards for the rights, support and protection of victims of crime in the EU member states.⁵ However, a study by the European Institute for Gender Equality (EIGE)⁶ highlights gaps in the provisions on support and protection for victims of genderbased violence. According to the institute, the Victim Protection Directive contains provisions which directly or indirectly refer to victims of genderbased violence but the wording of these provisions is too general. In the EU Gender Equality Strategy 2016–2019, combating (digital) violence against women as well as protecting and supporting victims is one of the five priorities.⁷ The fight against cybercrime, including digital violence against women, is one of three pillars of the European Agenda on Security adopted in 2015.⁸

Forms of digital violence

- **Cyber-harassment** means the harassment of a person through digital media (for example hate speech, sexual harassment, threats of rape or murder).
- **Cyber-bullying** means bullying of one or more persons by using digital media with the aim of specifically excluding, insulting or mocking the person concerned.
- **Cyber-stalking** means establishing contact against the will of the person concerned through digital media with the aim of threatening, harassing or tracking that person.
- **Doxing** means collecting and publishing personal data that can be found on the Internet or threatening the person concerned with such a publication. Doxing is often associated with the intention of threatening the person concerned with violence.
- **Hate Speech** means that people are either directly discredited, attacked or insulted, or hatred and violence is incited against them. The possibility of commenting makes Hate Speech happen in particular online and in social media.

Particularly women are rarely free to express their opinions online and are confronted with abuse, sexist harassment, threats of rape and death (in connection with the publication of personal data, see Doxing). As a result, many women participate less in digital discourse or withdraw from it completely.

In Revenge Porn, pictures or videos are published online without the consent of the women shown, for example by former partners or after a rape. Such pictures or videos are then distributed via social networks or shown and exchanged in special online forums.

---

¹ FRA – European Union Agency for Fundamental Rights (2012): Violence against women: an EU-wide survey. Results at a glance; p. 17; see here.
² A good overview on digital violence and what those affected can do against it can be found on the website “Aktiv gegen digitale Gewalt” (“active against digital violence”) of the German Federal Association of Women’s Counselling Centres and Women’s Helplines; see here (in German).
³ See here.
⁴ FRA 2012, p. 30 and 32.
⁵ See here.
⁶ EIGE – European Institute for Gender Equality (2014): Analysis of EU directives from a gendered perspective; see here.
⁷ See here.
⁸ See here.
So far, the European Union’s approaches on tackling digital violence against women have not been sufficient. According to an EIGE study published in 2017, there is a particular lack of a comprehensive conceptualisation as well as a lack of EU-level legislation on digital violence. Moreover, the European Parliament called on the European Commission in 2017, urging the latter to present a proposal for a directive and a comprehensive EU strategy against all forms of violence against women, including digital violence. However, the Commission has not complied with this request yet.

Nonetheless, the issue of digital violence against women remains on the EU’s political agenda: Based on the first EU-wide survey by the European Union Agency for Fundamental Rights from 2012, an additional survey on gender-based violence in Europe, including digital violence, will be carried out from 2020 to 2022. In addition to this, the European Union signed the Istanbul-Convention in 2017.

Conventional on preventing and combating violence against women and domestic violence (Istanbul-Convention)

The Istanbul-Convention is, to date, the most far-reaching international, legally binding instrument for preventing and combating violence against women as well as domestic violence. The convention was signed in Istanbul in 2011 and entered into force in 2014. By now, 34 countries have ratified the agreement. The aim of the Istanbul-Convention is to improve the protection of women against gender-based violence in Europe in a holistic approach and to create Europewide minimum standards. Specifically, the convention contains obligations with regard to coordinated approaches towards violence prevention, victim protection, prosecution and data collection. The Istanbul-Convention also provides for comprehensive monitoring of the implementation of obligations in the contracting states. This monitoring is performed by an independent group of 15 experts (Group of Experts on Action against Violence against Women and Domestic Violence, GREVIO).

The Istanbul-Convention adopts a comprehensive and broad concept of violence, which includes all acts that cause or may cause physical, sexual, psychological or economic harm or suffering to women. It thus generally encompasses all forms of violence. Though digital violence is not explicitly mentioned in the convention’s text, in the Explanatory Report to the Istanbul-Convention, digital violence is partially included in “stalking” as a form of violence. According to this definition, stalking can also include “following the victim in the virtual world” as well as “spreading untruthful information online.”

A recent mapping study by the Council of Europe also classifies psychological violence and sexual harassment as forms of violence that can have a digital equivalent. This classification traces back to the general assessment by GREVIO, which states that digital violence against women should be considered a “continuum of offline violence.”

The ratification of the Istanbul-Convention by the EU nourishes the hope that the monitoring of national approaches to combat and prevent (digital) violence against women within the EU may be improved. The aim of improving the fight against digital violence in Europe was explicitly taken into account when reaching this decision. However, due to the blockade by some member states in the European Council, it has not been fully ratified yet. The designated President of the European Commission

Violence against women

The convention considers violence against women to be a violation of human rights (article 3a IC), being an expression of a historically developed unequal power balance between men and women (premable), and to be considered an effect of structural discrimination. The Convention obliges the signatory states to contribute to the elimination of this form of discrimination against women and thus to their formal and factual equality.

Explicitly listed forms of violence in the Istanbul-Convention (IC)

- domestic violence (Article 3b IC),
- psychological violence (Article 33 IC),
- stalking (Article 34 IC),
- physical violence (Article 35 IC),
- sexual violence and rape (Article 36 IC),
- sexual harassment (Article 40 IC),
- forced marriage (Article 37 IC),
- female genital mutilation (Article 38 IC),
- forced abortion and forced sterilisation (Article 39 IC) and
- violence in the name of culture, religion or tradition; this also includes “violence in the name of honour” (Article 42 IC).

9 EIGE—European Institute for Gender Equality (2017): Cyber violence against women and girls; see here.
11 See here.
13 Council of Europe (2011): Convention on preventing and combating violence against women and domestic violence; see here.
15 Cybercrime Convention Committee (T-CY), Working Group on the protection of victims of online violence, especially against women and children (2018); Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018; S. 23f.; see here.
17 See footnote 12.
18 To date, all EU member states have signed the Istanbul-Convention for their country, but a total of eight European countries (Bulgaria, Latvia, Liechtenstein, Lithuania, Slovakia, the Czech Republic, Hungary, the United Kingdom) have not yet ratified it; see here. Especially in Bulgaria and Slovakia, there was massive political opposition against the ratification; see here.
Ursula von der Leyen announced that full EU accession to the Istanbul-Convention would be a key priority for the European Commission. In the event of failure, she has already announced: “If the accession remains blocked in the Council, I will consider tabling proposals on minimum standards regarding the definition of certain types of violence, and strengthening the Victims’ Rights Directive. I will propose adding violence against women to the list of EU crimes as defined in the Treaty.”

It remains to be seen whether digital forms of violence against women will also be taken into account.

### National approaches on handling digital violence against women, case example Austria

In 2018, a comprehensive legal review of cases of online violence against women and girls was presented in Austria by the Human Rights Research Centre of the University of Vienna and by the victim support organisation WEISSER RING for the first time. The study, financed by the Austrian Federal Government, includes both an analysis of the legal framework as well as the collection of quantitative and qualitative data. This allows for assertions to be made about the extent and forms of violence affecting women and girls online:

One third of women and girls in Austria have experienced online violence at least once in the past twelve months: “Most often, they were affected by online insults and verbal abuse due to their political worldview (12.8 percent) and by personal insults (11.6 percent). In addition, 10.9 percent of respondents received sexually suggestive messages (in the form of text, photos and videos) without their consent.”

The review also shows which effects digital assaults can have on those affected and which strategies could support affected women and girls in coping with these forms of violence.

**Doctor Dina Nachbaur** is the managing director of the victim support organisation WEISSER RING in Austria. The organisation WEISSER RING was founded in 1978 and is accessible to all crime victims throughout Austria. Dina Nachbaur is responsible for the areas of victim helpline, victim support and legal support as well as international networking. In her article, she discusses some current legal cases in Austria involving digital violence against women.

By **Doctor Dina Nachbaur, WEISSER RING, Austria**

An Austrian case has prompted the European Court of Justice (ECJ) to deliver a judgment that has already been the subject of controversy: A female politician had been defamed as a “rotten traitor of the people” (“Miese Volksverräterin”) on Facebook. The Austrian Supreme Court referred the legal question of whether comments identical in wording and, under certain circumstances, identical in meaning should be deleted to the ECJ – as a question of interpretation of the Directive on Electronic Commerce. The ECJ ruling now clarifies that EU law does not prohibit national courts from forcing host providers to delete unlawful comments as well as comments identical in wording and, under certain circumstances, also identical in meaning.

Another case of online defamtion of a former politician sparked a discussion about the criminal offence of insult. In Austrian criminal law, the legal good to be protected against insults is the “honour”, wherefore a certain “public”, which could have at least perceived the insult, is necessary. In this case, the female politician had been insulted in a particularly extreme sexist manner. However, this was done via private messaging. The case gained major attention as the victim did not see any other way of defending herself than by publicly naming the suspected violator (shaming), which led to her being convicted for socalled “discredit” against him. The court of appeal overturned the judgment and referred it back to the first court, where the case is currently still pending.

---

20 See [here](https://www.stop-cyberse-xisme.com) (in German).  
21 Ibid., p. 69.
Within the framework of the Protection against Violence Act 2019, several individual offences were revised within the Austrian Criminal Code. Among other things, from 1 January 2020 onwards, the criminal offence of “Beharrliche Verfolgung” (“persistent chasing/stalking”, note of the Observatory) within the meaning of Section 107a of the Austrian Criminal Code will be extended, so that publishing “facts or photographs of the most personal sphere” of a person’s life “without their consent” will now be punishable. In the explanatory remarks to the corresponding government bill, it is pointed out that there are reports of recurring cases in which photos were posted onto “cars, house walls and advertising boards” in the immediate vicinity of the victim’s house without their consent, sometimes accompanied by “(defamatory) texts”.

However, paragraph 107c of the Austrian Criminal Code, which attempts to cover acts of cyber-bullying, has not been amended as part of the recent revision. Under “continued harassment by means of telecommunications or a computer system”, making accessible facts or images of a person’s highly personal spheres of life (without their consent) to a larger number of people is being penalised, as are other violations. In practice, however, this type of offence poses recurrent problems, as it is considered a “continuous offence”, which in itself presupposes continued perpetration over a “prolonged period”. Particularly when publishing intimate images against the will of the person depicted, one reading of the laws suggests that there is already a “continuous offence” if a picture is uploaded on Facebook once and the accused person does over a prolonged period not undo his or her act by deleting the picture again. From a dogmatic point of view, however, this argumentation is contested, even though it could bring about the desired success in punishing such behaviour. However, not all social media platforms technically allow the subsequent deletion of uploaded content. Therefore, this creative interpretation of the law also does not result in closing the existing gap in legislation.

Interview on apps against stalking: initiatives from Denmark and Germany

Stalking is a form of violence that is exerted particularly often online and via digital media. Also when it comes to this form of violence, women are more often affected than men.

In Europe, 18 percent of all women above the age of 15 have been subject to stalking, about 14 percent experienced cyber-stalking. According to a Danish survey conducted in 2013, 63 percent of victims of stalking are women. Also in German criminal statistics, women make up the clear majority of 90 percent of stalking victims within partnerships.

Most female victims know the perpetrator. Stalking often takes place in the context of domestic violence and post-relationship stalking. Many victims do not know how they can counter or fight stalking. Proving the violations can be difficult – especially if they are committed online. Both the Danish Stalking Center as well as WEISSER RING e.V. in Germany have developed smartphone apps as digital aides in such cases. Using the apps, victims can document stalking activities, both physical and digital, with conclusive evidence.

In the following interview, Lise Linn Larsen of the Danish Stalking Center and Riccarda Theis of WEISSER RING e.V. Germany report about stalking, the effects of digitalisation and their experience with the new apps Skytsengel and NO STALK.

22 See footnote 1, p. 28.
24 For a summary of the study; see here (in Danish).
26 Bundesverband der Frauenberatungsstellen und Frauennotrufe (Frauen) (2017): Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff; see here (in German).
Lise Linn Larsen is the director of the Danish Stalking Center. It is the only specialised treatment, intervention and research center in Northern Europe, and offers guidance and counseling to professionals, as well as stalking victims and stalkers who are assessed to benefit from treatment. Ricarda Theis is responsible for Social Media at WEISSER Ring e.V. Germany. This support group for crime victims and their relatives is active throughout Germany. About 2,900 volunteers work in 400 branch offices for the victim helpline and the online counseling service of the organisation.

The interview was conducted by Sarah Molter, research assistant at the Observatory.

In what way has stalking changed due to digitalisation?

Larsen: Stalking is defined as a series of repeated unwanted and intrusive actions that are experienced as disruptive and intimidating by the stalking victim. In Danish Stalking Centre we understand digital stalking as serious as physical stalking. Digital stalking is doing serious harm to victims. All kinds of stalking are harming the victim.

Theis: Using various digital means, attacks on the stalking victims take place around the clock. The space for stalking has expanded. Instead of on their way to work, the victims now also meet the perpetrators in their personal digital space: on their own profile in social networks, in their mailbox, on their smartphone in their pocket, on their tablet in their living room, and so on. The violator is even closer, has more means of contact and is thus able to terrorise the victim even more. There is no time and no space for recovery, regeneration or clear thinking.

Larsen: Digital stalking consists of all kinds of attempts of contact on the phone, e-mail and social media. Victims report about: sharing of private photos, hacking and misuse of accounts, ordering things or services in the name of the stalking victim, attempts of contact from false profiles, surveillance via GPS or apps, digital sexual violation, manipulated photos with sexual or degrading content, creation of fake dating profiles and threats about sharing these with partners, on social networks or at the workplace. Digital stalking is very intrusive since the victim is exposed to it everywhere and at all times. Many victims of digital stalking explain how their personal space is constantly invaded as the digital stalking typically reaches them when they are at home and ought to feel safe.

Ms. Larsen, which new challenges and problems do stalking victims face?

Larsen: Most people use digital services and social media in everyday activities when communicating with relatives, to stay updated on news or when booking a fitness class. Activity on digital platforms is also required when interacting with authorities and for many people in their jobs.

Digitalisation introduces a new vulnerability that most people are not aware of. Avoiding leaving digital footprints behind requires technical knowledge that most people do not have. Online stalking is very accessible since the stalker faces no physical or timely restrictions on when and how to contact the stalking victim. In addition, the possibility of staying anonymous and the low costs of performing digital stalking make it easy and very widespread. Furthermore, legislation and punishment for digital stalking have not yet been aligned with the rising tendency and the farreaching consequences of the phenomenon. Protecting oneself requires a lot of technical insight and not least knowledge of how digital development is continuously changing. Thus it is challenging...
for ordinary people to stay ahead and take the precautions needed. The development of digital stalking brings forth the question: how do we live a digital life – and stay safe?

**You have developed an app as a means against stalking. What is the app’s purpose and how does it work? What are the app’s advantages?**

**Theis:** The app NO STALK is designed to collect evidence in order to be able to take action against the perpetrator. It is meant to empower the victim to switch from a passive into an active role: You are no longer helpless; you are taking action against the stalker.

The app contains information, documentation and emergency modules. The information module offers all relevant information on the issue of stalking. With the documentation module, you can track and collect all stalking activities (like pictures, videos, text messages). And this is done in real time – right in the moment when it happens. This has the advantage that the victim does not have to deal with it again later, for instance if you would be writing into a classic diary in the evening. This takes away some of the burden and stress. Plus, it also prevents later “modification” of the actual data through one’s own recollection or a somewhat unconscious downplaying of the situation (“Actually, it was not that bad”). Having this evidence, the victim can also contact the police. There, he or she can file a complaint and take legal action against the stalker or effect a so-called “Gefährderansprache” (official addressing of a potential violator, note of the Observatory). In 80 percent of all cases recorded by the police, stalking stops after such an addressing.

**Larsen:** As a response to the growing number of people facing digital stalking, Danish Stalking Centre is offering counselling on digital safety. Furthermore, we have developed the app, Skytsengel, to increase security and freedom of movement in the everyday life of stalking victims. The app is developed in cooperation with the Danish Police and specialists on digital safety. With just a few clicks, stalking victims can activate family and friends if they feel unsafe. Skytsengel has a function of three levels of alarms according to the severity of the situation. Another function in the app is a log, where the stalking victim can register and document all contact attempts from the stalker: e.g. screenshots of text messages, e-mails, and photos of unwanted presents. In Denmark, all registered episodes are included in the police assessment of the case, regarding the possibility of pressing charges or giving a restraining order.

**Ms. Theis, what kind of feedback did you receive regarding the app?**

**Theis:** The WEISSER RING foundation presented the idea of a NO STALK app for the first time at the Google.com Impact Challenge, a funding competition for digital innovations, in 2018. The reactions were extremely positive – we even received flagship project funding. However, in many conversations at other events where we presented the app, we also got a confirmation of what we had already suspected: Society is not susceptible to stalking and the serious consequences for those affected. There is an urgent need for education.

Apart from that, we have had discussions within our association, we have interviewed our victim consultants, who have been in charge of stalking cases, and we have talked to several experts. This is how the structure and the technical design of the app were established. Data security and protection of the collected evidence as well as their usefulness in court were key issues. Therefore, TÜV-certification for data security and functionality were particularly important to us. Since May 2019, the NO STALK app is available free of charge in the App Stores.
Which groups did you successfully target and reach with your app – and which not?

Thesis: Of course, people with a greater affinity for smartphones find it easier to install the app and use it, but we have also received feedback from outside of the “smartphone generation”, from people who like the idea of the app and thus make use of it. Sometimes, people have trouble regarding the handling or the installation of the app – which is somewhat complicated due to the high security settings. Then, we get a call and can assist. Many older people are also skeptical of the technology initially whereas many younger people think the app does not stretch far enough. In any case, it can be used as a means to collect evidence and to reflect on certain questions: What does the stalker do to me? What effect does this have on my life? Many people do not realise this until they see how frequent the stalking actually happens by reading through these diarylike entries in the app. The app is thus suitable for anyone affected by stalking. Of course, there is also still the possibility to get personal support from consultants at WEISSER RING.

Larsen: Skytsengel reaches a broad group of stalking victims, both men and women in different age groups are using the app. Users of Skytsengel have responded positively and reported that the app has improved their sense of security, for example when walking in public spaces.

Our app is not solving the problem of stalking as such, but it is an attempt to make life easier, safer and less constrained for victims of stalking. The app cannot stand alone, therefore Danish Stalking Centre is continuously lobbying for criminalising stalking through the adoption of separate stalking laws – including digital stalking.