



**The role of social partners in preventing third-party violence and harassment
EPSU/HOSPEEM/CEMR/CESI/EUPAE/ETUCE/ETF/UITP/ETNO EC-funded
project**

**Report of Webinar 4: Digitalisation and third-party violence and harassment at
work: challenges and risks**

16 December 2021

Introduction

The fourth project webinar on third-party violence and harassment and digitalisation was attended by over 60 representatives from employers and trade unions representing public services and telecoms sectors across Europe and was chaired by **Nadja Salson, EPSU**.

Nadja noted that digitalisation of the economy and public services was high on the agendas of the European Commission and increasingly of EU and national social partners. The changing world of work, along with the intensification of work and stress, protection of personal data, amongst other issues are raising concerns. The fourth project webinar provided an opportunity to start a discussion on digitalisation in relation to third-party violence or harassment at work: the scale, consequences of cyberviolence, the extent to which digitalisation creates or transforms the nature of violence and provide tools to prevent and respond to it, and whether and how the 2010 multisectoral Guidelines on prevention of third-party violence and harassment at work should be updated. She informed participants that two days before the meeting, the European Parliament's (2021) adopted a report "Combating gender-based violence: Cyber violence". The report includes alarming data on the significant increase in gender-based digital harassment. It was disappointing, however, that the report fails to mention the world of work and the role of social partners in preventing and tackling these worrying developments. This has been criticised by the ETUC in a letter addressed to MEPs.

In addition, Nadja noted that some of the project partners - EPSU, CESI, CEMR and ETUCE - issued a joint statement on violence against women on 25 November, reinforcing the importance of the world of work and the role of social partners in the forthcoming directive on gender-based violence, which will be issued on 8 March 2022.

Jane Pillinger, Expert and Project Consultant, gave an overview of the previous webinar on risk assessment, held on 24 September, noting also that the prevention of digital harassment is both a complex issue and a critical issue for risk assessment in the world of work. In relation to the project's ongoing survey, to be closed at the end of the year, to date responses have been received from 181 organisations, 62% from the employers' side and 48% from the trade unions. In relation to the topic of digitalisation, 9,5% of respondents stated



With the support of the European Commission

that the covid pandemic led to services going online. Initial findings suggest that cyber harassment is a growing area of concern (with 15% of respondents reporting that cyber harassment is a predominant type of TPV, and the fifth most important form of third-party violence and harassment after verbal harassment, psychological harassment, physical violence and sexual harassment). Delegates were reminded to fill in the questionnaire before the end of the year.

Panel: presentations by experts

The first presentation was given by **Mathias Wouters (Post-Doctoral labour law researcher, Leuven University, Belgium)**, co-author of the ILO report “Upgrading protection against cyberbullying and ICT-enabled violence and harassment in the world of work” (2020).¹ The report is the first comparative study on laws related to cyberbullying in the world of work, defined as a form of bullying which is repetitious, last in time and results from unequal power relations between the perpetrator and victim, and which may also be applicable beyond the world of work. Although digital abuse, such as posting one photo or message online, may be one-off, its effects can be repetitious. These acts are not always erasable, and unlike other forms of work-related violence, cyberbullying is often anonymous. Evidence of cyberbullying also shows the strong interconnections between work and home. While comparing data remains a difficult exercise, as definitions of cyberbullying can differ from one country to another, national studies reveal incidents of cyberbullying affecting 14-20% of university employees (UK), 22% of teachers (Czech Republic), 22% of journalists (Sweden), and 72% of public servants (Australia). There is a lack of gendered data but it is known that young women are at greater risk of cyber violence at work, as shown from examples of women journalists or politicians. Digital abuse is often not captured because bullying is defined as encompassing repeated acts, whereas many one-off acts of digital abuse are not reported or documented. Due to the often anonymous nature of cyberbullying, it remains difficult to identify whether perpetrators are from inside or outside the organisation or company. Based on the data available, the occurrence of cyberbullying comes principally from employees, but this may be due to the fact that external harassers are more difficult to identify.

There are valid reasons to consider this a priority for employers and workers, the consequences for the victims are very significant and can spread like a “wildfire”, affecting also bystanders and risk being replicated. While specific legal provisions on cyberbullying at work remain scarce, a number of different legal frameworks exist in labour laws/labour codes, OSH regulations, non-discrimination laws and human rights instruments regarding employers’ duty of care towards their employees. Furthermore, general data protection laws also mean that it is important to reduce risks of data exposure in the workplace. Companies or public services’ internal policies are also very relevant.

Examples include Belgium law, which puts obligations on employers to take preventive measures and ensure that employees have recourse through the cascade system: comprising informal resolution, formal resolution with a complaint to a labour inspector and/or professional prevention adviser and recommendations on prevention to the employer (or sanctions in case the employer has failed to put in place sufficient prevention or protection measures), and final recourse by lodging a legal case. For the latter, however, the absence of physical contact between a perpetrator and a victim can make it difficult to qualify a case of cyber abuse as bullying. Another national example is Article 173 of the Spanish Criminal Code, which addresses cyberbullying; it was amended in 2010 with a more specific focus on employment where the act of bullying takes advantage of a relationship of superiority.

¹ https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/departments-and-offices/workquality/WCMS_736235/lang--en/index.htm



In conclusion, Mathias recommended the importance of re-evaluating laws, policies and Collective Bargaining Agreements (CBAs) in relation to cyberbullying, not least to ensure that its scope covers all workers regardless of employment status, trainees, self-employed as well as ex-employees (who may have left because of workplace bullying), and also to consider taking into account the perpetrators' employers. It is important that prevention advisors and the courts are trained in digital harassment, that bystander responsibilities are emphasised, and that employer responsibilities are clearly defined. There is also a need for much greater worker involvement in data protection and risk assessment measures. Although there are some examples of CBAs and workplace policies that address digitalisation, there has been no systematic follow-up of their implementation.

The second presentation by **Tim Tregenza (EU-OSHA)** Senior Network Coordinator and private counsellor at OSHA, addressed the impact of new forms of digital harassment on third-party violence and harassment. Changes are occurring in relation to digital access to services, resulting from changed expectations by clients and customers for instant responses, while systems failures can lead to frustrations. Online harassment may be anonymous and the speed of sharing information can cause greater levels of harm. There is also a blurring of private and work life, the "always on" culture makes "switching off" difficult. Furthermore, the covid pandemic has led to a significant increase in telework and a corresponding increase in online harassment. It is important to recognise that employers have the legal duty to protect an employees' health and safety at work, including psychosocial risk factors such as risks of working online and risks faced by women and other vulnerable groups. In addition, data protection is now a health and safety issue.

In addressing the modern day challenges from digitalisation and teleworking, Tim noted that there is a need for a holistic, systemic and systematic approach that ensures policy coherence in data security, harassment, telework and OSH. To address all forms of violence, it is crucial to rely not only on criminal law, which deals with individual cases, but also on health and safety rules which provide for a collective approach. An OSH publication on telework was issued by EU-OSHA in 2021.² Risk assessments should be up-to-date so that they address risks associated with teleworking and new digital systems, including data protection. Easy-to-access and online reporting systems would also help to ensure that digital harassment and abuse are identifying and addressed, as is the case in Finland. It is crucial that there is ongoing dialogue with workers and other stakeholders such as parent-teacher associations and patient groups. Repeated information and training, especially for supervisors and managers, including proactive interventions and post-incident review and procedures, are all essential. Mental health and wellbeing promotion can also be important complements to workplace procedures and policies. Finally, new policy approaches are needed to raise the visibility of digital harassment and to give recognition to work-related stress, to ensure that workers talk about and report violence and harassment, and to raise awareness about the different forms of third-party violence and harassment and particularly sexual harassment.

Martina Di Ridolfo (ETUCE) highlighted the recent plenary meeting of sectoral social dialogue in education (15 December 2021),³ which adopted a social dialogue project on digitalization and issued an ETUCE/EFEE joint statement on challenges and opportunities of digitalisation for the education sector, including TPV. The joint statement commits to "Support education institutions, school leaders, teachers and other education personnel in addressing the health and safety issues stemming from digital education...and enhance social partner

² <https://osha.europa.eu/en/publications/telework-and-health-risks-context-covid-19-pandemic-evidence-field-and-policy-implications>

³ <https://www.csee-etu-ce.org/en/news/etu-ce/4695-european-sectoral-social-dialogue-in-education-etu-ce-and-efee-agreed-on-joint-work-for-2022-2023>



cooperation to embed the digitalisation dimension in the assessment tools (e.g., OiRA), while promoting a continuous monitoring of their efficacy."

Besides, in the framework of the joint work programme 2022/2023, European Sectoral Social Partners in education will work on promoting the implementation of and collecting of good practices on the ETUC framework agreement on digitalisation in the education sector. The education social partners also committed to enhanced joint cooperation on digitalisation in an ETUCE/EFEE Joint Statement on Promoting the Implementation of OiRA tools in Education Institutions by the European Sectoral Social Partners in Education, also adopted at the plenary meeting. The document highlights the importance of regular updates of risk assessment tools so that they take account of rapidly changing digital technologies. This builds on existing joint cooperation with EU-OSHA and findings of EFEE/ETUCE project 'OSH4Education' recognising that more action is needed to address cyberbullying through OiRA tools. In addition, the right to disconnect for teachers is increasingly important in the light of 24-hour contact between students and teachers.

In the central government sector, **Nadja Salson** reported the forthcoming sectoral social dialogue agreement on digitalisation will likely recognise both cyber harassment and domestic violence as part of health and safety risk assessments at work.

Aline Brüser, ETUC adviser, spoke about the European cross-sectoral social partner framework agreement on digitalisation (ETUC, Business Europe, SME United and CEEP 2020)⁴ which provides for a broad definition of quality work relations including employees, management, clients and third-parties and takes into account risks of violence and harassment. A big priority for the ETUC is to address cyber harassment in the forthcoming cross-sectoral social dialogue work programme (2022-2024). The work programme is not yet agreed, so more details would be available at a later stage. Of interest for the TPV project, the ETUC's survey of women trade union leaders in 21 European countries (March 2021) found that employers had not updated their policies relating to online abuse and teleworking. In this context, the ETUC has been active in pushing member states to ratify ILO C190 and is of the view that while EU-level ratification is desirable, it is not necessary as a pre-condition for member states to ratify the Convention. It is hoped that the French presidency will proactively address this issue, particularly as France, the Netherlands, Belgium and Finland have already completed the national ratification process. As part of this, the ETUC celebrated 25 November 2021 with a campaign on violence free workplaces. Issues of concern for the ETUC include the need to address gender and ethnic bias in artificial intelligence in the labour market and the role it plays in worker surveillance, and to ensure that the forthcoming draft directive on gender-based violence ensures the critically important role of the social partners.

The following points were raised in discussion:

- In Italy, there is a worrying increase in digital forms of violence against teachers; however, victims rarely complain.
- It is crucial to build a culture of trust and openness on digitalisation and to reinforce the employers' duty of care to ensure training, information and protection. A good example from the health sector is the use of health circles facilitated by OSH health experts to help staff deal with stress.

⁴ <https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020%20Agreement%20on%20Digitalisation%202020.pdf>



- Differences in definitions related to bullying or harassment; for instance, in the EU staff regulations sexual harassment is defined as a one-off unwanted conduct whereas psychological harassment requires a repetition of incidents.
- The Teachers Union of Ireland, noted the importance of teacher training in helping young and newly qualified teachers to implement protections against digital violence, for example, in reducing their presence on social media. Codes of professional conduct need to include clauses on appropriate language on harassment and the responsibilities of senior managers. Training on prevention prior recruitment of new employees is also crucial.
- It is important to have a lifecourse approach to occupational safety and health and adapt it to the needs of younger workers, while older workers may not be so “tech savvy”. The changing organisation of work means that there is now a blurring of the lines between internal and external violence.
- In Spain, the state administration is currently working on digitalization and a Royal Decree on telework for public servants is anticipated. However, unions are concerned that this will not address digitalisation as a risk in OSH prevention programmes. In relation to the Protocol on sexual harassment in public administration, the Royal Decree to implement it has not yet been issued. CC.OO-FSC anticipated that these issues will be addressed through social dialogue.
- It is essential to have clear definitions of violence and harassment, particularly because TPV is normalised and seen as part of job.
- Finally, a brief discussion was held about the possible updating of the multisectoral guidelines. The recent sectoral social dialogue seminar for local and regional government confirmed the need for some updating, refreshing of the language and reference to relevant international instruments.

The presentations are available [here](#).

