

Protecting the Researcher in Digital Contexts

Coppélie Cocq¹, Evelina Liliequist¹ and Lacey Okonski¹

¹ Umeå University, 901 87 Umeå, Sweden

Abstract

In recent years, a growing need for protecting researchers has become necessary as online risks such as death threats and “doxing” are more frequent risks in relation to an increased digital landscape of anti-gender, far right extremists, and anti-science movements. This paper suggests resources and strategies for preventing threats and protecting researchers. By improving safety and support, entities such as universities, departments, and research groups can avoid the negative impact of online harassment on researchers’ reputation and health, on academic research and for democracy.

Keywords

risky research; online abuse; research ethics

1. Introduction

In recent years, a growing need for protecting researchers has become necessary as greater levels of risk are posed to academics through online settings. In relation to an increased digital landscape of anti-gender, far right extremists, and anti-science movements, risks such as death threats and “doxing”, or sharing information publicly for the purposes of harassment and intimidation, have become more frequent. Especially targeted are researchers whose work, and/or whose public identity is norm breaking - e.g., ethnicity, minority identity, sexual identity, political activism, etc. [1, 2, 3, 4] or challenges white male supremacy, colonialism, heteronormativity, and/or in other ways critically studies power structures. Furthermore, Massanari (2018) observes how “[i]ndividuals working within the humanities and social sciences are particularly at risk, given the ontological and epistemological rationales for their research” [5, p. 2].

The growing need for developing resources to protect researchers has been emphasized by e.g. the Association of Internet Researchers, stating for instance that an “essential measure is that institutions develop policy detailing support procedures for researchers experiencing online threats or harassment related to their work” [6, p. 11]. Other texts and statements published by scientific societies encourage universities to develop policies and strategies for protecting researchers conducting risky research [see for instance 7].

In our research, we are taking a first step toward identifying and understanding unsafe research situations primarily in a Swedish context. This paper suggests resources and strategies for preventing threats and protecting researchers in the Humanities. By improving safety and support, entities such as universities, departments, and research groups can avoid the negative impact of online harassment on researchers’ reputation and health, and ensure that researchers do not drop funded lines of research for safety reasons.

¹The 6th Digital Humanities in the Nordic and Baltic Countries Conference (DHNb 2022), March 15–18, 2022, Uppsala, Sweden

EMAIL: coppelie.cocq@umu.se (A. 1); evelina.liliequist@umu.se (A. 2); lacey.okonski@gmail.com (A. 3)

ORCID: 0000-0001-7058-9955], (A. 1); 0000-0002-9214-0099 (A. 2); 0000-0003-4833-7270 (A. 3)



© 2022 Copyright for this paper by its authors.

Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

2. Understanding researchers at risk

Today, individuals and groups face increased visibility on social media. As new tools for seeing and being seen have been introduced in the era of social media the act of sharing has become a central, and often socially expected, aspect of participation in online communities [cf. 8, p. 1052]. For researchers in particular, visibility is often constructed as something positive to strive for: we are encouraged (and to some extent expected) by our employers and funding institutions to inform others about our research by having an online presence. Visibility is also necessary as a means for networking and for societal impact – we want people to read our publications, to know about our results, and to extend our findings beyond the ivory tower.

However, visibility and online presence have a dark side. In the context of online academic communication, researchers face the risk of becoming products, where focus is not only on what they do and on their findings, but also on who they are, something that McMillan Cottom (2015) describes as the construction of “microcelebrity”. This contributes to the development of a form of academic capitalism, i.e. “the ways in which knowledge production increasingly embeds universities in the new economy” [1, see also 9]. Moreover, one problematic aspect is the fact that researchers as professionals are expected to share information that sometimes touches upon their lives as private persons, in contexts where they do not have much control. The internet can function as a mechanism of harassment that shields harassers under “free speech” while offering limited protection to those exposed to risks and targeted. Social media sites function through a logic that encourages amplification of messages that can cause harmful content [e.g. 5].

In interdisciplinary contexts such as gender, minority, and environmental research, for instance, the exposure of researchers is an issue that has been addressed more recently in international research [10, 3]. The conducted studies indicate that safety considerations can restrict research and lead to termination of funded high-quality research in progress. Previous research [2, 3, 5] has also shown that being part of a marginalised group (e.g. female, Indigenous, black, lgbtq) may increase the level/risk exposure. Also, the implications of risk and the level of harm is often bigger in these groups than if you are part of a privileged community (e.g. white, cisgender, heterosexual, male). For example, Yelin & Clancy (2021) argue that threats and abusive comments are often gendered and that derogatory gender-based terms are used with the purpose of making women feel uncomfortable speaking out [3,11]. Vera-Gray (2017) also points out the added labour of ‘safety work’ as a problematic aspect as it “forms an invisible backdrop to the methodological decisions of many feminist researchers” [12, p. 62]. Implications of risks may also manifest as self-censorship as limiting oneself can be a strategy to avoid being put at risk.

Research about risky research in Swedish academic contexts is scarce, and addressed mostly in “grey literature” (reports, etc.). Surveys indicate that about 50% of respondents have experienced hate speech and/or toxic speech online [13, 14]. The Swedish Defence Research Agency recently published two brief reports addressing the issue of toxic language online. The first report [15] investigates toxic speech (hate speech and dangerous speech) in Swedish online forums and platforms, where “societal institutions” (a category that would include researchers) is mentioned as one category that receives these types of comments. The second report [16] observes that forms of derogatory comments vary between men and women. While men are exposed to devaluing comments about lack of competence or performance in their profession or in general, women are to a greater extent exposed to derogatory comments about appearance including allegations that a person is ugly or unattractive [3]. These reports underscore the scope of the problem of toxic language use in Swedish online contexts. Studies have focused on specific professional groups, i.e. journalists, politicians, influencers, comedians and artists [14; 17]. Exposure in academic contexts and towards researchers is less researched.

Another survey in a Swedish context found that people involved in societal issues are particularly exposed to threats and hatred [13]. This applies, for example, to elected representatives, journalists, artists, opinion leaders, researchers, and representatives of civil society. Academics and journalists who write about feminism and anti-racism often suffer from online hate in an organized form, something described in the report as “continuously opposed by more or less organized hatred” [13, p. 24]. These findings indicate that the democratic conversation is limited and important voices risk being silenced.

3. Risky research and its implications

While surveillance from the alt-right can intimidate researchers [5], giving researchers the resources they need to safely conduct research on topics such as gender, race, climate, and politics has far reaching implications for societal and political spheres and for research ethics and methodologies more generally. For example, if researchers do not have proper protections in place and avoid researching topics that put them at risk they may miss opportunities to conduct work that informs public debate and challenges harmful narratives/paradigms [3]. Alternatively, if researchers are enabled to publish risky projects within a research collective and with the institutional support of the university they may be able to spend more time contributing to research and less time mitigating risk factors.

Potentially, any researcher can be exposed, but recent examples in a Swedish context might help us to grasp the scope of the issue and, in relation to other international studies, discern some patterns.

In 2018, an employee at the Swedish National Secretariat for Gender Research found a suspicious object in a bag by the entrance. It later was found to be a dummy device that resembled a dangerous object, nonetheless we have good reasons to assume that fear and harm was inflicted, both emotionally and psychologically, to the staff, as well as having implications for gender scholars in general. This should not be regarded as an isolated event. Gender scholars in Swedish contexts report recurrent threats, often in conjunction with being published, as being part of everyday life for gender researchers [18]. This can also be understood as part of the increased threats towards gender research(ers) worldwide [3]. Other highly politicised fields and areas of research where dangerous or hate speech occur include minority studies and research concerned with marginalised groups. In the case of Indigenous and Sámi research, for instance, the existence of such fields of research in themselves is questioned, the identity, colonial heritage etc of these groups are questioned [19, 20, 21], and researchers are in the front line. These examples highlight the increased risk for threats towards certain groups in relation to gender and race.

Gendered and racial violence can also be noted in relation to the phenomena Zoombombing – a practice of crashing Zoom meetings and posting distressing and/or abusive comments, pictures or videos during the meeting. This is an increasing problem noted especially during the Covid-19 pandemic when meetings, lectures and seminars were transferred to exclusively online events [22]. As stated by Ling et al. 2021 “Online meeting tools like Zoom and Google Meet have become central to our professional, educational, and personal lives. This has opened up new opportunities for large scale harassment”. In *Racist Zoombombing* [22], the phenomenon is examined and explained as a form of racial violence in forms of racist harassment and hate speech. This malicious practice risks disturbing important academic work and events and, as Nakumara et al. (2021) show, racial abuse during zoom meetings can cause lasting trauma, anxiety, and anger [23].

Recently, scholars engaged in research related to the Covid-19 pandemics have also witnessed how they have been the target of massive threats and harassment [24]. Concerns have been raised by employers and scientific boards about the implications of such threats. Such a situation not only has consequences on the researchers’ work environment, but also severe implications for the willingness of researchers to engage in research of crucial importance for our societies. One example experienced by colleagues at another department at Umeå University (Sweden) occurred when students were conducting an online study about perceptions of climate change which revealed their email within the consent form as a part of standard practice in online research. They subsequently suffered email harassment from anti-climate activists causing the department to be hesitant to tackle such topics and nervous about protocols for conducting research which is extremely important to understanding attitudes towards climate and mitigation strategies. If these experiences continue, issues such as Covid-19 and climate would be less likely to be addressed in the social sciences and humanities literature and more vulnerable to disinformation from malicious actors.

Online harassment can take multiple forms. The threat is not always explicit and a researcher might experience a feeling of discomfort that may already have an impact on their well-being. For instance, Massanari (2018) brings attention to the phenomena of sea lioning, a type of trolling or harassment that consists of pursuing people with persistent requests for evidence or repeated questions, while

maintaining a pretence of civility and sincerity [5]. Doxing – sharing information publicly for the purposes of harassment and intimidation - is a more explicit form of threat that has been emphasised and addressed as an increasing problem, for instance, by the Association of Internet Researchers [6]. AoIR also points out potential risk for threats and retaliation should researchers' identities become known, in relation to field work, e.g. in research that investigates discussions or phenomena in toxic environments, for instance 8chan and to some extent Flashback, and/or in studies on anti-gender and ALT-right groups or other violent online and offline political extremists on social media. Related risks worth mentioning, which are also highlighted by AoIR [6], are the risks for psychological consequences involved with research that addresses directly sensitive topics - such as violence, pornography, religious fanaticism, etc. Although this constitutes another form of risk than the one illustrated above, it is important to consider what support researchers might need while doing fieldwork in potentially toxic environments and/or researching potentially heavy and heartbreaking subjects, and also afterwards while handling such data.

Online threat, harassment, hate, and dangerous speech can obviously have serious implications for individuals in terms of well-being and work environment. In addition, there are implications for the employer as well. A university may not be doxed but they may risk losing important research grants, having bad PR, or a decline in public support (with the rise of anti-intellectual sentiments). They risk not reaching their potential in research excellence if their employees are being harassed and face this additional emotional labour, intellectual labour and sometimes even legal battles. Highlighting the financial and PR risks the university could suffer may be key to get support at the university level.

4. Strategies

Based on literature and discussions with peers in international academic contexts, we have identified, and suggest below, a set of strategies for proactively and actively supporting and protecting scholars doing risky research, or being exposed for other reasons. This list of suggestions is far from being exhaustive, but can hopefully spark inspiration and discussion within research environments in need of addressing issues similar to those addressed in this paper. We also think and hope that these suggestions can be helpful for supervisors of students at different levels, as exposure and risky research can also be of immediate interest for students writing essays and theses on sensitive topics and/or doing fieldwork in toxic environments.

In all of these suggested strategies, we start from the idea of solidarity, with inspiration from ethics of care, which starts with “the real experience of being embedded in relationships with uneven power relations” [25, p. 67; see also 26].

4.1 Need for intersectional awareness

We see intersectionality as key for understanding how aspects of a person's identities combined create different modes of discrimination and privilege in relation to interlocking systems of power [27]. Intersectional perspectives highlight the complexity of the issue of researchers being increasingly at risk. It is an approach for understanding who, in what ways, and to what extent researchers, in relation to gender and gender identity, race, age, functionality, sexuality and so on, can be at risk in digital contexts with different implications.

We also want to highlight the potential different implications of risk in relation to employment status and academic career level, as junior, non-permanent, or not yet tenured scholars may have more to lose if their work is put under intense scrutiny in public forums or if they drop an important line of research. As stated by Massanari (2018) visibility can be profoundly damaging for researchers in precarious professional situations (eg adjuncts, graduate students, or job applicants) [5].

Intersectional awareness can help to be proactive. Also, an intersectional awareness helps to address the problem in a context-based way, rather than a one solution-fits all approach which may be excluding and/or fail to grasp the whole problem and potential long term implications, especially on an individual level.

4.2 Managing Visibility

While visibility is often central in our academic work, visibility can also be problematic, as we have stated in this paper. In this section, we will highlight some examples of situations where protecting one's identity might be needed, and suggestions for possible strategies.

Researchers often need (and want) to be part of the digital context they study, which involves immersion in the context: “social justice-oriented research on “alt-right” adjacent groups, such as entanglements are a form of risk—to students, researchers, their families, and their institutions” [10, p. 320]. Rambukkana (2019) suggests “engaging in covert invisible non-participatory observation” as a precaution to avoid being put at risk [see also 28].

When conducting online fieldwork, using computational tools etc, a technology awareness is necessary. VPN, ad blockers (against malicious code), and firewalls can offer some protection [29]. To establish support and consultation from an IT security team that can recommend software and hardware precautions is thus suggested for researchers and students prior to engaging with risky research and risky fieldwork situations.

Talking in a collective voice can serve as a good strategy in order to avoid individual researchers to stand on the front line, for instance when presenting sensitive results or in toxic contexts. A research group, a lab, or a department can be the primary contact when presenting a study or sharing results, or in publications. This can be especially useful for younger researchers. As senior researchers are more likely to have better support networks among their peers, as well as experience, and a less vulnerable employment situation, their engagement in communication of research as a collective voice is important. Again, due to the increased intersectional risk factors of being targeted, marginalised researchers can also benefit from being supported and/or represented through their peers. We suggest research groups early in the research phase discuss potential risk and plan strategies for dealing with potential unwanted attention.

Another strategy related to the collective voice is to publish anonymously or under a pseudonym [10]. Publishing anonymously in academic research is not a common practice. Transparency, responsibility, and accountability are core principles in research that stand in contradiction with anonymity in publication. However, there have been cases when journals have allowed authors to publish anonymously, for instance in the case of threat to personal safety [30]. Such a strategy needs to be used only upon careful consideration, as responsibility in authorship should be prioritised as much as possible. Also, there are implications for research impact when a scholar publishes anonymously or under a pseudonym.

An awareness of potential risks for researchers is also important for personnel working with communication in universities, at conferences and academic journals. News related to publications are likely to be spread in external communication including social media to gain positive attention to a department, journal, or author. Visibility can also become problematic. One way to avoid attracting unwanted attention is to inform the author of the article beforehand and give them the choice to be tagged or not, and on which social media platform. Tagging on social media is a great way to attract attention but it can also attract unwanted attention.

4.3 Planning online events

During the Covid-19 pandemic, our research lab relocated all academic and public events online. In this shift, we have experienced the balance and potential conflict between a need to promote events while still ensuring the safety of our invited speakers. The issue of safety can be illustrated with this (slightly edited) quote from one of our speakers in an email conversation about how and where to market the event: “I have been doing public talks about LGBTQ+ issues for 20 years. It feels really odd to be worried about visibility online, but this kind of security has been a major issue.” Having a dialogue beforehand with the invited speaker made it possible for us to decide together on a marketing plan that fit both parties' need for visibility, but in a manner that provided control and was based on consent.

Another example of how to ensure security during our events – and more specifically for avoiding the risk of “Zoombombing”- is to always require pre-sign up to events and not sharing the zoom link until a day or two before the event. Although anyone can sign up, this is a strategy to make it harder to get access to the meeting, as it requires more steps to the zoom-link [22]. This strategy increases

our control as event organisers. Further, Douglas suggests that “A general principle is that online activities should be mediated by an IT Security team with appropriate special responsibility and training” [29, p. 78]. For each of our events we have at least one technician present in the meeting, ready to act, with attention to any unwanted behaviour in the audience. In events deemed risky, we set up limits for how the audience can act during the meeting (e.g not turn on mics and cameras without the hosts’ permission). Having established a strategy for how to plan, promote, and conduct our events, we as organisers have better control and are better prepared. Hopefully seemingly small actions provide improved security and protection for our invited speakers and participants.

4.4 The responsibility of institutions

While many universities have established policies to address and deal with explicit harassment, threats, or violence, the vulnerability experienced by researchers in online environments is often addressed to a lesser extent. Based on previous research, we argue that individual researchers should not be left to fend for themselves, as work-related risks should be viewed as a work-related problem and the responsibility must be placed on an institutional level. Thus, protocols and strategies for ensuring the security and safety of all employees must be installed and continuously updated to include strategies for handling online risks and dealing with potential harm and hatred posed in and through digital contexts. As Yelin & Clancy (2021) state: “Universities have a duty of care to all researchers, not just during the media work, but before and afterwards. It is important for universities to take responsibility for the wellbeing of all researchers engaging in impact work which will benefit the academy” [3]. While many universities in a Swedish context have established policies to address and deal with explicit harassment, threats or violence, there is still a problematic absence of relevant university policies at many universities as many of these protocols (if existing at all) fail to include online risks and implications of such risks. They also fail to grasp the complex nature of how both risks and its implications can differ (and thus may need different solutions) depending on who, what, and where risks are posed. This is especially important in the case of researchers who are disadvantageously affected by intersectional implications and converging risk factors. Finally, there is a need for research to better understand where and why risks may arise, types of risk, and implications. We strongly recommend research groups and research leaders develop policies and preparedness for risky research. Resources listed in the next section can be a helpful start.

5. Resources

Already mentioned is the set of “Best practices for conducting risky research and protecting yourself from online harassment” by Marwick et al (2016) published by Data & Society [7]. This resource addresses primarily young researchers but is relevant for all academics. It also suggests a way to approach university administrations and suggest modes of action for providing support to their researchers. A list of additional valuable resources can also be found in this document.

Friedman et al. (2016) have developed resources “especially designed for women, people of color, trans and genderqueer people, and everyone else whose existing oppressions are made worse by digital violence”[31]. These are not specific for researchers, but include useful advice about security practices for online behaviour, documentation of misconduct, and addressing emotional impacts of digital violence. Other resources include websites specifically addressing online abuse, for instance Crash Override, a crisis helpline, advocacy group and resource centre that offers helpful tools, educational materials and DIY security guides [32]. The Swedish Crime Victim Authority provides information and advice through their campaign “Do not fall silent” against online hatred, abuse and threats [33]. Among other things, the website includes support and guidance on how to file a police rapport.

National, regional or local review boards are also resources toward which researchers can turn for support when preparing a risky project. Employers’ policies and their security services often include support in case of threats or violence. Even when those do not directly address the risks, threats, and/or harassments that researchers meet in online environments, these structures provide a first contact when in need of support or protection. Occupational health services might also provide support.

6. Conclusions

This paper aimed to provide an intersectional account of how researchers experience online risks, the types of risks they face, who is typically targeted, and how this risk exposure can be a detriment to research, to research institutions, and to the health of democracy. We argue that intersectional awareness needs to be the starting point for developing protocols and strategies for avoiding and dealing with risk.

A second aim in this paper was to identify already available resources and strategies that researchers and research groups can take to enable an increased intersectional awareness, manage visibility, and better plan for secure online events to mitigate the costly demands placed on at-risk researchers in online environments so that their resources can be better allocated to scholarly activities. We conclude by arguing that institutions themselves should bear a greater responsibility to care for researchers and take a more active approach in mitigating risk factors. Universities themselves stand to lose well-funded and high-profile projects if they do not act. It is unknown how many projects to date have been abandoned by researchers or have not been funded due to inadequate preparedness for online research. Online methodologies and online risks are increasing at an unprecedented rate. Meanwhile, online environments are increasingly the context where societal issues and misinformation are discussed, exacerbated, and propagated. Universities are not immune from these digital threats and, as online risk increases, universities will need to keep up with technology and develop clear guidelines and avenues of support to researchers. It is our most fervent hope that Swedish institutions develop these protocols with an openly intersectional approach. In this era of fake news, tweetstorms, and tik tok tidbits, democracy itself depends upon academic institutions protecting open dialogue in a responsible way.

7. References

- [1] McMillan Cottom, T. “‘Who Do You Think You Are?’: When Marginality Meets Academic Microcelebrity”. *Ada: A Journal of Gender, New Media, and Technology*, No.7. (2015). doi:[10.7264/N3319T5T](https://doi.org/10.7264/N3319T5T).
- [2] Vera-Gray, F. “‘talk about a cunt with too much idle time’: trolling feminist research”. *Feminist review*. 115(1): 61–78, (2017). doi: [10.1057/s41305-017-0038-y](https://doi.org/10.1057/s41305-017-0038-y)
- [3] Yelin, H. & Clancy, L. “‘Doing impact work while female: Hate tweets, ‘hot potatoes’ and having ‘enough of experts’”, *European Journal of Women’s Studies*, 28(2): 175–193, (2021). doi: [10.1177/1350506820910194](https://doi.org/10.1177/1350506820910194)
- [4] Engebretsen, E.L., *Scientizing Gender? An Examination of Anti-Gender Campaigns on Social Media*, Norway, in: Eslén–Ziya, H., Giorgi, A. (eds) *Populism and Science in Europe*. Palgrave Studies in European Political Sociology. Palgrave Macmillan, Cham (2022).
- [5] Massanari, A. L. “Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the ‘Alt-Right’ Gaze”. *Social media + society*. 4(2), (2018). doi: [10.1177/2056305118768302](https://doi.org/10.1177/2056305118768302).
- [6] Franzke, A. S., Bechmann, A., Zimmer, M., Ess, C. & the Association of Internet Researchers. *Internet Research: Ethical Guidelines 3.0*, (2020). URL: <https://aoir.org/reports/ethics3.pdf>.
- [7] Marwick, A., Blackwell, L., & Lo, K.. *Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment (Data & Society Guide)*. New York: Data & Society Research Institute (2016). URL: <https://datasociety.net/library/best-practices-for-conducting-risky-research/>.
- [8] Marwick, A. E. & Boyd, D. “Networked privacy: How teenagers negotiate context in social media”, *New Media & Society*, 16(7): 1051–1067 (2014, p. 1052). doi: [10.1177/1461444814543995](https://doi.org/10.1177/1461444814543995).
- [9] Berman, E. P. *Creating the market university: How academic science became an economic engine*. Princeton University Press, 2011.
- [10] Rambukkana, N. “The Politics of Gray Data: Digital Methods, Intimate Proximity, and Research Ethics for Work on the ‘Alt-Right’”. *Qualitative inquiry*. 25(3): 312–323 (2019). doi:[10.1177/1077800418806601](https://doi.org/10.1177/1077800418806601).

- [11] Sobieraj S. “Bitch, slut, skank, cunt: Patterned resistance to women’s visibility in digital publics”. *Information, Communication and Society* 21(11): 1700–1714 (2018). doi: [10.1080/1369118X.2017.1348535](https://doi.org/10.1080/1369118X.2017.1348535).
- [12] Vera-Gray, F. “‘talk about a cunt with too much idle time’: trolling feminist research”. *Feminist review*. 115(1): 61–78, (2017)
- [13] Svensson, M., Björkenfeldt, O., Åström, F., & Dahlstrand, K. *Näthat och demokratiskt deltagande – en kunskapsöversikt*. Brottsoffermyndigheten (2021).
- [14] Fernquist, J., Kaati, L., Pelzer, B., Lindberg, S., Akrami, N., Cohen, K. & Pollack Sarnecki, H. *Det digitala hatets karaktär: En studie av hat mot kvinnor och män i utsatta yrkesgrupper*. FOI Memo 7429, Totalförsvarets forskningsinstitut (FOI) (2020).
- [15] Kaati, L., Pelzer, B., Asplund Cohen, K., Wallgren, D. Akrami, N & Yourstone J. *Toxiskt språk i svenska digitala miljöer*. FOI Memo 7740, Totalförsvarets forskningsinstitut (FOI) (2021).
- [16] Kaati, L., Asplund Cohen, K., Pelzer, B., Wallgren, D., Akrami, N. Yourstone, J. *Könsskillnader i utsatthet för toxiskt språk online*. Memo 7741, Totalförsvarets forskningsinstitut (FOI) (2021).
- [17] Ministry of Culture. “Till det fria ordets försvar – åtgärder mot utsatthet för hot och hat bland journalister, förtroendevalda och konstnärer”. Regeringskansliet (2017).
- [18] Lofrup, J. “Gender researcher: threats and hate are part of everyday life” (2019). URL: <https://www.staff.lu.se/article/gender-researcher-threats-and-hate-are-part-everyday-life>.
- [19] Carlson, B. & Fazer R. *Indigenous Digital Life: The Practice and Politics of Being Indigenous on Social Media*. Springer International Publishing AG (2021).
- [20] Katz, I., Keeley, M., Spears, B., Bates, S., Swirski, T., & Taddeo, C. *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis Report, 2014*. URL: <https://www.communications.gov.au/publications/publications/research-youth-exposure-and-management-cyber-bullying-incident-australia-synthesis-report-june-2014>.
- [21] Mobin, A., Feng, C. X., & Neudorf, C. “Cybervictimization among pre-adolescents in a community-based sample in Canada: Prevalence and predictors”. *Canadian Journal of Public Health*, 108(5–6): e475–e481 (2017). doi: 10.17269/cjph.108.5878
- [22] Ling, C., Balci, U., Blackburn J. & Stringhini, G. *A First Look at Zoombombing*, 2021 IEEE Symposium on Security and Privacy (SP) (2021, pp. 1452-1467), doi: 10.1109/SP40001.2021.00061.
- [23] Nakamura, L., Stiverson, H., & Lindsey, K. *Racist Zoombombing*, 1st ed., New York: Routledge (2021).
- [24] Torkelsson, A-C. “Forskare vittnar om hot efter att ha pratat om covid-19 med media”. *Läkartidningen* (2021).
- [25] Franzke, A. S. “Feminist Research Ethics”, IRE 3.0 Companion 6.3, Association of Internet Researchers (2020). URL: <https://aoir.org/reports/ethics3.pdf>.
- [26] Suomela, T., Chee, F., Berendt, B. & Rockwell, G. *Applying an Ethics of Care to Internet Research: Gamergate and Digital Humanities*. *Digital Studies/Le champ numérique*, 9(1), 4. (2019, p.2). <https://www.digitalstudies.org/articles/10.16995/dscn.302/>.
- [27] Crenshaw, K. “Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color.” *Stanford law review* 43(6), (1991: 1241–1299).
- [28] Pollock, E. “Researching white supremacists online: Methodological concerns of researching hate online”. *Internet Journal of Criminology*, (2009).
- [29] Douglas, K. “Operational Security: Central Considerations”, IRE 3.0 Appendices 7.1, Association of Internet Researchers (2020). URL: <https://aoir.org/reports/ethics3.pdf>.
- [30] Council of Science Editors, Editorial Policy Committee, Authorship and Authorship Responsibilities (2020). URL: <https://www.councilscienceeditors.org/resource-library/editorial-policies/white-paper-on-publication-ethics/2-2-authorship-and-authorship-responsibilities/>
- [31] Friedman, J., Sarkeesian, A., & Sherman, R. B. “Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment” (2016). URL: <https://onlinesafety.feministfrequency.com/en/#about-us>.
- [32] <http://www.crashoverridenetwork.com/resources.html>
- [33] <https://www.tystnaint.se/en/>