ARTICLE 19

Investigating online harassment and abuse of women journalists

2020

First published by ARTICLE 19, 2020

ARTICLE 19

Free Word Centre
60 Farringdon Road
London EC1R 3GA
UK

www.article19.org

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by power-holders for transparency good governance and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

Contents

Executive summary

In recent years, digital technologies have expanded and created new spaces on which women and girls can exercise their right to freedom of expression and information. They have offered them new opportunities to make their voices and concerns heard. However, these spaces have also created new opportunities for gender-based harassment and abuse, that often mirror offline manifestations of discrimination and inequality.

Women face gender-based discrimination in various aspects of their lives, notably at home and at work and in the society at large, which denies them their full enjoyment of fundamental human rights. These problems are also faced by women journalists, who, not only often face gender-based discrimination but also suffer from violations of their right to freedom of expression related to their journalistic work.

Under international human rights law, States have the obligation to prevent, protect and remedy attacks against journalists, including protecting them from violence, threats of violence and various forms of harassment. Despite these obligations, it has been reported that States fail to efficiently investigate threats and attacks directed towards women journalists, including online harassment and abuse. If online gender-based harassment and abuse is not properly investigated, this will have a 'chilling effect' on women journalists' right to freedom of expression. It will, inevitably, reduce the space in which they can express themselves and deny them the opportunity to report in online spaces.

As a starting point, the briefing addresses in detail the standards on effective investigation of violence against journalists before exploring the standards on effective investigation of online harassment and abuse against women journalists.

Finally, ARTICLE 19 will recommend how States can ensure the protection of women journalists against online harassment and abuse by creating an online environment in which women's right to freedom of expression is guaranteed. In particular:

- States should recognise that online gender-based harassment and abuse against women journalists who are targeted for exercising journalism activities, is a serious problem and adopt integrated prevention, monitoring, and response mechanisms, including in public policy.
- States should adopt a comprehensive public policy approach to tackling forms of intolerance and prejudice of which manifestations of online harassment and abuse are symptomatic of. They must take action to counter discriminatory attitudes and norms and create an enabling environment where all women can fully participate in society.
- State officials should publicly, unequivocally and systematically condemn attacks against journalists, women journalists, and against those who exercise their right to freedom of expression, and should refrain from making statements that are likely to increase the risks that put women journalists in situation of vulnerability.
- Different regulatory measures should be adopted to tackle online gender-based harassment and abuse. Any regulation restricting or limiting the right to freedom of expression should comply with the three-part test under Article 19 para 3 of the ICCPR; while criminal law should be used in exceptional circumstances when online harassment and abuse reaches certain severity, such as causing serious harm.
- In cases where online gender-based harassment and abuse reach the level of severity prohibited under criminal law, States are obliged to *inter alia* undertake a prompt, expeditious, thorough, diligent and comprehensive investigations in a manner guaranteeing sufficient public scrutiny.
- States should adopt practical measures such as dedicated institutional resources, capacity and training to enable the legal system to deal with online gender-based harassment and abuse, and adequately resource them.
- States should improve reporting and monitoring of gender-based harassment and abuse, both offline and online, and include them in national statistics and measures to address equality and discrimination.
- States should also adopt holistic and well-resourced prevention and response mechanisms together with the private sector and civil society.

Introduction

Democracy depends on the ability of journalists to speak truth to power, investigate abuses, contribute to, and strengthen public debate, and provide people with information on the world around them. Impunity for abuses which seek to silence journalists is a global threat to freedom of expression and open societies worldwide.

Numerous reports and studies show that although women journalists are subjected to the same wide range of human rights violations that are directed against male journalists, they also face particular challenges and human rights violations when doing their work. Workplace and employment related discrimination, sexual and gender-based violence, intimidation and harassment are a particular concern in this respect, and one that persists year on year with little improvement. These violations are symptomatic of the gender-based inequality, discrimination and violence experienced by women globally across many aspects of their lives.[1]

Reports also show that women journalists are increasingly and persistently facing gender-based harassment and abuse online. It is often targeted at those women journalists or human rights defenders who speak out against government abuses and on women's rights issues, or who report on issues which have traditionally been considered more 'adequate' for men. Online harassment and abuse take many forms, including but not limited to blackmail, threats of sexual assault, intimidation, stalking, surveillance, and dissemination of private content without consent; that can often escalate to threats to physical safety. It can come from governments or private actors, and like offline attacks, can significantly restrict women's ability to speak out, criticise and shape debate.

Online gender-based harassment and abuse represent not only an attack on women's equality but can have a serious chilling effect on their exercise of free expression. When women using technology are routinely faced with threats or other digital attacks, it can have the effect of driving them offline and out of the debate, because they fear for their safety. Often, the barrage of online harassment and abuse becomes unbearable and prevents them from engaging on social media and in digital civic space. For women journalists, online harassment and abuse can limit their journalistic reporting, or their ability to collectively organise and challenge discrimination. Studies also show that it can result in self-censorship for women journalists, and how they perform in their reporting and journalistic activities or issues they cover. It can result in a range of psychological harms, as well as negative impacts on mental health, and certain negative behavioural effects, such as victims changing their lifestyles and routines, or exclusion from the engagement in online space.[2]

Under international human rights standards on safety of journalists, States are obliged to act on three fronts: prevent, protect and remedy attacks against journalists. This includes measures of protection from violence and discrimination by private parties, and effectively investigate and provide appropriate protection against intimidation, threats, and all other forms of harassment.

However, there is also an overwhelming body of reporting that a particular barrier to justice for women journalists, who face online harassment or receive threats of violence online, is a failure of public authorities to take these threats seriously. International and regional human rights bodies - as well as civil society organisations - have repeatedly called on law enforcement to take action against online harassment and abuse of women journalists, develop tools to better identify whether this kind of conduct falls under the purview of criminal or other offenses, and provide real protection for victims.[3]

In this briefing paper, ARTICLE 19 therefore outlines the scope of State obligations to address online harassment and abuse of women journalists and to conduct an effective investigation into online harassment and abuse. The underlying notion in this case is that the right to freedom of expression and the ability of women journalists to engage in journalistic activities is ineffective in an environment in which there is impunity for harassment, intimidation or threats of violence – online and offline - directed against them. The right is rendered similarly ineffective if there is a failure on the part of the State to carry out an effective investigation into the breaches, or threatened breaches, of their rights.

The briefing paper first outlines international and comparative standards on the effective investigation into violence against journalists, followed by standards and comparative examples on effective investigation of online harassment and abuse. It also looks into some challenges in identifying perpetrators and reliance on mutual legal assistance treaties in investigation of online harassment and abuse. Finally, the briefing paper puts forward recommendations for the appropriate approach to cases involving online harassment and abuse, consistent with the right to freedom of expression and other human rights standards.

Key concepts

Definition of gender-based online harassment and abuse

There is a broad range of terminology used to describe the phenomenon of discriminatory expression and other forms of complex abusive behaviour, that is committed, abetted or aggravated, in part or fully, by the use of information and communication technologies, such as mobile phones, the Internet, social media platforms, and email.[4] These range from *inter alia* "online violence," "cyber-violence," "cyber-bullying," "cyber-violence and harassment using new technologies," "technology related violence" or "online hate speech."[5]

Further, this terminology is used to collectively describe different types of problematic conduct which includes, but is not limited to:

- Sending direct or indirect threats of physical or sexual violence, sending offensive messages, targeted harassment (often take the form of 'pile-ons', with multiple perpetrators);
- Doxxing - the public dissemination of a woman's personal information, such as email, telephone or home address. This can often result in increased harassment, and create a safety risk;
- Gender-based abuse, which can include a wide range of types of speech and perpetuating gender stereotypes, content portraying women as sexual objects or targets of violence;
- Surveillance and stalking – this includes a range of behaviours monitoring of a woman's online and/or offline life through technological means or compiling information about a woman online and communicating with her against her will;
- Identity theft or unauthorised use of accounts – when someone is able to take control of, or in some way impersonate a woman's online presence and/or using the content to discredit her or damage her reputation;
- Breaking into accounts/devices – when someone gains access to a woman's private accounts or devices without their consent and/or with malicious intent. This can often lead to another form of attack, including blackmail;
- Non-consensual distribution of intimate or sexual images of a woman, which can be taken by the women herself, or by someone else, with or without her knowledge, and either by someone who has access to them with consent (but there is no consent for them to be further shared), or by someone who gains access through other means.

Often, these types of abuse are closely linked to offline violence against women, forming part of a continuum of violence, and can lead to or form part of offline attacks. Each of these might be defined differently in domestic legislation or in recommendations of regional and international human rights bodies.[6] Other institutions, social media companies or academics also produce their own lexicon to conceptualise this phenomenon.

While there is no universally agreed terminology to capture this phenomenon and its different forms, in this briefing, ARTICLE 19 has employed the term "online harassment and abuse" as generic term to capture the type of conduct described above.

Definition of 'journalist' and 'journalism'

In the context of State obligations to guarantee safety of journalists, it is important to point out that the concept of "journalism" has significantly evolved in the last decade. Although there is currently no agreed definition of 'journalism' or what constitutes 'activity of journalists' at the international level, international and regional human rights bodies and some domestic courts7 have provided tentative definitions and have recognised the important role that 'citizen journalists' play in the gathering and dissemination of information. Most significantly, they have proposed a *functional* definition of 'journalism,' one which encompasses those communicating publicly using new media, provided they fulfil certain criteria.

In its General Comment No. 34, the UN Human Rights Committee (Human Rights Committee), the treaty body of independent experts monitoring States' compliance with the International Covenant on Civil and Political Rights (ICCPR), defined 'journalism' as follows:

> Journalism is a function shared by a wide range of actors, including ... bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere, and general State systems of registration or licensing of journalists are incompatible with [Article 19] paragraph 3. Limited accreditation schemes are permissible only where necessary to provide journalists with privileged access to certain places and/or events. Such schemes should be applied in a manner that is non-discriminatory and compatible with Article 19 and other provisions of the Covenant, based on objective criteria and taking into account that journalism is a function shared by a wide range of actors.[8]

The Committee of Ministers of the Council of Europe (CoE) has adopted an equally broad definition of the term 'journalist.' In Recommendation No. R (2000)7, the Committee said:

> The term "journalist" means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication.[9]

It has also called on member States to:

- Adopt a new, broad notion of media which encompasses all actors involved in the production and dissemination, to potentially large numbers of people, of content (for example information, analysis, comment, opinion, education, culture, art and entertainment in text, audio, visual, audiovisual or other form) and applications which are designed to facilitate interactive mass communication (for example social networks) or other content-based large-scale interactive experiences (for example online games), while retaining (in all these cases) editorial control or oversight of the contents;
- Review regulatory needs in respect of all actors delivering services or products in the media ecosystem so as to guarantee people's right to seek, receive and impart information in accordance with Article 10 of the European Convention on Human Rights, and to extend to those actors relevant safeguards against interference that might otherwise have an adverse effect on Article 10 rights, including as regards situations which risk leading to undue self-restraint or self-censorship.[10]

In addition, the Committee of Ministers provided a set of indicators to determine whether a particular criterion is fulfilled. For example, a particular organisation or individual engaged in the dissemination of information will fully meet the public expectation criterion if it is available; is reliable; provides content that is diverse and respects the value of pluralism; respects professional and ethical standards; and is accountable and transparent.[11]

At the same time, the Committee of Ministers highlighted that each of the criterion should be applied flexibly.[12]

Hence, in this briefing, ARTICLE 19 maintains a functional definition of journalism, encompassing an activity, which consists of the collection and dissemination of information to the public via any means of communication.

Standards on effective investigation of violence against journalists

Under international human rights standards, States must protect the right to freedom of expression in law, policy and practice, to ensure a safe and enabling environment for journalists to carry out their work independently and without undue interference. States also have a positive obligation to ensure that crimes designed to silence journalists and freedom of expression are prohibited, attacks on journalists prevented, journalists are protected, and perpetrators and instigators of attacks are prosecuted.

These obligations are mandated under the International Covenant on Civil and Political Rights, resolutions of the UN Human Rights Council[13] and regional instruments and jurisprudence.

International human rights standards and jurisprudence demonstrate that in order to comply with their positive obligation to carry out the effective investigation, States must have a system of investigation which incorporates a number of safeguards. States are also required to prevent the interference in journalists' rights by private or non-state actors[14] and may "be found responsible for acts of private individuals" in fulfilment of their international human rights obligations.[15] Although these standards do not address the investigation into online harassment and abuse, the following recommendations can illustrate types of action that States should put in place to address online harassment and abuse of women journalists.

The 2012 **Joint Declaration on Crimes Against Freedom of Expression**[16] issued by international intergovernmental experts, recommends that States should *inter alia* ensure that crimes against freedom of expression are subject to independent, speedy and effective investigations and prosecutions. Among the principles related to the effectiveness of the investigations, the Joint Declaration includes:

- Sufficient resources and training should be allocated to ensure that investigations into crimes against freedom of expression are thorough, rigorous and effective and that all aspects of such crimes are explored properly;
- Law enforcement bodies should take all reasonable steps to secure relevant evidence and all witnesses should be questioned with a view to ascertaining the truth;
- The victims should be involved in the procedure to the extent necessary to safeguard their legitimate interests; this includes giving access to certain parts of the proceedings and also to the relevant documents to ensure participation is effective;
- Investigations should be conducted in a transparent manner, subject to the need to avoid prejudice to the investigation.

A number of resolutions of the Human Rights Council (HRC) set out the steps States have to take to prevent violence against journalists, protect them from such attacks, and prosecute the perpetrators. Most importantly, **HRC Resolution 33/2 on the Safety of Journalists**[17] mandates that States should:

- Dedicate necessary resources to investigate, prosecute, punish, and remedy attacks of all kinds, including gender-specific attacks, and ensuring that enforcement mechanisms have the capacity to systematically pay attention to the issue;
- Undertake protective measures to ensure accountability for threats and attacks against journalists through impartial, prompt, thorough, independent, and effective investigations. In particular, States should create special investigative units on crimes against journalists and specific investigation protocols adopted, recognising and taking seriously gender-specific attacks on women journalists;
- Ensure that victims have access to appropriate remedies (for example, compensation or socio-economic support, emergency and long-term physical and psychosocial healthcare). It also recognises that that pursuing judicial remedies may not always be the priority or preference of journalists who have experienced violations or abuse, in particular for survivors of sexual violence, access to such remedies should not be contingent on the filing of criminal complaints.

The Human Rights Committee, which interprets State obligations under the International Covenant on Civil and Political Rights (ICCPR) also repeatedly stressed States' obligations to ensure safety of journalists. In particular:

- In **General Comment No. 34**, the Human Rights Committee stressed that no attack on a person – including arbitrary arrest, torture, threats to life and killing – may be justified on the basis of that person's exercise of his or her freedom of expression.[18] When attacks do occur, States have duties to “vigorously investigate in a timely fashion" all such attacks on journalists and media workers and ensure that the perpetrators are prosecuted, and the victims receive appropriate forms of redress.[19]
- In **General Comment No. 36**, the Human Rights Committee mandates States “to enact a protective legal framework which includes effective criminal prohibitions on all manifestations of violence or incitement to violence that are likely to result in a deprivation of life;"[20] and also “respond urgently and effectively in order to protect individuals who find themselves under a specific threat, by adopting special measures such as the assignment of around-the-clock police protection, the issuance of protection and restraining orders against potential aggressors and, in exceptional cases, and only with the free and informed consent of the threatened individual, protective custody."[21]

Similar obligations have been outlined in the jurisprudence of regional human rights courts, in particular the European Court on Human Rights and the Inter-American Court and Commission on Human Rights. The regional courts do not specify in detail what procedures should be adopted, nor to conclude that one unified procedure which combines fact-finding, criminal investigation and prosecution is necessary. However, they found that certain crucial features are indispensable for maintaining public confidence in the rule of law and helping prevent suggestions of official collusion in or tolerance of unlawful acts. Their jurisprudence demonstrates that States are obliged to *inter alia* undertake a prompt, expeditious, thorough, diligent and comprehensive investigations in a manner guaranteeing sufficient public scrutiny.[22]

Standards on effective investigation of online harassment and abuse against women journalists

International standards

As noted earlier, numerous international and regional human rights bodies, as well as civil society organisations, have called on States to put in place measures to combat online gender-based harassment and abuse. For example:

- In 2016, the OSCE Representative on Freedom of Media (RFoM) report recommended *inter alia* that States recognise that threats and other forms of online abuse of women journalists and media actors are a direct attack on freedom of expression and freedom of the media. The RFoM called on States to strengthen the capacity of law enforcement agencies to understand international standards on human rights so they can identify real threats to safety and protect individuals in danger, including providing tools and training on technical and legal issues. Other recommendations included commissioning and supporting the collection and analysis of data related to online abuse and its effects, and creating a database of specific occurrences and followup from law enforcement.[23]
- In 2017, the UN Special Rapporteur on Freedom of Expression and Opinion and the UN Special Rapporteur on violence against women urged States to address online gender-based abuse, whilst warning against censorship.[24] They recommended that human rights-based responses which could be implemented by governments and others could include education, preventative measures, and steps to tackle the abuse-enabling environments often faced by women online.
- The HRC Resolution on promotion, protection and enjoyment of human rights on the Internet also addresses online harassment and abuse against women. In the Resolution, the HRC condemned "unequivocally online attacks against women, including sexual and gender-based violence and abuse of women, in particular where women journalists, media workers, public officials or others engaging in public debate are targeted for their expression;" and called "for gender-sensitive responses that take into account the particular forms of online discrimination" as well for ensuring "effective remedies for human rights violations, including those relating to the Internet, in accordance with their international obligations."[25]
- The 2019 UN **General Assembly Resolution on the safety of journalists and the issue of impunity called on States to** tackle gender-specific threats to journalists, making more comprehensive commitments in the latest resolution to ensure prevention and protection measures, as well as accountability and redress mechanisms, are gender-responsive, in particular in relation to online threats. It provided more details on addressing gendered and sexist threats, intimidation, and harassment, in particular considering the especially hostile responses women journalists can be exposed to.[26]
- In 2019, the RFoM report on report on online harassment or abuse of journalists, recommended that in cases when online harassment and abuse "is likely to cause serious harm, the police and prosecuting authorities must proactively and vigorously investigate the harassment or abuse in a timely fashion, and perpetrators should be prosecuted accordingly. Such a response should not be wholly dependent on the victim's coming forward and calling for the punishment of the perpetrators since the online harassment interferes with the right to freedom of expression of both the journalist and the public at large (and should, therefore, be treated as a public matter)."[27]

The Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention (Cybercrime Convention), sets out a number of procedural requirements for the investigation and prosecution of cybercrimes as defined by the Convention, including preservation orders, production orders and the search and seizure of computer data.[28] However, the Cybercrime Convention (with the exception of the Additional Protocol that deals with "racist and xenophobic nature committed through computer systems") does not deal with speech related offences, but rather offences against the systems and infrastructure. ARTICLE 19 does not suggest that content-based offences should be included under the Cyber-Crime Convention. However, we note that a recent report from the Cybercrime Convention Committee points at possible synergies between different standards and treaties when it comes to prevention of, protection from and prosecution of online gender-based violence and abuse. The report recommended that countries should consider implementing the procedural powers of Articles 16 to 21 of the Cybercrime Convention to facilitate international cooperation on electronic evidence in relation to online gender-based violence and abuse.[29]

Further, there does not appear to be comprehensive standard and specific guidelines at national level on what specific steps should law enforcement undertake when investigating online gender-based harassment and abuse. Also, regional and domestic courts are yet to provide specific guidance on what particular steps law enforcement should take to meet the standards of effective investigation under respective online harassment and abuse crimes.

Comparative national standards

At the states level, States' measures to address and target online harassment and abuse range from adopting new criminal offences that can be applied to online gender-based harassment and abuse, to preventive and educational measures to increase social media literacy in school curricula. Available research shows that there is a lack of clarity about how best to pursue legal accountability for online harassment and this can often lead to the adoption of new, overly broad laws that harm freedom of expression.[30] So far, it is also not clear how States implement the recommendations to prevent, prosecute and remedy online gender-based harassment and abuse of journalists in practice.

Online harassment and abuse as criminal offence

Similarly to the lack of uniform definition to collectively describe the phenomenon of online gender-based harassment and abuse, there is no universal definition of crimes that penalise this type of behaviour.

Overall, States take very different positions on whether different forms of online harassment and abuse should be a criminal offence. Even where there is general agreement that there should be criminal sanctions, there is a challenge on how precisely these crimes should be defined and when the threshold for criminal liability might arise.[31]

Even when the legislation sets a certain severity threshold – such as "substantive harm" or "true threat," – there is lack of comprehensive guidelines on when such threshold is reached. Studies show that if the conduct is prohibited under criminal law, prosecutions under respective criminal provisions are more complex to that of "offline" crime. This is sometimes due to the necessity of balancing freedom of expression versus the harm caused to the victims. But it also includes numerous other issues, such as "discovering what jurisdiction the offence was committed in; perpetrators being in different countries; perpetrators retaining anonymity through false names or avatars; technical capabilities and resources of the police; the role of Internet service providers; and the scale of offending behaviour."[32] For instance:

- The question of what constitutes a "true threat" was addressed in *Elonis v. United States*,[33] in which the defendant was indicted by a grand jury for a crime of transmitting "in interstate commerce 'any communication containing any threat… to injure the person of another.'"[34] Elonis made multiple threats on his Facebook page in the form of rap lyrics (such as threats to murder his wife, to shoot up a kindergarten, and to kill the FBI agents who came to his house to investigate the kindergarten threat). The jury was asked to consider and determine whether these were "true threats," meaning whether when made intentionally, "in a context or under such circumstance wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily injury or take the life of an individual." Elonis argued that he was simply exercising his First Amendment rights; but he was convicted under the negligence standard. The Supreme Court overturned the conviction, though not on the basis of the First Amendment grounds.[35] In his partially dissenting opinion, Justice Alito stated that "the Court's disposition of this case is certain to cause confusion and serious problems" because of its refusal to address the applicable standard.[36]
- The case of Jessikka Aro, an award-winning Finish journalist, shows the particular difficulties involved in prosecuting online harassment cases. Aro sustained four-years of online harassment against her which included publication of her phone number, numerous death threats and allegations that she was an agent of NATO and USA intelligence services. The case showed that the public prosecutor in Finland would not bring charges under the Criminal Law unless the injured part reports the offence, a lethal instrument has been used, or "where a very important public interest requires the case to be brought."[37] This means that the public prosecutor is not proactively pursuing cases of online abuse as they are not treated as falling within their purview.[38]

Existing guidelines for law enforcement on online harassment and abuse

Although States take divergent approaches to the problem of online harassment and abuse, the following positive examples can serve as guidance to law enforcement on investigation of online harassment and abuse against those who exercise their right to freedom of expression.

In the **United Kingdom**, the HM Inspectorate for Policing acknowledged that "the police response to digital crime should be capable of being provided by every police officer and member of police staff who deal directly with the public", due to "the prevalence of digital crime and that this requires police staff to have the relevant training to give them the necessary understanding of the technology."[39] The College of Policing provides a number of courses to law enforcement, covering topics including cyber-crime and policing and digital communication and social media. Furthermore, the reports show that introducing national tasking process and regional co-ordinators has provided some consistency in when, how, and to what level, is online harassment and abuse investigated. In 2017, the UK created a "national police online hate crime hub"[40] which acts as a single point through which all reports of online hate crime are channelled. The hub employs specially trained officers to liaise with the victim and collect relevant evidence that will be needed to bring a prosecution. According to available information, the hub can for example:

- Assess whether the circumstances relate to a crime or non-crime incident;
- Combine duplicate reports and seek to identify the perpetrator;
- Produce an evidence package for local recording and response where there is a positive line of enquiry;
- Update the complainant with progress and explain where there is no enforcement action possible;
- Advise local police colleagues on effective responses.

In **Canada**, in 2017, the Department of Justice published a "Handbook for Police and Crown Prosecutors on Criminal Harassment", which is intended to provide the police and Crown Prosecutors with guidelines for the investigation and prosecution of criminal harassment cases.[41] The Handbook also specifically deals with "online harassment" and explains to law enforcement which sections of the criminal code apply to online situations.[42] Although not legally binding, it details the Department of Justice's guidelines for best practice. The Handbook specifically advises law enforcement on collecting technological evidence.

In the **USA**, Katherine Clark, the representative for Massachusetts, proposed The Cybercrime Enforcement Training Assistance Act "to make grants to States and units of local government for the prevention, enforcement, and prosecution of cybercrimes against individuals, and for other purposes."[43] The proposed grants would be used to train law enforcement at all levels to "identify and protect victims of cybercrimes against individuals," "utilize Federal, State, local, and other resources to assist victims of cybercrimes against individuals, "identify and investigate cybercrimes against individuals," and "enforce and utilize the laws that prohibit cybercrimes against individuals." The Bill also proposes to earmark additional funds for "laws that prohibit cybercrimes against individuals," for public education, the establishment of cybercrime

task forces, the establishment or enlargement of digital forensics laboratories, the expenses involved in extraditing offenders from one state to another, and the transfer of "expertise and information" from federal to state law enforcement agencies.

Enforcement problems

In cases where the level of online gender-based harassment and abuse reaches the level of severity under criminal law, investigation and prosecution is often hampered by challenges such as determining jurisdiction of where the offence was committed (the perpetrator can be located in a different country or jurisdiction than the victim), problems with identification of perpetrators due to their anonymity (or perceived anonymity), access to evidence and problems in cooperation with the Internet service providers.[44]

It should be stressed out that when balancing the right to freedom of expression with the right to equality and dignity in criminal cases is not only limited to speech offences from a substantive point of view. Online anonymity or pseudo-anonymity are also important aspects of the right to freedom of expression and privacy, and must be guaranteed to prevent excessive and disproportionate surveillance by governments and private actors.

In investigations of online gender-based harassment and abuse, law enforcement will typically have to request information from the digital companies, especially social media and the Internet service providers, that are established outside their jurisdiction/abroad. In order to access evidence and identify perpetrators, law enforcement relies on formal international cooperation through mutual legal assistance treaties (MLATs).

In general, the available studies show that although MLATs are "the most resilient way of obtaining data," the reliance on them by law enforcement on them is low. Studies show that law enforcement officials have little confidence in successfully obtaining information through MLAT requests. MLAT processes are long (they can take months), require complex administrative legal processes in both countries and specially trained law enforcement personnel, and the costs and efforts required through this process might be prohibitive for law enforcement to pursue in the context of online harassment and abuse.[45] Studies also show that problems with MLATs include the inability to get all communications data relating to nationals, including content, under their own national laws; and the burden on government's central authorities responsible for processing incoming and outgoing requests.[46] Further, responses to MLAT requests by some States have been interpreted as a refusal to provide the information.[47]

Importantly, some MLATs condition that mutual legal assistance requests are subject to dual criminality and requests may be refused where execution is considered "contrary to national legislation," and establish seriousness thresholds for international cooperation requests.[48] Additionally, some MLATs – as well as the Cybercrime Convention - establish seriousness thresholds for international cooperation requests. There is no information to what extent has this threshold been applied to MLAT requests related to online harassment and abuse related offences. The available information only shows the usage of these instruments for extradition offences.

Civil society organisations have raised concerns about possible privacy concerns that MLATs and similar agreements pose, and the lack of transparency over their application. There is no comprehensive assessment on the extent to which States rely on MLATs to identify perpetrators of online harassment and abuse, and the effectiveness of MLATs requests to the USA, in particularly in the light of the possible First Amendment arguments.

At the same time, the reason why MLATs are to a certain extent cumbersome is because they provide privacy and other safeguards; and these are also the reasons why law enforcement are asking for lower thresholds in terms of the sharing of information. For instance, the recent US-UK Data Sharing Agreement under the USA CLOUD Act allows the UK to demand data directly from intermediaries holding data in the US;[49] while previously, UK law enforcement had to meet the higher standards set in the US to acquire user data. The new UK-US agreement is extremely problematic from a human rights perspective and might be incompatible with State obligations under the European Convention.[50]

On the other hand, States are not exempt from discharging their obligations on the basis that the offence is difficult to investigate or prosecute due to extraterritoriality or other reasons. In cases when the level of severity reaches the possibility of criminal sanctions, such as genuine death threats, law enforcement authorities should make the maximum efforts to identify perpetrators (in some cases, the identity can be established without major difficulties) and/or initiate legal processes to do so. This might include making requests to the service providers over the identity of the perpetrators based on the national legislation.

Free speech compliant investigation into online gender-based harassment and abuse against women journalists

Although the discrepancies in national approaches to online harassment and abuse make it difficult to formulate detailed recommendations on how to effectively investigate different online harassment and abuse cases against women journalists, the previous sections demonstrate that, at least, the following measures should be undertaken by States:

- States should recognise that online gender-based harassment and abuse, in particular against women journalists who are targeted for exercising journalism activities, is a serious problem and adopt integrated prevention, monitoring, and response mechanisms, including in public policy.
- States should adopt a comprehensive public policy approach to tackling forms of intolerance and prejudice of which manifestations of online harassment and abuse are symptomatic of. They must take action to counter discriminatory attitudes and norms and create an enabling environment where all women can fully participate in society.
- State officials should publicly, unequivocally and systematically condemn attacks against journalists, women journalists and against those who exercise their right to freedom of expression. They should refrain from making statements that are likely to increase the risks that put women journalists in situations of vulnerability.[51]
- Although there are concerns that the approach to online harassment and abuse in legal measures are piecemeal, there is a growing consensus that different regulatory measures should be adopted to tackle online gender-based harassment and abuse. Any regulation restricting or limiting the right to freedom of expression should comply with the three-part test under Article 19 para 3 of the ICCPR; while criminal law should be used in exceptional circumstances when online harassment and abuse reaches certain severity, such as causing serious harm.
- In cases where online gender-based harassment and abuse reach the level of severity prohibited under criminal law, including in cases of online harassment and abuse against women journalists, States are obliged to *inter alia* undertake a prompt, expeditious, thorough, diligent and comprehensive investigation in a manner guaranteeing sufficient public scrutiny.
- States should adopt practical measures such as dedicated institutional resources, capacity and training to enable the legal system to deal with online gender-based harassment and abuse, and adequately resource them. In particular:
- Law enforcement and the judiciary should be trained on States' international legal obligations and commitments on the safety of journalists. These should explicitly address gender-specific threats to women journalists to ensure these are taken seriously and to tackle any institutionalised discrimination.
- Law enforcement should be trained not only to respond to physical situations, but also to recognise that online harassment and abuse can have an impact on an individual's private and family life, freedom of expression and other human rights. Training materials on online harassment and abuse should be developed.
- States should improve reporting and monitoring of gender-based harassment and abuse and include them in national statistics and measures to address equality and discrimination.
- States should also adopt holistic and well-resourced prevention and response mechanisms together with the private sector and civil society.

About ARTICLE 19

ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19), is an independent human rights organisation that works around the world to protect and promote the rights to freedom of expression and information. It takes its name and mandate from Article 19 of the Universal Declaration of Human Rights which guarantees the right to freedom of expression.

ARTICLE 19 has produced a number of standard-setting documents and policy briefs based on international and comparative law and best practice on issues concerning the right to freedom of expression. Increasingly, ARTICLE 19 is also examining the role of international internet technical standard-setting bodies and internet governance bodies in protecting and promoting freedom of expression.

If you would like to discuss this brief further, or if you have a matter you would like to bring to the attention of ARTICLE 19, you can contact us by e-mail at info@article19.org.

End notes

1 UN General Assembly Resolution on The safety of journalists and the issue of impunity, A/C.3/72/L.35/Rev.1, 13 November 2017; UN Special Rapporteurs on freedom of opinion and expression and on violence against women, UN experts urge States and companies to address online gender-based abuse but warn against censorship, 8 March 2017.

2 Report of the Special Rapporteur on violence against women (Special Rapporteur on VAW), its causes and consequences on online violence against women and girls from a human rights perspective, July 2018; UK Law Commission, Abusive and offensive communications, 2018; Chakraborti, Garland & Hardy, The Hate Crime Project - Findings and conclusions, University of Leicester, 2014.

3 See, e.g. OSCE Representative on Freedom of the Media (OSCE RFoM), New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists, 2016; Special Rapporteur on VAW, ***op.cit;*** European Commission, Cyber violence and hate speech online against women Study for FEMM Committee, September 2018.

4 ***C.f.*** APC, Technology-related violence against women – a briefing paper, 2015.

5 *Ibid., c.f. also* Council of Europe, CoE Factsheet Hate Speech, 2017; European Commission, What is gender-based violence?, 2018; European Union Agency for Fundamental Rights (FRA), Violence against women: an EU-wide survey, 2014; UN General Assembly, Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women rights defenders, A/RES/68/181, 2014; Human Rights Council (HRC), Report of the Special Rapporteur on violence against women (Special Rapporteur on VAW), its causes and consequences on online violence against women and girls from a human rights perspective, July 2018; OSCE RFoM 2016 Report, ***op.cit.;*** OSCE RFoM, Legal Responses to Online Harassment and Abuse of Journalists: Perspectives from Finland, France and Ireland, 2019.

6 Ibid.

7 For example, the US Supreme Court found that "liberty of the press is the right of the lonely pamphleteer... just as much as of the large, metropolitan publisher" and that the reporter's privilege does not cover those who engage in journalism as part of a collective vocation, but "should apply with equal force to the lone, individual disseminator of news and information -- who engages in similar acts (i.e., of gathering news) and with the same intent (to disseminate that information to the public) as his or her more "traditional" brethren;" see *Branzburg v. Hayes*, 408 U.S. 665, 704 (1972). Subsequently, the US courts have applied the reporter's privilege to non-traditional journalists engaged in newsgathering; see, e.g., ***Silkwood v. Kerr-McGee***, 563 F.2d 433, 436 (10the Cir 1977) (applying the privilege to a documentary filmmaker); ***Shoen v. Shoen***, 7 5 F.3d 1289, 1293 (9th Cir. 1993) (author of book about a family feud over ownership of a company); *Alexander v. FBI*, 186 F.R.D. 21, 50 (D.D.C. 1998) (former presidential aide gathering information for a book); *Cusumano v. Microsoft Corp.*, 162 F.3d 708 (1st Cir. 1998) (academic involved in pre-publication research); *In re Petroleum Products Antitrust Litigation,* 680 F.2d 5 (2nd Cir. 1982) (trade newsletter compiling oil prices); or ***United States v. Garde***, 673 F. Supp. 604 (D.D.C. 1987) (non-profit organization could conceal names of whistle-blowers). The US courts have also recognized that the reporter's privilege extends to bloggers and website operators. For example, in *Blumenthal v. Drudge*, 992 F. Supp. 44 (DDC 1998), the court applied the reporter's privilege to the blog "The Drudge Report," which the court had characterized in a prior opinion as "a gossip column focusing on gossip from Hollywood and Washington, D.C.

8 Human Rights Committee, General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, para 44.

9 Committee of Ministers, Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, adopted by the Committee of Ministers on 8 March 2000 at the 701st meeting of the Ministers' Deputies.

10 Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, adopted on 21 September 2011.

11 Ibid.

12 Ibid.

13 The 2017 General Assembly Resolution on The

safety of journalists and the issue of impunity, *op.cit.*

14 *C.f.* for example, General Comment No 34, *op.cit.*, para 7; Inter-American Commission on Human Rights, Violence against Journalists and Media Workers: Inter-American Standards and National Practices on Prevention, Protection and Prosecution of Perpetrators, OEA/Ser.L/V/II, CIDH/RELE/INf.12/13, 31 December 2013, p. 22.

15 *C.f.* for example, Inter-American Court of Human Rights, *Mapiripán Massacre v Colombia*, Series C No 134, 15 September 2005, para 111 – 112; or *Pueblo Bello Massacre v Colombia*, Series C No 140, 31 January 2006, para 111.

16 Joint declaration on crimes against freedom of expression, the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 25 June 2012.

17 HRC, Resolution 33/2, The safety of journalists, A/HRC/RES/33/2, 6 October 2016.

18 General Comment No 34, *op.cit.*, para 23.

19 *Ibid.*

20 Human Rights Committee, General comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the right to life, CCPR/C/GC/36, 30 October 2018, para 23.

21 *Ibid.*

22 See, e.g. European Court on Human Rights, *Palomo Sanchez v Spain*, App. Nos. 28955/06, 28957/06, 28959/06, 28964/06; Özgür Gündem v Turkey, App. No. 23144/93; ***Dink v Turkey***, App. Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09. See also,

23 OSCE RFoM 2016 Report, *op.cit.* New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists, 2016.

24 The Joint Press Release of the UN Special Rapporteurs on FOE and on VAW, 08 March 2017.

25 HRC Resolution The promotion, protection and enjoyment of human rights on the Internet, A/HRC/38/L.10/Rev.1, 4 July 2018.

26 UN General Assembly, Resolution The safety of journalists and the issue of impunity, A/C.3/74/L.45/Rev.1, 13 November 2019.

27 OSCE RFoM, 2019, *op.cit.*, p. 39.

28 Council of Europe, Convention on Cybercrime, 23 November 2001.

29 Cyber-Crime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children, Mapping study on cyberviolence (Draft), 2018.

30 *C.f.* OSCE RFoM, 2019, *op.cit.*, p. 2.

31 Such prohibitions might not meet the criteria for restrictions on freedom of expression, set under international human rights standards.

32 See, e.g. A. Brown, What is so special about online (as compared to offline) hate speech?, Ethnicities,18(3):146879681770984, May 2017.

33 135 S. Ct. 2001 (2015).

34 18 U.S.C. § 875(c)

35 The Supreme Court held that "negligence is not sufficient to support a conviction," because "[f] ederal criminal liability generally does not turn solely on the results of an act without considering the defendant's mental state."

36 135 S. Ct. 2001 (2015), 2013; Alito concurring in part and dissenting in part.

37 The Criminal Code regulates the circumstances under which prosecutors may bring charges, and chapter 25, section 9(1) of the Criminal Code states that "[t]he public prosecutor may not bring charges for negligent deprivation of personal liberty, menace or coercion, unless the injured party reports the offence for the bringing of charges or unless a lethal instrument has been used to commit menace or coercion, or unless a very important public interest requires that charges be brought." (Chapter 25, section 9(1) of the Finnish Criminal Code). In OSCE RFoM, 2019, *op.cit.*

38 *Ibid.* The report also notes the case of Ms. Härkönen in Finland who intentionally withdrew her request for prosecution in an attempt to trigger the process where the prosecutor would have to determine whether a "very important public interest" required the charges to be brought, which would have set an important precedent for journalists and freedom of expression. The public prosecutor decided that her case did not meet this threshold, although it did not make reference to the role of journalists or to freedom of expression in making this judgement.

39 The HM Inspectorate for Policing, Digital crime and policing, Chapter 5.

40 Home Secretary announces new national online hate crime hub, 8 October 2017.

41 Canada: Department of Justice, Canada, A Handbook for Police and Crown Prosecutors on Criminal Harassment, January 2017.

42 *Ibid.*, Section 1.6.159.

43 The Cybercrime Enforcement Training Assistance Act, H.R. 4740, 114th Cong. (Mar. 15, 2016).

44 See, e.g. Law Commission, Abusive and Offensive Online Communications: A Scoping Report, 1 November 2018.

45 See, mutatis mutandis, e.g. UN, Comprehensive Study on Cybercrime Draft, February 2013; UK Parliament, Jurisdictional Issues – Requests addressed to overseas CPSs, December 2012; or The Center for Internet and Society, Stanford Law School, The mutual legal assistance problem explained, February 2015.

46 *Ibid.*

47 *Ibid.*

48 *C.f.* also the Cybercrime Convention.

49 US-UK Data Sharing Agreement, USA No. 6 (2019), Washington, 3 October 2019, presented to Parliament by the Secretary of State for Foreign and Commonwealth Affairs by Command of Her Majesty October 2019.

50 Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943).

51 See, e.g. Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, June 2012; UN HR Council Resolution 33/2, A/HRC/33/L.6, 26 September 2016.

article19.org