REUTERS / Khaled Abdullah

ONLINE ATTACKS AGAINST JOURNALISTS: **KNOW YOUR RIGHTS**

ONLINE ATTACKS AGAINST JOURNALISTS: KNOW YOUR RIGHTS

NOVEMBER 2021

INSI INTERNATIONAL NEWS SAFETY INSTITUTE

TrustLaw

THOMSON REUTERS FOUNDATION

With the support of UNESCO and the Swedish Postcode Foundation for the country chapters on Kenya and India

unesco

SVENSKA POSTKOD STIFTELSEN

With legal contributions from:

ARTHUR COX

Baker McKenzie.

BOWMANS

Dechert LLP

DLA PIPER

intel

KLA

LATHAM & WATKINS

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

PAUL HASTINGS

simmons + simmons

ABOUT

INTERNATIONAL NEWS SAFETY INSTITUTE

The International News Safety Institute (INSI) is a member-based organisation dedicated to journalists' safety, offering the news media industry a vital forum for information sharing via its membership portal, alerts and advisories, workshops and webinar discussions. In an industry defined by competitiveness, INSI provides a model for collaboration by bringing together some of the news industry's fiercest competitors, over the common priority of keeping journalists safe.

THOMSON REUTERS FOUNDATION

Thomson Reuters Foundation is the corporate foundation of Thomson Reuters, the global news and information services company. We work to advance media freedom, raise awareness of human rights issues, and foster more inclusive economies. Through news, media development, free legal assistance and convening initiatives, the Foundation combines its unique services to drive systemic change. TrustLaw is the Thomson Reuters Foundation's global pro bono legal programme, connecting the best law firms and corporate legal teams around the world with high-impact NGOs and social enterprises working to create social and environmental change. We produce ground-breaking legal research and offer innovative training courses worldwide.

UNESCO

UNESCO is the UN agency with the mandate to "promote the free flow of ideas by word and image". The Organization works to advance freedom of expression and the United Nations Plan of Action on the Safety of Journalists. Moreover, UNESCO combats online hate speech, as well as disinformation and misinformation through awareness raising initiatives, steady monitoring, capacity-building activities, and technical support to Member States.

REUTERS/Khaled Abdullah

REUTERS/Omar Sobhani

ACKNOWLEDGEMENTS

INSI, UNESCO and the Thomson Reuters Foundation would like to acknowledge and extend their gratitude to the legal teams listed below who contributed their time and expertise on a pro bono basis to make this report possible. Special thanks to Dechert LLP for coordinating and editing this report, along with contributing pro bono research and drafting.

CONTRIBUTING LAW FIRMS AND IN-HOUSE TEAMS

- **Arthur Cox**
- **Baker McKenzie**
- **Bowmans**
- **Dechert LLP**
- **DLA Piper**
- **Intel Corporation**
- **KLA - Koury Lopes Advogados**
- **Latham & Watkins LLP**
- **Nishith Desai Associates**
- **Paul Hastings**
- **Simmons & Simmons LLP**

REUTERS/Paul Ratje

DISCLAIMER

This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances.

We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. INSI, UNESCO, the Thomson Reuters Foundation and the contributing legal teams, accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

The legal teams listed above generously provided pro bono research to INSI and UNESCO. However, the contents of this report should not be taken to reflect the views of the contributing legal teams or the lawyers who contributed.

Similarly, Thomson Reuters Foundation is proud to support our TrustLaw member INSI with their work on this report, including with publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we do not take a position on the contents of, or views expressed in, this report.

REUTERS/Thierry Gouegnon

REUTERS/Hugo Correia

CONTENTS

INTRODUCTION 12

EXECUTIVE SUMMARY 14

COUNTRY SUMMARIES 19

Australia 19

Brazil 31

Finland 37

France 47

Germany 59

India 65

Ireland 75

Japan 85

Kenya 96

The Netherlands 104

Sweden 110

United Kingdom 119

United States 135

INTRODUCTION

In recent years, online harassment targeting journalists has grown dramatically in both frequency and intensity. Few journalists know how it feels to be shot at, but most journalists by now have experienced first-hand what it's like to be abused or threatened online. The impact on individuals and the whole profession is devastating, leading many to describe online harassment as one of the most serious threats to press freedom globally today.

Some of these attacks may amount to actual crimes and, as such, require accountability. Yet the lack of a clear path to legal recourse means most of these crimes end up being treated as an occupational hazard, often leaving victims feeling vulnerable and isolated. Many journalists, particularly women, leave the profession as a result.

To address this critical gap in the protection of journalists, the International News Safety Institute has partnered with TrustLaw to research and deliver a Know Your Rights Guide to help journalists better understand what the law can do for them to address online harassment in all its forms. We hope it will be useful.

Elena Cosentino,
INSI Director

Online harassment is a particularly pernicious form of violence, which affects journalists working in all countries, including those usually best ranked in the World Press Freedom Index. Its impact can be dramatic, as new technologies are easily manipulated to amplify hateful messages and online harassment is multifaceted. It can take a variety of forms, from unmistakable insults and threats, to more vicious means such as stalking or online impersonation. It can be orchestrated by organised political groups and ideological movements or carried out by a few isolated individuals. It can remain purely virtual, or give rise to subsequent physical attacks, for instance when a journalist's private or personally identifiable information is broadcasted online (doxxing).

It is particularly difficult for journalists to protect themselves from it, as the use of online resources and exposure on social networks are often essential to their work. Online harassment provides any individual displeased with media coverage of a specific topic with an unprecedented echo chamber and has thus become a new way of censoring journalists and curtailing the freedom to inform.

This practical guide aims to provide journalists with concrete legal tools to deal with online harassment, be it to identify punishable offences, to seek help from appropriate organisations, to efficiently gather evidence and to take steps should they decide to file a complaint against the perpetrators. Where appropriate, it also presents examples of litigation initiated by journalists who were victims of online harassment.

It covers online harassment of journalists in Australia, Brazil, Finland, France, Germany, India, Ireland, Japan, Kenya, the Netherlands, Sweden, the United Kingdom (England and Wales) and the United States.

Although none of these countries provide specific provisions sanctioning online harassment of journalists, they all offer civil and criminal law provisions that make it possible to apprehend, punish and compensate all or part of the most common abuses committed against journalists.

In addition to the comprehensive presentation of the legal tools available for journalists in each of these jurisdictions, this guide aims to provide journalists with an overview of the solutions available to combat situations of online harassment, in order to enable them to choose the best legal forum to exercise their rights. In this regard, the table shown at pages 16 to 17 summarises the potential actions that can be taken in each jurisdiction to deal with the main types of behaviour that may characterise online harassment.

It lists the most common types of abuses, and provides a general legal qualification for each behaviour, with a reference to the corresponding chapter where this behaviour is covered by the law. Abuses that are not listed in the table may nonetheless be covered by existing law in each country. When in doubt, journalists are strongly encouraged to seek legal advice in the countries concerned.

Finally, this guide provides journalists with guidance regarding cross-border harassment situations, as well as practical information and contacts.

The publication of this guide was only made possible thanks to the generous pro bono contributions of Arthur Cox, Baker McKenzie, Bowmans, Dechert LLP, DLA Piper, Intel Corporation, KLA - Koury Lopes Advogados, Latham & Watkins LLP, Nishith Desai Associates, Paul Hastings and Simmons & Simmons LLP. Special thanks to Dechert LLP for coordinating and editing this guide, along with contributing pro bono research and drafting.

EXECUTIVE SUMMARY

Online harassment in general, and against journalists in particular, is a relatively recent phenomenon that has proliferated very rapidly. Most national and international legal systems, which are relatively slow in evolving both by nature and by tradition, have not yet adapted to deal with the full range of online practices that may characterise such harassment.

Yet, violations of journalists' rights have immediate effects on their ability to provide information, and consequently on the right to information, which constitutes one of the major counter-powers of democratic regimes. The work of journalists is all the more important now as it directly contributes to the fight against the increasingly widespread phenomenon of online disinformation or misinformation, which threatens the public debate.

It is therefore crucial that journalists, whenever they experience some form of online harassment, can defend themselves against such practices by legal means. Although no country has yet developed a comprehensive legal framework for dealing with online harassment behaviours, such practices may nevertheless be punished in most jurisdictions under existing legal provisions prohibiting, for example, insults, defamation or threats.

Indeed, even countries that are considered progressive in the Reporters Without Borders' 2020 World Press Freedom Index, such as Finland and Sweden, have no specific legislation dealing with online harassment. Harassing practices are thus analysed under the existing criminal provisions with a focus on encouraging victims to file complaints, so that these infringements can be brought before the courts.

In this regard, recent case law – including outside of Scandinavia – reflects the growing awareness of the courts as to the effects of online harassment on the mental and physical health of victims. Online threats, for instance, have recently been successfully prosecuted in several countries with the same penalties as those applicable to "real life" ones.

As an example, in 2019, self-described "internet troll" Brendan D., who harassed six Irish female journalists by sending them hundreds of abusive emails, was sentenced to five years imprisonment. The Irish judge commented that the "the internet had wonderful advantages", but also a "dark side which allows a man sitting in his house to inflict huge amounts of trauma on six women".

Similarly, in France, radio journalist Nadia D., who was insulted and threatened along with her 11-year-old daughter by users of an online forum, filed a complaint which resulted in one of her harassers being convicted both at first instance and later on appeal in 2020. The Paris Court of Appeal ruled that the incriminated messages, which were "intended to 'punish' Nadia D. as a journalist, defending the cause of women", deserved "a sentence sufficiently dissuasive to prevent a new offence, particularly via the internet, a communication tool perfectly mastered by the accused who, acting under a pseudonym, which proves his cowardice, could only be identified thanks to the cyber investigations of the police".

In addition to these existing provisions, some countries have undertaken to strengthen their legal arsenal to specifically address online harassment, including any targeting journalists. This approach shows the growing awareness of many national legislators to these issues, as well as their willingness to give the courts the legal means to prosecute and condemn such practices.

One can only hope that it will, in the years to come, make it easier to punish other types of behaviour that are very specific to the virtual world, such as revealing a journalist's contact details online (doxxing) or interfering in a debate in such a way as to disrupt it (trolling).

In this regard, encouraging trends have been seen in several countries. Ireland, for instance, has recently passed the Harassment, Harmful Communications and Related Offences Act 2020, which expressly includes communication by "electronic means" in the definition of harassment. Following a similar trend, Germany passed a law in January 2021 reinforcing police powers to investigate online hate speech. Likewise, in France, a new Act called Reinforcing Respect of the Principles of the Republic, which includes provisions on online hate was passed.

In September 2021, the European Commission also adopted a Recommendation on the protection, safety and empowerment of journalists which is intended to encourage Member States to take further legal steps to ensure safer working conditions for all media professionals, free from fear and intimidation, whether online or offline.

While further developments to better protect journalists and media organisations are in progress, it should be stressed that journalists and media professionals are not powerless. This guide therefore aims to provide journalists and media professionals with the means to analyse the various forms of harassment that they face and to defend themselves against those.

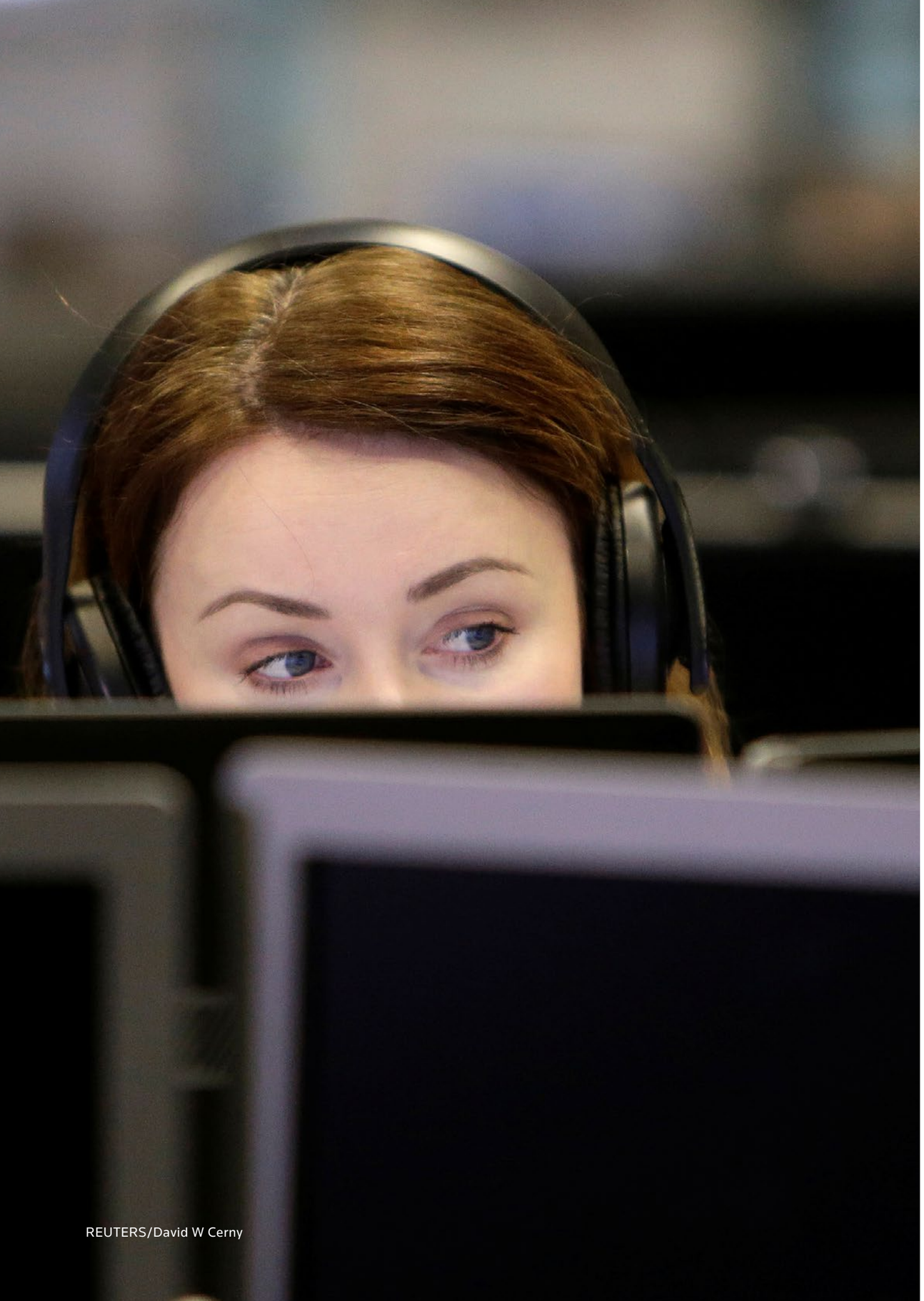
In terms of methodology, this guide examines incidents of online harassment of journalists in selected countries and highlights legal measures available in those countries to address the problem. It offers a survey of relevant resources and legal tools in 13 jurisdictions, selected based on the relevant developments in this area: Australia, Brazil, Finland, France, Germany, India, Ireland, Japan, Kenya, the Netherlands, Sweden, the United Kingdom (England and Wales) and the United States. In order to make the guide as user-friendly as possible, especially for journalists or media organisations facing transnational issues, each chapter has been structured according to a well-defined identical framework that addresses the following issues:

- The legal standing of both journalists and media organisations to take action against online harassment (**Section 1.a**);
- The handling of international jurisdictional issues when it comes to online attacks, including evidence gathering (**Section 1.b**);
- The legal framework applicable to online harassment against journalists and media organisations, including a detailed examination of online harassment in general (**Section 2.a**) and of each of the following types of abuse: threats, intimidation, cyberstalking, doxxing, online impersonation, trolling and brigading (**Section 2.b**);
- A review of the existing laws, not necessarily conceived for online crimes, that can be or have been used to prosecute online harassment (**Section 2.c**), as well as of the additional legal avenues that can be used when race and gender are a factor in the abuse (**Section 2.d**);
- Where appropriate, examples where any such laws have been found to infringe on freedom of speech laws (**Section 2.e**);
- Practical guidance as to what can legally be done by a journalist to identify an anonymous harasser, and useful resources (**Section 3**).

This guide also displays a summary table providing journalists with a practical overview of the tools at their disposal and of the global trends across all 13 jurisdictions.

EXAMPLES OF BEHAVIOURS THAT CONSTITUTE ONLINE ATTACKS AGAINST JOURNALISTS	TYPE OF ABUSE	Australia	Brazil	Finland	France	Germany	Ireland	Japan	Netherlands	Sweden	United Kingdom	United States
• Systematic offensive comments directed at a journalist posted by one or more users of a website or social network (for example "Journalist X is an idiot who doesn't know what he/she is talking about", followed by "Journalist X should crawl back in the hole where he/she comes from"). • Repeated online messages directly sent to a journalist that cause him/her to feel distressed. • Monitoring the use by a journalist of the internet, email or any other form of electronic communication (for example creating a twitter account aimed at reporting everything a journalist says and does).	Cyberstalking	Yes	Yes[1]	Yes	Yes	Yes	Yes[1]	Yes	Yes	No[3]	Yes[1]	Yes
• Degrading or offensive messages, which can be based on the race, gender, or sexual orientation of the journalist. • Public statements that adversely affects a journalist's reputation (for example "I know for a fact that Journalist X was paid by a foreign government to hide information about this or that issue").	Insults Defamation	Yes	Yes	Yes	Yes	Yes	No	Yes[4]	Yes	Yes	Yes	Yes
• Threats to commit a crime or an offence against the journalist. • Threats to harm a journalist's relatives. • Implicit threats (for example "People like Journalist X need to be taught a lesson").	Threat Intimidation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Collection and disclosure of personal information on a journalist (for example his/her home address or private contact details). • Collection and disclosure of personal information on their partner or children (for example "Journalist X's children attend School Y and they get out at 4pm every day. Just saying…").	Doxxing	Yes[1]	Yes[2]	Yes	Yes	Yes	Yes1	Yes	Yes1	Yes	Yes	Yes[5]
• Identity theft (for example by creating a false profile page / account on a social network in order to pretend to be a journalist). • Hacking of a journalist's website, account or electronic device to post content in their place that is intended to harm them or their reputation (for example hackers posting racist insults from a journalist's account).	Online impersonation	Yes[1]	Yes	Yes	Yes	Yes1	Yes[1]	Yes	Yes	Yes	Yes[1]	No[6]
• Constant disruption of debates involving a journalist with an intent to cause them to feel distressed. • False advice, distortion of facts or mockery targeting a journalist through provocative messages (for example repeated mocking of a journalist's name). • Manipulation of users of a forum/social network to get them to turn against a journalist.	Trolling	Yes[1]	No[3]	No[3]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	No	No[3]	Yes[1]	Yes[1]
• Hacking of a journalist's website, account or electronic device and threatening to leak them if the journalist does not pay a sum of money.	Threat	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
• Coordinated behaviour by several users acting as a group to harm a journalist, for example through any of the aforementioned attacks.	Cyberstalking Brigading	Yes[1]	No[3]	Yes[1]	Yes	Yes	Yes[1]	Yes[1]	No	No[3]	Yes1	Yes[1]

1 There is no specific legislation regarding this type of behaviour. It is only sanctioned under general provisions.
2 Only if the information is of a confidential nature, a private document or a document under seal.
3 Other specific national criminal legislation might however apply, see relevant section.
4 However, under the Hate Speech Law, this only applies to hate speech made on the grounds that a person or their ancestor come from a country other than Japan.
5 Limited to certain categories of individuals (e.g. US officials, jurors, informants), see relevant section.
6 There is no federal legislation, however nine states (including New York, California and Texas) have online impersonation laws.



REUTERS/David W Cerny

AUSTRALIA

1. PRELIMINARY CONSIDERATIONS:

A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

In the context of online harassment, there are limited circumstances in which a media organisation (as opposed to a journalist) will have standing to take legal action.

For example:

- **Defamation**: A media organisation will only have standing to sue for defamation if they have fewer than 10 full-time employees[1] (unless they are a non-for-profit and not a public body).
- **Injurious falsehood**: A media organisation may have standing to sue for injurious falsehood where a person:
    - makes a false statement regarding the media organisation's business;
    - the statement is made with malice (generally an improper motive); and
    - the statement leads to actual loss, such as a loss of a customer or contract as opposed to some general loss such as loss of reputation.

  However, it is typically difficult to succeed on an injurious falsehood claim.
- **Misleading and deceptive conduct:** A media organisation may have standing to sue for misleading and deceptive conduct where a statement is made that is misleading or deceptive (or is likely to be so) and is made in trade or commerce.
- **Civil matters:** To show standing in other civil matters related to vilification and harassment, a media organisation must demonstrate that the harassment is impacting a private right of the organisation, or that they have a special interest in protecting their employees, in order to have standing before a court. A special interest must be more than merely an intellectual or emotional interest. It must be an interest in the matter of a kind that separates the media organisation from the rest of the public. A media organisation will not have standing unless it can be shown that they are likely to obtain some advantage, other than the mere satisfaction of righting a wrong or upholding a principle.
- **Criminal matters:** Both individuals and organisations may lodge police reports and seek a police investigation. However, in practice, it is typically difficult for a person to engage in and/or succeed in criminal prosecution unless a victim is identified and is able to testify.

B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

Commencing legal proceedings and extradition

Assuming the harasser can be identified, there are two options available to an individual seeking formal legal recourse:

- Commence legal proceedings in Australia; or
- Commence legal proceedings in the foreign jurisdiction that the harasser is located in.

It is possible to commence proceedings against foreign individuals in Australian courts. However, even if it is assumed that the harasser can be identified (see question 3 below for more information on identification), it remains difficult to enforce any orders made by Australian courts against the foreign individual. This is because if the harasser that is subject to a court's orders has no assets in Australia, it is virtually impossible to obtain any compensation from them. Furthermore, if the harasser is located in a foreign jurisdiction, an Australian court order to cease the harassing activity would have little to no effect.

It is also possible to launch new proceedings in the foreign jurisdiction that the harasser is located in. However, the ability to commence the proceedings and prospects of success of such proceedings will ultimately depend on the laws of that foreign jurisdiction. It should also be noted that any proceeding in court will incur legal and administrative costs. This, combined with the uncertainty of identifying a harasser and enforcing court orders, renders the avenue of seeking court remedies as a complex solution.

In respect of criminal charges, the Extradition Act 1988 (Cth) provides the legislative basis in Australia for extradition and sets out mandatory requirements in order for Australia to accept or make an extradition request. Australia has bilateral extradition treaties and/or agreements with multiple countries including, but not limited to, the US, Switzerland, Hong Kong and Brazil.

Evidence gathering

Australia is a party to various Mutual Legal Assistance Treaties (MLATs) which provide a formal process of sharing evidence relating to criminal investigations or prosecutions between countries. Australia is a party to bilateral MLATs with multiple countries including, but not limited to, the UK, the US, Hong Kong and China.

Enforcing foreign judgments

Australia is not a party to MLATs concerning the recognition of or enforcement of foreign judgments such as the Hague Convention on Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters 1971 and the Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters 2019 (except with the UK and New Zealand). However, it is possible to seek the enforcement of an Australia court's judgment in foreign jurisdictions, or enforce applicable criminal and civil foreign judgments in Australia under the Foreign Judgments Act 1991 (Cth), the corresponding regulations, the Foreign Proceedings (Excess of Jurisdiction) Act 1984 (Cth) and the Trans-Tasman Proceedings Act 2010 (Cth).

Enforcement of an Australian court judgment in a foreign jurisdiction may be assisted by obtaining a letter of request from the Australian court that made the order that a foreign court grant the relevant orders in the foreign jurisdiction. However, this avenue is a typically complex process and depends on the jurisdiction where enforcement of the Australian judgment is being sought.

Enforcement of a foreign judgment in Australia is limited to, among other requirements, judgments or orders given or made in civil proceedings, and judgments or orders given or made in criminal proceedings for the payment of a sum of money. In instances when there is no international or statutory agreement, the foreign judgment must be enforced under Australian common law principles.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

There are no specific laws in Australia which deal with the online harassment of journalists. However, there is legislation at a Federal, State and Territory level which may provide recourse for online harassment that journalists may be able to employ.

Federal

The table below provides a breakdown of certain Federal laws which are relevant to online harassment and the jurisdictions that those laws operate in.

LEGISLATION	RELEVANT PROVISIONS		MAXIMUM PENALTIES
Criminal Code Act 1995 (Cth)	Section 11.4	Incitement of an offence.	If the offence incited is : • punishable by life imprisonment - imprisonment for up to 10 years; • punishable by imprisonment for 14 years or more - imprisonment for up to 7 years; • punishable by imprisonment for 10 years or more - imprisonment for up to 5 years; • otherwise punishable by imprisonment - imprisonment for up to 3 years or for the maximum term of imprisonment for the offence cited (whichever is lesser). If the offence is not punishable by imprisonment - a fine up to the amount equal to the maximum fine payable applicable to the offence incited.
	Section 474.14	Using a telecommunications network with the intention to commit a serious offence.	Punishable by a penalty not exceeding the penalty applicable to the serious offence itself.
	Section 474.15	Using a carriage service to make a threat.	• For a threat to kill - imprisonment for up to 10 years; • For a threat to cause serious harm - imprisonment for up to 7 years.
	Section 474.16	Using a carriage service for a hoax threat.	Imprisonment for up to 10 years.
	Section 474.17	Using a carriage service to menace, harass or cause offence. An aggravated offence in relation to non-consensual sharing of intimate images exists under Section 474.17A.	• Generally. imprisonment for up to 3 years; • Standard aggravated offence - imprisonment for up to 5 years; • Special aggravated offence - imprisonment for up to 7 years.
	Section 474.29A	Using a carriage service for suicide related material.	Up to AUS$ 222,000 fine.
Racial Discrimination Act 1975 (Cth)	Section 18C provides that it is unlawful to act in a way that is reasonably likely in all the circumstances to offend, insult or intimidate another person or group of people and is done because of the race, colour or national or ethnic origin of the other person.		Complaints are made to the Australian Human Rights Commission. If the complaint remains unresolved, an application may be made to the Federal Court.

LEGISLATION	RELEVANT PROVISIONS		MAXIMUM PENALTIES
Online Safety Act 2021 (Cth) **(Commencing 23 January 2022)**	Section 75	End-user posting, or threatening to post, an intimate image without the consent of the person depicted in the image.	Up to AU$111,000 in fines for individuals, and AU$555,000 for a body corporate. The eSafety Commissioner ('Commissioner') may also issue a formal warning and begin an investigation where a complaint is received in relation to a contravention of this section.
	Section 77	Provider of online services with the sole or primary purpose of enabling online social interaction between end-users ('Social Media Service'), electronic services that allow end-users to communicate with other end-users ('Relevant Electronic Service'), or internet carriage services to the public ('Designated Internet Service') providing an intimate image without the consent of the person depicted.	The Commissioner may issue a removal notice requiring the removal of the intimate image or cyber-abuse material from the service within 24 hours. The Commissioner will generally only provide such notice if the material was already the subject of a complaint made to the service provider, end-user, or host, and the Prohibited Content has not been removed within 48 hours. However, in its discretion, the Commissioner may provide a removal notice without an individual's complaint. If the removal notice is not complied with to the extent the person is capable of doing so, there is a civil penalty of up to AU$111,000 in fines for individuals, and AU$555,000 for a body corporate. The Commissioner may also issue a formal warning.
	Section 78	End-user of a Social Media Service, Relevant Electronic Service, or Designated Internet Service posting an intimate image without the consent of the person depicted.	
	Section 79	Hosting service provider hosting an intimate image without the consent of the person depicted.	
	Section 88	Provider of a Social Media Service, Relevant Electronic Service, or Designated Internet Service providing cyber-abuse material targeted at an Australian adult.	
	Section 89	End-user of a Social Media Service, Relevant Electronic Service, or Designated Internet Service posting cyber-abuse material targeted at an Australian adult .	
	Section 90	Hosting service provider hosting cyber-abuse material targeted at an Australian adult.	

State and Territory

Each state and territory jurisdiction has separate laws relevant to online harassment. Whilst the laws are not identical across all states, most states have largely similar protections in the areas of law outlined in the table below. It should be noted that under state and territory laws, the anti-discrimination and vilification legislation related to online harassment provides that discriminatory/vilifying behaviour will only amount to an offence if it occurred in the public domain.

AREA OF LAW	LEGISLATIVE PROVISION		MAXIMUM PENALTIES
Stalking & Threats	New South Wales (NSW)	Crimes (Domestic and Personal Violence) Act 2007 (NSW) at Sections 8 and 13 (stalking or intimidation with intent to cause fear of physical or mental harm).	Imprisonment for up to 5 years or a fine of up to $11,100 (or both).
		Crimes Act 1900 (NSW) at Sections 31 (documents containing threats) and 545B (intimidation or annoyance by violence or otherwise).	• Documents containing threats - imprisonment for up to 10 years; • Intimidation or annoyance by violence or otherwise - imprisonment for up to 2 years or a fine of up to $11,100 (or both).
	Victoria	Crimes Act 1958 (Vic) at Sections 20 (threats to kill), 21 (threats to inflict serious injury), and 21A (stalking).	• Threats to kill - imprisonment for up to 10 years; • Threats to inflict serious injury - imprisonment for up to 5 years; • Stalking - imprisonment for up to 10 years.
	Queensland	Criminal Code Act 1899 (Qld) at Sections 308 (threats to murder in document), 359 (threats), and 359A to 359F (stalking).	• Threats to murder in a document - imprisonment for up to 7 years; • Threats - imprisonment for up to 5 years; • Stalking - imprisonment for up to 5 years (up to 7 years if the person also uses/threatens violence against property, possesses a weapon or contravenes/threatens to contravene an injunction imposed by the court).
	South Australia	Criminal Law Consolidation Act 1935 (SA) at Sections 19 (threats) and 19AA (stalking).	• Threats - imprisonment for up to 10 years (aggravated offence is up to 12 years); • Stalking - imprisonment for up to 3 years (aggravated offence is imprisonment for up to 5 years).
	Tasmania	Criminal Code Act 1924 (Tas) at Sections 162 (threats to kill in writing) and 192 (stalking).	The maximum penalty for all crimes other than murder and treason and subject to the *Sentencing Act 1997* (Tas) is imprisonment for up to 21 years.

AREA OF LAW	LEGISLATIVE PROVISION		MAXIMUM PENALTIES
	Western Australia	Criminal Code Act Compilation Act 1913 (WA) at Sections 338A to 338C (threats) and 338D to 338E (stalking).	• Threats to kill- imprisonment for up to 10 years (aggravated offence is up to 14 years); • Other threats - imprisonment for up to 7 years (aggravated offence is up to 10 years).
	Australian Capital Territory (ACT)	Crimes Act 1900 (ACT) at Sections 30 (threat to kill), 31 (threat to inflict grievous bodily harm), and 35 (stalking).	• Threats to kill - imprisonment for up to 10 years; • Threat to inflict grievous bodily harm - imprisonment for up to 5 years; • Stalking - imprisonment for up to 2 years (up to 5 years if stalking involved contravening an injunction or possession of offensive weapon).
	Northern Territory	Criminal Code Act 1983 (NT) at Sections 166 (threats to kill) and 189 (stalking).	• Threats to kill - imprisonment for up to 7 years; • Stalking - imprisonment for up to 2 years (up to 5 years if stalking involved contravening an injunction or possession of offensive weapon).
Anti-Vilification and Racial Discrimination	NSW	Anti-Discrimination Act 1977 (NSW) at Sections 20C, 38S, 49ZT & 49ZXB (unlawful vilification).	Complaints are dealt with by the Anti-Discrimination Board of NSW.
		Crimes Act 1900 (NSW) at Section 93Z (criminal offence for public threats or inciting violence on discriminatory grounds).	For an individual - imprisonment for up to 3 years or fine of up to $22,200 (or both). For a corporation - fine of up to $111,000.
	Victoria	Racial and Religious Intolerance Act 2001 (Vic) at Section 7, 8, 24 & 25 (unlawful vilification).	Complaints are dealt with by the Victorian Equal Opportunity & Human Rights Commission or the Victorian Civil and Administrative Tribunal.
	Queensland	Anti-Discrimination Act 1991 (Qld) at Section 124A, s 131A.	Complaints are dealt with by the relevant state Anti-Discrimination Board/Commission (or equivalent).
	South Australia	Racial Vilification Act 1996 (SA) at Section 4 (racial vilification).	Complaints are dealt with by the relevant state Anti-Discrimination Board/Commission (or equivalent).
	Tasmania	Anti-Discrimination Act 1998 (Tas) at Section 19 (public act inciting hatred, serious contempt or severe ridicule on the basis of race, disability, sexual orientation, religion or gender identity).	Complaints are dealt with by the relevant state Anti-Discrimination Board/Commission (or equivalent).

AREA OF LAW	LEGISLATIVE PROVISION		MAXIMUM PENALTIES
	Western Australia	Criminal Code Compilation Act 1913 (WA) at Sections 77 (intentionally inciting racial animosity or harassment), 78 (conduct likely to incite racial animosity or harassment) and 80A (intentional racial harassment).	• Inciting racial animosity or harassment - imprisonment for up to 14 years. • Conduct likely to incite racial animosity or hatred - imprisonment for up to 5 years (summary penalty of imprisonment for up to 2 years and a fine of up to $24,000). • Intentional racial harassment - imprisonment for up to 5 years (summary penalty of imprisonment for up to 2 years and a fine of up to $24,000).
	ACT	Discrimination Act 1991 (ACT) at Section 67A (unlawful vilification).	Complaints are dealt with by the relevant state Anti-Discrimination Board/Commission (or equivalent).
	Northern Territory	Anti-Discrimination Act 1992 (NT) at Section 19 (prohibition on discrimination against race, sex, sexuality, among others). NB: there is no separate anti-vilification provision in the Northern Territory, however Section 19 functions as a general anti-discrimination provision.	Complaints are dealt with by the relevant state Anti-Discrimination Board/Commission (or equivalent).
Non-consensual sharing of intimate images	All states and territories	Each of the states and territories prohibit distributing or threatening to distribute intimate images without consent in their respective Crimes Act, Criminal Code or Summary Offences Act.	Depends on state/territory legislation. For example, in NSW, imprisonment for up to 3 years or a fine of up to $22,200 (or both).
Defamation	All states and territories	• Uniform defamation laws exist across the states and territories which make it an offence to publish something that has the consequence of: • Exposing the person to ridicule; • lowering the person's reputation in the eyes of the community; • causes people to shun or avoid the person; or • injures the person's professional reputation. Criminal offences for defamation also exist under state and territory legislation but are rarely used and have not been used in the prosecution of individuals harassing journalists.	• Damages generally considered in civil jurisdiction.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

The following laws may apply to online threats, depending on the type of threat(s) made:

- **Threats & Stalking Legislation**: There is legislation to protect against threats at both a Federal (Criminal Code Act 1995 (Cth) s 474.15-16 and the Online Safety Act 2021 (Cth) s 75) and State/ Territory level. For example, in 2019, an individual was charged in the state of New South Wales with the criminal offence of using a carriage service to threaten serious harm and using a carriage service to menace, harass or offend after he was alleged to have made repeated and explicit violent threats against a Melbourne journalist and lawyer. See ***Threats & Stalking*** section in the table provided at Question 2(a) above.
- **Racially Motivated Threats**: A separate offence exists under NSW legislation which prohibits inciting violence on discriminatory grounds. In practice, this provision is typically used by individuals against news media organisations in relation to published Articles, rather than cases in which a journalist is the alleged victim of discrimination.[2]
- **Tort**: If a direct threat made by a person causes a reasonable fear of imminent physical contact with the person who made the threat, it may be possible to sue the maker of the threat for assault under Australian tort law. Australian courts have not recognised a common law cause of action for harassment.

II. INTIMIDATION:

The laws which may apply will depend on the specific facts of the intimidating behaviour on a case by case basis, where some forms of intimidation may overlap with laws applicable to threats (as outlined above at Question 2(b)).

At a Federal level, Section 18C of the Racial Discrimination Act 1975 (Cth) makes it unlawful to act in a way that is reasonably likely in all the circumstances to intimidate another person or group of people on the basis of race, colour or national or ethnic origin. Similarly, Section 91 of the Online Safety Act 2021 (Cth) (which commences 23 January 2022) makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued. See the table above at Question 2(a).

III. CYBERSTALKING:

At a Federal level, Section 474.17 of the Criminal Code Act 1995 (Cth) makes it an offence to use a carriage service to menace or harass. Furthermore, laws protecting against stalking at a State/ Territory level will also generally apply to cyberstalking. In practice, Australian police will generally caution or warn an offender in the first instance. See the table above at Question 2(a). Section 91 of the Online Safety Act 2021 (Cth) makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued. See the table above at Question 2(a).

IV. DOXXING:

At a Federal level, doxxing is broadly covered by Section 474.17 of the Criminal Code Act 1995 (Cth) which makes it an offence to use a carriage service to menace or harass. Similarly, Section 91 of the Online Safety Act 2021 (Cth) makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued. See the table above at Question 2(a).

V. ONLINE IMPERSONATION:

The relevant law will depend on the specific facts of the impersonating behaviour on a case by case basis. Whilst there are laws which prohibit using someone else's identity to conduct fraud (Criminal Code Act 1995 (Cth) Part 9.5) and criminalise hacking a computer (Criminal Code Act 1995 (Cth) Division 477.1), there are no specific laws which make impersonating someone online unlawful. Depending on the behaviour, it is possible that online impersonation could fall within the scope of Section 474.17 of the Criminal Code Act 1995 (Cth) which makes it an offence to use a carriage service to menace or harass or Section 91 of the Online Safety Act 2021 (Cth) which makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued.

VI. TROLLING:

The relevant law will depend on the specific facts of the trolling behaviour on a case by case basis.

In the event the trolling can be characterised as abusive in nature, it is possible that it will be covered by Section 474.17 of the Criminal Code Act 1995 (Cth) which makes it an offence to use a carriage service to menace or harass or Section 91 of the Online Safety Act 2021 (Cth) which makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued. Examples of prosecutions under the Criminal Code Act 1995 (Cth) include posting offensive pictures and comments on Facebook tribute pages,[3] posting menacing messages on Facebook[4] and sending repeated menacing emails.[5]

If the trolling can be characterized as abuse that is racially motivated, it may be an offence under Section 18C of the Racial Discrimination Act (Cth). Where the trolling can be characterised as discriminatory on other grounds, state and territory anti-discrimination laws described in the table above at Question 2(a) may prohibit such behaviour.

Finally, if the trolling can be characterised as being designed to spread false information about an individual, it may provide grounds for a defamation claim being brought under state/ territory legislation as described in the table above at Question 2(a).

VII. BRIGADING:

There are no specific laws in Australia that protect against brigading behaviour. However, it may be possible for brigading to fall within Section 474.17 of the Criminal Code Act 1995 (Cth) which makes it an offence to use a carriage service to menace or harass or Section 91 of the Online Safety Act 2021 (Cth) which makes it an offence for a service provider, end-user, or host to fail to remove material regarded as menacing, harassing, or offensive with the intention of causing serious harm to a particular person where a removal notice has been issued. It may also be possible to categorise brigading under incitement and conspiracy offences under Sections 11.4 and 11.5 of the Criminal Code Act 1995 (Cth) if the perpetrators are encouraging others to engage in harassing behaviour. Furthermore, if the brigading can be characterised as including the use of threats and/ or stalking, it will be possible to use the Federal and state laws described in the table above at Question 2(a).

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

See table above in Question 2(a).

As an illustrative example, the case of *Jones v Toben* [2002] FCA 1150 successfully applied Section 18C of the Racial Discrimination Act 1975 (Cth) in the context of online harassment. In this case, it was held that the respondent published material on a website that denied the Holocaust and vilified Jewish people. The Federal Court of Australia found that the publication of such material was unlawful under Section 18C and ordered the offensive material to be removed from the internet.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

See the ***Anti-Discrimination and Vilification*** section of the table above at Question 2(a). Under state/ territory laws, the anti-discrimination and vilification laws related to online harassment only make the discriminatory/ vilifying behaviour an offence if it occurred in the public domain.

Specifically, in New South Wales, Queensland, South Australia, the relevant conduct is only an offence where the conduct is considered a 'public act'. For the purposes of the relevant legislation as outlined above in Question 2(a), this includes communication to the public and any conduct observable by the public. Dissemination of any matter to the public is also considered a public act in the jurisdictions of New South Wales and Tasmania.

Similarly, in Victoria and Western Australia, it is an exception to the offence where the conduct is considered to be 'private', i.e. occurring in circumstances in which it is reasonably expected that the conduct may not be heard or seen by someone else.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Whilst Australia has a constitutional right to freedom of political expression, it does not have an explicit right to freedom of speech. Therefore, no such example exists where anti-harassment/discrimination laws have been found to conflict with freedom of speech laws.

However, in 2017 the Federal government attempted to repeal Section 18C of the Racial Discrimination Act 1975 (Cth) on the basis that it was too broad and therefore infringed on the ability to speak freely. The attempt to repeal it was unsuccessful.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

The prevalence of fake accounts and the common use of VPNs makes it particularly difficult to identify anonymous harassers online, including to identify the location of the computer or individual responsible for online harassment.

However, recent developments have demonstrated that it is possible to require organisations, including large technology companies, to identify certain information about online harassers if such information is in (or was in) their control. In a recent Federal Court case, *Kabbabe v Google LLC* [2020] FCA 126, an individual plaintiff was successful in obtaining orders in an Australian court that required Google LLC to discover the personal details (by way of information such as names, phone numbers, metadata and IP addresses) of an anonymous account that allegedly engaged in defamatory behaviour. The Court held that the plaintiff was entitled to require Google to discover a document or thing in its control to the plaintiff, which included personal information of an internet user who had allegedly left a defamatory review about the plaintiff's dental business.

PRACTICAL INFORMATION

Websites:

- Report harassment to the eSafety Commissioner.
- Lodge a police report with the relevant Federal, state and territory police force, who respectively have powers under various criminal and other legislation to request or compel organisations to provide certain information and/or documents, and/or to issue search and arrest warrants.

Phone numbers:

- Call "000" (the national emergency line in Australia) in an emergency or if a person in Australia is in immediate danger.

Other Options

- Seek legal advice on compelling internet service providers and hosts of social media websites/forums to reveal the IP address and identity of harassers.
- Block and report fake/troll accounts or harassing material to the relevant social media provider (Facebook, Twitter, Instagram etc.) through their respective complaints processes.

BRAZIL

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

In Brazil, there are three types of criminal actions:

- Unconditional public prosecution, in which the Public Prosecutor's Office must prosecute the defendant, even if the victim has no interest in the criminal action;
- Conditioned public prosecution**,** in which the victim has 6 months to express interest in the investigation and/or criminal action for the Public Prosecutor's Office to file the case against the defendant; and
- Private prosecution, in which the victim or its representative has 6 months to file the criminal complaint. In both conditioned public prosecution and private prosecution, the statute of limitation starts from the moment the perpetrator is identified.

Most of the cybercrimes against journalists are subject to private prosecution or conditioned public prosecution. It is therefore up to the journalists themselves to take an active role in the prosecution, with the media organisation having no standing in these cases.

Where the crime committed against the journalist is subject to unconditional public prosecution, any person, including media organisations, may file a request for the opening of investigations.

Media organisations can also be victims of online crimes, such as slander. In such case, they may request the opening of investigations or file a private criminal action. Media organisations may also bring actions for moral damages (pain and suffering) when they themselves are the target of online harassment. Damages will only be awarded to organisations that can prove that their image, reputation or market value were affected by the online harassment.

It is also worth mentioning that moral damages (pain and/or suffering) can only be exercised by the person whose rights have been infringed. For this reason, media organisations have no standing to file civil lawsuits for moral damages on behalf of a journalist.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

In general, Brazil only has jurisdiction to prosecute crimes committed in its territory. However, Brazilian law considers the location of a crime as the place where it took place or where the results occurred.

Brazil has signed the Budapest Convention regarding cybercrimes, which provides several measures that can be useful in the fight against cybercrimes, including more efficient tools for international cooperation and evidence sharing between countries.

Regarding civil matters, there is no specific international legislation regarding illegal acts perpetrated on the internet. This does not mean that a journalist cannot submit a claim against the individual that committed this illegal act. According to Brazilian case law, even if the illegal act is perpetrated on the internet, Brazil has jurisdiction to analyse the claim if the origin of the illegal act can be traced back to a computer/means of communication to the internet that is located in the Brazilian territory.

In this scenario, the illegal act is assumed to have been perpetrated in Brazil. Therefore, Brazilian Courts have jurisdiction to rule these civil claims, as established by the Brazilian Civil Procedure Code (Law 13.105/2015): "Article 21. Brazilian courts have jurisdiction to try actions in which: III – the grounds are facts that that occurred, or acts that were performed, in Brazil".

Even though Brazilian Courts have jurisdiction to rule on these civil claims, all procedures related to process, and enforcement of the decision would rely on letters of rogatory and international treaties between Brazil and the country of residence of the defendant.

Similarly, all evidence production and gathering would have to follow the Brazilian Civil Procedure rules, which provide that it is the plaintiff's burden to prove the alleged facts and rights. It should be noted that further evidence can be produced through letters of rogatory, such as the defendant's hearing, if it is deemed necessary by the Brazilian Court.

Evidence that cannot be obtained locally, may be obtained through international cooperation. Brazil has Mutual Legal Assistance Treaties ("MLATs") that involve evidence sharing with many countries such as China,[6] Colombia,[7] South Korea,[8] Cuba,[9] Spain,[10] USA,[11] France,[12] Honduras,[13] Italy,[14] Mexico,[15] Nigeria,[16] Panama,[17], Peru,[18] Poland,[19] Portugal,[20] United Kingdom,[21] Switzerland,[22] Suriname[23] and Ukraine.[24]

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

Regarding criminal law, there is no legislation dealing with online harassment. However, it is possible to charge someone for online harassment through some crimes provided by the Penal Code.

Regarding civil matters, there is also no specific legislation regarding online harassment. Therefore, the matter is regulated by the Brazilian Federal Constitution, the Brazilian Civil Code (Law n. 10.406) and the Brazilian Civil Rights Framework for the Internet (Law n. 12.965/2014).

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

Criminal threat is a crime under Article 147 of the Brazilian Penal Code (Decree Law n. 2.848/1940) and it is carried through a conditioned public prosecution.

In March 2018, the journalist Maíra Azevêdo was a victim of racial slurs and a death threat. Azevêdo contacted the police and requested the opening of investigations. With the help of the authorities, the person involved in the wrong doings was identified and turned himself in.[25] In October 2018, the journalist Anne Barretto requested the opening of police investigations to identify the author of a social media post containing rape threats.[26] No further information has been released on the progress or outcome of this case.

II. INTIMIDATION:

Criminal threat (see above) covers acts of intimidation.

III. STALKING (CYBERSTALKING):

In March 2021, Law n. 14.132/21 was enacted to establish the crime of stalking under Article 147-A of the Brazilian Penal Code. The crime may be committed by any means, including through the internet. Cyberstalking is subject to conditioned prosecution by the victim's criminal complaint.

IV. DOXXING:

There is no specific doxxing crime in Brazil. Nonetheless if the information being exposed is of a confidential nature, a private document, or a document under seal (such as bank extracts), then it can be considered as a crime under Articles 153 and 153, §1º of the Brazilian Penal Code. These crimes are carried through conditioned public prosecution. If the practice of Doxxing involves the improper disclosure of Personal Data, there will be an infringement of Federal Law n. 13.709/18, known as the Brazilian General Data Protection Law ("LGPD"). Although there is no provision for crimes, there are administrative sanctions that may be applied in case of non-compliance with the Law, if a Processing Party (Controller or Processor) is involved in the crime.

V. ONLINE IMPERSONATION:

Online impersonation may be considered the crime of false identity under Article 307 of the Brazilian Penal Code. This crime is carried through an unconditional public prosecution.

VI. TROLLING:

In Brazil, trolling is not a crime, except if someone commits any crime against the honour, such as: (i) calumny (to falsely accuse somebody of something defined as a crime); (ii) defamation (to spread statements that are offensive to someone's reputation); and (iii) insult (to offend someone's dignity). These crimes are carried through a private prosecution.

In 2015, the journalist Leonardo Moretti Sakamoto was a victim of defamation. A website with a slanderous title against him was being promoted through Google Adwords. Sakamoto filed a lawsuit against Google to identify the person who paid for the advertisement. To settle the matter, Google promptly presented IP addresses and e-mails of the individuals who paid for the advertisement.

VII. BRIGADING:

In Brazil, there is no law about brigading. Although, similar to trolling, individuals that partake may be held liable for crimes against honour.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

The laws mentioned above were not preconceived for online crimes. However, they can be used to prosecute harassment.

Regarding civil matters, the Brazilian Civil Code (Law n. 10.406) and the Brazilian Civil Rights Framework for the Internet (Law n. 12.965/2014) are used to identify the perpetrators of the online harassment.

Victims can file compensation lawsuits against the perpetrators of the online harassment listed above. In these lawsuits the victims may request repair of the damages incurred, such as material damages and moral damages (pain and/or suffering), as established by the Brazilian Federal Constitution: "Article 5, V – the right of reply is ensured, in proportion to the offense, as well as compensation for property or moral damages or for damages to the image".

If the perpetrator of the online harassment can be easily identified, the victim can request a civil judicial order for the perpetrator to cease the harassment, as well as request the right of reply or rectification of the information used to harass the victim, which needs to be carried out by the same media outlet used by the perpetrator.

Brazilian Courts can issue orders to determine that internet application providers (for example Facebook, Twitter, Instagram) must remove the post/content of the online harassment. Internet application providers can only be held liable if they do not comply with the judicial order, as established by the Brazilian Civil Rights Framework for the Internet: "Article 19 - In order to ensure freedom of expression and to prevent censorship, the provider of Internet applications can only be liable for civil damages arising out of content generated by third parties if it does not act, after specific court order, within the framework and technical limits of its services and timely mentioned, to make the content identified as infringing unavailable, except for contrary established statutory provisions". The exception involves the release of nudity or private sexual content of the victim. In this scenario the victim can request the removal of the content/post directly to the internet application provider, as provided by Article 21 from the Brazilian Civil Rights Framework.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Under Article 140, §3, of the Brazilian Penal Code, it is a crime to insult a person based on race, colour, ethnicity, religion or origin, disability, or age. While a regular insult may have a prison sentence of one to six months, in case of racial insult, the prison sentence may be of one to three years. Racial insults are subject to conditioned prosecution by the Victim's Criminal Complaint.

Regarding civil matters, there is no specific regulation regarding race or gender targeted by online harassment. However, discrimination on account of race or gender implies a serious offence against the personality, honour and image rights of the victim and privacy and data protection principles. Therefore, victims can submit a lawsuit against their perpetrators requesting moral (pain and/or suffering) damages.

Furthermore, it is worth highlighting that the amount of moral damages awarded may vary from case to case, considering the specificities of the case.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

The Brazilian Constitution provides in its Article 5, items IV and IX, that the "expression of thought is free and anonymity is forbidden"; and "the expression of intellectual, artistic, scientific, and communication activity is free, irrespective of censorship or license". In the same way, Article 220 provides that the "manifestation of thought, the creation, the expression and the information, in any form, process or medium shall not be subject to any restriction". In addition, the first paragraph of the same Article provides that "no law shall contain any provision which may represent a hindrance to full freedom of press in any medium of social communication".

Brazil previously had in place the Press Law (Law 5.250/1967), which was enacted during its military dictatorship. In April 2009, the Brazilian Supreme Court of Justice repealed this on the basis that it was unconstitutional. Nowadays, there is no legislation that breaches freedom of speech. However, freedom of speech is not an absolute right, and it can be limited in some situations if it violates other fundamental rights, such as the right of human dignity and honour. Therefore, freedom of speech cannot be used to spread hate or discriminatory ideas.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

In the virtual environment, anyone who connects to the internet must be linked to an IP address together with the period of the access (including the start and end dates), according to the guidelines of the Brazilian Civil Rights Framework for the Internet. Therefore, even in the event that the harasser is using an account with false data, it is possible to determine their approximate location through its IP address. Such information can be obtained by means of a criminal or civil court decision that orders the supply of data by the person responsible for keeping connection or internet application accesses records.

On civil matters the IP address can be obtained by filing an affirmative covenant or anticipated production of evidence lawsuit against the platform in which the harasser took action before the competent state court. These lawsuits can only be filed by the victim (journalist) or by the victim's close relatives if the victim is no longer alive. The Courts may grant an injunction to order the platform to disclose the personal data of the perpetrator. The IP address or any other information provided on these lawsuits may then be used to track down the harasser and link this information to the harassment perpetrated, consolidating the evidence necessary to claim damages against the harasser.

However, it is important to emphasize that the request for the provision of such data will only be granted if the interested party demonstrates: (i) evidence of the occurrence of an illegal act on the part of the user; (ii) motivated justification of the usefulness of the records requested for the purpose of investigation or evidence; and (iii) period to which the records refer, as established in Article 22 of the Brazilian Civil Rights Framework for the Internet.

On criminal matters, the IP address can be obtained through a police investigation. If the crime is either a private prosecution or conditioned private prosecution, the victim or the victim's close relatives if the victim is no longer alive, may request that the local police station open a police investigation. In all other cases, anyone may file a report and investigations may be opened even if there is no report. During the investigation, it is possible to make a request to the competent court to obtain the IP address involved in the wrongdoing.

Internet service providers are required to maintain such access records for a period of one year, unless requested by a police or administrative authority or the Public Ministry, which may require a longer custody period. Thus, it is recommended that the journalist who is a victim of cyberattacks pursues a legal solution quickly to avoid the possible disposal of the access record by the provider during the period of court analysis of the request.

It is recommended that victims keep all information related to the attack. The best way to keep the information is to request a notary act with all the relevant information that could be used in the investigation or in the civil lawsuit. This includes phone messages, e-mails and print screens of websites or social media. Printing or saving on the computer is also useful, but it is important to bear in mind that, without a notary act, such evidence may be questioned, as defendants may argue that the information is not original or was edited.

PRACTICAL INFORMATION

Websites:

- Brazilian Investigative Journalism Association
- Civil Rights Framework for the Internet - Federal Law no. 12,965/14
- Brazilian General Data Protection Law ("LGPD") – Federal Law no. 13,709/18

Phone numbers:

- 100 – Reporting channel for human rights violation
- 190 – Brazilian emergency phone number

FINLAND

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

There is no specific legislation that would give media organisations standing to take legal action as opposed to the journalists. However, the media organisation as an employer could be compelled to take measures in order to remedy certain situations such as harassment of employees (Section 28 of the Occupational Safety and Health Act (738/2002, as amended)). Pursuant to this Section, if harassment or other inappropriate treatment of an employee occurs at work and causes hazards or risks to the employee's health, the employer, after becoming aware of the matter, shall by all available means take measures for remedying this situation. Media organisations could also have standing in situations where they are able to prove that the online harassment in question has caused them damage.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

First, with respect to civil law, the Finnish Code of Judicial Procedure (4/1734, as amended) defines jurisdiction in civil cases in Finland. Pursuant to Chapter 10 Section 1 of the Code of Judicial Procedure, a claim against a natural person is considered by the district court with jurisdiction over the place where he or she has his or her domicile or habitual residence. Chapter 10 Sections 25 and 26 concern international jurisdiction. According to Section 25, a Finnish court is competent to consider a case with an international nature, if the case is connected to Finland in certain situations specified in the Act, unless the judgment to be given by the Finnish court in the case could clearly not have legal relevance for the parties. According to Section 26, a Finnish court shall consider on its own motion whether, in accordance with Section 25, it is competent to consider a case with an international nature.

However, it should be noted, that Chapter 10 Section 17 stipulates that the provisions of Chapter 10 regarding general jurisdiction apply, unless otherwise provided by another Act, legislation of the European Community or an international agreement binding on Finland.

In this respect, it should be stressed that the conflict of law rules in the European Union are set out in the Brussels 1 Regulation, which governs the recognition and enforcement of judgments in civil and commercial matters.[27] According to this Regulation, the competent jurisdiction in which to pursue a case is the one in which the defendant has its domicile or, in matters relating to tort, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez* (Cases C-509/09 and C-161/10), the Court of Justice of the European Union considered the conflict of law concerns relating to the alleged infringement of personality rights caused by the online publication of defamatory content. It held that Member State courts will have jurisdiction, where the impugned content is or has been accessible within their territory. However, this jurisdiction extends only to that damage which was caused to the plaintiff's reputation within their borders. Recognising that the impact of any infringement may best be assessed by the court in which the alleged victim has their "centre of interests", the CJEU held that "a person who has suffered an infringement of a personality right by means of the internet may bring an action in one forum in respect of all of the damage caused". As set out in paragraph 52 of the judgment, this "one forum" may be either the jurisdiction in which the victim has their habitual residence, or the Member State in which the publisher of the infringing content is established. The decision in this case has made it significantly easier for victims of online defamation to pursue civil remedies against their perpetrators.

It is worth mentioning that the Evidence Regulation[28] strengthens the cooperation of the courts of the Member States regarding the transmission of evidence in civil and commercial proceedings. This regulation speeds up the process of evidence sharing by providing the potential to directly transmit evidence between the courts.

Second, with respect to criminal law, the Criminal Code of Finland (39/1889, as amended) applies only to crimes that are considered to have been committed in Finland according to Chapter 1 Section 1 of the Criminal Code. However, pursuant to Chapter 1 Section 10 of the Criminal Code, an offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent. This means that online attacks happening outside of Finland could be prosecuted in Finland, provided their consequence contained in the statutory definition of the offence is proven to have taken place in Finland. It should also be noted that pursuant to Chapter 1 Sections 5 and 6 of the Criminal Code, Finnish law could be applied to a crime committed outside of Finland if the crime has been directed at a Finnish citizen or a Finnish citizen committed it.

It is worth mentioning that judicial co-operation has been strengthened within the European Union. Indeed, any Member State may issue a judicial decision (known as a "European investigation order") requesting another Member State to carry out investigations on its territory within a certain period of time in order to obtain evidence relating to a criminal offence or to communicate evidence already in its possession.[29]

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

There is no specific legislation dealing with online harassment. However, different violations of the Criminal Code of Finland (39/1889, as amended), Occupational Safety and Health Act (738/2002, as amended) and Non-discrimination Act (1325/2014, as amended) could apply to online harassment targeting journalists depending on the type of harassment in question. Especially some of the offences against privacy, public peace and personal reputation and offences against personal liberty and data and communications listed in Chapters 24, 25 and 38 of the Criminal Code could be used to deal with online harassment. The potentially applicable offences include the following:

Harassing communications (Chapter 24, Section 1(a)) (879/2013)

A person who, with intent to disturb, repeatedly sends messages or calls another so that the act is conducive to causing said other person considerable disturbance or harm, shall be sentenced for harassing communications to a fine or to imprisonment for at most six months.

Dissemination of information violating personal privacy (Chapter 24, Section 8) (879/2013)

A person who unlawfully (i) through the use of the mass media or (ii) otherwise by making available to many persons disseminates information, an insinuation or an image of the private life of another person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for dissemination of information violating personal privacy to a fine.

The spreading of information, an insinuation or an image of the private life of a person in politics, business, public office or public position, or in a comparable position, does not constitute dissemination of information violating personal privacy, if it may affect the evaluation of that person's activities in the position in question and if it is necessary for the purposes of dealing with a matter of importance to society.

Presentation of an expression in the consideration of a matter of general importance shall also not be considered dissemination of information violating personal privacy if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

Defamation (Chapter 24, Section 9) (879/2013)

A person who (i) spreads false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt or (ii) disparages shall be sentenced for defamation to a fine. Also a person who spreads false information or a false insinuation about a deceased person, so that the act is conducive to causing suffering to a person to whom the deceased was particularly close, shall be sentenced for defamation.

Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in comparable public activity and that does not obviously exceed the limits of propriety does not constitute defamation. Presentation of an expression in the consideration of a matter of general importance shall also not be considered defamation if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

Menace (Chapter 25, Section 7) (578/1995)

A person who raises a weapon at another or otherwise threatens another with an offence under such circumstances that the person so threatened has justified reason to believe that his or her personal safety or property or that of someone else is in serious danger shall, unless a more severe penalty has been provided elsewhere in law for the act, be sentenced for menace to a fine or to imprisonment for at most two years.

Stalking (Chapter 25, Section 7(a)) (879/2013)

A person who repeatedly threatens, observes, contacts or in another comparable manner unjustifiably stalks another so that this is conducive towards instilling fear or anxiety in the person being stalked, shall, unless an equally or a more severe penalty is provided elsewhere in law for the act, be sentenced for stalking to a fine or to imprisonment for at most two years.

Message interception (Chapter 38, Section 3) (368/2015)

A person who unlawfully (i) opens a letter or another closed communication addressed to another or by hacking obtains information on the contents of an electronic or other technically recorded message which is protected from outsiders, or (ii) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable tele message transmitted by telecommunications or an information system or on the transmission or reception of such a message shall be sentenced for message interception to a fine or to imprisonment for at most two years.

An attempt is punishable.

Interference with communications (Chapter 38, Section 5) (578/1995)

A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for interference with communications to a fine or to imprisonment for at most two years.

An attempt is punishable (540/2007).

Interference in an information system (Chapter 38, Section 7(a)) (368/2015)

A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for interference in an information system to a fine or to imprisonment for at most two years.

An attempt is punishable.

Computer break-in (Chapter 38, Section 8) (368/2015)

A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a computer break-in to a fine or to imprisonment for at most two years.

Also a person who, without hacking into the information system or a part thereof, (i) by using a special technical device or (ii) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in.

An attempt is punishable. This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

Identity theft (Chapter 38, Section 9(a)) (368/2015)

A person who in order to deceive a third party unlawfully uses the personal information, access codes or other corresponding identifying information of another and in this manner causes economic loss or more than petty impediment to the person to whom the information belongs, shall be sentenced for identity theft to a fine.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

Threats could constitute the following offences: Menace (Criminal Code, Chapter 25 Section 7) and Stalking (Criminal Code, Chapter 27, Section 7(a)).

II. INTIMIDATION:

Intimidation could constitute the following offences: Menace (Criminal Code, Chapter 25, Section 7) and Stalking (Criminal Code, Chapter 27, Section 7(a)).

III. CYBERSTALKING:

Cyberstalking could constitute Stalking (Criminal Code, Chapter 27, Section 7a).

IV. DOXXING:

Doxxing could constitute a number of offences depending on how the information has been acquired and what information is being disseminated. Most likely it could constitute dissemination of information violating personal privacy (Criminal Code, Chapter 25, Section 8 and 8(a)).

V. ONLINE IMPERSONATION:

Online impersonation could constitute identity theft defined in Chapter 38 Section 9 (a) of the Criminal Code.

VI. TROLLING:

Finnish legislation does not recognise trolling as an offence, but such activity could constitute the following offences: Stalking (Criminal Code, Chapter 25, Section 7a) and Defamation (Criminal Code, Chapter 24, Section 9).

VII. BRIGADING

Depending on the activity, brigading could constitute the following offences: Menace (Criminal Code, Chapter 25 Section 7) and Defamation (Criminal Code, Chapter 24, Section 9).

The offences described above are primarily complainant offences, i.e. the police will not investigate the offence unless the injured party demands punishment. However, there is currently a legislative amendment in preparation, which would make menace an offence subject to public prosecution meaning that a prosecutor could press charges even if the injured party does not demand punishment.

In addition, the injured party can seek damages pursuant to Chapter 5 Section 6 of the Tort Liability Act (412/1974, as amended).

The main issue with the offences described above appears to be that proving the elements of such crimes requires a lot of evidence and the elements, as they are written in the Criminal Code of Finland, do not necessarily fit that well into the modern practices of online attacks. For example, in order for online shaming to be considered stalking it would need to happen repeatedly and target the same person. It is also difficult to identify the online attackers reliably as, for example, just finding out the IP-address of the user sending offensive messages does not necessarily prove the identity of the person who actually sent the messages.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

There is one known case where the offences of stalking, aggravated defamation and instigated defamation were used to charge for online harassment of a journalist. The defendant intentionally gave false information regarding the journalist in question for four articles which were published in Russian online publications. The defendant characterised the journalist for example as a "known representative of the American-Baltic special services". The defendant also persuaded a newspaper to publish defamatory material on the journalist. The defendant was later found guilty on appeal only for instigated aggravated defamation. Charges for stalking and aggravated defamation were dismissed. At this stage, the Supreme Court of Finland has granted the journalist the right to appeal the Court of Appeal's decision to dismiss the charge of stalking.

In other situations that have not involved journalists, stalking, menace, defamation have been frequently used in cases of online harassment. However, most cases involve relationships of private people. Cases involving public figures like politicians typically include arguments of freedom of speech.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

When race is a factor in the abuse, in addition to the criminal proceedings which could follow, the abuse could be a violation of the Non-discrimination Act of Finland (as amended, 1325/2014). In such situations the journalist can also turn to the Non-discrimination Ombudsman of Finland. The Non-discrimination Ombudsman of Finland can counsel, investigate individual cases, promote conciliation, provide training, gather information and provide legal assistance.

When gender is a factor in the abuse, it could be a violation of the Act on Equality between Women and Men (609/1986, as amended). In such situations the journalist can turn to the Equality Ombudsman of Finland. The Equality Ombudsman of Finland can take actions if, for example, a woman journalist is being harassed due to her gender in their work and is therefore put in a worse working condition than men.

It is important to note that if the harassment is in violation of Section 28 of the Occupational Safety and Health Act, such actions could be reported to the Regional State Administrative Agencies' Divisions of Occupational Safety and Health. The Occupational Safety and Health Authority can provide instructions and advice and order the employer to act on a report of harassment. Contacting the Non-discrimination or Equality Ombudsman of Finland or the competent Regional State Administrative Agency could be relevant especially if the journalist is being targeted by online harassers and the employer of the journalist is not remedying the situation as they should pursuant to Section 28 of the Occupational Safety Act referred to in question 1 above.

Furthermore, if race is a factor in the abuse, the harasser can be charged with ethnic agitation pursuant to Chapter 11 Sections 10 and 10 (a) of the Criminal Code. In addition, it is worth noting that pursuant to Chapter 6 Section 5 of the Criminal Code, committing an offence for a motive based on race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or another corresponding ground can be grounds for the court to increase the punishment. Related to this, the current government has made a proposal (HE 7/2021) for amending Chapter 6 Section 5 of the Criminal Code to also include gender motivated offences as potential grounds to increase the punishment.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Freedom of speech arguments are usually seen used as a defence, especially in defamation cases. However, the Finnish courts have historically emphasized in their cases the protection of personal privacy and honour whereas the European Court of Human Rights (ECHR) has emphasized freedom of speech. However, it is worth noting that the courts have repeatedly found that racism or hate speech are not protected by freedom of speech.

As an example, the Supreme Court of Finland handled a case regarding the offence of dissemination of information violating personal privacy in relation to freedom of speech in case *KKO 2018:81*. In this case, A had videotaped two minor children being taken into care. B had later, upon request of A, published the video online from which the children were identifiable even though their faces had been blurred. The Supreme Court of Finland viewed publishing the video to be related to a public interest, but that it had, however, clearly crossed the line of what can be considered acceptable. A and B were found guilty of disseminating information violating personal privacy.

In case *KKO 2018:51* a person had published B's photo on an open Facebook page advocating for victims of paedophilia and linked it to a news story online which stated that B had four months earlier been convicted of aggravated sexual abuse of a child. In respect of freedom speech, the court stated, among other things, that the obligation to respect privacy concerns online conversation just like the media. When weighing freedom of speech and the protection of privacy in an individual case, it is relevant to consider what quantity of the online publication has content which has been created in line with journalistic principles and what kind of significance the publication bears in this relation to the dissemination of the information and public discussion. The person was found guilty of disseminating information violating B's personal privacy.

In case *KKO 2010:88* a television program had suggested that three persons, who were named in the program, were part of a group funding a terrorist organisation located overseas. The same persons were arrested in Iraq for terrorism connections based on the information from Finland but were later acquitted. The claims and suggestions made in the show were based on statements from interviews and the journalist refused later to disclose the sources. The Supreme Court of Finland pointed out that to raise discussion on important matters in the society did not require the apparent labelling of the persons as clearly suspected of especially reprehensible actions. The court found the defendants guilty of defamation and also noted that the offence of defamation does not require the defendant to be aware of the truthfulness of the information they publish.

In another quite famous case *KKO 2010:39* concerning publishing a book about the Prime Minister of Finland at the time, the Supreme Court of Finland found that the weight of freedom of speech is highlighted in respect of parts of the book presenting significant facts regarding matters of public discussion which are viewed as interesting or important. However, those matters were not handled in the parts of the book which were seen to

fulfil the elements of disseminating information violating privacy of the Prime Minister. The European Court of Human Rights later affirmed this interpretation (*Ruusunen v Finland*, Chamber Judgement [2014] ECHR 35).

There is one example case where the District Court of Helsinki refused to grant a restraining order for online harassment of a journalist partially based on freedom of speech arguments. The District Court viewed that granting the restraining order was supported by the fact that the actions of the two individuals were seriously disturbing to the journalist and the actions had caused the journalist fear and anxiety. However, the District Court viewed that the physical and immediate harassment was not serious in its nature. The Court also referred to the Act on the Exercise of Freedom of Expression in Mass Media (460/2003 as amended) as it stated that it prohibited publishing messages online. It is also noteworthy that, the Supreme Court of Finland has granted the right to appeal in another case involving the same journalist where it will be assessed whether publishing and repeatedly sending certain dismissive and disparaging messages had constituted the offence of stalking.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Legally there are not many options to identify an anonymous harasser other than reporting the offence to the police. Further, pursuant to Section 17 Act on the Exercise of Freedom of Expression in Mass Media (460/2003 as amended) at the request of the injured party, a court may order the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the message are such that providing it to the public is a criminal offence.

A journalist can always turn to the online service provider and request them to voluntarily delete the information and/or the abusive messages and content.

PRACTICAL INFORMATION

Websites:

- https://journalistiliitto.fi/en/
- https://www.poliisi.fi/crimes/reporting_an_offence_online
- https://www.tyosuojelu.fi/web/en/working-conditions/unfair-treatment
- https://syrjinta.fi/en/front-page
- https://tasa-arvo.fi/en/front-page
- https://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf
- https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf
- https://www.finlex.fi/fi/laki/alkup/2017/20170430 (only available in Finnish)

Phone numbers:

- +358 295 470 011 (Finnish police switchboard, Helsinki)

REUTERS/POOL New

FRANCE

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

As a preliminary remark, it should be stressed that media organisations include media outlets (i.e. newspaper, magazine, other paper publication, radio, television, or other medium of mass communication), as well as professional organisations.

In principle, it is up to the victim of an alleged offence to bring an action before the courts ("*nul ne plaide par procureur*").

Indeed, Articles 1 and 2 of the French Code of Criminal Procedure provide that:

- criminal action against an offence can be initiated either by judges, civil servants entrusted by law, or victims of the offence;
- civil action for damages can only be initiated by those who have personally suffered the damage caused by the offence.

By way of exception, professional associations can bring an action when facts are directly or indirectly prejudicial to the "collective interest of the profession", provided that their statutes specify that they are meant to protect such collective interest (Article L. 2132-3 of the French Labor Code).

However, such an action cannot extend to the defense of the individual interest of one journalist. Therefore, professional associations cannot act on behalf of a journalist victim of online harassment. Neither can the other media organisations (media outlets), which cannot even protect collective interests.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

As a preliminary remark, it should be stressed that online attacks are criminal offences under French law. There are therefore two distinct actions with separate rules: the criminal actions which aim at punishing the offence and the civil remedies which aim at repairing the damage suffered by the victim.

Criminal offences

First, as regards competence, French jurisdictions have jurisdiction over any offence committed in France and whose victim is French, even if the perpetrator is of another nationality (in accordance with the territoriality principle laid down in Article 113-2 of the French Criminal Code). Article 113-2-1 of the French Criminal Code specifies that an offence committed on the internet is considered to be committed in France when the victim resides in France.

French courts also have jurisdiction for any offences (under French law or under any law) committed outside France when it is committed by a French national (Article 689 of the French Code of Criminal Procedure) or when the victim is of French nationality (Article 689-1 of the French Code of Criminal Procedure).

Secondly, as regards evidence gathering, France may cooperate with any other country to gather evidence. The forms of cooperation have to be considered on a case by case basis depending on the existence of bilateral/multilateral treaties.

Judicial co-operation has been strengthened within the European Union. Indeed, any Member State may issue a judicial decision (known as a "European investigation order") requesting another Member State to carry out investigations on its territory within a certain period of time in order to obtain evidence relating to a criminal offence or to communicate evidence already in its possession.[30]

Civil remedies

First, as regards the competence, French jurisdictions have jurisdiction over any litigation in which the defendant resides in France (Article 46 of the French Code of Civil Procedure). They also have jurisdiction over any litigation in which the damage or the damaging action is located in France, provided that the defendant does not live in another Member State (Article 46 of the French Code of Civil Procedure).

In case the damage occurs via the internet (as is the case for online attacks), French jurisdictions consider that they have jurisdiction where the litigious content is accessible in France (the damage being deemed to have occurred on French territory).[31]

It should be noted that the conflict of law rules in the European Union are set out in the Brussels 1 Regulation, which governs the recognition and enforcement of judgments in civil and commercial matters.[32] According to this Regulation, the competent jurisdiction in which to pursue a case is the one in which the defendant has its domicile or, in matters relating to tort, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez* of 25 October 2014 (Cases C-509/09 and C-161/10), the Court of Justice of the European Union considered the conflict of law concerns relating to the alleged infringement of personality rights caused by the online publication of defamatory content. See above, Finland analysis at Section 1 (b) for further information.

The Evidence Regulation[33] strengthens the cooperation of the courts of the Member States regarding the transmission of evidence in civil and commercial proceedings. This regulation speeds up the process of evidence sharing by providing the potential to directly transmit evidence between the courts.

Secondly, as regards evidence gathering, access by a French Court to evidence gathered by a jurisdiction of another country has to be considered on a case-by-case basis depending on the existence of bilateral/multilateral treaties.

Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters strengthens the cooperation of the civil courts of the Member States regarding the transmission of evidence. This regulation speeds up the process of transmission of evidence by providing the potential direct transmission of evidence between the courts.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

Online harassment is considered as a form of moral harassment under French law. It is covered by provisions of Article 222-33-2-2 of the French Criminal Code, which makes it an offence to "harass a person by repeated words or behaviour having the object or effect of degrading his or her living conditions in such a way as to impair his or her physical or mental health".

Harassment thus results from a plurality of words or acts, whether it is the repetition of words or behaviour by the same person, or the multiplicity of single words or behaviour by several people. Article 222-33-2-2 of the French Criminal Code specifies that harassment is characterised:

> "(a) Where such words or behaviour are imposed on the same victim by several persons, in a concerted manner or at the instigation of one of them, even though each of those persons has not acted repeatedly;
>
> (b) Where such words or behaviour are imposed on the same victim successively by several persons who, even in the absence of concerted action, are aware that such words or behaviour are repeated".

Harassment is punishable by up to two years' imprisonment and a fine of up to EUR 30,000 "when committed through the use of an online public communication service or through a digital or electronic medium". These penalties may be increased to take into account other aggravating circumstances, for instance, where harassment results in a temporary incapacity to work (TIW) of more than 8 days, or where it is committed on a particularly vulnerable person (for example due to illness, disability or pregnancy) and that this vulnerability is known by the perpetrator(s).

In practice, as long as there is a plurality of words or behaviour, all forms of online harassment of journalists are covered by Article 222-33-2-2 of the French Criminal Code. However, other Articles of the French Criminal Code as well as of the French Civil Code can also apply to specific types of online abuse.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

A threat can be defined as any act of intimidation that inspires fear of harm. Online threats are not subject to specific provisions, but are nevertheless punishable under general provisions of the French Criminal Code.

French criminal law distinguishes between simple threats, and threats involving an order to do something or refrain from doing something. It also provides for different penalties depending on the degree of egregiousness of the threats: threats to commit a crime or a major offence ("*délit*") may result in a much greater penalty than threats to commit a misdemeanour.

Under Article 222-17 of the French Criminal Code, "threatening to commit a crime or an offence against persons (...) is punishable by up to six months' imprisonment and a fine of EUR 7,500 when it is either repeated or materialized in writing, through a picture or through any other object". The penalty is increased to three years' imprisonment and EUR 45,000 in case of a death threat.

In practice, this Article was recently applied in a widely publicised case of online harassment. Nadia Daam is a French journalist who holds a radio chronicle on France's main radio channels. In November 2017, she denounced the sabotage, by members of a platform called "Jeuxvideo.com", on a feminist initiative aimed at helping victims of street harassment. She described the platform as "a non-recyclable rubbish bin". Following her chronicle, she herself was insulted and threatened on the platform, as well as by emails, the threats also being directed at her 11-year-old daughter. There were knocks on her door at night, and she also discovered photomontages of herself about to be beheaded by ISIS.

Nadia Daam filed a complaint with the French police, who identified seven people, including a man who posted a message on the forum, in which he threatened to rape the journalist. On 3 July 2018, he was sentenced by the criminal chamber of the Paris court (*Tribunal de Grande Instance de Paris*) to a 6-month suspended prison sentence on the grounds of Article 222-17 of the French Criminal Code. He was also ordered to pay EUR 2,000 to Nadia Daam for moral damages, as well as EUR 600 to cover her legal fees.

The defendant appealed this decision before the Paris Court of Appeal ("PCA"), which upheld the conviction on all counts and added a fine of EUR 1,500, as well as EUR 1,000 to cover her legal fees. In its 3 March 2020 judgment, the PCA stated that "by taking part in a wave of particularly violent remarks, he was necessarily aware of the significance of his message and nevertheless decided to post it, which characterizes criminal intent". The PCA added that "the incriminated message, although the defendant denies it, is a reaction to the chronicle and was intended to 'punish' Nadia Daam as a journalist, defending the cause of women, but also as a woman (...) by making abusive and degrading but also violent remarks", which deserves "a sentence sufficiently dissuasive to prevent a new offence, particularly via the Internet, a communication tool perfectly mastered by the accused who, acting under a pseudonym, which proves his cowardice, could only be identified thanks to the cyber investigations of the police".[34]

Under Article 222-18 of the French Criminal Code, "threatening, by any means whatsoever, to commit a crime or offence against persons is punishable by three years' imprisonment and a fine of EUR 45,000, when made with the order to fulfil a condition", i.e. to do or refrain from doing something. The penalty is increased to five years' imprisonment and a fine of EUR 75,000 in case of a death threat.

Under Articles 131-12 and R. 623-1 of the French Criminal Code, a threat to commit a misdemeanour not covered by the provisions of Articles 222-17 and 222-18 is punishable by a fine of up to EUR 450, "when this threat is either repeated or materialized in writing, through a picture or through any other object".

In practice, the penalties that theoretically apply to the major types of online threats are the following:

THREAT RELATING TO	DOES THE ONLINE THREAT INVOLVE AN ORDER TO DO OR NOT DO SOMETHING?	IS THE ONLINE THREAT REPEATED OR MATERIALIZED?	PENALTY
A crime, such as homicide, rape or torture for instance	**Yes**		Up to 3 years' imprisonment + EUR 45,000
	No ⇉	**Yes**	Up to 6 months' imprisonment + EUR 7,500
		No	No penalty
A major offence, such as molestation, moral harassment, discrimination or theft for instance	**Yes**		Up to 3 years' imprisonment + EUR 45,000
	No ⇉	**Yes**	Up to 6 months' imprisonment + EUR 7,500
		No	No penalty
A misdemeanor, such as minor violence or damage to property for instance		**Yes**	Up to EUR 450
		No	No penalty

II. INTIMIDATION:

Under French law, intimidation is considered as a form of threat (see above).

III. CYBERSTALKING:

Cyberstalking, which can be defined as illegally following and watching someone through digital means over a period of time, is not covered by any specific provision under French criminal law.

However, with respect to its repetitive nature, it can be considered as a form of online harassment and punishable under Article 222-33-2-2 of the French Criminal Code, whether it is implemented by one person or by a group of people (see above question 2.a).

IV. DOXXING:

Doxxing refers to the practice of collecting personal information about someone (such as his or her full name, contact details, home address etc.), and publishing it online in order to harm the victim or to incite others to harass him or her.

Under Article 226-4-1 of the French Criminal Code, "using one or more data of any kind that could identify [a person] in order to disturb his or her peace or that of others, or to harm his or her honor or consideration, is punishable by one year's imprisonment and a fine of EUR 15,000....This offence is punishable by the same penalties when it is committed on an online public communication network".

The French legislator also very recently created a new offence codified under Article 223-1-1 of the French Criminal Code[35], which provides that "revealing, disseminating or transmitting, by any means whatsoever, information related to the private, family or professional life of a person that makes it possible to identify this person or to locate him or her, for the purpose of exposing him or her or the members of his or her family to a direct risk of harm to the person or property, which the perpetrator could not be unaware of, is punishable by three years' imprisonment and a fine of EUR 45,000". The fact that such doxxing targets a journalist constitutes an aggravating circumstance, increasing the penalty to five years' imprisonment and a fine of EUR 75,000.

This new offence broadens the application of the French legal framework on doxxing to situations which could not previously be apprehended under Article 226-4-1 of the French Criminal Code.

Prior to the implementation of the aforementioned law, depending on the means of implementation, doxxing could be prosecuted as:

- Violation of privacy, under Articles 226-1 et seq. of the French Criminal Code;
- Violation of the representation of a person, under Articles 226-8 et seq. of the French Criminal Code;
- Moral harassment, under Article 222-33-2-2 of the French Criminal Code.

To sum up, doxxing practices ought to be prosecuted:

- on the basis of Article 226-4-1 of the French Criminal Code if they have been implemented from 1 August 2020 and aim at disturbing the journalist's peace;
- on the basis of Article 223-1-1 of the French Criminal Code if they have been implemented as of 25 August 2021 and aim at exposing the journalist or his or her relatives to a direct risk of harm; or
- on the basis of Articles 222-33-2-2 or 226 of the French Criminal Code if the practices have been implemented prior to these dates.

V. ONLINE IMPERSONATION:

Online impersonation constitutes a form of identity theft and is punishable under Article 226-4-1 of the French Criminal Code, which provides that "impersonating someone (...) in order to disturb his or her peace or that of others, or to harm his or her honour or consideration, is punishable by one year's imprisonment and a fine of EUR 15,000... This offence is punishable by the same penalties when it is committed on an online public communication network".

VI. TROLLING:

Trolling can be defined as a manipulation intended to harm the integrity of the community, by a person who, even if he or she has no particular interest in the subject matter, participates in debates with the aim of disrupting them. Trolls pretend to be honest participants to pollute a debate, for instance by giving false advice, distorting facts or mocking other members through provocative messages.

There are no specific provisions punishing trolling in France. However, general criminal provisions can cover certain forms of trolling. For instance, Articles 23, 24 and 24 *bis* of the Freedom of the Press Act of 29 July 1881 ("Freedom of the Press Act") prohibits public statements, by any means of electronic communication to the public, that amount to:

- Hate speech: "[condoning] war crimes, crimes against humanity, crimes of enslavement or exploitation of a person enslaved or crimes and offences of collaboration with the enemy, even if these crimes have not led to the conviction of the perpetrators" is punishable by up to five years' imprisonment and EUR 45,000;
- Holocaust denial: "[disputing] the existence of one or more crimes against humanity as defined in (...) the London Agreement of 8 August 1945" is punishable by up to five years' imprisonment and EUR 45,000;
- Incitement to violence: "[provoking] discrimination, hatred or violence against a person or group of persons on account of their origin or their belonging or non-belonging to a particular ethnic group, nation, race or religion" or for reason of "sex, sexual orientation, gender identity or disability" is punishable by up to one year's imprisonment and a fine of EUR 45,000, and up to three years' imprisonment and a fine of EUR 75,000 when committed by a representative of public authority in the performance of his or her duties.

Certain situations can also be covered by the provisions punishing online harassment, if the applicable criteria set by Article 222-33-2-2 are met (see above).

In practice though, these provisions are of limited effect due to the relative anonymity enjoyed by trolls, and by the extent of the trolling phenomena that can involve a host of people whose identification for the purposes of prosecution is often problematic.

VII. BRIGADING:

Brigading is a concerted action, by which a group of people organize themselves to harass an individual or another group.

It is covered by the provisions of Article 222-33-2-2 of the French Criminal Code, which makes it an offence to "harass a person by repeated words or behaviour having the object or effect of degrading his or her living conditions in such a way as to impair his or her physical or mental health", it being specified that harassment is characterised:

> "(a) Where such words or behaviour are imposed on the same victim by several persons, in a concerted manner or at the instigation of one of them, even though each of those persons has not acted repeatedly;
>
> (b) Where such words or behaviour are imposed on the same victim successively by several persons who, even in the absence of concerted action, are aware that such words or behaviour are repeated".

Brigading is punishable by up to two years' imprisonment and a fine of up to EUR 30,000 "when committed through the use of an online public communication service or through a digital or electronic medium".

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

Most of the laws mentioned above in (b) have not been drafted to prosecute online harassment in particular. However, they can be and have been used to address such behaviours.

Other criminal provisions that can apply include for instance:

- Article 223-13 of the French Criminal Code, if online harassment has led to the suicide of the victim: "provoking the suicide of another person is punishable by three years' imprisonment and a fine of EUR 45,000 when the provocation was followed by suicide or attempted suicide";
- Article 24 of the Freedom of the Press Act, which prohibits public statements, by any means of electronic communication to the public, that amount to "[provoking], in the event that such provocation is not followed by action, to commit one of the following offences (...): 1° Voluntary attacks on life, voluntary attacks on personal integrity and sexual assault (...); 2° Theft, extortion and wilful destruction, damage and deterioration that is dangerous to persons". This behaviour is punishable by up to five years' imprisonment and a fine of EUR 45,000.
- Articles 32 and 33 of the Freedom of the Press Act, which provide that public defamation and public insults are punishable with fines of up to EUR 12,000. When committed due to the victim's race, ethnic group, nation, religion, sex, sexual orientation or disability, defamation is punishable by up to one-year imprisonment and EUR 45,000, and public insults are punishable by up to 6-months' imprisonment and EUR 22,500.

Moreover, civil law provisions can also apply, along or independently from criminal proceedings. For instance, Article 835 of the French Code of Civil Procedure provides that the judge can prescribe protective measures to "prevent imminent damage or to put an end to an obviously unlawful situation".

In practice, this means that the judge can order that content that is obviously illegal be taken down from a website, or even have this website blocked. Judicial actions based on Article 835 have proven quite effective to take down illegal contents without delay.

Article 835 was used for instance in 2018, to take down the neo-Nazi website "democratieparticipative.biz" on which users published racial insults, hate speech and incitement to violence, some of them targeting journalists. On 11 October 2018, the French Public Prosecutor filed a request based on Article 809 of the French Code of Civil Procedure (now Article 835), asking the Paris court (*Tribunal de Grande Instance de Paris*) to order internet providers to "block access from French territory and/or by their subscribers located on French territory" to this website.

After recalling that blocking measures "may be pronounced when public order is threatened, which cannot be disputed when reading the hateful publications", the Paris court ruled on 27 November 2018 that they appeared "totally appropriate and proportionate" in this case. It therefore ordered the internet providers to proceed with the blocking of access to the website within 15 days.[36]

Please note that such action can be followed or combined with parallel criminal actions aimed at identifying and punishing the authors of the illegal contents or the website administrators.

This was the case in 2019, when one of the journalists insulted on this Neo-nazi website filed a criminal complaint. In 2017, Julie Hainaut, who worked for a local newspaper, wrote a column about a restaurant in which she claimed that the owners had made dubious comments glorifying the colonial era. Her column triggered extremely violent reactions among far right-wing circles, especially on "democratieparticipative.biz" where users posted Articles calling for "mobilization" and published stolen photos of her alongside gifs representing Hitler, as well as graphic rape and death threats.

After a one-year investigation, the police were able to identify one user of the forum who had relayed a very violent article against Julie Hainaut. On 18 December 2019, the criminal chamber of the Lyon court (*Tribunal de Grande Instance de Lyon*) found him guilty of aggravated insults, and sentenced him to a 6-month suspended prison sentence. He was also ordered to pay EUR 5,000 to the journalist for moral damages. However, he was later acquitted by the Lyon Court of Appeal, which ruled on 17 December 2020 that the facts were time-barred.

Article 1240 of the French Civil Code allows the victims to request compensation for the damage they suffered, by providing that "any act of man, which causes damage to another, obliges the one by whose fault it occurred to repair it".

Please note that the French Parliament passed a new law on 24 August 2021 titled Reinforcing Respect of the Principles of the Republic, which includes provisions against online hate. Under Article 46 of this law, an alleged perpetrator of online hate content may be subject to immediate appearance in court (*comparution immediate*) when he or she is apprehended on the grounds of either Article 24, 24 *bis* or 33 of the Freedom of the Press Act of 29 July 1881 (punishing amongst other offences hate speech, holocaust denial and incitement to violence) and provided that the concerned content is not controlled by a publishing director. This measure is aimed at speeding up proceedings and limiting the dissemination of the content.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Some of the provisions referenced above prohibit racist, sexist and homophobic hate speech or incitement to violence, including online.

More generally, racism, sexism and homophobia are considered in French law as aggravating circumstances when they have motivated the commission of a crime or offence. According to Articles 132-76 and 132-77 of the French Criminal Code:

> "Where a crime or offence is preceded, accompanied or followed by words, writing, images, objects or acts of any kind which either violate the honour or reputation of the victim, or of a group of persons to which the victim belongs, by reason of his or her actual or supposed belonging or non-belonging to a specific race, ethnic group, nation or religion", or "because of his or her sex, sexual orientation or gender identity, real or perceived", "or establish that the acts were committed against the victim for one of these reasons, the maximum custodial penalties shall be increased as follows:
>
> (...) 6° It shall be increased to seven years' imprisonment where the offence is punishable by five years' imprisonment;
>
> 7° It is doubled when the offence is punishable by up to three years' imprisonment".

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Yes. The draft law of 9 July 2019 - the so-called "Avia Bill" - notably sought to introduce a procedure for reporting hate speech on the internet in order to force platforms to react within 24 hours in the event of a report of manifestly illegal content. This mainly concerned content relating to human dignity, and in particular racist, homophobic or sexist content.

However, it has been the subject of numerous criticisms. The National Human Rights Commission (CNCDH), for instance, considered that by giving the platforms the responsibility to qualify and remove hateful content, the Bill ran the risk of "encourage[ing] excessive withdrawals, creating a risk of censorship". It also strengthened "the power of the most powerful platforms to the detriment of the smallest", while recalling that "it is up to the judge, and to him alone, to assess the abusive nature of the exercise of freedom of expression".

When asked to assess the conformity of the Avia Bill before it was adopted, the French Constitutional Council ruled that "in view of the difficulties in assessing the manifestly illegal nature of the content reported within the time limit, the penalty incurred from the first infringement and the absence of a specific cause for exoneration from liability, the contested provisions can only encourage online platform operators to withdraw content reported to them, whether or not it is manifestly illegal. Therefore, they infringe the exercise of freedom of speech in a way that is unnecessary, inappropriate and not proportionate" (*Decision no. 2020-801 DC of 18 June 2020*). As a result, the Constitutional Council censored most of the provisions of the law.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Any journalist who has been the victim of an online offence can (i) report the illegal content on PHAROS, the online platform set up by the French police (see ***Practical Information*** below), and (ii) lodge a complaint with the French police or "gendarmerie". If the journalist does not know the identity of the perpetrator(s), he or she can file a "complaint against X".

The French police are trained to track online attackers that hide behind a pseudonym to obtain their IP address from the website or the social network on which the offence occurred.

Under the French Law for Trust in the Digital Economy (LCEN) law of 21 June 2004, content hosts or internet service providers must retain data that allows the identification of anyone who contributed to the creation of the content that they provide, as they can be ordered to communicate such information by a judge.

Until the entry into force of the 24 August 2021 law, neither content hosts nor internet service providers were subject to any general obligation to monitor the content they provide, or to search for facts or circumstances indicating illegal activities. They could however incur civil and in some cases criminal liability for offences committed online under certain circumstances. Indeed, Article 6 of the LCEN law provides that they will not be held liable for the content they provide (i) if they were not aware of its unlawful nature or of facts and circumstances that would indicate such nature, or (ii) if from the moment they had such knowledge, they acted promptly to remove or block access to this content.

Since the entry into force of the 24 August 2021 law, operators of online platforms (for example social networks, video sharing platforms, search engines) with a number of users that exceeds a certain threshold

(to be specified by decree) are required to collaborate with judicial or administrative authorities, as well as to withdraw and block hate content reported to them. To do so, they must put in place a mechanism for reporting and analysing reports, including a mechanism for priority review of reports received from "trusted third-party" (such as PHAROS). More generally, operators have to react to the notifications "promptly".

Please note that generally speaking, only the authors of the content will be held liable for it. In practice, the journalist must then collect evidence, mostly by taking screenshots of the illegal contents. It is important to take a screenshot of the entire screen, in order to show the date and URL bar of the page where the content is hosted. Furthermore, it can be useful to have these screenshots taken or certified by a bailiff, to lower the risk that this evidence be disputed in the event of a trial.

In the meantime, the journalist can of course ask the website hosting the content to remove it. They can also request a judge to prescribe protective measures (see Section 2.c above).

Moreover and from a very practical standpoint, if the case goes to trial, French law provides that the unsuccessful party may be ordered to pay all or part of the other party's legal fees (in both civil and criminal matters, under Articles 700 of the Code of Civil Procedure and 475-1 of the Code of Criminal Procedure). This means that a journalist whose harasser is convicted may be reimbursed for all or part of his or her legal costs.

Please note that Reporters Without Borders recommends that the following steps be taken by journalists in case of online harassment or attacks:

- First, especially in case of online impersonation, warn their sources and contacts;
- Second, collect evidence (screenshots, bailiff's report etc.);
- Third, report the attack using the mechanisms set up by the local authorities to report cases of harassment (in France, the PHAROS platform);
- Finally, file a complaint with the police station - insist that a proper complaint ("plainte") be registered, rather than a report ("main courante").

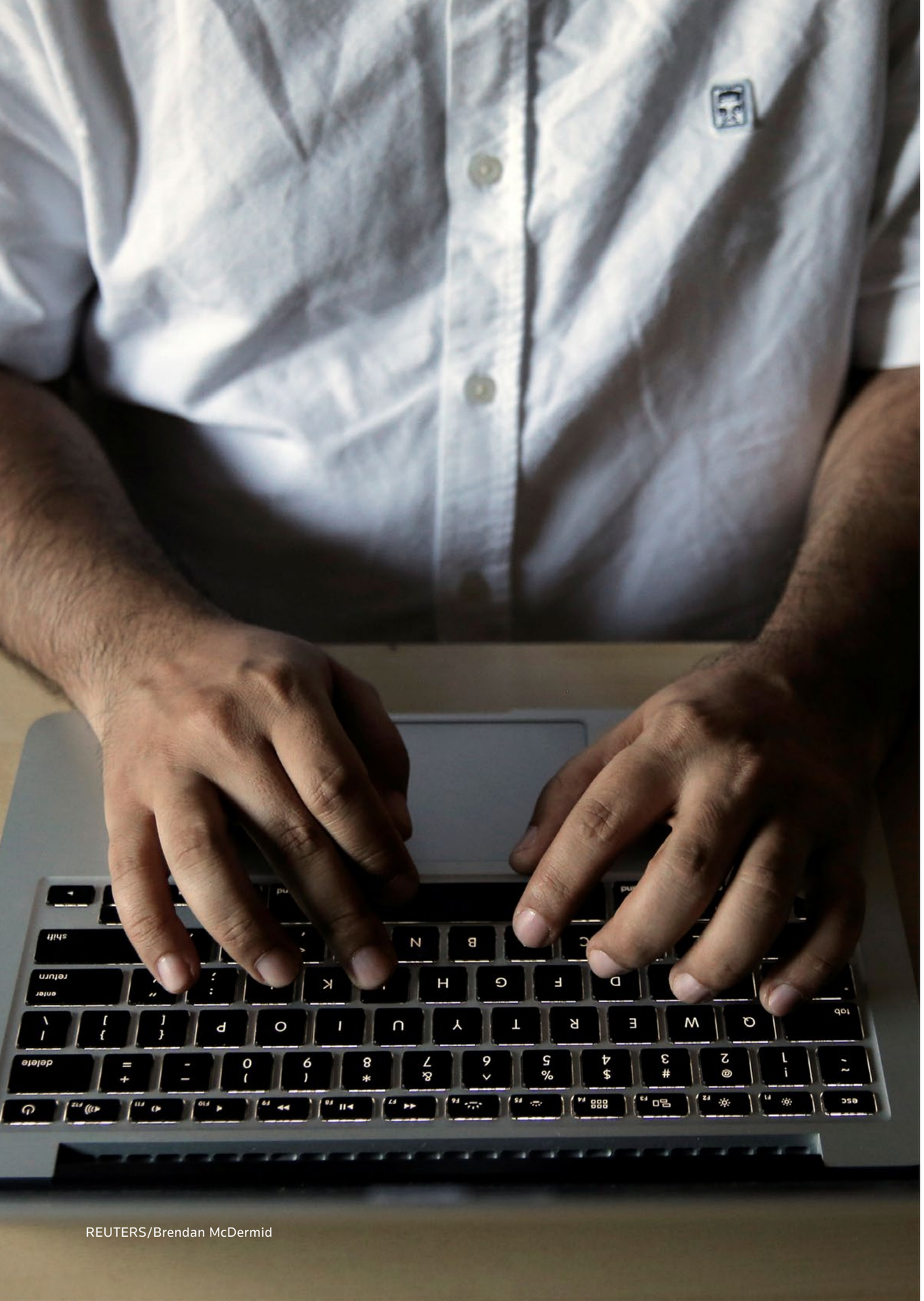
PRACTICAL INFORMATION

Websites:

- PHAROS (online platform set by the French government to report illegal content on the internet). This platform theoretically aims at collecting reports of paedophilia, incitement to hatred or discrimination, threats or incitement to violence, injury or defamation and terrorism, but it can often be used to report online harassment involving these types of offences.
- Guidance on online harassment (in French).

Phone numbers:

- To ask questions about online harassment anonymously and confidentially: +33 800 200 000 (available from Monday to Friday, 9 am – 7pm).



REUTERS/Brendan McDermid

GERMANY

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

Civil Law

Anyone who has a claim can bring it in civil courts. In instances where a journalist has been harassed, a media organisation would probably not have any "original" claims of its own. A journalist could assign their own claims to a media organisation, making such claims the respective organisation's and enabling them to sue in civil court (such assignation requires a written agreement between assignee and assignor). Please note that not all claims can be assigned to third parties; this applies in particular to claims of a highly personal nature, such as claims to cease and desist (*Unterlassungsanspruch*).

Criminal Law

As far as criminal law is concerned, the German legal system is an inquisitorial one, not an adversarial one – so all state players involved, be it the prosecution or the court, must investigate all facts of the case (as opposed to only those facts that build a specific case). This leaves little room for taking your own legal action against crimes – whether one is a citizen or an organisation. An organisation could report a crime committed against a journalist to the state authorities, thereby starting an investigation; state investigative measures include obtaining data from telecoms providers (particularly relevant for crimes committed on the internet). Neither victims of crimes nor any of their representatives have any comparable capabilities, with one exception: in certain instances, private prosecution is a possibility (Section 374 et seq. of the German Code of Criminal Procedure). However, this mainly transfers responsibility for investigative measures regarding the circumstances of the crime to the court.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

Firstly, with respect to civil law, the general rule is that for complaints arising from tort, the court in the jurisdiction of which the tortious act was committed shall have jurisdiction. If the act is typically one that is committed in one place but where its consequences arise in a completely different place, the place where the tortious act had its consequences will also be considered the place where "the tortious act was committed" (principle of ubiquity).

It should be stressed that the conflict of law rules in the European Union are governed by Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. According to this Regulation, the competent jurisdiction is the one in which the defendant has its domicile or, in matters relating to tort, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez* of 25 October 2011[37], the Court of Justice of the European Union considered that the criterion of the place where the damage occurred confers jurisdiction to courts in each Member State where the online content is or has been accessible. It further specified that those courts have jurisdiction only in respect of the damage caused in the territory of their Member State.

It is worth mentioning that Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters strengthens the cooperation of the civil courts of the Member States regarding the transmission of evidence. This regulation speeds up the process of transmission of evidence by providing the potential direct transmission of evidence between the courts.

Secondly, with respect to criminal law, whether an offence committed will be tried under German law is determined by Section 3, 9 of the German Criminal Code. It will be relevant whether the act itself was committed in Germany, or – broadly speaking – its consequences arose in Germany. Under certain circumstances, an offence that was committed abroad can also be tried under German law (for instance, German criminal law applies to offences committed abroad if the act is a criminal offence at the place of its commission and if the offender was a German national at the time of the offence or became a German national after its commission).

It is worth mentioning that judicial co-operation has been strengthened within the European Union. Indeed, any Member State may issue a judicial decision (known as a "European investigation order") requesting another Member State to carry out investigations on its territory within a certain period of time in order to obtain evidence relating to a criminal offence or to communicate evidence already in its possession.[38]

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

In 2017, the Network Enforcement Act (*NetzDG*) was passed into law. It aims to support fighting hate crimes and the spread of fake news, in particular on social media, and it mainly operates by imposing fines on social media operators.

Apart from this, no specific set of laws exists to tackle online harassment. Laws that are applicable to harassment in general apply to online harassment as well.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

Threatening someone with a crime which the offender has (or pretends to have) any influence on, in order to make the victim do something, is punishable under Section 241 of the German Criminal Code (*Bedrohung*). A "crime" has a somewhat high threshold, though – not all contents of a threat would be punishable under German criminal law. Death threats or rape threats would qualify; threatening to bodily harm someone may not necessarily qualify. Such behaviour will often also amount to coercion, as per Section 240 of the German Criminal Code (*Nötigung*). Someone who threatens to commit a serious criminal offence incurs a penalty of imprisonment for a term not exceeding one year or a fine; for coercion, it is a penalty of imprisonment for a term not exceeding three years or a fine (in especially serious cases, the penalty is imprisonment for a term of between six months and five years).

II. INTIMIDATION:

Depending on the specifics of the case, intimidating behaviour could amount to a threat (*Bedrohung*, see above; Section 241 of the German Criminal Code) or a coercion (*Nötigung*), Section 240 of the German Criminal Code (this makes threatening someone in order for them to behave in a certain manner punishable). Someone who threatens to commit a serious criminal offence incurs a penalty of imprisonment for a term not exceeding one year or a fine; for coercion, it is a penalty of imprisonment for a term not exceeding three years or a fine (in especially serious cases, the penalty is imprisonment for a term of between six months and five years).

III. CYBERSTALKING:

Stalking is punishable under Section 238 of the German Criminal Code. A stalker incurs a penalty of imprisonment for a term not exceeding three years or a fine; the penalty is imprisonment for a term of between three months and five years if the offender places the victim, a relative of or another person close to the victim in danger of death or at risk of serious damage to health on account of the act.

IV. DOXXING:

Researching and publicly broadcasting private or identifying information is often meant to set up other behaviour (such as harassment). In itself, if personal data was obtained illegally, i.e. by hacking, this will often amount to offences punishable under German law, such as Section 202a of the German Criminal Code (data espionage). Data espionage incurs a penalty of imprisonment for a term not exceeding three years or a fine.

V. ONLINE IMPERSONATION:

Depending on the circumstances and the offender's actions while impersonating another individual, this may amount to coercion (*Nötigung*, Section 240 of the German Criminal Code), insult (*Beleidigung*, Section 185 of the German Criminal Code) malicious gossip (*üble Nachrede*, Section 186 of the German Criminal Code), defamation (*Verleumdung*, Section 187 of the German Criminal Code). Clause 185 incurs a penalty of imprisonment for a term not exceeding one year or a fine (or, if the insult is committed by means of an assault,

imprisonment for a term not exceeding two years or a fine); clause 186 incurs a penalty of imprisonment for a term not exceeding one year or a fine (or, if the offence was committed publicly or by disseminating material (Section 11 para. 3), a penalty of imprisonment for a term not exceeding two years or a fine); and clause 187 incurs a penalty of imprisonment for a term not exceeding two years or a fine (or, if the act was committed publicly, in a meeting or by disseminating material (Section 11 (3)), a penalty of imprisonment for a term not exceeding five years or a fine).

VI. TROLLING:

Depending on the specifics of the behaviour displayed, this may amount to coercion (*Nötigung*, Section 40 of the German Criminal Code) or stalking (Section 283 of the German Criminal Code). For the penalties incurred, please see above.

VII. BRIGADING:

As an act of a group rallying against an individual, this again depends on the actual behaviour of the group displayed. Behaviour may amount to any of the offences listed above.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

Since Germany has no specific legislation dealing with online harassment, all of the named laws and provisions above are related to the general protections against harassment and are therefore not specifically conceived for online crimes. Civil law cease and desist orders can be sought based on violations of a person's general right of personality. Civil damages can be sought based on this as well, as per clause 823 para. 2 of the German Civil Code.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

If there is a race and/or gender component in the abuse, Section 130 of the German Criminal Code may apply (incitement of masses; *Volksverhetzung*). This provision criminalises disturbing public peace by inciting hatred i.e. against women or certain ethnicities.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Freedom of speech is one of the basic fundamental rights in Germany and as such, enshrined in the German Constitution. Some of the laws described above do, per se, infringe upon freedom of speech (i.e. Section 185 of the German Criminal Code which prohibits insulting someone). All German laws must be viewed in light of and interpreted in accordance with the German Constitution. If one person's fundamental rights (i.e. a harasser's right to freedom of speech) are infringed for the benefit of another's (i.e. a journalist's general right of personality), the underlying statutory laws (i.e. provisions that prohibit the harassing) are potentially open for judicial review. In the past, though, courts have upheld the above-mentioned provisions in the German

Criminal Code against claims that they infringe on the perpetrator's basic fundamental rights. German Criminal Code provisions are well-tested in that regard and it is unlikely that they would be overturned at some point.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Based on Section 242 of the German Civil Code, Section 14 para 3, and Section 15 paragraph 5 of the German Telemedia Act, a victim can demand information about the perpetrator (i.e. user and traffic data) from a social network provider. This right only extends insofar as a perpetrator has committed certain criminal offences, such as incitement of masses (*Volksverhetzung;* Section. 130 of the German Criminal Code) or threatening someone with a crime which the offender has (or pretends to have) any influence on, in order to make the victim do something, is punishable under Section 241 of the German Criminal Code (*Bedrohung*).

The victim must obtain a court order, to be served to the social network provider. If the network provider refuses to provide the information, the victim may have to obtain another court order in order to force the network provider to actually disclose the requested data.

Involving state prosecutorial services may also help, as they can employ investigative measures that private citizens cannot.

REUTERS/Faisal Mahmood

INDIA

PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

There is no clear distinction as regards the grounds on which media organisations or journalists can take legal action in the context of online harassment.

There have been instances in the past where media organisations have initiated action in relation to cyber-harassment and cyber bullying. The grounds on which such actions have been initiated are:

In cases of Defamation – As per Section 499 of the Indian Penal Code, 1860 ("IPC") an imputation made against a company or an association of persons may constitute defamation if the imputation is made with the intent to harm their reputation or with the knowledge that their reputation would be harmed as a result.[39] Since it falls under the ambit of this provision, a media organisation may file a defamation claim in case they feel that they have been defamed or their reputation has been harmed by means of written or verbal communication. Defamation under Section 499 of the IPC extends to electronic means as well.[40]

Instances of Injurious Falsehood - A media organisation may have standing to sue for injurious falsehood against a person who makes a statement regarding the media organisation's business, when:

- such statement is false and calculated to cause financial damage;
- the statement is made maliciously, without just cause or excuse, with an intent to cause injury; and
- the statement leads to special damage, such as actual loss of a customer or contract as opposed to some general loss such as loss of reputation.

Whereas defamation has a penal provision, injurious falsehood is a variant of the tort of trade libel. Hence, a loss of reputation is not sufficient to constitute injurious falsehood; a special trade damage must be demonstrated.

It is typically difficult to succeed on an injurious falsehood claim. Proof of malice is essential for such claim to succeed, the burden of which would fall on the media organisation. A defamation claim would be a more convenient route as the statement is presumed to be false and the defendant has to prove that it is true.

Provocation of damage to property of Media Institutions - In the state of Maharashtra, a media institution is protected from damage to its property by state-specific legislation known as the Maharashtra Media Persons and Media Institutions Act (Prevention of Violence and Damage or Loss to Property), 2017 ("Maharashtra

Act").[41] Section 3 of this Act, not only prohibits any act of violence against a Media Person[42] but also prohibits any loss or damage to the property of a Media Person or Media Institution.[43]

Furthermore, as per Section 4 of the Act, any person who commits or attempts to commit, abets, instigates, or provokes an act that causes damage to the property of the Media Institution shall be liable to imprisonment up to three years or with a fine of fifty thousand rupees or both.

Although the legislation does not address cybercrimes particularly, the scope of Section 4 is sufficiently broad to encompass online instigation, abetment, or provocation of an offence. Hence, such acts would be punishable under this legislation.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

In India, the Information Technology Act, 2000 ("IT Act") confers the "extraterritorial jurisdiction" by virtue of Section 75. This section clearly sets out that an offender shall be governed by the provisions of the IT Act irrespective of whether he is an Indian citizen or not, provided the offence relates to computer systems or network that is situated in India, even if the offence takes place outside India. Though there is a solution under Indian laws to address extraterritorial jurisdiction and enforcement issues, it is limited.

Enforcement of foreign judgments and decrees in India is governed by Section 44-A read with Section 13 of the Code of Civil Procedure, 1908 ("CPC"). A foreign judgment which is conclusive under Section 13 of the CPC may be enforced by instituting execution proceedings under Section 44-A in the case of 'reciprocating territories'[44] or by instituting a civil suit on the judgment in the case of non-reciprocating territories.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

There is no separate legal framework specifically addressing online harassment of journalists in India. However, there are relevant provisions under different laws dealing with various individual components of online and offline harassment such as circulation of obscene material, forgery to harm reputation, criminal intimidation etc.

The relevant provisions of different Indian laws applicable to the issue are:

Indian Penal Code, 1860 (IPC)

- **Section 469 - Forgery for purpose of harming reputation**
  This section of the IPC has been amended by the IT Act to address forgery of an "electronic record". The section now provides that a person who commits forgery with the intention that the forged document or electronic record should harm someone's reputation, or with the knowledge that it would be used for such purpose, shall be liable for fine and imprisonment.

- **Section 507 – Criminal intimidation by an anonymous communication**
  This section states that whoever commits the offence of criminal intimidation by an anonymous communication, or takes precautions to conceal their name or abode, shall be punished with imprisonment in addition to the punishment provided for criminal intimidation generally. While the provisions regarding criminal intimidation apply generally, Section 507 addresses the dimension of anonymity that is widespread in online intimidation and harassment.
- **Section 509 - Word, gesture or act intended to insult the modesty of a woman**
  This section stated that whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.

State Specific Amendment in Chhattisgarh

An amendment has been brought in Chhattisgarh wherein after Section 509 of the Penal Code, 1860, Section 509A and 509B has been inserted.

- **Section 509A - Sexual harassment by relative**
  This section states that whoever, being related to a woman through blood, adoption or marriage, and not being her husband, takes the advantage of his proximity and induces, seduces or threatens such woman with intent to insult her modesty by word, gesture or act shall be punished with rigorous imprisonment which shall not be less than one year but which may extend to five years and shall also be liable to a fine.
- **Section 509B - Sexual harassment by electronic mode**
  This section states that whoever, by means of telecommunication device or by any other electronic mode including internet, makes creates, solicits or initiates the transmission of any comment, request, suggestion, proposal, image or other communication, which is obscene, lewd, lascivious, filthy or indecent with intent to harass or cause or having knowledge that it would harass or cause annoyance or mental agony to a woman shall be punished with rigorous imprisonment for a term which shall not be less than six months but may extend to two years and shall also be liable to a fine.

Information Technology Act, 2000 (IT Act)

- **Section 66C - Punishment for identity theft**
  This section addresses the fraudulent or dishonest use of the electronic signature, password or any other unique identification feature of any other person and provides that the offender making such fraudulent or dishonest use shall be punished with imprisonment and fine.
- **Section 66D - Punishment for cheating by personation by using computer resource**
  This provision addresses offences of cheating by personation that takes place over electronic means and thus covers such offences that take place online. It states that a person who cheats by personation, by means of any communication device or computer resource, shall be liable to imprisonment and fine.
- **Section 66E – Punishment for Violation of Privacy**
  Section 66E, along with Section 354C of the IPC, deal with "voyeurism". This section states that whoever intentionally transmits the images of private areas of any person, without the consent of that person, is liable for violating the privacy of that person and therefore, is liable to be punished.

- In the case of *State of West Bengal v. Animesh Boxi,*[45] the accused was convicted by the District Court of West Bengal for taking some private and obscene photographs of the victim by hacking into her phone, blackmailing her by threatening to upload the stolen pictures and videos on the internet and subsequently uploading her private pictures and intimate videos onto an obscene website. He was convicted under Sections 354A, 354C, 354D, 509 of the IPC and Sections 66C and 66E of the IT Act.
- **Section 67 – Punishment for publishing or transmitting obscene material in electronic form**
  This section relates to publishing obscene material in "electronic form". Practically, it addresses the online dimension of the offence of stalking. A person who publishes any obscene material about the victim on social media i.e., in electronic form so as to bully the victim, shall be liable for imprisonment and fine.
- **Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form**
  This section relates to the cyberstalking crime. Added by the 2008 IT Amendment Act, it states that a person who publishes any "sexually explicit" material in electronic form i.e., through emails, messages, or on social media, shall be liable to imprisonment and fine. The maximum imprisonment prescribed under Section 67A of the IT Act is greater as compared to the penalties under Section 67 of the IT Act.
- **Section 72 - Penalty for breach of confidentiality and privacy**
  As per this provision, if any person, in pursuance of any of the powers conferred under the IT Act, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and further discloses the same to any other person, then such person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
- **Section 72A - Punishment for disclosure of information in breach of lawful contract**
  This provision deals with a confidentiality breach by a service provider. It contemplates an act wherein a person, including an intermediary, has secured access to any material containing personal information about another person, while providing services under the terms of lawful contract, and discloses the material to any other person. If this act is committed with the intent to cause or knowing that it is likely to cause wrongful loss or wrongful gain and without the consent of the person concerned, or in breach of a lawful contract, the offender shall be liable to imprisonment or fine.
- **Section 73 - Penalty for publishing electronic signature certificate false in certain particulars**
  As per the provisions of this section, no person shall publish an electronic signature certificate or otherwise make it available to any other person with the knowledge that–
  - (a) the Certifying Authority listed in the certificate has not issued it; or
  - (b) the subscriber listed in the certificate has not accepted it; or
  - (c) the certificate has been revoked or suspended,

  unless such publication is for the purpose of verifying an electronic signature created prior to such suspension or revocation. Any person who contravenes the above provisions shall be punished with imprisonment and fine.
- **Section 74 - Publication for fraudulent purpose**
  Anyone who knowingly creates, publishes or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment and fine.

The Young Persons (Harmful Publications) Act, 1956

This Act aims to protect young persons, under the age of 20 years, against any malicious or harmful publication that might lead to dissemination of certain publications harmful to young persons. A person convicted under this Act for harmful publication shall be punishable with imprisonment.

State Specific Laws

The Maharashtra Act is the first law in the country which ensures protection specifically for journalists. Section 4 of the Act provides that any person who commits, abets, instigates, or provokes an act of violence against a media person (including journalist) shall be liable to imprisonment or fine. Under Section 6, such person shall also be liable to pay compensation for property damage or medical expenses.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS

There are no specific laws that deal with online threats in India. However, Section 354D, 507 of the IPC can be applied to dealing with cases of online threats. Section 354D pertains to instances of stalking, including cyber stalking wherein if any man follows a woman or contacts or attempts to contact such women persistently despite a clear indication of disinterest by that woman virtually or physically is punishable under law. Section 507 pertains to criminal intimidation also constituting a threat under the IPC.

II. INTIMIDATION

Section 507 of the IPC specifically talks about "criminal intimidation." As there is no specific law to deal with online intimidation in India, this section can be applied to dealing with cases of online intimidation.

III. CYBERSTALKING

There is no separate law or provision dealing with cyberstalking in India. However, Section 354D of the IPC added through the Criminal Law Amendment Act, 2013 defines 'Stalking'. This section can be applied to dealing with the cases of cyberstalking. Other sections like Sections 500, 506, 507 of IPC and Sections 67, 67A, 67B of the IT Act can also be applied in order to prosecute the offences related to cyberstalking.

The application of these sections is observed in the case of *Kalandi Charan Lenka v State of Odisha.*[46] The petitioner was a victim of stalking, where a fake account of her was created which was used to send obscene and vulgar messages to the victim's acquaintances by the accused. A morphed naked picture was also posted on the walls of the hostel where the victim stayed. The High Court of Odisha upheld the liability of the accused under the relevant sections of the IPC and the IT Act.

IV. DOXXING

In India, there is no separate law to address the crime of doxxing. However, Sections 66C, 66E, 66 of the IT Act can be applied. Certain sections of the IPC pertaining to sale of obscene publications,[47] physical or virtual stalking,[48] defamation,[49] criminal intimidation[50] and criminal intimidation by anonymous forms of communication[51] can also be applied.

V. ONLINE IMPERSONATION

Section 66C and Section 66D of the IT Act deal with impersonation. There is no specific law to deal with online impersonation in India. Other provisions of the IPC like Sections 499 and 507 can also be applied.

In the case of *Jitender Singh Grewal v. The State of West Bengal*,[52] the accused created a fake Facebook account of the victim and uploaded obscene pictures to such fake Facebook account. After the authorities charge-sheeted the accused under Sections 354A, 354D, 500, 509, 507 of IPC and Section 67A of the IT Act, he filed a bail application. The trial court rejected the bail application of the accused and the Calcutta High Court upheld the trial court's decision.

VI. TROLLING

There is no separate law for trolling in India. However, Sections 66E, 67, 67A and 67B of the IT Act, can be used to address trolling in India. Certain sections of the IPC like Sections 292, 354D, 500, 503, 506 and 507 can also be applied.

Trolling is common in India as happened in the Sandhya Ravishankar case. Sandhya Ravishankar is a Chennai-based freelancer. In 2017 she had written a four-part series in The Wire that implicates Tirunelveli-based mining baron S. Vaikundarajan in illegal sand mining. She faced harsh feedback from his audience on social media platforms such as Twitter and Facebook where the writer received abusive calls and various other threats. Her mobile number was also released on social media by anonymous trolls due to which she began receiving a flood of threatening and abusive calls from unknown people. Her matter has not yet reached a conclusion.

VII. CYBER THEFT

Sections 43 and 66 of the IT Act, penalise activities such as computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. Section 378 of the IPC relating to "theft" of movable property applies to the theft of any data, online or otherwise as Section 22 of the IPC states that the words "movable property" includes corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

In *Gagan Harsh Sharma v. The State of Maharashtra*[53], certain individuals were accused of theft of data and software from their employer and were charged under Sections 408 and 420 of the IPC and also under Sections 43, 65 and 66 of the IT Act.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

Section 292 – Sale, etc., of obscene books, etc.

The offence of cyberstalking takes within its purview the act of sending obscene materials to the victim on a social networking site or through emails or messages etc. A person who attempts to deprave another person by sending any obscene material on the internet with the intention that the other person would read, see or hear the content of such material, shall be guilty of the offence under Section 292 of IPC.

Section 503 – Criminal Intimidation

This provision deals with a person who threatens another with any physical injury or injury to reputation or property. If the intent of the threat is to cause alarm to the other person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, in order to avoid the execution of that threat, the person giving such threat commits criminal intimidation. The offender is liable to imprisonment and fine.

Under the provision, the threat is not limited to that of injury to the other person, but injury to anyone that person may be interested in.

The provisions of IPC as discussed above are frequently used when dealing with cases of online harassment. Sections 292, 354D, 469, 499, 507, 509 amongst others are a few examples.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Gender-based sections in the Indian Penal Code, 1860

- **Section 354D, IPC – Stalking**
  This section states that if any man follows a woman or contacts or attempts to contact a woman repeatedly despite a clear indication of disinterest by that woman or monitors the use of internet, email or any other form of electronic communication by that woman shall be punished on first conviction for a term which may extend to three years and shall be liable to fine. On subsequent conviction shall be punished for a term which may extend to five years and also be liable to a fine.
- **Section 509, IPC – Word, gesture or act intended to insult the modesty of a woman (IPC)**
  Section 509 states that if any individual in public commits any act such as utterance of any word or any sound or gesture, with the intention to affect the reputation and modesty of woman shall be punished for a term which may be extended to one year, or with fine, or both.

Suhas Katti v. State of Tamil Nadu[54] was the first case in India relying upon Section 67 of the IT Act relating to publishing or transmitting obscene material. In this case the accused sent an email in the name of the victim that implied she was a prostitute, resulting in people calling her and asking for her rates. The victim filed a complaint and the accused was charged under Sections 469 and 509 of the IPC and Section 67 of the IT Act and was sentenced to rigorous imprisonment for 2 years under Section 469 IPC, 1-year simple imprisonment under Section 509 IPC and 2 years imprisonment under Section 67 of the IT Act (5 years in total) and fined 5000 Rupees.

The Indecent Representation of Women (Prohibition) Act, 1986

- **Section 3**
  No person shall publish, or cause to be published, or arrange or take part in the publication or exhibition of, any advertisement which contains indecent representation of women in any form.
- **Section 4**
  No person shall produce or cause to be produced, sell, let to hire, distribute, circulate or send by post any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation or figure which contains indecent representation of women in any form.

- **Section 6**
  Any person who contravenes the provisions of Sections 3 or 4 shall be punishable on first conviction with imprisonment of either description for a term which may extend to two years, and with a fine which may extend to two thousand rupees, and in the event of a second or subsequent conviction with imprisonment for a term of not less than six months but which may extend to five years and also with a fine not less than ten thousand rupees but which may extend to one lakh rupees.

Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013

Online harassment also encompasses sexual harassment which is defined under Section 2(n) of the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013 as unwelcomed. The definition includes contact and advances, a demand or request for sexual favours, making sexually coloured remarks, showing pornography, any other unwelcome physical, verbal or nonverbal conduct of sexual nature.

In the recent case of *Sanjeev Mishra vs. Bank of Baroda,*[55] the Rajasthan High Court has widened the scope of the term 'workplace harassment' to include online harassment.

The Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989

In India, caste-based violence is prevalent and specific laws have been enacted with the aim to protect minorities and scheduled castes. One such law as discussed below gives special protections against sexual harassment to women belonging to a Scheduled Caste or a Scheduled Tribe.

- **Section 3 (w): Punishments for offences atrocities**
  Any person who intentionally touches (the touch being sexual in nature) a woman belonging to a Scheduled Caste or a Scheduled Tribe without the recipient's consent; or uses words, acts or gestures of a sexual nature towards such woman, can be punished under the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Until as recently as March 2015, most variants of online harassment would have constituted offences under Section 66A of the IT Act. However, the Supreme Court of India in March 2015 struck down Section 66A of the IT Act, as unconstitutional, finding that it was violative of free speech in the landmark case of *Shreya Singhal and Ors. v. Union of India*.[56]

The Supreme Court's order was justified on the grounds that the provision violated the constitutionally guaranteed Fundamental Rights to Equality before Law, and Life and Personal Liberty guaranteed under Articles 14 and 21 of the Indian Constitution respectively, because it discriminated between those using the internet and those using other means of communication to commit alleged infringements, while no such *intelligible differentia* actually exists.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Cybercrime complaints can be filed with the cybercrime cells on National Cyber Crime Reporting Portal. The process of filing the complaint is both online and offline. The cybercrime complaint can be registered with any of the cybercrime cells established in India as cybercrime comes under the purview of global jurisdiction. Section 1(2) of IT Act, 2000 states that the Act shall extend to the whole of India and, barring as otherwise provided in the Act, it shall apply to any offence or contravention committed outside India by any person. Section 75 of the IT Act states that the Act will apply to an offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Cyber cells: Cells have been established specifically to deal with victims of cybercrime. They come under the purview of the Crime Investigation Department. In case a cyber cell is lacking where the victim resides, then the victim can file a First Information Report ("F.I.R") at a local police station. If a victim is unable to file an F.I.R., they can approach the police commissioner. It is compulsory for a police station to register an F.I.R.

Report to CERT: The IT Act, 2008 has designated the Indian Computer Emergency Response Team (CERT-IN) as the national nodal agency for tackling the issues relating to computer security threats. Both the users and System Administrators can approach CERT-IN to report computer security incidents and vulnerabilities such as E-mail related issues viz. mail bombing, spamming, attempt to obtain unauthorised access to a system or data contained therein etc.

Reporting on social media websites: If both of the above are difficult to do for any reason, reporting on social media websites is also an option. Most of these websites have the option of reporting the crime since they are obliged under the IT rules 2011, to take action within 36 hours of reporting to stop the offensive content from spreading.

PRACTICAL INFORMATION

- Cyber Crime Prevention against Women and Children
- @CyberDostTwitter handle www. cybercrime. gov.in-online portal of MHA
- Ministry of Women and Child Development has a dedicated e-mail address complaintmwcd@gov.in

REUTERS/Inquam Photos

IRELAND

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

The question of whether media organisations have standing to take legal action depends in part on whether the remedy pursued is criminal or civil in nature.

In criminal matters, media organisations do not have standing to bring a complaint on behalf of a journalist. In practice, they may be able to provide support to the victim and assist them in formulating their complaint. However, they will have no formal role in the process. To the extent the victim enjoys certain rights under the Criminal Justice (Victims of Crime) Act 2017, including the right to information regarding ongoing investigations and criminal proceedings (Article 8), the Garda Síochána and/or the Director of Public Prosecutions will not provide such information to media organisations.

Similarly, in civil matters, such as defamation, media organisation do not have standing to take or participate in legal action. This also extends to assisting in financing civil claims. In *Persona Digital Technology Ltd v Minister for Public Expenditure*[57] the Supreme Court held that third party funding of litigation is not permitted in Ireland as it offends the rules on maintenance and champerty. Similarly, in *SPV Osus Limited v HSBC Institutional Trust Services (Ireland) Limited & others*[58] the Supreme Court held that the assignment of a cause of action to a third party offends these rules and is prohibited.

Media organisations may have standing to take legal action on constitutional grounds. The courts will permit a citizen to challenge an actual or threatened breach of a constitutional norm where there is no other suitable plaintiff or where the threatened breach is likely to affect all citizens in general.[59] However, while there is an argument to be made that certain forms of harassment may amount to a violation of the constitutional rights to the protection of the person (Article 40.3.2°) and the inviolability of the dwelling (Article 40.5°), the remedy in such a case would be a declaration of unconstitutionality against a piece of legislation or a decision of the government and it is difficult to see how that would be of assistance as a general remedy to instances of online harassment.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

Prior to the Harassment, Harmful Communications and Related Offences Act 2020 (the 2020 Act) which came into force on 10 February 2021, Ireland did not have any bespoke legislation for dealing with online harassment.[60] Victims must seek redress within the available civil and criminal channels, both of which carry their own concerns with respect to territorial jurisdiction.

First, in the civil context, territorial jurisdiction poses challenges in terms of assessing and calculating damages and in enforcing any order of the Irish courts. The primary civil remedy for the purposes of online attacks against journalists is likely to be defamation law. Even where a person secures an order through the Irish courts, it can prove difficult to secure recognition and enforcement of the judgment. This may be a particular problem in cases involving US defendants, where the US courts may be reluctant to enforce any order that infringes upon the First Amendment right to freedom of speech.

It should be noted that the conflict of law rules in the European Union are set out in the Brussels 1 Regulation, which governs the recognition and enforcement of judgments in civil and commercial matters.[61] According to this Regulation, the competent jurisdiction in which to pursue a case is the one in which the defendant has its domicile or, in matters relating to tort, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez*[62] of 25 October 2014 (Cases C-509/09 and C-161/10), the Court of Justice of the European Union considered the conflict of law concerns relating to the alleged infringement of personality rights caused by the online publication of defamatory content. See above, Finland analysis at Section 1 (b) for further information.

It is worth mentioning that the Evidence Regulation[63] strengthens the cooperation of the courts of the Member States regarding the transmission of evidence in civil and commercial proceedings. This regulation speeds up the process of evidence sharing by providing the potential to directly transmit evidence between the courts.

Secondly, turning to criminal matters, unless otherwise provided for by statute, criminal jurisdiction is restricted to offences committed within the territory of the State. This is irrespective of the nationality or domicile of the perpetrator. The available offences were developed before the advent of digital connectivity and lack extra-territorial effect. This results in a lacuna, whereby acts which would have amounted to an offence were they to have been committed within the State, cannot be pursued. While the legislature recognises this issue and addressed it in the cross party bill in 2017[64], it has not been addressed in the 2020 Act.

Even where the alleged offence has been committed within the State, territorial jurisdiction may prove a hindrance in respect of evidence gathering, in particular where the evidence is stored on servers which are located outside of the State.

Mutual Legal Assistance Treaties (MLAT) are in place to facilitate cross-border co-operation among law enforcement agencies and the Criminal Justice (Mutual Assistance) Act 2008 governs the operation of these. This Act allows Ireland to seek and provide mutual legal assistance from other countries in criminal matters. Where a search power exists in Ireland in relation to the conduct giving rise to an offence, a request may be made for help in obtaining specified evidence for the purpose of a criminal investigation or proceeding. The Act may also be used to obtain identification evidence.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

The 2020 Act has modernised Irish law relating to harassment and has broadened the pre-existing offence to specifically target online harassment.

Section 10 of the Non-Fatal Offences Against the Person Act 1997 (the 1997 Act) is the primary legislative provision in Ireland for the prosecution of incidents of harassment. Section 10 provides that a person who "without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence." The section goes on to provide that a person harasses another where their "acts intentionally or recklessly, seriously interfere with the other's peace and privacy or causes alarm, distress or harm to the other."

The assessment of whether certain conduct reaches the threshold of harassment under Section 10 of the 1997 Act therefore comprises an objective test. The test is provided in the wording "he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other". This has been interpreted as meaning that the acts of the defendant must be such that a reasonable person would realise that the acts would seriously interfere with the peace and privacy of another or cause them alarm, distress or harm. This ensures that self-deluded harassers cannot escape liability under the section, because even if they believe their behaviour is reasonable they still come within Section 10 if their actions are seen as objectively likely to cause interference, alarm, distress or harm.[65] In this way, there is no overarching list of criteria to determine whether conduct amounts to harassment. Each case will turn on its own facts with the Court examining whether:

- the accused's conduct seriously interfered with the peace and privacy of the victim or caused them alarm, distress or harm; and
- a reasonable person would have realised that the conduct would have had this impact.

The wording "by any means" allows for online harassment to be captured by Section 10. However, a criticism of this provision is that the word "persistently" limits the protection afforded under Section 10 to victims. The inclusion of this word means one-off incidents (for example one-off posts on social media platforms) are not covered by Section 10. "Persistence" in the context of this offence was found by the Irish courts[66] to apply only to acts which are "continuous" meaning either:

- a number of incidents that are separated by intervening lapses of time, or
- a single, but continuous, incident such as following a person on an unbroken journey over a prolonged distance.

The 2020 Act has amended the general offence of harassment under Section 10 of the 1997 Act to include persistent communications "about" a person. While the 1997 Act was worded sufficiently broadly to capture incidents of online harassment, there remained gaps in the law. Ireland's legislative framework, through the 2020 Act, now clearly addresses indirect harassment as well as other forms of online harassment. The Act has provided welcome clarification that communications "with or about" a person fall within the scope of harassment. The maximum penalty for that offence has increased from 7 to 10 years' imprisonment. It also

incorporates specific offences for the taking and distributing of intimate images without consent and the distribution of threatening or false messages.

While Section 10 of the 1997 Act appeared restrictive insofar as it may only apply to instances of direct harassment, the Irish courts have found a perpetrator guilty of an offence under Section 10 for indirect harassment whereby the perpetrator posted offensive material about the victim on a website but did not make direct contact with the victim (see the *Paul Managhan* case below). This successful prosecution appeared to conflict with the wording of Section 10 resulting in ambiguity as to the section's application to incidents of indirect harassment. This, however, has now been reconciled by the 2020 Act which specifically includes instances of indirect harassment in the definition of harassment removing any uncertainty.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS:

Section 4 of the 2020 Act specifically provides that a person who distributes or publishes "any threatening or grossly offensive communication about" or "to another person with intent by so distributing, publishing or sending to cause harm… is guilty of an offence." This offence carries a maximum penalty of two years' imprisonment and/or an unlimited fine.

In addition, Section 5 of the 1997 Act can be used in instances of online threats to kill or cause serious harm, as it provides that a person who "without lawful excuse, makes to another a threat, by any means intending the other to believe it will be carried out, to kill or cause serious harm to that other or a third person shall be guilty of an offence."

The inclusion of the wording "by any means" allows for online threats to be covered by this offence. This Section has the clear limitation that it only applies to the most serious threats – to kill or cause serious harm. In addition, a potential barrier to prosecution is the requirement to prove the perpetrator "intended the other to believe" the threat would be carried out. Therefore, it is not sufficient for the threat to cause the recipient alarm, distress or harm. It must be established that the perpetrator intended for the threat to be believed. This could prove a significant obstacle to prosecution in the current regrettable climate where online threats are so widespread and are, for the most part, unsupported by an intention to carry out the threat. A person found guilty of an offence under Section 5 of the 1997 Act is liable on summary conviction to a fine not exceeding €2,500 and/or to imprisonment for a term not exceeding 12 months and on conviction on indictment to a fine and/or imprisonment for a term not exceeding 10 years.

Depending on the circumstances, it may be possible to prosecute the perpetrator of online threats which do not constitute a threat to kill or cause serious harm. This could be done under Section 10 of the 1997 Act but in order to rely on this section the threats would need to be persistent in nature.

II. INTIMIDATION:

No offence of "intimidation" exists in Ireland. However, provided the conduct is persistent it is liable to be prosecuted as an offence under Section 10 of the 1997 as such conduct will amount to "pestering", "besetting" or "communicating with" the victim.

III. CYBERSTALKING:

There is no specific offence of stalking or cyberstalking in Ireland. The 2020 Act does however, strengthen the protection afforded to victims of harassment with the inclusion of indirect harassment. The offence of harassment under Section 10 of the 1997 is considered sufficiently broad to cover acts of stalking. As Section 10 includes the wording "by any means" it covers cyberstalking. As outlined above the persistence requirement must be satisfied to constitute an offence but as persistence is an inherent feature of cyberstalking this would not prove to a barrier in pursuing prosecution. Notwithstanding that stalking is covered by the offence of harassment under Section 10 of the 1997 Act, Ireland's Law Reform Commission has recommended that a separate offence of stalking be introduced with the same elements as the offence of harassment

IV. DOXXING:

If the conduct is persistent it is likely to fall within the offence of harassment provided for in Section 10 of the 1997 Act as it would amount to "pestering" the victim and would cause the victim alarm or distress. Note the Paul Monaghan example outlined below which concerned conduct which comprised of both "doxxing" and online impersonation and which resulted in successful prosecution.

V. ONLINE IMPERSONATION:

The Criminal Damage Act 1991 and Section 10 of the 1997 Act have been used to prosecute perpetrators of online impersonation (see the Facebook status case and the Paul Monaghan case below). A person found guilty of an offence under Section 2 of the Criminal Damage Act 1991 is liable on summary conviction to a fine not exceeding €2,500 and/or to imprisonment for a term not exceeding 12 months and on conviction on indictment to a fine and/or imprisonment for a term not exceeding 10 years.

VI. TROLLING:

Given the variety of online conduct which can be said to fall within the term "trolling", incidents of trolling will need to be assessed on a case-by-case basis to determine if they can be prosecuted. The 2020 Act offers a new avenue for prosecution as Section 4 of the 2020 Act provides for "distributing, publishing or sending threatening or grossly offensive communication" as well as providing for offences relating to the recording, distribution or publication of intimate images. Previously, the most likely avenue for prosecution was Section 10 of the 1997 Act, provided the conduct is persistent.

VII. BRIGADING:

As above, the viability of pursuing a prosecution for brigading will turn on the facts of each particular scenario. Section 10 of the 1997 Act again represents the most likely option for prosecution. However, given the collective nature of brigading, the persistence requirement of Section 10 may prove an obstacle in prosecuting the offending parties. If all individuals who contribute to a pattern of harassment, only engage in one act (i.e. a single online post) this would prevent prosecution due to the lack of persistence. Any individual who makes more than one comment exposes themselves to possible prosecution under Section 10.

Following the commencement of the 2020 Act, a person found guilty of an offence under Section 10 of the 1997 Act, is now liable on summary conviction to a fine not exceeding €2,500 and/or to imprisonment for a term not exceeding 12 months and on conviction on indictment to a fine and/or imprisonment for a term not exceeding 10 years. The 2020 Act imposes a higher fine of €5,000 for the offence of harassment on summary conviction.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

The Criminal Damage Act 1991

Section 2 of the 1991 Act makes it an offence to "damage any property belonging to another intending to damage any such property or being reckless as to whether any such property would be damaged." The definition of "property" in the Act includes data. Note the following example of prosecution for online harassment under this Act:

- **The Facebook Status case (June 2014)**: In June 2014 a man was successfully prosecuted under the 1991 Act when he took his ex-girlfriend's phone and posted an offensive status on her Facebook page, purportedly from her, stating that she was a "whore" who would "take any offers". The man was not named in news reports due to a pending criminal trial for rape. The man pleaded guilty to criminal damage under the 1991 Act and the judge imposed a €2,000 fine. Prosecution for this one-off action was possible because it arose under the Criminal Damage Act 1991 which, unlike Section 10 of the 1997 Act, does not contain a persistence requirement. The Criminal Damage was to the victim's property (her social media account). Prosecution under the 1991 Act would not have been possible if the perpetrator had posted a damaging comment from his own account or a fake account because it would not have constituted damage to the victim's property.

The Non-Fatal Offences Against the Person Act 1997

As is apparent from the above, though not specifically drafted with online crimes in mind, Section 10 of the Non-Fatal Offences Against the Person Act 1997 is the preeminent legislative provision used in Ireland to prosecute online harassment. Note the following examples of prosecution for online harassment under this Act:

- **Brendan Doolin & six female irish journalists case (November 2019)**: Mr Doolin harassed the six women by sending them hundreds of abusive emails. One victim, Kate McEvoy was informed that the sender of the emails was in the area where she lived and on one occasion when she tweeted that her housemate had gone out for the evening, he replied "good, I'll be over soon". Another victim, Christine Bohan, who got over 450 messages from Mr Doolin, also received a 10-year-old political leaflet from him which carried a photograph of her on it. She was also sent an image of her from a dinner at her old college. She was not named in either image. Each of the women received hundreds of emails, usually using the same unusual font, containing insults such as calling the women "wannabes, nobodies, whiteist, bigots, lefties and pseudo intellectuals". Mr Doolin accused them of being narcissistic attention seekers, self-obsessed and concerned with their own self-promotion, referring to their "twitter bubble" and suggesting that they do not care for others. Mr Doolin used a number of different email addresses to contact the women, quite often following an article they had published or a radio or a television appearance. Another victim, Sinead O'Carroll, a news editor, was contacted and told to "break both legs" after she tweeted to promote an upcoming appearance on a television programme. At trial, Judge Nolan sentenced Mr Doolin to five years imprisonment, but suspended the final two years of the sentence on strict conditions including that he be under supervision of the Probation Service for two years post-release and that he not contact any of the victims for the rest of his life. The Court heard that a breach of this order is a criminal offence with a maximum sentence of seven years imprisonment. After the sentencing the victims released a joint statement which stated: "We hope this case shows other men and women in this situation that what they say will be taken seriously if they come forward, and that online harassment is harassment and will be treated as such."

- **Paul Murphy & Justine O'Rourke case (April 2019)**: Mr Murphy harassed actress Justine O'Rourke online through a series of posts, comments, private messages and emails. Mr Murphy pleaded guilty and was prosecuted for harassment under Section 10 of the 1997 Act. He was given an 18 month sentence which was suspended for two years upon Mr Murphy paying Ms O'Rourke €1,500 and agreeing to never contact the victim again. Some of the comments forming part of the harassment were not sent directly to the victim nor was she tagged in them. However, other messages were sent directly/included tagging, therefore the offending conduct comprised both direct and indirect harassment.
- **Conor O'Hora & Sharon Ní Bheoláin case (March 2018)**: This case involved a man who doctored pornographic images to insert Ms Ní Bheoláin's face on to them. The images appeared when one searched Ms Ní Bheoláin's name on Google. He also had online conversations with a man which contained threats of serious sexual violence including references to Ms Ní Bheoláin. He was charged under Section 10 of the 1997 Act and sentenced to four and half years in prison, the last 18 months were suspended (he was also charged under the Child Trafficking and Pornography Act). When sentencing Mr. O'Hora, Judge Martin Nolan described his actions as an "insidious form of harassment" and "debasing behaviour". Judge Nolan went on to note that the "information on [Ms. Ní Bheoláin] will be out there forever" and "no doubt it caused considerable distress to [Ms. Ní Bheoláin] and her family. [Mr. O'Hora] must have known that. It was reprehensible and he should be thoroughly ashamed." It was not reported to what extent the judge took into account the impact on Ms. Ní Bheoláin's journalistic freedom when sentencing Mr. O'Hora.
- **Paul Monaghan & a care worker (March 2014) case:** Mr Monaghan posted messages about his ex-girlfriend on a website stating that she was offering sexual favours. Her name and address were posted on the website and reports state that the posts happened over an eight month period (thereby meeting the persistence requirement). Mr Monaghan pleaded guilty to harassment and was given a four year suspended sentence. As noted above, prosecution of this conduct under Section 10 of the 1997 Act was somewhat out-of-step with the wording of the section which requires direct communication with the victim, as opposed to indirect communication as applied in this case. However, Mr Monaghan plead guilty to the charge, thus this technical point was not considered by the Court.
- **DPP v Doherty case (2020):** The accused in this case, a Detective Garda, began a campaign of offensive communications from September 2011 to March 2013 about a neighbour. The appellant sent offensive emails and letters to various people very closely associated with the victim, including the DPP, the family medical practitioner and other prominent individuals. She also placed leaflets on cars and pillars throughout the neighbourhood. Despite the volume of these communications, only one communication was directly sent to the victim. The Supreme Court considered whether this was sufficient communication with the victim for the purposes of the 1997 Act. The Court held that to consider this course of action to be anything other than communication with the victim "... would be to introduce a meaning far removed from the statutory intent and the common sense meaning of the words used." The Supreme Court extended the scope of the offence of harassment to include communications that were not directly addressed or sent to the subject, offering more robust legal protection to victims.

The Harassment, Harmful Communications and Related Offences Act 2020

To date there has been no known prosecutions in respect of this newly published Act, which came into force on 10 February 2021. However, the Minister for Justice has confirmed that a number of investigations are ongoing.[67]

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

According to the UN Committee on the Elimination of Racial Discrimination, Ireland lacks substantive hate crime offences. While it has signed the Council of Europe Convention on Cybercrime, it has not yet ratified the Convention and it is not clear whether Ireland will adopt the Additional Protocol to the Convention which would require the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Many of the provisions of this Additional Protocol are present in the European Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law (the "2008 Framework Decision"), which was adopted in 2008. Article 1(1) and Article 3(2) require Ireland to "take the measures necessary to ensure that … publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin…" is punishable "… by criminal penalties of a maximum of at least between 1 and 3 years of imprisonment." While Article 10 requires Ireland to comply with the Framework decision by November 2010, Ireland has not yet enacted any transposing legislation.

The Prohibition of Incitement to Hatred Act 1989 (the "1989 Act") is Ireland's primary legislation in this area. This prohibits incitement to hatred, outside the context of a private residence, against a group of persons on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation. This applies to both online and offline incitement. In 2020 the Department of Justice published their report on "Legislating for Hate Speech and Hate Crime in Ireland",[68] the purpose of which was to begin reviewing and updating the 1989 Act. The Report considers all forms of abuse including abuse on online platforms which did not exist in 1989. It is hoped that this Bill when drafted will complement the Online Safety and Media Regulation Bill 202169 by "establishing a robust regulatory framework to deal with the spread of harmful online content."[70]

There are at least two fundamental limitations with respect to this Act. Firstly, gender, disability and age are not protected characteristics despite being covered by other equality legislation. Secondly, unlike the 2008 Framework Decision which seeks to provide protection to groups of people with protected characteristics and to individuals of those groups, the 1989 Act makes reference only to a "group of persons". This means that abusive online harassment targeted at an individual journalist cannot be prosecuted under the provisions of the 1989 Act.

While a prosecution for harassment under Section 10 of the 1997 Act may be possible, race and gender are not considered aggravating factors for the purpose of the 1997 Act.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

No examples have been identified where the above described laws have been found to infringe on the constitutional right to freedom of expression.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

The anonymous nature of online harassment creates significant challenges for victims. While it may sometimes be possible to identify an individual through their IP address, this process can prove expensive and drawn-out. It becomes even more challenging, if the harasser takes efforts to obfuscate their identity, such as through the use of a VPN.

Journalists may seek a *Norwich Pharmacal* order, which allows for the disclosure of the name and IP address of parties unknown to the plaintiff against whom the plaintiff intends to issue civil proceedings for alleged wrongful conduct. However, since there is no legislative basis for such orders, victims must apply to the High Court. This usually involves first seeking an order against the relevant website to disclose user and IP details. Once furnished, these details may lead to data held by a telecoms company, many of whom require a second *Norwich Pharmacal* order before agreeing to the disclosure.

Legal aid for such applications is not available and the rules against maintenance and champerty discussed in Q1.1 apply also to the funding of applications for *Norwich Pharmacal* orders. As a result, this process is prohibitively expensive for most individuals. Even for individuals with the means, the Courts have noted that such orders "must be sparingly used" due to the interference with the right to privacy of other individuals. Therefore, in order to obtain a *Norwich Pharmacal* order, a "very clear and unambiguous establishment of wrongdoing" is required.[71]

This uncertainty, coupled with the prohibitive cost of making such an application to the High Court, often renders journalists' efforts to identify online harassers impossible.

PRACTICAL INFORMATION

Websites:

- Cosc - The National Office for the Prevention of Domestic, Sexual and Gender-based Violence.
- Victims of Crime Office.
- An Garda Síochána – Victim Services.
- Free Legal Advice Centre.
- Commission for the Support of Victims of Crime Victim Services List.
- Law Reform Commission Report on Harmful Communications and Digital Safety.

Phone numbers:

- Crime Victims Helpline: Free Phone: 116 006; Text: (+353) 85 1 33 77 11; For callers outside the Republic of Ireland: +353 1 4161908

REUTERS/Thomas Peter

JAPAN

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

If the rights of a media organisation itself are infringed, the organisation has standing to take legal action on its own behalf. The typical case is the assertion of a defamation claim by the organisation.

Proving defamation under Japanese law means showing that the societal judgment (i.e., society's approval or esteem) by the public of the defamed person or legal entity has been damaged. Actions that lead to the deterioration of public societal standing of media organisations may constitute defamation.

If acts of defamation or privacy violation are made solely against a journalist as an individual, affiliated media organisations do not have standing to take legal action. The standing belongs solely to such journalist as an individual, who is entitled to assert actions in tort on their own behalf for defamation or the privacy violation at issue.

As a general rule, it is theoretically possible for a person with standing to bring a legal action to voluntarily confer such standing to a third party ("voluntary plaintiff standing"). However, this is permitted only in exceptional situations that satisfy certain criteria. Such criteria are not rule-based but principle-based and require that either (1) voluntary plaintiff standing will facilitate the judicial procedures, or (2) a nature/characteristic of the plaintiff or right in question makes it difficult for the plaintiff to resort to a civil judicial remedy without utilising voluntary plaintiff standing. Given the open-ended nature of these criteria, their application will be highly fact-driven.

No case law providing that voluntary plaintiff standing status may be conferred on a company on behalf of its employee has been identified. In 2005,[72] a production company filed suit against a magazine company on behalf of its entertainers, asserting infringement of their rights of publicity and defamation.[73] In this case, the standing of the production company was denied, and only the standing of the individual entertainers to bring suit on their own behalf was affirmed by the court. Based on this case, it seems unlikely that Japanese courts would adjudge that a journalist may confer their standing on a media organisation.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

The Existence of Territorial Jurisdiction

When a victim of cross-border online harassment (assuming actionable conduct that legally constitutes defamation or privacy violation exists) seeks to resolve the dispute by filing for civil litigation in Japan, a question will arise as to whether such victim can establish jurisdiction to file suit in the Japanese courts.

Common fact patterns potentially raising jurisdictional issues include: (1) A person domiciled outside of Japan engages in conduct on the internet that defames or violates the privacy of a person domiciled in Japan, or (2) conversely, a person domiciled in Japan engages in conduct on the internet that defames or violates the privacy of a person domiciled outside of Japan.

As described further below, under Japanese law, damages claims arising from defamation or violation of privacy causes of action are based upon a theory of torts. Under the Japanese Code of Civil Procedure, Japanese courts have jurisdiction over tort claims where (A) the defendant is domiciled in Japan, or (B) "the place where the tort occurred" is Japan. Therefore, if a person domiciled in Japan engages in conduct on the internet that defames or violates the privacy of a person domiciled outside of Japan, the victim may file suit in the Japanese courts because the defendant is domiciled in Japan.

"The place where the tort occurred" includes the location where the consequences of the defendant's act take effect. This may be the place where a person who was defamed, or had their privacy rights violated, suffers the consequences (i.e., experiences damage to societal judgment). There is case law recognising jurisdiction in Japan on the grounds that "there is a possibility that a person other than the plaintiff had access to the relevant publication on the internet, in Japan, in a matter regarding a publication allegedly violating the plaintiff's privacy rights.[74] On such basis, jurisdiction may be easily recognised with respect to publications on the internet that are accessible to third parties.

Japanese courts do not have jurisdiction when "the consequences of a wrongful act committed in a foreign country have arisen within Japan but it would not ordinarily have been possible to foresee those consequences arising within Japan" (Article 3-3 of the Code of Civil Procedure). However, when a publication on the internet that is accessible to third parties has defamed or violated the privacy rights of a person domiciled in Japan, in most cases, a Japanese court will determine that such wrongful act's consequences in Japan were foreseeable.

Accordingly, if a person domiciled outside of Japan engages in conduct on the internet that defames or violates the privacy of a person domiciled in Japan, the victim usually files suit in Japan, and the Japanese courts will have jurisdiction over the action.

However, even when the Japanese courts can exercise jurisdiction over an action, a court may discretionarily dismiss all or part of the claims presented if it finds that "special circumstances" apply to the case. These "special circumstances" are a catch all exception, and cases will be judged on an ad hoc, case-by-case basis depending on the relevant facts and circumstances. In one notable case, Japanese residents filed suit in a Japanese court claiming that they were defamed by a U.S. company on the internet. The Japanese Supreme Court dismissed the action on the grounds that (A) the action was derivative of a lawsuit already filed in the U.S., (B) the relevant evidence was primarily located in the U.S., and (C) responding to the action in Japan would be burdensome to the defendant.

International Jurisdiction Issue relating to Evidence-Gathering

If a civil action is filed in the Japanese courts regarding a dispute with respect to which the Japanese courts have jurisdiction, the Japanese Code of Civil Procedure will govern the rules of evidence-gathering.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

Neither the legal concept of "online harassment" nor legislation specifically dealing with this concept exists in Japan. However, an "Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders" (commonly known as the "Provider Liability Law")[75] specially addresses the violation of rights resulting from publication on the internet.

The Provider Liability Law provides two main options for journalists and media organisations dealing with infringement of rights resulting from online harassment: (1) making a demand that the offending online content is deleted, and (2) seeking identification of the person responsible for the offending online content.

The victim may also request that an Internet Service Provider ("ISP") delete the offending content. However, this request itself is not legally enforceable. In order to legally compel an ISP to delete content, it is necessary to seek a provisional injunction from a court based upon an assertion of personal rights (see Section 2(b) below).

In order to claim legal liability against a person publishing content anonymously on the internet, it is necessary to determine that person's identity as a first step. The Provider Liability Law provides the methods for identifying such persons (see Section 3 below).

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS

Online content having the effect of notifying the victim of the perpetrator's intent "to harm an individual's life, body, freedom, reputation or property" constitutes the crime of intimidation (Article 222 of the Penal Code, Act No. 45 of 1907, as amended) (hereinafter the "Penal Code"). Recently, the number of legally prosecuted acts of intimidation on the internet has been increasing. Typically, such prosecution results from an arrest upon investigating comments along the lines of "I will kill X" on an anonymous bulletin board on the Internet. The punishment is imprisonment for up to two years, or a fine of up to 300,000 yen.

Moreover, notifying the victim of the perpetrator's intent "to harm an individual's life, body, freedom, reputation or property" constitutes a tort as an infringement of human rights under Japanese law, and thus the victim may claim monetary damages (compensation) in civil proceedings based on that cause of action.

Several cases in the jurisprudence relate to threats made on the internet through various platforms such as social media (widely referred to in Japan "social networking services" or "SNS"), blogs, and video-sharing sites (for example, though comment functions). The method of publication on the Internet does not seem to affect whether or not the content constitutes the crime of intimidation under Japanese law.[76]

II. INTIMIDATION

Same as "Threats" above.

III. CYBERSTALKING

The following actions ("Prohibited Stalker Actions") are prohibited as long as such actions are made with the intent of "expressing the emotion of resentment or hatred arising from the non-satisfaction of personal gratification, such as romantic feelings" (Article 2.1 of the Anti-Stalking Act, Act No. 81 of 2000, as amended) (hereinafter the "Anti-Stalking Act").

- Repeatedly sending direct messages via SNS or on personal blogs despite previous rejection.[77]
- Repeatedly writing comments via SNS or on personal blogs despite previous rejection.
- Publishing content that indicates that the target person is being monitored (for example, keeping track of the activities of a journalist on a given day).

If a Prohibited Stalker Action is committed, even on a single occasion, the victim may request the police to issue a warning to the alleged perpetrator not to repeat the Prohibited Stalker Action. However, a one-time Prohibited Stalker Action does not constitute a crime. Prohibited Stalker Actions may constitute a crime if they are repeated and cause the target to feel threatened with regard to their physical safety, peaceful enjoyment of residence and fame, or freedom to act (Article 2.3 of the Anti-Stalking Act). The legal punishment is imprisonment for up to one year or a fine of up to 1 million yen.

IV. DOXXING

Whether or not doxxing is legally actionable depends on the content of the information that is disclosed. The issue is whether or not the disclosed content constitutes defamation or a privacy violation.

If such disclosed information constitutes defamation or a privacy violation, the following actions may be available in civil proceedings (Articles 709, 710, and 723 of the Civil Code, Act No. 89 of 1896, as amended) (hereinafter the "Civil Code"):

- Claim compensation. In addition, claims for other damages are available if a plaintiff can prove such damages. Based on past cases, the amount of compensation to be awarded is not likely to exceed 1 million yen, with the typical compensation amount around 300,000 to 600,000 yen.
- Seeking a published apology in a newspaper. In privacy violation cases (as opposed to defamation cases), courts have rarely ordered publication of an apology in a newspaper.
- Demanding deletion of the disclosed information by obtaining an injunction (i.e., in Japanese legal parlance, a "disposition"). Although this is a provisional disposition, once the content is deleted, the reinstatement of such content on the internet does not usually occur. This procedure usually takes one to two months to litigate.

Defamation may also constitute a crime under Japanese law (Article 230 of the Penal Code). The punishment for criminal defamation is imprisonment (with or without forced labour) for up to three years, or a fine of up to 500,000 yen. On the other hand, privacy violation is not punishable as a crime.

Legal Framework of Defamation

If (1) certain facts are asserted, and (2) such facts damage the societal judgment of a person, this constitutes defamation. However, this general rule is subject to a number of limitations potentially relevant in the case of criticism and commentary of journalism and journalists:

- Criticism or commentary regarding the target subject's value, morality, quality, etc., without asserting facts (i.e., without asserting any subject matter which could be proved true or false by evidence) will not rise to the level of defamation unless such criticism or commentary is so severe as to constitute a direct personal attack on the character and ethics of the target subject.
- Regarding "commentary" in the context of journalism: In one case, a journalist (referred to as appellant X) sued for defamation arguing that certain commentary about his article – that "someone could reasonably say that the work was intentional misrepresentation" and "someone could reasonably say that it is fake news"[78] – was defamatory. However, the court ruled that no defamation had occurred, because of the nature of the commentary (commentary on the news), and that "even if it can be said to be cruel criticism, it does not include language to show contempt for appellant X personally, and it is not presented as a personal attack beyond the criticism on the contents of the article".[79]
- Where a written statement contains facts objectively relating to the "public interest", and the writer's subjective intent is to promote the public interest, such written statement will not be held to constitute defamation as long as such facts are true or are believed to be true at the time of writing, based on reasonable inquiry, even if ultimately determined to be false.

There is a tendency in Japanese courts to find that the "public interest" defence applies where journalists have been criticized. In one case, a journalist claimed to have been defamed by a magazine piece that argued that such journalist had fabricated another article. The journalist lost the case because the court determined that criticizing the factual validity of an article written by a journalist, or the journalist's methods for collecting information, was covered by the public interest defence.[80] In another case, a defendant criticised a journalist via SNS and a personal blog, questioning the journalist's methods for collecting information. The court ruled in favour of the defendant on the grounds that the public interest defence covered criticism of a journalist's methods for collecting information.[81]

In privacy violation cases, where an offensive comment was merely posted on an anonymous online bulletin board, courts tend to reject the public interest defence. However, no such tendency exists in relation to defamation claims. In other words, in the case of defamation claims, courts are likely to take into consideration various factors, including the platform on which the offensive comment was posted, for purposes of analysing the merit of the relevant public interest defence.

Legal Framework Required for Privacy Violation Claims

A privacy violation under Japanese law occurs if (1) facts in private life or "matters that may be recognised" as such are disclosed, (2) the disclosed matters are those that ordinary people do not wish to have disclosed, and (3) the disclosed matters were previously unknown to the general public. Examples include:

- Information that can be easily recognised as private (i.e., especially sensitive matters): (A) divorce

status, (B) family structure, (C) sexual life, (D) sexual preference, (E) private medical condition, and (F) income information.

- Information that may be recognised as private on a case-by-case basis; for example: (A) marital status; (B) biographical information such as date of birth, address, name and telephone number, and (C) occupation.

Cases of "flaming" (i.e., hostile and insulting online interaction that typically occurs in a public internet forum) may involve repeated postings of the same information. In such cases, Japanese courts have nonetheless tended to find that element (3) of a Japanese privacy violation – the disclosure of matters previously unknown to the general public – can be satisfied notwithstanding the existence of previous, substantially similar "flaming" posts that may have been seen by the general public.

As a defence against a claim of privacy violation, a defendant will raise their right to "freedom of expression", which must be weighed and considered in court in its various elements: (1) the nature of the person whose privacy has allegedly been violated (for example, whether such person is a public figure), (2) the degree of sensitivity of the privacy interest being violated, and (3) whether there is a legitimate social interest involved.

Unlike in cases of defamation, the truth or falsity of the information disclosed is not relevant to the court's consideration of the "freedom of expression" defence. However, where (as is often the case) the posting of private information on an internet bulletin board is simply motivated by the personal interests of the commenter, courts are less likely to engage in a detailed weighing and consideration of the "freedom of expression" defence. In the majority of case law in these circumstances, a privacy violation is found to have occurred based on the simple factual situation that private information was posted on an anonymous online bulletin board.

V. ONLINE IMPERSONATION

As a general rule, the act of online impersonation by falsifying names, etc., may harm a person's "interest in maintaining personal identity", and may be a cause of action for damages, or an order to delete the relevant content as an infringement of personal rights. However, practically speaking, it is likely to be highly difficult to prevail on a legal action based upon this theory alone, absent other objectionable conduct.

One recent case involving online impersonation demonstrated that courts are hesitant to find infringement of personal rights in such cases of impersonation – with the court noting that "it is difficult to say a clear, common understanding exists regarding this situation as to the acceptable limits to the interest in maintaining personal identity…it is not easy to judge in what situation the impersonation harming the interest in maintaining personal identity was made, and therefore legal judgment on such impersonation should be cautiously made". [82] In this case, even the plaintiff's second-step identification procedure demand for identification of the person in question (see Section 3 below) was denied.

If the conduct in question extends beyond mere impersonation, to actions separately constituting actionable defamation or violation of privacy, claims for damages, etc., will be available on the grounds described above. For example:

- In one case, a court found that posting the date of birth, address, and telephone number of a person, among other matters, in order to impersonate such person, constituted a privacy violation.[83]

- In another case, a court ordered the deletion of a social media account, rather than the deletion of individual comments posted on the account. Here, the defendant had created an SNS account under the plaintiff's name and repeatedly posted comments falsely implying that the plaintiff was an adult entertainer. The court held that the entire account, in causing readers to confuse the plaintiff for an adult entertainer, constituted defamation.[84]

Similarly, online impersonation that makes use of another person's SNS accounts (i.e., via their account ID or password) without the account holder's permission will constitute criminal access under Article 3 of the Act on Prohibition of Unauthorized Computer Access, Act No. 128 of 1999, as amended. The punishment is imprisonment for up to three years or a fine of up to 1 million yen.

VI. TROLLING

Cases of "trolling" are treated under the law in the same manner as claims for defamation or privacy violation as discussed above, and are subject to claims for damages or a demand for deletion of the offending content, as in the doxxing cases discussed above (Articles 709, 710, and 723 of the Civil Code).

VII. BRIGADING

When a potential claim of defamation or privacy violation is based on the incorporation of a citation from another source within an online comment, the legal issues regarding linking to such other source are as follows (Articles 709, 710, and 723 of the Civil Code).

If the post containing the link is determined to "incorporate" the contents of that link, and the link contains information that is defamatory or in violation of privacy rights, then the post can also be found to be defamatory or in violation of privacy rights. The question of whether the overall structure of the post containing the link "incorporates" the linked content will be fact-dependent.

Clicking "like" is merely an indication of approval. Therefore, such an act is unlikely to constitute defamation or a privacy violation unless exceptional facts exist. Retweeting a statement may be considered the same as making the original statement. Therefore, if the original tweet constitutes defamation or a privacy violation, absent exceptional facts, then a retweet may constitute defamation or a privacy violation as well.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

Japan has no specific legal scheme that comprehensively regulates "online harassment". However, based upon the type of harassment, certain laws or regulations (in addition to those described above) may apply to provide relief to a plaintiff.

The act of insulting another person online without demonstrating facts (for example, use of the adjective "stupid") is seen as commonplace and does not constitute defamation or a privacy violation under Japanese law.

Theoretically, Article 231 of the Penal Code prohibits insulting others. The criminal punishment for violating this law is penal detention for a period less than 30 days, or a petty fine ranging from 1,000 to 10,000 yen. However, few cases are prosecuted under this law. No criminal cases, regardless of outcome, dealing with the application of this law to conduct on the internet were identified.

On the other hand, an insult can be the basis for making a claim under torts in a civil proceeding (herein referred to as "Insult Tort") (Articles 709 and 710 of the Civil Code), even if the insult does not constitute defamation or a privacy violation. Where an insult tort is found to have occurred, monetary compensation may be available – based on past cases, a plaintiff might expect an award ranging from 10,000 to 500,000 yen. Unlike a case for defamation, the remedy of obtaining the defendant's public apology in a newspaper is not available in the case of an insult tort.

The required elements for establishing an insult tort claim are as follows:

- Injury to feelings of personal dignity: This means the subjective "feeling or sentiment owned by oneself regarding its own value" held by the plaintiff.
  - The making of common Japanese insults such as *baka* (stupid), *aho* (idiot), and *manuke* (fool) have been found to infringe on feelings of personal dignity and cause injury.
  - Unlike cases of defamation or privacy violation, the insult must have been communicated to the person in question. Therefore, not all insulting statements published on the internet will constitute an actionable insult tort claim. For example, if an insulting statement is posted on an SNS page that can only be accessed by permitted users (i.e., friends, followers, etc.), and the victim does not have access to such content, no insult tort claim will exist.
- "Exceeding the permissible limits of socially-accepted conventions"
  - No clear-cut rule can be applied to determine whether a particular statement, made in a particular medium, constitutes an insult tort. This determination depends on various case-specific factors, such as the content and number of the posted statements, the types of websites where the statements were posted, the position, occupation, and age of the targeted person, and whether the defendant had a legitimate purpose in making such statements.
  - Case law provides a few specific examples for context:
    - » Commenting on a person's physical appearance: In one case, a court found that the statement "[the target person's] face is also ugly" exceeded the permissible limits of socially accepted conventions. However, in another case, a court found that a statement that the target person was "bald and fat" did not. As for use of the expression *busu* (extremely ugly), some cases have found violation of the law, while others have not.
    - » Commenting on a person's ability: One case involving the word *kichigai* (madman, or useless) was found not to have violated the law, while other cases involving the words *baka* (stupid) or *aho* (idiot) were found to have violated the law.

Due to the rapid evolution of online discourse and the potential for novel forms of harassment, it is possible that other Japanese laws (beyond Article 231 of the Penal Code, and the Insult Tort claim) may also apply, and provide a legal remedy, based on specific facts and circumstances.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Japan's Hate Speech Law, which was enacted in 2016, applies specifically to hate speech made on the grounds that a person or their ancestor came from a country other than Japan, i.e., xenophobic hate speech towards

people who are not ethnically Japanese. This law does not apply to gender-based discrimination and does not broadly apply to all cases of racial discrimination

The application of the Hate Speech Law is limited to speech that "openly incites exclusion of person(s) from countries outside of Japan from the local Japanese community" for the purpose of "causing or promoting the public sense to discriminate" against such foreigners by the method of "making public statements that create the risk of harming the life, person, freedom or public esteem [of the target(s)] or are significantly insulting".

Notably, the Hate Speech Law provides only the "principle" to eliminate such speech from Japanese society. There is no actual provision to enforce the prohibition of such speech nor legal liability for making such speech under this law. In one judicial precedent,[85] the court referred to the Hate Speech Law as a logical basis to support its affirmation of injunctive relief (by stressing the importance of protection against hate speech) – but the Hate Speech Law itself was not a source of legal liability.

Instead, the legal causes of actions and remedies available in cases of hate speech are those in accordance with the generally applicable legal framework of defamation, as described in Section 2(b), above.

Even in cases in which a discriminatory expression is made against a group identified as a specific gender or race, such expression itself does not constitute an actionable tort, and a person belonging to the specifically targeted race or gender does not have a right to tort remedies. However, if the discriminatory expression is made against a specific individual or legal person regarding the group (race or gender) to which they belong and this expression injures the societal judgment of the target, such speech may be actionable as a defamation claim.

In particular, with respect to a demonstration containing speech that constituted hate speech as defined in the Hate Speech Law, claims for damages and injunctive relief against the demonstration were considered by a court on the grounds that the conduct could constitute a tort claim by the target person of the demonstration[86] or by the residents of the town (which was home to a concentrated population of the foreign-born residents being targeted).[87]

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

No precedents have been identified. Rather, the legal framework for defamation and privacy violation has been formed by case law through which Japanese courts have sought to strike a balance between the right to publicity and privacy, on the one hand, and freedom of speech, on the other. In other words, such balance is embedded in the defence that is available for a defendant under the legal framework.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER

Subject Matter of the Procedure

As described in Section 2(a), with respect to written harassment published on the internet that is accessible to the general public, the targeted person may demand that the relevant ISP disclose personal information regarding the poster (the writer) in accordance with the Provider Liability Law.

However, with respect to anonymous harassment carried out using direct messaging functions, such as a mail, messenger, or direct message service of an SNS, there is no legal avenue for identifying the person in question, because these functions are not the subject matter of the Provider Liability Law.

Process Flow

The specific procedure for demanding disclosure, if applicable, requires two steps as follows:

Step (1): Obtaining IP Address and Time Stamp

An individual who is anonymously harassed may request the content provider (i.e., the company or service that provides the public with the relevant content) to disclose the IP address and time stamp ("non-judicial disclosure request"). In that case, the content provider first contacts the person whose identity is in question in writing and inquires whether or not they agree to disclosure of their identity (the "inquiry of opinion"). The content provider will reject the disclosure request if (A) the person in question raises an objection, and (B) the content provider does not think there is a clear violation of rights, or is uncertain whether a violation of rights occurred. As a practical matter, content providers often reject such disclosure requests.

A victim may file a claim in the courts to compel the disclosure if their non-judicial disclosure request is rejected – or may elect to forego making a non-judicial disclosure request and proceed directly to a claim in the courts to compel the disclosure. In case of a court proceeding, typically a provisional disposition is used as the relevant court judgment, and it would require two to four weeks to obtain the disclosure of the harasser's identity if the petitioner is successful on the claim.

Step (2): Information That Can Identify the Person in Question (Such as Their Name) Corresponding to the IP Address

In Japan, based upon the IP address obtained from the content provider, by using Whois,[88] etc., the ISP servicing the person in question can be identified. The harassed individual can make a request to the relevant ISP for disclosure of the name and address of the user assigned to such IP address as of the relevant time. The procedure for such request is the same as Step (1) above with respect to content providers. Also in this case, as a practical matter, the ISP often refuses to make such disclosure.

If a judicial remedy is sought, a provisional disposition will not be available, and standard litigation procedures will apply. Obtaining the disclosure of the identity of the anonymous harasser, if the action is successful, would typically require three to six months.

Practical Points for Consideration

In either of the two steps set out above, the disclosure of the anonymous harasser's identity will not always be successfully obtained. In order to successfully compel disclosure, the victim is required to demonstrate prima facie proof (in case of a provisional disposition under Step (1)), or prove a high probability of success (in the case of litigation under Step (2)) that tortious conduct resulting in the violation of legal rights (such as defamation or the violation of privacy) has occurred. Therefore, the burden of proof in the litigation proceeding to compel disclosure of the anonymous harasser is nearly the same as that which would apply in the actual litigation based on the tort claim itself, if the harasser's identity were known.[89]

In addition, if the ISP has ceased to maintain the relevant IP address logs, etc., it will not be possible for the ISP to make the relevant disclosure, even if the victim of the harassment prevails in a lawsuit to compel such

action. Although the preservation period for such logs differs by ISP, a log usually is deleted approximately three months from the time when the recording is made. In this regard, it was therefore absolutely necessary in the past to file a provisional disposition against the ISP to prohibit deletion of the relevant log after performing Step (1) discussed above.

Recently, however, if the non-judicial disclosure request pursuant to Step (2) set out above is made in a form prescribed by the Japanese Telecom Services Association (the so-called "TELESA form") outside of court, most ISPs will automatically retain the information of the person in question (in paper format), from the time when the inquiry from the ISP to the person whose identity in question is made. Therefore, with respect to most ISPs, a victim who has made the non-judicial disclosure request in the TELESA form may be able to obtain relevant information from the ISP, even if a provisional disposition to prohibit the ISP from deleting the log is not filed. In any event, a victim must be careful about what kind of policy the relevant ISP has regarding retention of the information in question. In summary, it is still necessary to demand the disclosure as set out in Step (2) above, or to file a provisional disposition to prohibit the deletion of the log, within three months from the time when the writing is made.

PRACTICAL INFORMATION

- Japanese Law Translation.

KENYA

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

A media organisation would have the right to institute proceedings on its own behalf where its own rights are infringed. They may also institute actions on behalf of their members. The Constitution of Kenya (the Constitution) expands the *locus standi* on who may institute constitutional proceedings claiming a right under the constitutional Bill of Rights has been infringed, denied, threatened or violated. In particular, it provides that such court proceedings may be instituted by:[90]

- a person acting on behalf of another person who cannot act in their own name;
- a person acting as a member of, or in the interest of, a group or class of persons;
- a person acting in the public interest; or
- an association acting in the interest of one or more of its members.

The Constitution further clarifies that a person when used in the Constitution is to be interpreted as including a company, association, or other body of persons whether incorporated or unincorporated. This constitutional provision has therefore expanded the understanding on who may institute a constitutional petition in Kenya to virtually anyone with even a remote interest, since virtually any person acting in the interest of another may institute an action in Kenyan courts.

However, practically and to avoid procedural irregularity claims, where the right enforced is of a personal nature (for example the right to privacy of one's personal data), the person or journalist would have to be enjoined to the proceedings as a personal right such as a data protection right applies to a person and not a legal person.

In relation to statutory and tort claims not grounded on the Constitution (such as defamation), these claims are typically instituted by the journalist him/herself since locus standi in these matters is not expanded in the manner outlined in the Constitutions. Media organisations may however be enjoined to these proceedings where appropriate.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

The applicable law in Kenya relating to online attacks is the Computer Misuse and Cyber Crimes Act No. 5 of 2018, (the CMCA).

Territorial Jurisdiction

Generally speaking, an offence under the CMCA which is committed outside Kenya would be deemed to have been committed in Kenya if:[91]

- the person committing the act or omission is:
    i. a citizen of Kenya; or
    ii. ordinarily resident in Kenya; and
- the act or omission is committed:
    i. against a citizen of Kenya;
    ii. against property belonging to the Government of Kenya outside Kenya; or
    iii. to compel the Government of Kenya to do or refrain from doing any act; or
- the person who commits the act or omission is, after its commission or omission, present in Kenya.

In any of these instances, the authorities in Kenya would have the right under the CMCA to enforce its provisions regardless of whether the offence was committed outside Kenya.

International Jurisdiction

The CMCA establishes the National Computer and Cybercrimes Co-ordination Committee (the Committee), which is comprised of various high-level government officials. The Committee is mandated to advise the Kenyan government on cybercrime issues generally, and with the responsibility to cooperate with computer incident response teams and other relevant bodies, locally and internationally on response to threats of computer and cybercrime and incidents.

The CMCA also establishes the Central Authority as part of the enforcement bodies under the Act. The Central Authority, which is the Office of the Attorney General and Department of Justice, is also part of the Committee and therefore privy to all cybercrime issues that the Committee deals with. The CMCA establishes that the Central Authority has the power to enforce the CMCA's provisions in accordance with the Mutual Legal Assistance Act, No. 36 of 2011 (the MLA).

The MLA is the establishing law in Kenya that provides for mutual legal assistance to be given and received by Kenya in investigations, prosecutions and judicial proceedings in relation to criminal matters, and for connected purposes.

To this end, the CMCA allows the Central Authority to cooperate with other international agencies and requesting states in relation to any criminal matter that they may need assistance. That said however, the Central Authority is not required to cooperate with these international agencies or other states, and each request is subject to the Central Authority's discretion.

Similarly, the Central Authority is also empowered to send such requests to other states for enforcement and particularly to request for mutual assistance from other states in:

(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or data;

(b) collecting evidence of an offence in electronic form; or

(c) obtaining expeditious preservation and disclosure of traffic data, real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act.

Extradition requests may also be made to the Central Authority, subject to existing laws on extradition. Note that in Kenya, the process for extradition from and to Commonwealth countries is different from other countries.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

Yes. Section 27 of the CMCA provides that cyber harassment is an offence punishable to a fine of up to KES 20,000,000 (approx. USD 200,000) and/or up to 10 years imprisonment. Cyber harassment under the CMCA is defined as wilful communication by either an individual or a group, either directly or indirectly, with another person or anyone known to that person, which:

- is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or
- detrimentally affects that person; or
- is in whole or part, of an indecent or grossly offensive nature and affects the person.

An amendment bill to the CMCA was gazetted in April 2021, which proposes to expand the definition of cyber harassment to include conduct that:

- is likely to cause those persons to commit suicide or cause any other harm to themselves; or
- is likely to cause other persons to join or participate in unlicensed and extreme religious or cult activities.

Section 27 of the CMCA further empowers any aggrieved person (or an intermediary on behalf of a complainant) to make an application to court to compel a person to stop any conduct deemed as cyber harassment. The Courts are empowered under this Section to grant interim orders and hear such an application within 14 days. The Court may also order a service provider to provide any subscriber information in its possession for identifying a person whose conduct is complained of under this Section. A service provider under the CMCA is broadly defined and includes any public or private entity that provides to users of its services the means to communicate by use of a computer system, and any other entity that processes or stores computer data on behalf of that entity or its users. A person who fails to comply with such court orders commit an offence and

may be liable on conviction to a fine of up to KES 1,000,000 (approx. USD 10,000) and/or up to 6 months imprisonment.

Aside from cyber harassment, the CMCA also criminalises non-consensual dissemination of intimate images (NCII), popularly known as 'revenge porn', under Section 37. Section 37 provides that any person that transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence under the CMCA. The offence is punishable on conviction to a fine of up to KES 200,000 (approx. USD 2,000) and/or up to 2 years imprisonment.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

I. THREATS

Given the wide definition of cyber harassment above in (a), online threats would also be covered under this Section of the law, and one may use the court reliefs provided thereunder. In addition to this, one may use the Penal Code (Cap. 63 of the Laws of Kenya) which has the following helpful provisions:

- Section 223, which criminalises threatening to kill another person. Such a threat is punishable by imprisonment for up to ten years;
- Section 299, which criminalises demanding of property by threats providing a corresponding penalty of imprisonment for up to fourteen years;
- Section 344, which criminalises sending, delivering, or uttering of any letter or writing intended at threatening to burn someone's property. Any guilty party is liable to imprisonment for seven years.

II. INTIMIDATION

Intimidation is understood as the act of threatening or frightening someone to force them to do something that you want. Online intimidation can certainly be enforced as cyber harassment and/or threats as outlined above. In addition to this, the Penal Code at Section 238 criminalises intimidation and provides that a guilty party shall be liable upon conviction to up to 3 years in prison. This Section specifically defines intimidation as where a person intimidates another person:

- with intent to cause alarm to that person or to cause him to do any act which he is not legally bound to do or to omit to do any act which he is legally entitled to do;
- causes or threatens to cause unlawful injury to the person, reputation or property of that person or anyone in whom that person is interested.

Practically, journalists have had challenges enforcing these provisions particularly where the government levies the threats or intimidating attacks against them. Kenyan journalists have been targets of intimidation by the police, especially when covering contentious issues such as police brutality.

III. CYBERSTALKING

- There are no specific provisions that outlaw cyberstalking, however one may use the CMCA provision on cyber harassment and Penal Code provisions on threats and intimidation.

IV. DOXXING

Doxxing is understood as searching for and publishing private or identifying information about (a particular individual) on the internet, typically with malicious intent.

The Constitution of Kenya guarantees the right to privacy under Article 31. In particular, the Constitution provides that as part of the right to privacy, one has the right not to have information relating to their family or private affairs unnecessarily required or revealed, or the privacy of their communications infringed. Flowing from this, one would have the right to lodge a constitutional petition with the High Court enforcing this right where their privacy is breached. For example in *M W K v another v Attorney General & three others [2017] eKLR*, the case involved the sharing of a child's nude photos online. In this matter, the court awarded the Petitioner KES 4,000,000 (approx. USD 40,000) and it declared that the respondent's conduct violated among others, the child's right to privacy.

Where the doxxing involves sharing of intimate images, Section 37 of the CMCA on NCII may also be used.

In addition, Kenya enacted a comprehensive Data Protection Act, No. 24 of 2019 (the DPA), which prohibits unlawful processing of personal data. The DPA mirrors the GDPR in many ways and provides similar protections to data subjects who are the victims of unlawful processing of data. A data subject who is aggrieved by a decision of any person under the DPA may lodge a complaint with the Data Commissioner. Law enforcement officials may also enforce these DPA provisions. For example, in 2020, the police arrested a famous Kenyan blogger for publishing on social media a copy of a visa issued to a famous vlogger, which included details relating to her full name and date of birth. The outcome of this case is still pending.

Where the information shared is of a defamatory nature, i.e. it tends to lower the reputation of the person involved among the right-thinking members of the society, one may also sue for defamation. Defamation laws in Kenya are only enforced in civil proceedings, as criminal defamation was ruled unconstitutional in Kenya.[92]

V. ONLINE IMPERSONATION

Under Section 29 of the CMCA, any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine of up to KES 200,000 (approx. USD 2,000) and/or to imprisonment for a term of up to 3 years.

In addition, Section 28 of the CMCA also criminalises intentionally taking or making use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right. This offence is punishable on conviction to a fine not exceeding KES 200,000 (approx. USD 2,000) or imprisonment for a term not exceeding two years or both.

VI. TROLLING

No specific laws apply to trolling. However, where the trolling is severe and meets the threshold of harassment, threats or intimidation, one may utilise the provisions outlined above. Where the trolling is also defamatory in nature, one may also sue for defamation as outlined above to recover damages.

VII. BRIGADING

There is no specific provision that outlaws brigading in Kenya. However, provisions that prohibit the sending of offensive messages online can, similar to trolling above, be utilised to deal with brigading.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

Defamation Act

As we have outlined above, the Defamation Act, Cap. 36 may apply where the online harassment constitutes publishing statements that tends to lower the reputation of the person involved among the right-thinking members of the society. For a claim of defamation to be sustained and successful, one must establish:

- a false statement purporting to be fact;
- publication or communication of that statement to a third person, in this case, online publication would be sufficient; and
- damages, or some harm caused to the person or entity who is the subject of the statement.

As we have explained above, defamation can only be enforced as a civil matter in Kenya, as criminal defamation was ruled unconstitutional and impinging on freedom of speech laws.

Penal Code

As outlined above, where the online harassment constitutes threats or intimidation under the Penal Code, one may also press charges with the police under these Sections.

National Cohesion and Integration Act

The National Cohesion and Integration Act, No. 12 of 2008 (the NCIA) outlaws any discrimination or harassment based on one's ethnicity. Complaints under the NCIA can be made to the National Cohesion and Integration Commission.

The Sexual Offences Act

The Sexual Offences Act, No. 3 of 2006 (the Sexual Offences Act) prohibits sexual harassment, which is the making of unwanted sexual advances by a person in authority, or a public office holder who reasonably knows that the advances are unwelcome. Where online harassment is of a sexual nature and is committed by public office holders, one may press charges under this Section of the Sexual Offences Act. A person convicted for sexual harassment is liable on conviction to imprisonment for a term of up to 3 years and/or to a fine of not less than KES 100,000 (approx. USD 1,000).

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Constitution of Kenya

The Constitution in Article 27 grants all persons the right to equality and freedom from discrimination of any kind. Where the abuse includes discriminatory conduct based on race and/or gender, one may file a constitutional petition enforcing their right under this Article.

National Cohesion and Integration Act

As outlined above, any harassment or discrimination based on one's ethnicity is prohibited under the NCIA. In addition, the NCIA outlaws hate speech – defined as the publication or distribution of material that is abusive and calculated to cause ethnic hatred. If found culpable, one is liable to imprisonment for a term not exceeding five years or a fine of KES 5,000,000 (approx. USD 5,000) or both.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Yes. There are cases where laws relating to online activity and harassment have been found to be unconstitutional. In addition to criminal defamation laws as outlined above, the courts have also ruled that the following provisions infringe on freedom of speech:

- **The Kenya Information and Communications Act, No. 2 of 1988 (KICA), Section 29.** This provision outlawed the use of a telecommunications network to send a message that was grossly offensive or of an indecent, obscene or menacing character. The Petitioner *in Geoffrey Andare v Attorney General & two others [2016] eKLR* challenged the Constitutionality of this provision based on existing freedom of speech laws. The court held that the penal provision was unconstitutional as it imposed consequences both broadly and vaguely.
- **The Penal Code, Section 132**. This provision outlawed the publishing or uttering of words calculated at undermining the authority of a public officer and any person found guilty would be liable for imprisonment for three years. In *Robert Alai v The Hon Attorney General & another [2017] eKLR,* the Court declared that the provision was unconstitutional as it violated the petitioner's constitutional right to freedom of expression.
- **The CMCA.** Prior to commencement of the CMCA, the Bloggers Association of Kenya (BAKE) filed Petition 206 of 2018 at the High Court challenging the constitutionality of twenty six (26) Sections of the CMCA alleging that they were excessive and impinged on the constitutional freedom of expressions. Some of the salient provisions that were suspended covered the composition of the National Computer and Cybercrimes Co-ordination Committee and the establishment of certain offences. The High Court suspended the contested Sections on 30 May 2018 and the suspension was lifted on 20 February 2020 when the High Court dismissed the petition.[93]

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Kenyan laws are not specifically adapted to dealing with anonymous online harassment. There are however some practical avenues that a journalist may use to identify an anonymous harasser, such as:

File a complaint with the Directorate of Criminal Investigations

The complainant can file a complaint with the Directorate of Criminal Investigations (DCI) and provide the alleged post as evidence. The DCI will then investigate by coordinating with the National Kenya Computer Incident Response Team – Coordination Centre (the KE-CIRT/CC). The Centre shall assist the DCI in compiling the evidence and once complete, the DCI refers the matter to the Office of the Director of Public Prosecutions (ODPP) to commence prosecution.

National Kenya Computer Incident Response Team – Coordination Centre

Alternatively, one may also report the incident to the KE-CIRT/CC, who can coordinate directly with the DCI as outlined above. The KE-CIRT/CC is an online enforcement agency established under the KICA to mitigate cyber threats and foster a safer Kenyan cyberspace. The KE-CIRT/CC is a multi-agency collaboration framework that is responsible for the national coordination of cyber security as well as Kenya's national point of contact on cyber security matters.

PRACTICAL INFORMATION

- National KE-CIRT/CC website.

THE NETHERLANDS

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

Media organisations do not have individual legal standing to take action before the courts in case of online harassment of journalists.

That being said, media organisations can (and do) provide guidance and advice, including legal advice to journalists suffering such harassment. It is also conceivable that they would serve as experts in a civil or criminal trial. In addition, they could theoretically initiate civil proceedings in the form of a class action (*collectieve actie*) for example in case of directed, systematic wrongdoings perpetrated by individuals or groups of individuals. Journalists are encouraged by their professional organisations to file complaints for criminal offences with the police, either themselves, or through their employers.[94]

Furthermore, a dedicated platform called 'persveilig.nl' ("Persveilig" - see ***Practical Information Section*** below) has been initiated by media organisations in conjunction with (i) the police and (ii) the public prosecutor's office. This platform can provide advice and support in case of grave harassment as well as tools for the collection and filing of less serious matters. The primary contact point is the Dutch Association of Journalists, with complaints able to be escalated to the police and public prosecutors where necessary.

Persveilig also produced various road maps aimed at providing a safe work environment to journalists. These include:

- **The collective norm for the media sector (*collectieve norm media sector*)**[95] which includes a list of situations in which players in the media sector and public enforcement (i.e. media organisations, journalists' associations, public prosecutors and the police) have agreed to always file a report at the police. This includes:
  - Threats (for example verbally, via a threatening letter, social media or their own sources);
  - Physical violence;
  - Sexual violence (rape, assault, groping, etc.);
  - Discrimination (based on inter alia skin colour, religion, sex, and/or sexual orientation);
  - Stalking/ systematic intimidation (whether or not via social media);
  - Theft; and
  - Intentional destruction of property.

- **The Dutch Media Safety Plan (*veiligheidsplan Nederlandse media*)**[96] which is a practical guide for journalists, employers of journalists and other media organisations. It includes inter alia:
  - Points of action for employers to make sure that (new) employees are and feel safe whilst doing their work, including guidelines on how to install a 'crisis management team';
  - Points of action for journalists on how to safely use social media, this includes inter alia an annex on shielding (of social media) guidance;
  - Points of action for journalists and their employers on how to act in case of involvement in legal proceedings;
  - A list of actions against journalists that are illegal. These include:
    - Threats (of i.a. violence, rape, murder). 'Wishful thinking' meaning for example "I want to rape/murder/hit you" does (in principle) not qualify as making a threat;
    - Physical violence;
    - Sexual violence;
    - Discrimination;
    - Stalking;
    - Theft;
    - Points of action for journalists working abroad and points of action for employers sending their employees on missions abroad.
- **The Protocol Safe Press (*Protocol Persveilig*)**[97] which includes certain ground rules such as that employers should be the one reporting criminal offences at the police, instead of the individual journalist. It also:
  - includes a reference to the Dutch Media Safety Plan (see above);
  - includes a promise from the police that journalists have a preferential position when they press charges. When filing a complaint at the police, journalist are encouraged to emphasise that they are being harassed in/due to the performance of their job as journalists. This will provide higher priority to their cases with the police investigation and will constitute an aggravating circumstance, thereby leading the public prosecutor to argue in favour of a higher sentence (in cases where the harassment is taken to court); and
  - includes a commitment of the public prosecutor's office to demand twice the punishment against perpetrators who have shown violence or aggression against journalists.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

First, according to the Dutch Civil Procedure Code, claimants seeking redress with the Dutch courts have standing with the Dutch courts where the wrongful act was conducted in the Netherlands or had its effect in the Netherlands. In relation to online harassment, Dutch civil procedure and the Civil Code cover cases where the perpetrator, victim or platform is based in the Netherlands could be admissible before the Dutch courts.

It should however be stressed that the conflict of law rules in the European Union are governed by Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement

of judgments in civil and commercial matters. According to this Regulation, the competent jurisdiction is the one in which the defendant has its domicile or, in matters relating to tort, delict or quasi-delict, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez* of 25 October 2011,[98] the Court of Justice of the European Union considered that the criterion of the place where the damage occurred confers jurisdiction to courts in each Member State where the online content is or has been accessible. It further specified that those courts have jurisdiction only in respect of the damage caused in the territory of their Member State.

Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters strengthens the cooperation of the civil courts of the Member States regarding the transmission of evidence. This regulation speeds up the process of transmission of evidence by providing the potential direct transmission of evidence between the courts.

Secondly, according to the Criminal Procedure Code, Dutch criminal courts are competent to adjudicate matters where offences were committed in the Netherlands with limited (but nonetheless extensive) extraterritorial jurisdiction, including in case of (online) threats (art. 284 Criminal Code).

Judicial co-operation has been strengthened within the European Union. Indeed, any Member State may issue a judicial decision (known as a "European investigation order" or EIO) requesting another Member State to carry out investigations on its territory within a certain period of time in order to obtain evidence relating to a criminal offence or to communicate evidence already in its possession.[99]

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

There are no specific laws regarding online harassment. This does not mean that online harassment is not illegal. Online harassment usually falls within one of the categories specified below.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE:

I. THREATS:

Article 285 of the Criminal Code relates to threats, including when made online.

II. INTIMIDATION:

Article 284 of the Criminal Code relates to intimidation, including when occurring online.

III. CYBERSTALKING:

Article 285b of the Criminal Code relates to cyberstalking.

IV. DOXXING:

Doxxing can be seen as a form of intimidation (see above under (ii)) or as a breach of the GDPR (EU General Data Protection Regulation).

V. ONLINE IMPERSONATION:

Article 231 of the Criminal Code.

VI. TROLLING:

There are no specific laws to capture trolling.

VII. BRIGADING:

There are no specific laws to capture brigading.

In addition to the above, online harassment can in some cases also qualify as hate-mongering (Article 137d of the Criminal Code) or group defamation (Article 137c of the Criminal Code).

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

The Criminal Code (*wetboek van strafrecht*), for example the aforementioned Articles 284, 285 and 285b of the Criminal Code (as set out above) which can be used to prosecute offences committed regardless of whether they were committed online or offline. Additionally, the provisions on slander (261 Criminal Code) and insults (266 and 271 Criminal Code) could be utilised.

In addition to the above, it should be noted that under Dutch law, it is also possible for victims of crimes to make a civil claim for compensation of damages within, during or as part of the criminal proceedings.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Article 1 of the Dutch Constitution entails a prohibition of all forms of discrimination. Article 137 of the Criminal Code consequently allows for the filing of complaints concerning the prohibition of discrimination with the competent authorities. This prohibition is also incorporated into various articles of the Criminal Code. Discrimination or discriminatory statements are therefore possible crimes under Dutch laws and can also be aggravating circumstances in the context of other crimes (such as, for example, violent acts).

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Yes, in the Netherlands there is a continued tension between, on the one hand, freedom of speech and, on the other hand, the prohibition of discrimination. A famous example is a case in which politician Geert Wilders was charged for discriminatory statements/hate-mongering at the expense of the Moroccan community in the Netherlands in which he claimed he was only using his freedom of speech privileges. Wilders was found guilty of insulting an entire group, but was acquitted of hate-mongering. No punishment was imposed.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

From a practical perspective, while individual investigations may, in some cases, allow a journalist to identify an anonymous harasser based on information published online, this may not be the wisest course of action as it may, inadvertently, entail using information illegitimately collected (for example, under GDPR).

Subsequently, a police report can be filed; police (and public prosecutors) have the most far-reaching investigatory options in relation to crimes perpetrated. However due to capacity issues, the police may not always be able to fully and/or rapidly process reports.

Therefore, journalists may consider initiating civil lawsuits or injunctions to network providers (see for example, the aforementioned Facebook case) to obtain information to identify the anonymous harasser. This information can then be shared with police, which in turn may prompt a swifter response from police.

PRACTICAL INFORMATION

Websites:

- www.persveilig.nl
- www.nvj.nl
  - www.nvj.nl/rechtshulp
  - www.nvj.nl/balie-persvrijheid
- www.persvrijheidsfonds.nl/
- www.nvj.nl/balie-persvrijheid
- www.stdem.org/nieuwsbrief/
- www.discriminatie.nl/#/home

Phone numbers:

- Balie Persvrijheid (a professional organisation for journalists, which offers free legal advice): +31 (0)20 - 30 39 791
- NVJ Legal Services: +31 (0)20-30 39 700.
- Police: +31 (0)900-8844

SWEDEN

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

To take legal action against online harassment, the online harassment must constitute a crime. Media organisations have no specific standing to take legal action against online harassment of journalists under Swedish law. When a journalist is the victim of online harassment, only he or she has legal standing to initiate a criminal procedure. However, media organisations may claim damages in a civil procedure, provided that they have suffered economic loss as a result of the harasser's criminal actions. In practice, this is generally difficult to prove.

Some crimes can be reported to the police by anyone and it is up to the prosecutor to decide if a prosecution shall be brought before a court. However, crimes such as unlawful violation of personal integrity, for example the spreading of an image or other information online regarding a person's sexual habits, may only be prosecuted by a public prosecutor if the victim reports the crime, or it is called for from a public standpoint. In addition, insult and defamation are only available for private prosecution (i.e. initiated by the victim), and the public prosecutor may only prosecute them if they affect the public interest, for example if the defamation involves very serious accusations or the defamation has reached a very large number of people.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

First, with respect to civil matters it should be stressed that the conflict of law rules in the European Union are governed by Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. According to this Regulation, the competent jurisdiction is the one in which the defendant has its domicile or, in matters relating to tort, delict or quasi-delict, the courts for the place where the harmful event occurred or may occur.

In its ruling *eDate Advertising and Martinez* of 25 October 2011,[100] the Court of Justice of the European Union considered that the criterion of the place where the damage occurred confers jurisdiction to courts in each Member State where the online content is or has been accessible. It further specified that those courts have jurisdiction only in respect of the damage caused in the territory of their Member State.

Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters strengthens the cooperation of the civil courts of the Member

States regarding the transmission of evidence. This regulation speeds up the process of transmission of evidence by providing the potential direct transmission of evidence between the courts.

The above mentioned EU regulations are only applicable between member states of the EU. In the case of an international jurisdictional issue, which does not involve another EU member state, Swedish national legislation regulates whether Swedish courts have jurisdiction. According to Chapter 10 of the Swedish Code of Judicial Procedure[101], the court that has jurisdiction is either:

- the court in which the defendant is domiciled;[102]
- the court in which jurisdiction the defendant resides, if the defendant is not domiciled in Sweden, and does not have a known domicile abroad;[103]
- the court in which jurisdiction the defendant was last known to be domiciled or last known to reside, if the defendant is a Swedish citizen, resides outside of Sweden or it is not known where the defendant resides;[104]
- the court where the defendant has property, if neither i, ii nor iii apply and if the claim is in regard to a dispute concerning the obligation to pay a compensation claim;[105] or
- the court where the damage occurred, provided the claim is based on a tortious act.[106]

Please note that if a civil claim is also the subject of criminal proceeding, the jurisdictional regulations for criminal proceedings will prevail on that applicable to civil proceedings (see below).

Secondly, with respect to criminal matters, according to the Swedish Penal Code[107] Chapter 2 Section 2, Swedish courts have jurisdiction over crimes committed on the internet if:

- the crime was committed or completed in Sweden;
- there is reason to assume that the crime has been committed in Sweden;
- the crime was committed by a Swedish citizen or by a foreigner domiciled in Sweden;
- the crime was committed by a foreigner without domicile in Sweden, but who after the crime became a Swedish citizen or has moved to Sweden;
- the perpetrator is a Danish, Finnish, Icelandic or Norwegian citizen and is in Sweden; and
- the crime was committed by a foreigner who is in Sweden and the legal penalty may include six months imprisonment.

The fact that the necessary conditions mentioned above are met in online harassment cases must be assessed on the basis of the circumstances of each individual case. Unfortunately, there is not much case law in Sweden in which the issue of territorial jurisdiction has been assessed with regard to online harassment.

When the evidence of a crime committed online may be found in another state, such information may be obtained through legal assistance via international judicial co-operation. Such international judicial co-operation may only be requested by the authorities. Most of Sweden's co-operation agreements have been codified in the Swedish act (2000: 562) on international legal assistance in criminal cases[108] and the Swedish act (2017: 1000) on a European investigation order[109] ("EIO"). EIO is implementing Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. In accordance with EIO, a Swedish prosecutor may issue an investigation order if the conditions to take the corresponding investigation measure in a Swedish preliminary investigation, or in a trial in a criminal case, are met.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

There is no specific legislation dealing with online harassment, and harassment as such is not defined under Swedish law. Instead, online harassment can include a number of criminal acts which are prohibited by the regular criminal legislation, see question 2(b) below.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

The relevant legislation is primarily the Swedish criminal code ("BrB"). In addition, the journalist may also be entitled to make a compensation claim against the harasser for the violation of the journalist's person, peace or honour.

I. THREATS:

Unlawful threats, BrB, Chapter 4, Section 5. A threat constitutes an unlawful threat if it includes a threat of a criminal act and is such that it typically evokes serious fear for the threatened person's own safety or for the safety of someone else's person, property, freedom or peace. The penalty for an unlawful threat consists of fines or imprisonment for up to one year. If the criminal act is deemed as a serious crime, the penalty is instead imprisonment for a minimum of nine months, and up to four years. However, it is less common that unlawful threats made online results in prison sentences, the most common penalty for unlawful threats made online being fines.

II. INTIMIDATION:

Intimidation is not defined as a criminal offence. However, the act of intimidation may include criminal offences. Intimidation may include *unlawful threats*, see (i) above.

Molestation, BrB, Chapter 4, Section 7. Intimidation may also include molestation. Molestation is defined as the act of exposing someone to unsettling contacts or other reckless conduct, if the act is likely to violate the victim's peace in a tangible way. Molestation does not necessarily imply a sexual connotation (see below). In the case of molestation on the internet, the act could include for example a very large number of messages on social media, e-mail or SMS when the recipient makes it clear that he or she does not wish to receive the messages. If the content is offensive, a smaller number of messages might also constitute molestation. It is less common that a single message is considered molestation. However, a single message might be considered molestation if it questions for example someone's human dignity, right to life and their security or otherwise expresses hatred towards someone. The penalty for molestation is fines or imprisonment for up to one year, although it is usually only punished by a fine.

Sexual molestation, BrB, Chapter 6, Section 10. Intimidation may also include sexual molestation. Sexual molestation is when the offender molests another in a way that is typically sufficient to violate the victim's sexual integrity. Examples of when acts on the internet have been regarded as sexual molestation is changing a person's profile on a social media and sending messages from that person´s account which presented the victim in a derogatory manner and sending of messages a sexual nature which violates the victim's sexual integrity. The penalty for sexual molestation is fines or imprisonment up to two years, although the most common penalties imposed for sexual molestation online are usually fines or shorter prison sentences.

III. CYBERSTALKING:

Cyberstalking is not defined as a criminal offence. However, the acts that constitute cyberstalking may include criminal acts.

Unlawful threats, see (i) above.

Molestation, see (ii) above.

Sexual molestation, see (ii) above.

Unlawful violation of personal integrity, see (iv) below.

Identity theft, see (v) below.

Unlawful persecution, BrB, Chapter 4, Section 4b. If the criminal acts of, for example, unlawful threats, molestation, sexual molestation, identity theft and unlawful violation of personal integrity have been part of a repeated violation of the victim's integrity, that constitutes unlawful persecution. A single unlawful threat of other criminal act does not constitute unlawful persecution, rather there must be repeated criminal acts. The more serious each separate act is, the fewer acts are required for the violation of integrity to be considered repeated. For repeated criminal acts to be considered unlawful persecution, the acts must have been committed against the same victim, and the repeated acts must have entailed a particular violation of the victim's integrity. The penalty for unlawful persecution can be up to four years imprisonment. The penalty in each case is highly dependent on the nature of the actions which constitute the unlawful persecution.

IV. DOXXING:

Unlawful violation of personal integrity, BrB, Chapter 4, Section 6c. The spreading of an image or other information regarding a person's sexual habits, health or information that a person has been the victim of a crime which includes an attack on the victim's person, freedom or peace is a criminal offence if the spreading is likely to cause serious harm to the victim. The same is true for the spreading of images depicting a person in a very vulnerable situation or images of a naked, or partially naked, person. For the spreading to be considered likely to cause serious harm the image or information generally has to be available to a larger group of people. It is however not required that a larger group of people have actually seen the image or information. The penalty for unlawful violation of personal integrity consists of fines or up to two years imprisonment. If the criminal act is deemed as a serious crime, the penalty is instead imprisonment for a minimum of six months, and up to four years.

The spreading of information such as contact details is not in itself criminalised under Swedish law. However, an individual may be entitled to request websites to remove personal information in accordance with the European General Data Protection Regulation (GDPR).

V. ONLINE IMPERSONATION:

Identity theft, BrB, Chapter 4, Section 6b. Identity theft is when someone, through the unlawful use of another person's personal information pretends to be them. Personal information includes only, in this case, information which is sufficient to identify the victim, for example, name, address, date of birth, photo, e-mail address or Swedish personal identity number. The act is only considered unlawful if the use of the personal information led to harm or inconvenience for the victim. The standard for what is considered harm or inconvenience is rather low. The penalty for identity theft is fines or up to two years imprisonment.

VII. TROLLING:

Trolling can be defined as a manipulation intended to harm the integrity of the community, by a person who, even if they have no particular interest in the subject matter, participates in debates with the aim of disrupting them. Trolling, defined as such, is not considered a criminal offence and there are no specific provisions punishing trolling in Sweden. However, the act of trolling may include criminal offences.

Unlawful threats, see (i) above.

Molestation, see (ii) above.

Sexual molestation, see (ii) above.

Insult, see (iv) below.

Defamation, see (iv) below.

Agitation against an ethnic or national group, see (d) below.

VII. BRIGADING:

Brigading is not defined as a criminal offence. However, the act of intimidation may include criminal offences such as unlawful threats, see (i) above, molestation and sexual molestation, see (ii) above.

It is not possible to prosecute a person for the acts of a group. However, it may be possible to argue that the circumstances in which one individual posted a message has an impact on the assessment of a message, if it can be shown that the person posting the message was aware of the situation in which it was posted. However, there is very limited case law on this issue. It may also be noted that it is not just the original posting of a statement or image that might be considered a criminal offence. The sharing and re-posting of the statement can also be a criminal offence.

Incitement to criminal behaviour, BrB, Chapter 16, Section 5. To incite others to commit criminal acts is in itself a criminal act. Comments online, which are not directed to a small closed group of people, which urges others to commit a crime, or praise a crime, can be considered inciting criminal behaviour. The penalty for inciting criminal behaviour consists of a fine or up to six months imprisonment. If the incitement is with regard to serious crimes, the penalty can reach up to four years imprisonment. However, no penalties shall be imposed if the incitement is deemed as a minor offence.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

The Swedish Act (1998: 112) on responsibility for electronic bulletin boards[110] ("BBS") imposes a responsibility on the provider of an electronic messaging service to remove messages from the service or otherwise prevent further spread of the message, if the message contains, for example, unlawful threats, unlawful violation of personal integrity, inciting of criminal behaviour or incitement to racial hatred. If the provider of the service does not, by intent or grossly negligent behaviour, comply with this responsibility it constitutes a criminal act.

Insult, BrB, Chapter 5, Section 3. An accusation, derogatory statement or humiliating behaviour may constitute an insult. Such a statement is only considered a criminal insult if it is aimed directly at the victim, the statement comes to the victim's attention, and the statement is such that it typically hurts the victim's self-esteem, i.e. the victim's subjective honour. The penalty for a criminal insult consists of a fine. If the act is considered a serious crime, the penalty consists of a fine or up to six months imprisonment.

Defamation, BrB, Chapter 5, Section 1. A statement constitutes defamation when it claims that a person is a criminal or otherwise reprehensible and the statement is such that it typically makes others think ill of the victim. The statement must contain information which can somehow be objectively verified. A value judgement, for example "he is ugly", does not constitute defamation. Defamation is not criminalised if (i) the information was true, or the person who made the statement had reasonable cause to believe that the information was true and (ii) the person who made the statement had a justifiable cause to provide the information. Even if the information is true it may still constitute defamation if the person who made the statement did not have a justifiable cause to provide the information. The penalty for defamation consists of a fine. If the act is considered a serious crime, the penalty consists of a fine or up to two years imprisonment.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Harassing comments online can be such that they constitute agitation against an ethnic or national group, which is a criminal offence.

Agitation against an ethnic or national group, BrB, Chapter 16, Section 8. A message online can constitute such agitation if it is spread outside the strictly personal sphere and threatens or expresses contempt, directly or indirectly, for an ethnic group or other such group of persons with reference to race, colour, national or ethnic origin, religion, sexual orientation or transgender identity. This can be sanctioned by up to two years imprisonment. If the act is considered a minor offence, the penalty consists of a fine. However, if the act is considered a serious crime, the penalty can range from a minimum of six months up to four years imprisonment.

In addition, if race or gender is a predominant factor in other criminal offences, for example insult, defamation or unlawful threats, it may be considered as an aggravating circumstance.

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

The legislation mentioned in this Section has been designed bearing freedom of speech in mind. Therefore, the legislation itself does not infringe freedom of speech. However, when the criminal legislation is enforced, the court will weigh the interest of prosecuting criminal statements against freedom of speech. As a consequence, some statements, which objectively fall under the legislation described above, may not be considered criminal.

For example, in a political debate, harsh and demeaning statements are generally tolerated to a larger extent.

It should also be noted that statements made on platforms which are encompassed by the Swedish Fundamental Law on Freedom of Expression[111] ("YGL") are subject to special criminal and procedural legislation. If the platform on which the statement is made is encompassed by YGL, the publisher is the sole person responsible for all criminal statements made on that platform. In such case, it is not possible to prosecute the individual who made the statement. Only the following acts are criminal if made on a platform encompassed by YGL; unlawful threats, defamation, insult, inciting of criminal behaviour and agitation against an ethnic or national group.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

If the harassment in question can be deemed a crime, the law enforcement authorities may request and obtain information such as the IP address or account details of an anonymous user from the electronic communication service or network provider. The providers of electronic communication services do not have any obligation to provide such information to private individuals, for example journalists.

Some of the most common types of online harassment, such as insult and defamation, are subject to private prosecution. The prosecution may be brought by a public prosecutor only if considered to be called for in the public interest. Due to the fact that the obligation to provide information is limited to the request of a law enforcement authority in connection to suspicion of crime, a journalist in the capacity of an injured party will be unlikely to get access to such information, especially since such information is generally confidential.

Another key issue is the fact that many communication service providers and other platforms are located outside Sweden. In these cases, international judicial co-operation through legal assistance might be necessary to obtain the IP address of an anonymous harasser. Such international judicial co-operation may only be requested by the authorities.

In conclusion, it may be very difficult for a journalist to identify an anonymous harasser. However, it is recommended to save, through for example screen shots, any information on the anonymous harasser such as usernames and e-mail addresses.

PRACTICAL INFORMATION

When subject to online harassment, the journalist is advised to;

- report the harassment to the police (the journalist does not have to be sure that the harassment constitutes a crime);
- save any evidence, for example the threatening messages, e-mail addresses or usernames;
- take screenshots (in case the message is deleted by the perpetrator);
- ask a friend or a colleague to witness the screenshots;
- save the screenshots in paper format and in digital form;
- if the message has been sent on social media, for example Facebook, or on an electronic bulletin board, for example a newspaper's comment section, ask the provider of the platform to remove the message; and
- report the harassment to your employer.

It is important to report harassment to the police. Even if the perpetrator is not convicted of a crime, the police reports can be used if the harassment is repeated by the same perpetrator.

If a journalist, or any other person, is subject to harassment which may cause the journalist to fear for his or her safety, the journalist may request that his or her address in the national registration is marked as confidential. An application is made to the Swedish Tax Agency. With such a marking in the national register, third parties will not be able to obtain the journalist's home address, unless the authorities assess that it will not cause harm to the journalist.

Websites:

- https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/nathat/
- https://polisen.se/lagar-och-regler/lagar-och-fakta-om-brott/it-relaterade-brott/nathat/
- https://polisen.se/utsatt-for-brott/olika-typer-av-brott/nathat/
- https://www.datainspektionen.se/vagledningar/oschysst-behandlad-pa-natet/#journalistiska
- https://www4.skatteverket.se/rattsligvagledning/330544.html

Phone numbers:

- 0046 114 14 (Swedish Police switchboard)

REUTERS/Peter Nicholls

UNITED KINGDOM - ENGLAND AND WALES

1. PRELIMINARY CONSIDERATIONS:

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

Whether a media organisation (as opposed to the journalist) will have standing to take legal action depends on the type of legal proceedings that will be brought. In some claims, it may be open to either the media organisation or the journalist to take legal action, while in others there will be strict rules as to who can do so.

A brief overview of the position for some of the most common types of legal action taken in response to online attacks against journalists is set out below. However, the rules regarding who has standing to bring a legal action are complex, so both journalists and media organisations should always take legal advice before pursuing legal action.

- **Harassment (civil).** A civil claim for harassment may generally only be brought by the person who is the target of the relevant conduct, or by others who have been foreseeably and directly harmed by the relevant conduct (even though they are not themselves the target of that conduct). If a journalist has been harassed, it is therefore unlikely to be possible for a media organisation to take legal action for that harassment on behalf of the journalist unless the media organisation can show that it has been foreseeably and directly harmed by the relevant conduct.
- **Defamation.** A defamation claim may generally only be brought by the person who believes that they have been defamed and may not be assigned or brought on someone else's behalf. If a journalist has been attacked online, it is therefore unlikely to be possible for a media organisation to take legal action for defamation on their behalf.
- **Criminal offences.** The first step if you believe that a criminal offence has been committed should be to report that offence to the police. It is open to media organisations to report criminal offences as well as journalists. If the police are unwilling to act in relation to a report that a criminal offence has been committed, it is also open to any person, including media organisations, to bring a private prosecution of the possible criminal offence. Please see Section 3 of this Chapter for more details.
- **Misuse of Private Information.** A claim for misuse of private information may generally only be brought by the individual whose private information has been misused. If a journalist's private information has been misused, it is therefore unlikely to be possible for a media organisation to bring legal action on behalf of the journalist.
- **Data Protection.** A claim for compensation under data protection law may generally only be brought by the data subject – the individual whose personal data has been processed inappropriately. If a journalist's personal data has been processed inappropriately, it is therefore unlikely to be possible for a media organisation to bring legal action on behalf of the journalist.

It is worth noting that, from a practical perspective, even where it is the journalist who must take legal action, media organisations may assist journalists with their legal action, for example, by providing financial assistance in engaging legal advisors or by providing practical assistance with the collection of relevant evidence.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

Criminal Offences

The way in which international jurisdictional issues relating to online attacks are handled for criminal offences depends on where the actions constituting a crime have taken place, and on the approach adopted by prosecutors. Whether prosecutors in England and Wales will have jurisdiction in relation to online attacks is not a straightforward question and one that needs to be considered on a case-by-case basis. The general rule is that criminal offences are only triable in the jurisdiction in which the offence has taken place. However, this approach is not well suited to online crimes where the victim(s), the witness(es), the accused and the evidence may all be in different countries.

In cases involving multiple jurisdictions, the general rule is that an offence must have a "substantial connection" with England and Wales for the courts of England and Wales to have jurisdiction. It follows that where several different activities constituting a crime take place in England and Wales, the courts will have jurisdiction.

Certain aspects of the current framework for jurisdiction and evidence gathering overseas are likely to be affected by the departure of the UK from the European Union. In particular, a substantial number of arrangements in relation to jurisdiction and evidence sharing that are currently in place with EU members states have been disrupted.

Civil Remedies

The way in which international jurisdictional issues relating to online attacks are handled for civil remedies depends on the domicile of the person that has perpetrated the online attack, the defendant. Currently, different regimes apply depending on whether the defendant is domiciled in England and Wales, in an EU member state or outside of the EU.

The issue of jurisdiction in civil remedies can be complex and there are likely to be additional costs involved in trying to obtain civil remedies from a perpetrator of online attacks based abroad, so you should seek legal advice on jurisdiction when considering whether and where it is appropriate to bring a claim against a defendant domiciled abroad.

From a practical perspective, it is important to reiterate that the England and Wales regime for jurisdiction in respect of civil remedies is complex. It is, however, open to you to commence a claim even where jurisdiction is not clear cut: either the Court will deal with the issue in due course or the other party may raise it themselves.

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

The laws of England and Wales do not currently have specific legislation focusing solely on online harassment. Under the current framework, a patchwork of laws can be utilised to address online harassment through both criminal offences and civil actions. It is likely, however, that reform in this area will be forthcoming in the next few years.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

As noted above, there is a significant 'patchwork' of civil and criminal laws which may be relevant to online attacks, depending on the facts. We have grouped the various laws into nine categories. The relevant categories are compared to the various types of online abuse in the table below, to show which are most likely to be relevant depending on the circumstances of the case.

As mentioned previously, England and Wales does not have specific legislation focusing solely on online harassment. Under the current framework, a number of different laws could be utilised to address online harassment - some are criminal offences and others can only be actioned in the civil courts.

	THREATS	INTIMIDATION	CYBERSTALKING	DOXING	ONLINE IMPERSONATION	TROLLING	BRIGADING
Harassment Offences	X	X	X	X	X	X	X
Communication Offences	X	X	X	X		X	
Defamation					X	X	
IP Infringement					X	X	
Misuse of Private Information			X	X	X		X
Data Protection			X	X	X	X	X
Sexual Offences	X	X	X	X	X	X	X
Inchoate Offences	X	X		X		X	X
'Threat' Offences	X	X				X	X

It may often be easier, as a private individual that is the victim of relevant conduct, to pursue your case as a civil matter, rather than through seeking a prosecution by the Crown Prosecution Service on behalf of the relevant police authority. That is both because of the resourcing issues and the difficulties in investigating these cases as described elsewhere in this chapter, but also because when criminal cases come to trial the "standard of proof" is extremely high. This means that a jury must be satisfied "beyond reasonable doubt" that the evidence shows the criminal defendant is guilty. Please note that, throughout this UK guide, we

have expressed the 'worst case' penalties for the criminal offences listed – but certain maximum sentences will differ depending on which court the offence is tried in and how. Please seek advice on these details if the precise penalty is key to your decision making in how to take action against a harasser. As noted elsewhere, you should always report an issue to the police if you believe you or someone else is in danger.

The "standard of proof" in a civil dispute is lower than in a criminal case, requiring the judge to make his or her decision on the "balance of probabilities". This means that if you are concerned your evidence may not meet the higher criminal threshold, a civil action may be more appropriate. Furthermore, if there is urgency in coming to a resolution, the civil courts may generally resolve matters quicker than the criminal courts.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

See (b) above.

Defamation

What are the elements of defamation?

In order for online abuse to be considered 'defamatory' it must include: (i) the publication of words or other matter that refer to the claimant, (ii) an imputation from those words which is capable of causing serious harm to the claimant's reputation and (iii) the words cannot be proved to be true or excusable by any other legal defence.

The 'publication' of the defamatory material must be to at least one other person than the claimant. If there has not been substantial dissemination of the publication, this will make it more difficult to prove the potential for serious harm to the claimant's reputation.

Each communication of the defamatory material generally constitutes a separate 'publication'. Claimants only have one year from the time the defamatory material was published to make a claim. In the case of material available on the internet, the time of publication is treated as the time when it is downloaded by an internet user and the place of publication is the place where the material is accessed or downloaded.

In order to show 'serious harm' claimants have to prove that, on the balance of probabilities, serious reputational harm had been caused by, or was likely to result from, the publication complained of. The court is entitled to have regard to all the relevant circumstances, including evidence of what actually happened after publication.

There are a number of defences available to defendants, including (among others) so-called 'honest opinion', that the statements complained of were true, and protection on the grounds of the 'public interest'. If the alleged offender can demonstrate any of these defences, they may not be liable for defaming you.

In *Monroe v Hopkins*[112], for example, following a memorial being graffitied during a protest, the defendant tweeted the following:

"@MsJackMonroe scrawled on any memorials recently? Vandalised the memory of those who fought for your freedom".

"Can someone explain to me - in 10 words or less - the difference between irritant @PennyRed and social anthrax @Jack Monroe".

The court held that the tweets were meant to imply that the claimant approved of the vandalising of the memorials. This was defamatory and caused serious harm to the claimant's reputation. The claimant was awarded £24,000 in damages and costs incurred in bringing the claim.

What is the penalty or remedy?

As defamation is a civil cause of action the likely remedy will be damages. However, the courts may impose an injunction to stop the perpetrator from continuing to post the false information. The damages awarded will depend on the facts of the case, but cases have ranged from £10,000[113] to £200,000. Claims involving higher figures generally involve a newspaper publishing defamatory information to thousands of readers.

Harassment

Harassment is both a civil cause of action and a criminal offence. The primary source of legislation regulating harassment is the Protection from Harassment Act 1997 ("PHA 1997"). This sets out the legal definition of the behaviour (both civil and criminal) and what a victim can claim from their harasser in the civil courts. There are further criminal offences that are also referred to as 'harassment' under the Public Order Act 1986 that are covered below, but generally the PHA 1997 is more widely used.

What are the elements of Harassment?

Section 1(1) PHA 1997 prohibits a person from carrying out a "course of conduct" that (i) amounts to harassment of another and (ii) the person knows or ought to have known that the conduct amounts to harassment.

The first element is subjective and requires the victim to actually be caused alarm or distress. For the second element, the question is whether a reasonable person would think the course of conduct amounted to harassment. A "course of conduct" requires there to be at least two instances, which must be in sequence, as opposed to distinct and distant events.

There is a second, similar, prohibition under Section 1 (1A) PHA 1997 - which was introduced to prevent the harassment of employees in order to compel or encourage their employer to do something.

In *WXY v Gewanter*,[114] for example, the High Court held that the online publication and further threats to publish private information online amounted to harassment. In this case the allegations were that the claimant (i) had a sexual relationship with another person, (ii) had perjured themselves by lying to a court about the relationship (iii) had, during 'pillow talk' with the other party, told them that the Head of State of a foreign country provided support for terrorism and (iii) had made attempts to help obtain payment of a judgment debt.

In *GYH v Persons Unknown*,[115] the claimant was the victim of an online campaign to publish various pieces of personal information or information that purported to be about the claimant. The allegations published online included details of her sex life, allegations that she had HIV/AIDS, and information about her physical and mental health. The claimant claimed that some of the allegations were false and sought an injunction. This case raised difficulties as the harasser was anonymous. Despite this, the court still allowed the injunction ordering that the defendant was not allowed to contact the claimant anymore and had to "...consent to, co-operate with, and to do all such things as are in his power to procure, the erasure of any of the specified information from the websites in question, and other places on the internet." The claimant had to use best endeavours to trace and serve the court order on the defendant. If the claimant was unable to identify the defendant and serve the court documents, using her best endeavours, within 28 days, then filing at the court was considered sufficient for this type of case.

What is the penalty or remedy?

Criminal Penalty

A person guilty of the offence of harassment can be imprisoned for a term of up to six months or given an unlimited fine (or both).

Civil Remedies

Section 3 PHA 1997 allows a victim (or, for Section 1(1A), the third party whose behaviour the harassment is intended to impact) to obtain a court order to prevent the harasser from continuing the behaviour, for example, by banning them from contacting the victim in any way. The civil courts may also impose damages to compensate for anxiety and financial loss. The amount of damages would be case dependent but could range from £3,000 to £30,000 in exceptional cases.[116]

Any breach of such an order made by the court (called 'injunctions', and also often referred to as 'restraining orders') entitles the victim to apply immediately for a warrant for the defendant's arrest. The application can be made directly to the civil court that issued the injunction, rather than to a criminal court, and the court can impose a prison sentence or a fine. The maximum sentence for breaching the order is five years imprisonment. Breaching the order would also be likely to constitute a contempt of court, which is a separate offence which can result in an unlimited fine or a two-year prison sentence.

Stalking

What are the elements of a stalking offence?

There is a further offence of stalking under Section 2A PHA 1997.[117] This targets the same type of conduct as harassment above, but where the behaviour has the character of stalking.

The most relevant acts and omissions for our purposes are (i) contacting, or attempting to contact, a person by any means, (ii) publishing any statement or other material (relating or purporting to relate to a person or purporting to originate from a person), (iii) monitoring the use by a person of the internet, email or any other form of electronic communication and (iv) watching or spying on a person.

This is a list of examples and is not exhaustive.

In *Hayes v Willoughby*,[118] for example, the Supreme Court found that the repeated and oppressive attempts to detect crime would be sufficient to be considered stalking. In this case the defendant undertook a campaign to send numerous letters to the police and various government departments alleging that that the respondent was engaged in fraud, embezzlement and tax evasion. The Court found there was no factual basis to these allegations.

What is the penalty or remedy?

A person guilty of the offence of stalking can be imprisoned for a term of up to one year, or fined, or both. If the offence involves a course of conduct that puts a person in fear of violence, this carries a potential sentence of ten years in prison. The actual penalty imposed is decided by the court in each case

The Stalking Protection Act 2019 gives magistrates the power to grant a civil stalking protection order. This

can impose certain prohibitions on the individual accused of stalking. This can include prohibitions on:[119] (i) contacting the victim by any means, including via telephone, post, email, SMS text message or social media, (ii) making reference to the victim on social media either directly or indirectly (iii) using any device capable of accessing the internet unless it has the capacity to retain and display the history of internet use and/or (iv) engaging in any form of surveillance of the victim by any means.

The order could also include positive requirements to surrender devices and/or provide the police with access to social media accounts, mobile phones, computers, tablets and passwords/codes.

It is a criminal offence for the individual to breach the prohibition. This may be an appropriate remedy when the criminal threshold has not, or has not yet, been met (such as while a criminal case is being built).

Malicious Communications

What are the elements of a Malicious Communications Offence?

The Malicious Communications Act 1988 introduced an offence of sending communications with intent to cause distress or anxiety. This covers online communications that (i) convey a threat, include a grossly offensive or indecent message or false information, and (ii) have the intention to cause distress or anxiety to the reader or recipient.

There is no legal requirement for the communication in question to reach the subject or intended recipient; it is the act of publishing or sending the communication and the intention to cause distress that counts. Whether or not something is "grossly offensive" is a question of fact decided by reference to a reasonable person test. The courts will consider context and circumstances, particularly as "usages and sensitivities may change over time".

In *Connolly v DPP*,[120] for example, the defendant sent three pharmacists pictures of an aborted foetus. She was charged under the Malicious Communications Act. She argued that she did not intend to cause distress or anxiety, but to protest the morning after pill. The High Court held that even if they were sent for political or educational purposes, the communications could still also have been sent for the purposes of causing distress or anxiety.

In 2020, a defendant plead guilty to breaching Section 1 of the Malicious Communications Act after sending a UK footballer a homophobic and threatening email. He was sentenced to pay £100 compensation and £85 in costs, and the court imposed a three-month curfew and electronic monitoring.[121]

What is the penalty or remedy?

A person guilty of the offence can be penalized with a term of imprisonment of up to two years, or a fine, or both

Section 127 Communications Act

What are the elements of a Section 127 Communications Act Offence?

The sending of an electronic communication may also be an offence under the Communications Act 2003. Section 127(1), provides that it is an offence to use public electronic communications equipment to send a message that is (i) false, (ii) grossly offensive or (iii) of an indecent, obscene or menacing character.

It is also an offence under Section 127(2) to send a communication through a public network intended to cause annoyance, inconvenience or needless anxiety to the recipient. There is no need for the message to have been received by the intended recipient. In fact, no one needs to have seen it or been offended by it at all for the offence to have been committed.

Case law has confirmed that messages sent via social media such as Twitter are sent via a "public electronic communications network" for the purposes of the Communications Act 2003.[122] Similarly, cases have confirmed comments on YouTube videos[123] and linking to offensive content can be a breach of Section 127.[124] However, the communications will be read in context. In one case, a message that was perceived to be threatening was ultimately found to lack 'menace', as reading the message in light of the previous posts changed the meaning.

In *Chabloz v CPS*,[125] for example, a blog writer had posted hyperlinks to YouTube videos of herself performing three grossly offensive antisemitic songs. The songs were a collection of antisemitic tropes or motifs that emphasised holocaust denial. Two of the songs were also set to the tune of well-known Hebrew songs. She was convicted under Section 127 of the Communications Act by the Magistrates' Court both in relation to the hyperlinks and for the uploading of one of the YouTube videos.

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term of up six months, or given a fine, or both.

Misuse of Private Information

What are the elements of Misuse of Private Information?

An individual's general privacy can be protected by the tort of "misuse of private information". This covers two aspects: (i) the actual misuse (for example, publication) of private information (the so-called 'confidentiality component) and (ii) preventing intrusion into an individual's right to privacy (the so-called 'intrusion component').

The confidentiality component protects the "wrongful disclosure of private information". This is, broadly, the unauthorised use of information in respect of which the claimant can be said to have a reasonable expectation of privacy. It can occur even where there is no pre-existing relationship of confidence between the parties.

The intrusion component is very significant. It means that, in essence, information alleged to be private may still, in appropriate cases, be protected even where it is in the public domain to some degree. This dimension is particularly important in the internet age, since information which is the subject of an interim non-disclosure order may, despite the order, nevertheless be made available on the internet.

An individual could be protected by the tort of misuse of private information:

- if the information was obviously private: the principal test for determining whether or not information is private is to ask whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy; or
- where there is room for doubt whether information is private, if disclosure of the information about the individual concerned would give substantial offence to a person of ordinary sensibilities placed in similar circumstances to that individual.

The publisher of the information may have a defence if they can argue that information was already public or that the right to privacy is outweighed by their freedom of expression. Usually this will require the publisher to show information is in the public interest.

In *Weller v Associated Newspapers Limited*,[126] for example, the court held that the MailOnline should not have published photos of a famous individual's children. This was because their rights outweighed those of the website. This case is one example that illustrates many of these cases are related to newspapers and celebrities. It shows that the publication of photos can be a misuse of private information. Ultimately, £10,000 damages were awarded by the court (in total).

What is the penalty or remedy?

As Misuse of Private Information is a civil cause of action the likely remedy will be damages. However, the courts may impose an injunction to stop the perpetrator from continuing to post the private information. This will depend on the facts of the case but range from £2,000 to £260,000.

Computer Misuse Act 1990

What are the elements of an offence under the Computer Misuse Act 1990?

Section 1-3 of the Computer Misuse Act 1990 introduced offences for (i) the unauthorised access to computer material, (ii) unauthorised modification and use of computer material and (iii) the use of a computer to assist in a criminal offence.

These offences are commonly referred to as 'hacking' and could be relied upon where the use of a computer has allowed the offender to access confidential information which is then used to harass or impersonate another person or is published online. Because the use of a computer is very likely involved in all online communications, the vast majority of criminal offences detailed in this note would be within scope of the Computer Misuse Act 1990.

In *R v Jack Shepherd*, for example, the defendant hacked into various social media and gaming accounts in order to sell the victim's personal data. He also used software to log into unsecure webcams and use their microphones as speakers. He was sentenced to four months in prison (as a suspended sentence).[127]

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term of up to 12 months or given an unlimited fine.

Data Protection Act offences

What are the elements of an offence under the Data Protection Act 2018?

Section 170 – 172 DPA 2018 also includes criminal offences for the obtaining, disclosing or retaining personal data without the consent of the data controller. The offence(s) may be committed in several ways. However, for our purposes this will most likely involve either (i) the removal of customer or client data by a disgruntled, corrupt or departing employee or (ii) by the offender misrepresenting either their identity, or the purpose of their enquiry (or both), to induce the disclosure of personal data which would not be disclosed if the true nature of the enquiry was known.

There have (as yet) been very few prosecutions under the DPA 2018. This may be due to the limitations in penalties (see below). As the only punishment available under DPA 2018 is a fine, for more serious doxxing, prosecutors may pursue other offences mentioned in this chapter.

What is the penalty or remedy?

All of the offences under the DPA 2018 are punishable by fines only. The actual penalty imposed is decided by the court in each case. Fines for individuals prosecuted on the ICO website vary from £400 to £1,050.

Threats to Kill

What are the elements of threats to kill a person?

Under Section 16 Offences Against the Person Act 1861 ('OAPA'), English law prohibits threatening to kill a person. The offence requires a threat to kill a person (or third party) with the intention that the person fears the threat will be carried out.

The person subjected to the threat does not need to be aware that the threat was made (it is what is referred to as a 'conduct crime'). It is also not a requirement for the threat to be explicit - an implied or conditional threat is sufficient. The person making the threat does not need to have an intention to actually carry out the threat, if they intend to create the relevant fear in the recipient.

In *R v Mawji*,[128] the defendant was travelling to the United Kingdom. He emailed his wife the following: *"Hi* [b*tch]*, don't think you are safe in the UK I am going to kill you I will make sure I get my hands on you, your loving husband Riz* [sic]*"*. Even though the defendant was not in the UK we when he emailed the content (and therefore the threat was not imminent), the offence was still made out - and the defendant was found guilty under Section 16 OAPA.

In *R v Furmage*,[129] the defendant threatened to kill two people. He sent multiple WhatsApp and Snapchat messages to one of the victims, including: "If you make me pull my gun out I will [f*cking] murder you". The defendant also sent a picture of a firearm on his sofa. He also threatened to kill the first victim's friend (the second victim). Ultimately the defendant was found guilty under Section 16 OAPA and sentenced to four years in prison.

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term not exceeding 10 years.

Common Assault

What are the elements of Common Assault?

The offence of assault is committed by a person who intentionally or recklessly causes another to apprehend immediate and unlawful violence. As with certain other offences highlighted here, there is no need for any actual violence to occur. The threat can occur via online means such as email, social media messages or public posts; however, proving assault in the context of online abuse may not be the most appropriate route where there is no apprehension of "immediate" harm. There is no 'assault' where the fear is of harm at another time. In one case however, the threat of violence was considered to be 'immediate' even though the defendant was outside the victim's home and needed to gain entry to the locked property. As such, if there is sufficient reason to think this offence is made out it may nevertheless be relevant to online communications.

In *R v Ireland*,[130] for example, the defendant made a series of phone calls to the victim. The defendant made no noise on these calls. The court still found that silence could be enough to cause the victim to apprehend immediate and unlawful violence.

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term not exceeding 6 months.

Blackmail

What are the elements of Blackmail?

Section 21 Theft Act 1968 prohibits the act of blackmail. A person is guilty of blackmail if (i) they make unwarranted and menacing demands of another person (ii) with a view to gain for themselves or another or with intent to cause loss to another.

A demand with menaces is unwarranted unless the person making it does so in the belief that they have reasonable grounds for making the demand, and that the use of menace is a proper means of reinforcing the demand.

The nature of the act or omission demanded is not relevant. It is also immaterial whether the menaces relate to an action to be taken by the person making the demand, or by a third party.

In *R v Qaiser*,[131] the defendant hacked into his victims' computers and locked them so that the victims could not access their documents. He threatened the victims with criminal prosecution (pretending to be a law enforcement agency) and demanded they pay a "fine". He made £500,000 running these ransomware scams. He eventually plead guilty to three counts of blackmail (among other offences) and was sentenced to six years and five months in prison.

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term not exceeding 14 years.

Threats to Property

What are the elements of threats to destroy or damage property?

Threats to destroy or damage property are prohibited under Section 2 of the Criminal Damage Act 1971. The offence requires (i) a threat to another, (ii) to destroy or damage any property belonging to that other or a third person, or to destroy or damage his own property in a way which he knows is likely to endanger the life of that other or third person, and (iii) with the intention that the other person fears the threat will be carried out.

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term not exceeding 10 years.

Encouraging, assisting or conspiring in an offence

What are the elements of these 'inchoate' offences?

Under Section 44 to 46 of the Serious Crime Act 2007 there are three general offences relating to the encouragement of crime: (i) intentionally encouraging or assisting an offence, (ii) encouraging or assisting an offence believing it will be committed and (iii) encouraging or assisting offences believing one or more will be committed.

The encouragement of the crime is sufficient for a person to be found guilty of this offence - there is no need for the offence to actually be carried out. These offences are broad and even the most marginal conduct may suffice to amount to assistance or encouragement.

In the case of *R v Blackshaw,*[132] for example, two defendants plead guilty to Section 44 and Section 46 offences.

The first defendant made a Facebook page called "The Warrington Riots". On this web page he included a photograph of police officers in riot equipment in a "stand-off position" with a group of rioters. He also included a photograph of himself and others in a pose described by police as "gangster like". He sent invitations on his Facebook to 400 contacts. They were invited to meet at a carvery in Warrington at 7pm on 10th August. He plead guilty to the Section 44 offence - intentionally encouraging or assisting an offence.

The second defendant used Facebook to set up and plan a public event called "Smash down in Northwick Town". The purpose of his site was to wreak "criminal damage and rioting in the centre of Northwich, and the event called for participants to meet in a restaurant in Northwich at lunchtime on 9th August. The website was aimed at his close associates, who he referred to as the "Mob Hill Massive", and his friends. He posted a message of encouragement on the website that read "we'll need to get on this, kicking off all over". He pleaded guilty to the Section 46 offence - encouraging or assisting offences believing one or more will be committed.

Under Section 1 (and 1A) of the Criminal Law Act 1977, it is an offence for two or more persons to conspire to commit a crime.

This requires an agreement between the parties that a course of conduct will be pursued that would amount to the commission of an offence if carried out in accordance with the defendants' intentions. It is necessary to show that the parties had an intention to agree and an intention that the agreement will be carried out. It also necessary to show the parties had an intention or knowledge as to any circumstances forming part of the substantive offence.

This offence can be useful in the context of online abuse, as a person can be convicted of conspiracy even though they will not be involved in the commission of the substantive crime. Further to this, the fact that the course of conduct rendered the substantive offence impossible does not prevent a conviction for conspiracy.

In *R v Coulson*,[133] for example, five journalists were charged with conspiring unlawfully to intercept communications in the course of their transmission without lawful authority contrary to Section 1 of the Criminal Law Act 1977. The relevant conduct, or "hacking", involved the remote accessing of a voicemail box by dialling, from another telephone, the telephone number relating to it and bypassing any security feature, so as to be able to listen to the message contents, without the knowledge or consent of the subscriber, at a time when the recorded message was stored there, not yet having been deleted.

What is the penalty or remedy?

A person guilty of one of the Serious Crime Act offences above can be imprisoned for a term of the maximum of the offence they are encouraging. The actual penalty imposed is decided by the court in each case. Please see ***Criminal vs Civil Remedies*** above for a brief summary of what a court will consider when sentencing.

A person guilty of the offence of conspiracy can be imprisoned for a term of the maximum of the offence they are conspiring to commit.

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

Crime and Disorder Act 1998

Section 32 of the Crime and Disorder Act 1998 introduced separate racially or religiously aggravated version of many of the offences covered above. This includes: (i) harassment and stalking under PHA 1997, (ii) Section 4A of the Public Order Act, (iii) Section 5 of the Public Order Act and (iv) common assault.

What are the elements of the offences?

In order to demonstrate these offences, it must be proved either: (i) the perpetrator demonstrated (at the time of the offence or immediately before) hostility based on the victim's race or religious group or (ii) the offence was motivated by hostility towards members of a racial or religious group.

The use of a racial slur before the offence will normally be sufficient to show to demonstrate the hostility.

What is the penalty or remedy?

Each of these offences effectively increases the maximum sentence for the underlying offence. The actual penalty imposed is decided by the court in each case.

Criminal Justice Act 2003

Under Section 145 and 146 Criminal Justice Act 2003, provisions for enhanced sentencing guidelines were introduced for other offences. Unlike under the Crime and Disorder Act 1998 this does not mean that the maximum sentence for the specific offences above is increased, but means it is more likely the maximum sentence (or a higher sentence) will be imposed. It will need to be shown either: (i) the perpetrator demonstrated at the time of the offence (including immediately before or after) hostility based on the victim's characteristics or (ii) the offence was motivated by hostility towards a person based on one of the characteristics.

The characteristics that are protected, and may give rise to the enhanced sentencing effect, are race, religion, disability, sexual orientation and transgender identity.

Public Order Act 1986

Under the Public Order Act 1986 ("POA 1986"), there are various offences of incitement or stirring up of hatred, which also apply to race, religion and sexual orientation. These will all apply in an online context.

What are the elements of the offences?

The offences catch multiple types of conduct, the most relevant are: (i) use of words which are threatening, abusive or insulting, (ii) displaying written material which is threatening, abusive or insulting, (iii) publishing or distributing written material which is threatening, abusive or insulting, (iv) distributing, showing or playing, a recording of visual images or sounds which are threatening, abusive or insulting and (v) possession of material which is threatening, abusive or insulting with a view to display, publish, distribute, show or play the material.

Stirring Up Racial Hatred

For all of these offences, to be found guilty of stirring up racial hatred it must be shown either that (i) the person engaged in the conduct intended to stir up racial hatred or (ii) the racial hatred was likely to be stirred up by their conduct.

The conduct above is also an offence if the intention is to stir up hatred based on religion or sexual orientation. However, these offences are narrower. It is not sufficient for the conduct to be abusive or insulting, it must be threatening; (i) there must be intention to stir up hatred and (ii) there are specific 'freedom of expression' defences (these are covered in answer to question 2(d) below).

What is the penalty or remedy?

A person guilty of the offence can be imprisoned for a term not exceeding seven years.

(D) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

None of the laws listed above have been found to be fundamentally incompatible with freedom of speech laws in England and Wales. Instead the courts have sought to adjudge on a case by case basis whether acts are legitimate exercises of freedom of speech rather than acts that are capable of being prosecuted or liable to court intervention.

For example, in *Merlin Entertainment LPC and others v Peter Cave,*[134] Merlin sought an injunction against Mr Cave, pursuant to the Protection from Harassment Act, to prevent him continuing an email and web campaign criticising the safety at the theme park following injury to a child. The injunction was unsuccessful on the grounds that it was a legitimate exercise of Mr Cave's freedom of speech.

At the other end of the spectrum, extreme hate speech will fall outside of Article 10 of the European Convention of Human Rights ('ECHR') (which protects free speech) due to Article 17 of ECHR which states that convention rights cannot be used to "engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms". For example, an English man was unsuccessful in seeking to rely on his "freedom of speech" under Article 10 to leave a sign in his window which read "Islam out of Britain – Protect the British People" with a picture of the Twin Towers ablaze.[135]

Determining these cases is very dependent on the context in which the speech takes place, whether that be in private, in the workplace or even during an election.[136] The CPS will also take freedom of speech into account when deciding whether to prosecute an individual. CPS guidance makes clear that for prosecution to be taken forward the interference in a person's freedom of expression must be "unquestionably prescribed by law, necessary and proportionate".[137]

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

It will assist in any private action or law enforcement action (if any) if you are able to collate and/or obtain evidence - safely - about the attacks you are experiencing and the identity of your attacker. It would be prudent to keep very detailed records of your experiences (such as screenshots, copies of emails and other messages, and logs of any behaviour which does not leave a record). Anything that evidences the attack itself is key, as is any piece of information which leads you (based on the below) to identifying the person or persons involved.

Due to the potential for online activity to be conducted under the cloak of effective anonymity, there can be significant practical difficulties in identifying the 'real' person behind an online attack. It can also be difficult for law enforcement to help for the same reason. It is important to remember that if the behaviour leads a person to believe that they are in physical danger, they should call '999' immediately. There is also the option to call '101' for non-urgent issues.

Ultimately, if an entity holds the relevant information, but it cannot be obtained directly or they are not willing to release the information voluntarily, then a court order application will be required to get a 'Norwich Pharmacal' order in the civil courts (although doing so will be costly and it may be very difficult to obtain an order).

Taking action

There are many different types of conduct which online attacks can correspond to, and some result in civil liability, while others are criminal, and some may be both.

If it is a civil matter, then a claim can be commenced against the attacker in the so-called 'civil' courts. This involves making a claim for any financial damages the attacker has caused, or seeking an order to make them do something, or stop them from doing something. Anyone can bring a claim, but there are very specific procedural rules involved, as well as knowledge of the law – and therefore it is likely that a lawyer will be needed to pursue a claim, and there may be costs incurred from this, as well as fees payable to the court itself (for issuing the claim, and for hearings and other elements of the process).

Ultimately, it is often the case that successful claimants in civil cases can reclaim some (but rarely all) of their costs from the defendant – but this is by no means certain and it is extremely rare that all costs are recovered. Organisations such as Citizen's Advice, and legal advice clinics (see a list here for example: https://www.lawworks.org.uk/legal-advice-individuals/find-legal-advice-clinic-near-you), may be of assistance in the first instance if considering commencing a claim.

If evidence is obtained of the attacker's identity but the victim is unable to engage the assistance of law enforcement, one potential option open (albeit, again, a difficult one) is to commence a private prosecution against them. This involves the victim effectively stepping into the shoes of the UK prosecuting authority (the CPS) to bring criminal charges, and requires following all the detailed rules around criminal procedure – so, again, a speicalist lawyer is likely to be required to comply with the requirements.

In any private prosecution, it is worth noting that the CPS can take over the case at any time and either continue the proceedings itself, or terminate them. The court itself may also terminate the proceedings if, for example, it views them as an abuse of process. If the case continues then, depending on the circumstances and the outcome of the case, the victim may benefit from an order for your costs to be repaid out of public funds, or by the person convicted.

REUTERS/Bernadett Szabo

UNITED STATES

(A) STANDING: WHEN DO MEDIA ORGANISATIONS (AS OPPOSED TO THE JOURNALIST) HAVE STANDING TO TAKE LEGAL ACTION?

In the United States, there are no specific rules applicable to media organisations. As a general rule, there are two main routes by which organisations and advocacy groups can claim standing: (i) direct organisational standing and (ii) representative standing.

Direct organisational standing

The U.S. Supreme Court recognisedd (the "Court") in *Warth v. Seldin*[138] ("Warth") that "[t]here is no question that an association may have standing in its own right to seek judicial relief from injury to itself and to vindicate whatever rights and immunities the association itself may enjoy". In a 1977 case, *Village of Arlington Heights v. Metropolitan Housing Development Corp.*,[139] the Court outlined two kinds of direct standing that an association can pursue: (i) standing based on injury to its economic interests and (ii) frustration of the organisation's mission (see also *Havens Realty Corp. v. Coleman*,[140] where the Court concluded that "[s]uch concrete and demonstrable injury to the organisation's activities - with the consequent drain on the organisation's resources - constitutes far more than simply a setback to the organisation's abstract social interests").

It should be noted that, while most jurisdictions require organisations to show only one of these forms of injuries, some jurisdictions require organisations to show both (notably the Ninth Circuit).[141]

Representative standing

In Warth, the Court also asserted that an organisation has standing "solely as the representative of its members". The Court stated the test for representational organisational standing in *Hunt v. Washington State Apple Advertising Commission*[142]. Summarizing precedents, the Court explained that "an association has standing to bring suit on behalf of its members" when three conditions are met: "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organisation's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit". Having a membership is, clearly, essential to establish representative standing.

(B) TERRITORIAL JURISDICTION: HOW ARE INTERNATIONAL JURISDICTIONAL ISSUES HANDLED WHEN IT COMES TO ONLINE ATTACKS, INCLUDING EVIDENCE GATHERING?

The internet has no territorial boundaries: it is a virtual world of interconnected computer networks, known as cyberspace. The internet is therefore an interstate and international medium. In the United States, jurisdiction is determined by an analysis of the interactivity of the websites concerned. Three categories have emerged:

- Passive websites: present information but do not accept information, sell products or offer services (for example, newspapers' websites). Generally, United States courts do not extend their territorial jurisdiction to these websites.
- Intermediate websites: United States courts assess the level of interactivity and commercial nature of the exchange of information (for example, websites that allow for registration and interaction with the user, but it mostly a one-way street for information). The question is whether the nature of the activity (often commercial) is substantial enough to be a substitute for a physical store.
- Active websites: jurisdiction is found over providers of websites that actively conduct their business over the internet by displaying products or services and allowing the user to enter into contracts and purchase products (for example Twitter, Facebook, and Instagram).

Territorial jurisdiction is the court's power to bind the parties to the action. This law determines the scope of federal and state court power. State court territorial jurisdiction is determined by the Due Process Clause of the Constitution's Fourteenth Amendment and the federal court territorial jurisdiction is determined by the Due Process Clause of the Constitution's Fifth Amendment. Furthermore, Rule 4 of the Federal Rules of Civil Procedure (and its amendments) clarifies how the question of territorial jurisdiction should be answered in Federal Courts.

In summary, federal courts will hear cases if:

- The United States is a party (for example, if the sue is against a federal government official in their official capacity or government corporations);
- The case involves violations of the U.S. Constitution, treaties or federal laws;
- It is a legal dispute between citizens of different states or foreign citizens (so called "diversity of citizenship jurisdiction");
- It is a criminal matter listed in the U.S. Code (which, includes, internet defamation and related cases. See Section 2 below).

On the other hand, state or local courts will hear:

- Cases concerning laws passed by state legislature or local authorities (for example, if the sue is against a state or city government official in their official capacity or government corporations);
- Criminal cases.

In addition, it should be noted that civil actions brought in a federal court under the diversity statute must meet the jurisdictional amount requirement, i.e., the matter in controversy must be in excess of US$75,000, exclusive of interest and costs. The amount is determined from what is claimed in the complaint, disregarding potential defences or counterclaims. Usually, all that is necessary is a good faith allegation that the amount of the damages or injuries in controversy exceeds, exclusive of interest and cost, the sum of US$75,000.

For a state court to hear a case, that court will typically need to satisfy the constitutional due process requirement for territorial jurisdiction as well as the state statutory requirement, which is typically known as a state's long-arm statute (i.e., the power of a state court to exercise jurisdiction over foreigner defendants). The Court has held that a person must have minimum contacts with a state, in order for a court in one state to assert personal jurisdiction over a defendant from another state.

Internet defamation and cyber cases often turn on personal jurisdiction issues if a plaintiff is suing in a state court an out-of-state defendant for comments made on the internet where the defendant has little or no connection to such state. The issue of jurisdiction turns on whether the defendant targeted that plaintiff in such state.

Once a defendant has moved for dismissal based on lack of personal jurisdiction, the plaintiff bears the burden of demonstrating the existence of jurisdiction. In ruling on a motion to dismiss for lack of personal jurisdiction, a federal district court sitting in diversity must apply the personal jurisdiction rules of the state in which it sits.

Every U.S. state has a different statute. For instance, under the governing Illinois statute, Illinois permits its courts to exercise personal jurisdiction up to the limits of the Due Process Clause of the Fourteenth Amendment (735 ILCS 5/2-209(c)). Since Illinois law does not indicate that Illinois' constitutional standards would differ from federal law, "the state statutory and federal constitutional inquiries merge" into one analysis.

The Federal Due Process Clause authorizes personal jurisdiction over out-of-state defendants when the defendant has "certain minimum contacts with [the state] such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice."

Courts recognise two types of personal jurisdiction: general and specific. General jurisdiction is "all-purpose"; it exists only "when the [party's] affiliations with the state in which suit is brought are so constant and pervasive as to render it essentially at home in the forum state". Specific jurisdiction is case-specific; the claim must be linked to the activities or contacts with the forum. A defamation plaintiff can prevail in asserting personal jurisdiction for online posts if either general jurisdiction or specific jurisdiction exists.

General Jurisdiction

In recent years, the Supreme Court has clarified and raised the bar for general jurisdiction and held that general jurisdiction should not be lightly found. Isolated or sporadic contacts are insufficient for general jurisdiction. General jurisdiction exists only when the organisation is "essentially at home" in the forum state.

With respect to websites or internet posts, the maintenance of a website or posting on the internet, without more, is not sufficient to establish general jurisdiction.[143]

Generally speaking, when an out-of-state defendant, who has made allegedly defamatory internet posts, does not reside, work, or own any property in the state and has never transacted business or have any other connection to the state, then general personal jurisdiction would be lacking.

Specific Jurisdiction

Specific personal jurisdiction can only exist when a plaintiff's claims arise out of the defendant's constitutionally sufficient contacts with the forum state.[144] On general terms, specific jurisdiction requires that: (1) the defendant has purposely directed his activities at the forum state or purposefully availed himself of the privilege of conducting business in the state, and (2) the alleged injury arises out of the defendant's forum-related activities.

For cases involving torts allegedly committed over the internet, the Seventh Circuit, for instance, has stated that the three requirements for specific personal jurisdiction are: (1) intentional conduct; (2) expressly aimed at the forum state; and (3) with the defendant's knowledge that the effects would be felt (plaintiff would be injured) in the forum state.

Recently, the Court held that the forum of plaintiff's injury is relevant but not sufficient to establish minimum contacts. *Walden v. Fiore*[145]. The *Walden* court emphasized that the relation between the foreign defendant and the forum state "must arise out of contacts that the defendant himself creates with the forum state". The analysis looks to the defendant's contacts with the forum state itself, not the defendant's contacts with persons who reside there. The *Walden* court also stated that "the plaintiff cannot be the only link between the defendant and the forum", but it "is the defendant's conduct that must form the necessary connection with the forum state" *Advanced Tactical Ordnance Sys., LLC v. Real Action Paintball, Inc.*, (7th Cir. 2014) (holding: (1) *de minimis* sales in forum would not support personal jurisdiction; (2) the foreseeability of plaintiff's injury in the forum, was not relevant to whether the defendant itself had created contacts with the forum state; (3) the sending of two emails to a list of subscribers that included Indiana residents was not enough to establish that Indiana was targeted; and (4) maintenance of an interactive website did not show that the defendant targeted Indiana).

Subjecting a foreign defendant to personal jurisdiction requires not only an alleged injury in the forum state, but "something more" directed at that state. According to the *Young* court, if a publisher of online content does not manifest intent to reach the subject forum, even if the content is available for anyone to read, including people in the subject forum, then there is not sufficient contacts with the forum to permit the exercise of specific personal jurisdiction.

A federal court in Chicago has recently held that there can be no specific personal jurisdiction over a defendant for alleged defamation and false light for internet postings, where those internet postings were not directed at Illinois.[146] The *Bittman* court dismissed plaintiff's complaint for lack of personal jurisdiction where the complaint failed to allege that the defendant created any contacts with the state of Illinois other than the fact that his website may be accessed by Illinois residents (the plaintiff's connection to the forum state cannot be the hook providing personal jurisdiction). The *Bittman* court held that operating even an interactive website should not open a defendant up to personal jurisdiction "in every spot on the planet where that interactive website is accessible".

In cases in which the defendant's alleged contacts with the forum state occurred online, the Seventh Circuit has noted that the relevant inquiry typically "boils down" to whether the defendant has purposely exploited or in some way targeted the forum state's market. "If the defendant merely operates a website, even a 'highly interactive' website, that is accessible from, but does not target, the forum state, then the defendant may not be hauled into court in that state without offending the Constitution." "Courts should be careful in resolving questions of personal jurisdiction involving online contacts to ensure that a defendant is not hauled into court simply because the defendant owns or operates a website that is accessible in the forum state, even if that site is interactive."). Thus, "[a] plaintiff cannot satisfy the *Colder* standard [i.e., the "express aiming" test] simply by showing that the defendant maintained a website accessible to residents of the forum state and alleging that the defendant caused harm through that website").[147]

2. LEGAL FRAMEWORK APPLICABLE TO ONLINE HARASSMENT AGAINST JOURNALISTS AND MEDIA ORGANISATIONS:

(A) IS THERE SPECIFIC LEGISLATION DEALING WITH ONLINE HARASSMENT?

Yes. Under federal law, 18 U.S. Code § 2261A Stalking, the use of electronic communication or interactive computer services that "places [a] person in reasonable fear of the death of or serious bodily injury to a person, a pet, a service animal, an emotional support animal, or a horse described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A) [i.e., (i) that person; (ii) an immediate family member of that person; (iii) a spouse or intimate partner of that person; or (iv) the pet, service animal, emotional support animal, or horse of that person]; or (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A)", is punishable by law.

(B) WHAT LAWS CAN BE USED AGAINST EACH OF THE FOLLOWING TYPES OF ONLINE ABUSE?

The elements needed to prove each crime below depends on the applicable federal or state statute. Under 18 U.S. Code § 2261A, the prosecution must prove that the person had the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, that (i) places that person in reasonable fear of the death of, or serious bodily injury; or (ii) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress.

Violation of these laws can result in fine and/or imprisonment depending on various factors, including not only the violation of federal statute, but also any applicable state law. In general, a person who violates Section 18 U.S. Code § 2261A shall be fined and/or imprisoned (1) for life or any term of years, if death of the victim results; (2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results; (3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offence; (4) and for not more than five years, in any other case. In addition, whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or other order described shall be punished by imprisonment for not less than one year.

I. THREATS:

Covered by 18 U.S. Code § 2261A.

II. INTIMIDATION:

Covered by 18 U.S. Code § 2261A.

III. CYBERSTALKING:

Other than under 18 U.S. Code § 2261A, cyberstalking is also legislated under federal law in the Violence Against Women Reauthorization Act 2013, which specifically incorporates cyberstalking into the definition of stalking through Section 107.

IV. DOXXING:

Under U.S. Federal Law, 18 USC § 119 Making Public Restricted Personal Information criminalizes certain conducts which can be considered "doxxing," but its application is limited to certain categories of individuals (i.e., (i) any officer or employee of the United States or of any agency in any branch of the United States Government (including any member of the uniformed services); (ii) jurors, witnesses, or other officer in or of, any court; (iii) informants or witnesses in a federal criminal investigation or prosecution; (iv) a State or local officer or employee whose restricted personal information is made publicly available because of the participation in, or assistance provided to, a federal criminal investigation by that officer or employee.

Although journalists would not generally fall into one of these categories, the federal law against online harassment/stalking may apply to many doxxing incidents (see 18 U.S. Code § 2261A).

V. ONLINE IMPERSONATION:

In the United States, there are no federal internet impersonation laws, and only nine states (including New York, California and Texas) had online impersonation laws as of 2017.

VI. TROLLING:

In the United States, trolling per se is not a crime under federal law. However, it can fall under 18 U.S. Code § 2261A, if the conduct amounts to harassment, threat or stalking. In addition, it can fall under the laws of many states regarding harassment, stalking, and/or cyberbullying.

VII. BRIGADING:

In the United States, brigading per se is not a crime under federal law. However, it can fall under 18 U.S. Code § 2261A, if the conduct amounts to harassment, threat or stalking. In addition, it can fall under the laws of many states regarding harassment, stalking, and/or cyberbullying.

(C) WHAT EXISTING LAWS, NOT NECESSARILY CONCEIVED FOR ONLINE CRIMES, CAN BE/HAVE BEEN USED TO PROSECUTE ONLINE HARASSMENT?

In addition to the criminal federal laws illustrated above, there are civil law remedies that may apply to online harassment: (i) defamation laws and (ii) copyrights laws (if the harassment includes, for example, the sharing of self-taken photos).

(D) WHAT ADDITIONAL LEGAL AVENUES CAN BE USED WHEN RACE AND GENDER ARE A FACTOR IN THE ABUSE?

The federal laws of the United States prohibit discrimination based on a person's national origin, race, color, religion, disability, sex, and familial status. Laws prohibiting national origin discrimination make it illegal to discriminate because of a person's birthplace, ancestry, culture or language. In addition, harassment based on race or gender is punishable under many state laws.

If a crime is also committed in violation of antidiscrimination laws, such circumstance can be used as an aggregating factor in sentencing. However, this will depend on many factors, including the state and federal district court that has jurisdiction over the criminal matter. Despite federal sentencing guidelines meant to set out a uniform sentencing policy for defendants convicted in the United States federal court system, such rules are non-binding. The guidelines provide for "very precise calibration of sentences, depending upon a number of factors. These factors relate both to the subjective guilt of the defendant and to the harm caused by his facts" (*Payne v. Tennessee,* 501 U.S. 808, 820 (1991)).

(E) ARE THERE EXAMPLES WHERE ANY SUCH LAWS HAVE BEEN FOUND TO INFRINGE ON FREEDOM OF SPEECH LAWS?

Freedom of speech is a constitutionally protected right enshrined in the First Amendment to the U.S. Constitution. Whether the First Amendment or the relevant laws prevail, it would be based on a case-by-case analysis.

The issue of threats and the limits of free speech on social media was discussed for the first time by the Court in *Elonis v. United States*.[148] In this case, a man from Pennsylvania was charged with threatening his ex-wife, co-workers, a kindergarten class, the local police, and an FBI agent. The defendant had posted statements on his Facebook page that appeared to threaten his ex-wife and other people in his life. The Court reversed Elonis' conviction of threatening to kill and threatening to injure.

One of the main defendant's arguments was that he was exercising his First Amendment rights. The Court, however, decided to opt out of specifically ruling on the First Amendment issues raised, instead reversing the conviction of the defendant on other grounds. The issue remains therefore open.

Several courts have been faced with the problem of school regulations against cyber-bullying. In *Coy Ex Rel. Coy v. Board Of Educ. Of Canton City,*[149] a district court was faced with the case of a student who created a website on his home computer and on his own time which contained mostly biographical information about himself and some of his friends. However, there was a Section titled "Losers," that contained the pictures of three boys who attended the same school as the defendant. The court refused to grant summary judgment, but clarified that, if the school did in fact punish the student for the content of his website, then the student would prevail because such punishment would be unconstitutional under the First Amendment.

In another case, *Killion v. Franklin Regional School,*[150] a student compiled a list of insults directed at a school official and emailed the list to several of his friends. A fellow student eventually printed off the list and distributed it on school property. The student who originally created the list was suspended ten days and eventually brought suit alleging that his rights under the First Amendment had been violated. The court ruled in favour of the student and decided the suspension was indeed a violation of the First Amendment, given that the school officials have less authority in regulating speech that occurs off school grounds, as the speech here did.

3. PERPETRATOR: WHAT CAN LEGALLY BE DONE BY A JOURNALIST TO IDENTIFY AN ANONYMOUS HARASSER?

Other than reporting the harassment to the police and let them deal with the investigation, a journalist could hire a private investigatory team of internet lawyers/experts that will try to obtain details of the identity of online harassers by securing it from the site owner, domain registrar or Internet Service Provider.

Once they have established the defaming publisher's identity and contacted them, they may also contact all administrators, copyright holders, technical teams and advertisers of where the defamation on the internet has been published to make them aware of the potential legal liabilities and ultimately persuade them to remove all defamatory material without delay.

PRACTICAL INFORMATION

Legal framework:

- https://www.law.cornell.edu/uscode/text/18/2261A (Stalking).
- https://www.congress.gov/113/plaws/publ4/PLAW-113publ4.pdf (Violence Against Women Act 2013).
- https://www.law.cornell.edu/uscode/text/18/119 (Protection of individuals performing certain official duties).

Journalists organisations (United States):

- The NewsGuild of New York. The NewsGuild of New York is the union for news professionals in America's media capital.
- The Committee to Protect Journalists. CPJ is an independent, non-profit organisation that promotes press freedom worldwide. It defends the right of journalists to report the news safely and without fear of reprisal.
- Reporters Sans Frontiers/Reporters Without Borders. Reporters Without Borders is an independent NGO with consultative status with the United Nations, UNESCO, the Council of Europe and the International Organisation of the Francophonie (OIF).
- Other U.S. journalist organisations are listed here.

ENDNOTES

1 An employee includes any individual (whether or not an independent contractor) who is engaged in the day-to-day operations of the media organisation, other than as a volunteer, and subject to the control and direction of the corporation. Part-time employees are counted as the appropriate fraction of a full-time employee.

2 For example, see *Clarke v Nationwide News Pty Ltd trading as the Sunday Times* [2012] FCA 307.

3 *R v Hampson* [2011] QCA 132.

4 *Agostino v Cleaves* [2010] ATSC 19.

5 *R v Ogawa* [2009] QCA 307.

6 Decree n. 6,282/2007.

7 Decree n. 3,895/2001.

8 Decree n. 5,721/2006.

9 Decree n. 6,462/2008.

10 Decrees n. 6,681/2008 and 8,048/2013.

11 Decree n. 3,810/2001.

12 Decree n. 3,324/1999.

13 Decree n. 8,046/2013.

14 Decree n. 862/2013.

15 Decree n. 7,595/2011.

16 Decree n. 7,582/2011.

17 Decree n. 7,596/2011

18 Decree 3,988/2001.

19 Decree n. 8,882/2016.

20 Decree n. 1,320/1994.

21 Decree n. 8,047/2013.

22 Decree n. 6,974/2009

23 Decree n. 6,832/2009.

24 Decree n. 5.984/2006.

25 https://noticias.r7.com/bahia/suspeito-de-praticar-racismo-contra-tia-ma-se-apresenta-a-policia-14032018.

26 https://tvjornal.ne10.uol.com.br/tv-jornal-meiodia/2018/10/03/aberto-inquerito-para-identificar-autor-de-ameaca-contra-apresentadora-114995.

27 Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

28 Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

29 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, transposed into Finnish national legislation with the Act on Implementing the Directive regarding the European Investigation Order in criminal matters (430/2017).

30 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, transposed into the French Code of Criminal Procedure (Articles 694-15 to 694-19).

31 Supreme Court, Civ., 18 October 2017, No. 16-10.428; Supreme Court, Com., 5 July 2017, No. 14-16.737.

32 Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

33 Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

34 Paris Court of Appeal, 3 March 2020, RG no.19/01495.

35 Law no. 2021-1109 of 24 August 2021 strengthening the respect of the principles of the French Republic.

36 Tribunal de grande instance de Paris, 27 November 2020, LICRA, MRAP et autres/Orange, SFR, Free et autres.

37 Cases C-509/09 and C-161/10.

38 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, transposed into sect. 91a et seq. of the German Code on International Assistance on Crimes (IRG).

39 The IPC (Act 45 of 1860).

40 *M/S Spentex Industries Ltd & Anr v Pulak Chowdhary (2019) CS No. 219/18.*

41 Maharashtra Media Persons and Media Institutions Act (Prevention of Violence and Damage or Loss to Property), 2017 (Act 29 of 2019).

42 Person whose principal vocation is that of a journalist and who is employed as a journalist, either on regular or contract basis, in, or in relation to, one or more media institutions and includes an editor, sub-editor, reporter, correspondent, cartoonist, news-photographer, television cameraman, writer, feature writer, copy tester and proof-reader, but does not include any such person employed in an administrative or supervisory capacity.

43 Any registered newspaper establishment, news channel establishment, news-based electronic media establishment or news station establishment.

44 India has executed bilateral treaties with various countries regarding reciprocity in enforcement of judgments and decrees. Whenever any such treaty is entered into with any country, that country is declared a 'reciprocating territory' by the Indian government by way of a notification.

45 *State of West Bengal v Animesh Boxi* (2018) GR No. 1587 of 2017.

46 *Kalandi Charan Lenka vs. State of Odisha* (2017) BLAPL No. 7596/2016, (Ori HC).

47 The IPC (Act 45 of 1860) (IPC) sec 292.

48 IPC (n 9) sec 354D.

49 IPC (n 9) sec 500.

50 IPC (n 9) sec 503.

51 IPC (n 9) sec 507.

52 *Jitender Singh Grewal v The State of West Bengal* (2018) Criminal Miscellaneous Petition No. 7252 of 2018.

53 In *Gagan Harsh Sharma v. The State of Maharashtra,* 2019 CriLJ 1398.

54 *Suhas Katti v State of Tamil Nadu* (2004) C No. 4680 of 2004.

55 *Sanjeev Mishra vs. Bank of Baroda* (2021) Civil Writ Petition No. 150/2021 (Raj HC).

56 *Shreya Singhal v Union of India AIR* 2015 SC 1523.

57 [2017] IESC 27.

58 [2018] IESC 44.

59 *Society for the Protection of Unborn Children (Ire) Ltd v Coogan* [1989] IR 734 at 747.

60 Harassment, Harmful Communications and Related Offences Act 2020.

61 Regulation Brussels 1 (recast) No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

62 *Case C-255/09* [2011] C 370/12.

63 Regulation No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

64 The Harassment, Harmful Communications and Related Offences Bill 2017.

65 Charleton, McDermott and Bolger, Criminal Law (Butterworths, 1999), paragraph 8.205.

66 *Director of Public Prosecutions (O'Dowd) v Lynch* [2008] IEHC 183, [2010] 3 IR 434.

67 Parliamentary Questions 1397 [27th July 2021].

68 Department of Justice, Legislating for Hate Speech and Hate Crime in Ireland (2020).

69 Online Safety and Media Regulation Bill 2021.

70 Department of Justice, Legislating for Hate Speech and Hate Crime in Ireland, (2020).

71 *Megaleasing UK Ltd v Barrett (No. 2)* [1993] ILRM 497.

72 Tokyo District Court Judgement dated 31 August 2005, Case No. 2004 (wa) 7252 and 25166.

73 The details of the contractual relationship between the entertainers and the production company are unclear, based on the facts recognised by the court, including whether the entertainers were employees or subcontractors of the company.

74 Supreme Court Judgement dated 10 March 2016, Case No. 2014 (ju) 1985; Tokyo District Court Judgement dated 30 November 2016, Case No. 2015 (wa) 1973.

75 The 2021 Amendment to the Provider Liability Law is expected to come into full force and effect in Sep-Oct 2022. This Japan chapter only summarises the framework under the pre-amended Provider Liability Law that is currently in full force and effect (as of Sep 2021).

76 Examples: Tokyo District Court Judgement dated 29 March 2017, Case No. 2016 (wa) 9254 and 36513; Tokyo District Court Judgement dated 24 February 2017, Case No. 2016 (wa) 5884; Tokyo District Court Judgement dated 2 June 2016, Case No. 2014 (wa) 13397; Tokyo District Court Judgement dated 18 May 2015, Case No. 2014 (wa) 23331, 26898, 27200, 27725, 27726, 27727 and 32779.

77 The law does not clearly define or describe "rejection" or indicate whether it is the comments, or the commenter, that has been "previously rejected".

78 Sapporo High Court Judgement dated 6 February 2020, Case No. 2018 (ne) 302.

79 Sapporo High Court Judgement dated 6 February 2020, Case No. 2018 (ne) 302.

80 Sapporo High Court Judgement dated 6 February 2020, Case No. 2018 (ne) 302.

81 Tokyo District Court Judgement dated 30 August 2016, Case No. 2015 (wa) 8495.

82 Osaka District Court Judgement dated 8 February 2016, Case No. 2015 (wa) 10086.

83 Tokyo District Court Judgement dated 9 July 2015, Case No. 2015 (wa) 13689.

84 Saitama District Court Decision dated 3 October 2017, Case No. 2017 (yo) 200.

85 Yokohama District Court (Kawasaki Branch) Decision dated 2 June 2016, Case No. 2016 (yo) 42.

86 Takamatsu High Court Judgement dated 25 April 2016, Case No. 2015 (ne) 144 and 254; Osaka High Court Judgement dated 8 July 2014, Case No. 2013 (ne) 3235.

87 Yokohama District Court (Kawasaki Branch) Decision dated 2 June 2016, Case No. 2016 (yo) 42.

88 "Whois" is the Internet protocol searching the owner of domain, IP address, Autonomous Systems number.

89 "A high probability" (i.e., a degree to which an average person would have no doubt) is the required standard of proof in such litigation (i.e., the second-step identification procedure). With respect to the interim relief (i.e., the first-step identification procedure), the required standard of proof is lessened to prima facie evidence.

90 Article 22 (2), Constitution of Kenya (2010).

91 Section 66, Computer Misuse and Cybercrimes Act (No. 5 of 2018).

92 Criminal defamation under section 194 of the Penal Code was ruled unconstitutional in Petition 397 of 2016 - Jacqueline Okuta & another v Attorney General & 2 others [2017] eKLR.

93 A notice of appeal was lodged by BAKE in the Court of Appeal, and it is likely that there may be further litigation on this. The CMCA was also one of 23 laws nullified on 29th October 2020, when a 3 Judge Bench of the High Court in Petition No. 284 of 2019: The Senate v The Speaker of the National Assembly & Another nullified 23 Acts of Parliament enacted by the National Assembly without reference to and input of the Senate as required under Article 110(3) of the Constitution of Kenya. The court suspended the nullification of the Laws for a period of 9 months from the date of the decision (29 October 2020) to allow time for the National Assembly to comply with the provisions of Article 110 (3) of the Constitution and regularise the Laws.

94 This means that media organisations that are the employer of a specific journalist can act in criminal proceedings.

95 https://www.persveilig.nl/wp-content/uploads/2019/10/collectieve-norm-mediasector.pdf (in Dutch).

96 https://www.persveilig.nl/wp-content/uploads/2019/10/veiligheid-splan-nederlandse-media.pdf (in Dutch).

97 https://www.persveilig.nl/wp-content/uploads/2019/10/Protocol-Persveilig.pdf (in Dutch).

98 Cases C-509/09 and C-161/10

99 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, transposed into Articles 5.4.1-5.4.17 of the Criminal Procedure Code

100 Cases C-509/09 and C-161/10.

101 Sw. Rättegångsbalken.

102 Swedish Code of Judicial Procedure, Chapter 10 Section 1.

103 Swedish Code of Judicial Procedure, Chapter 10 Section 3.

104 Swedish Code of Judicial Procedure, Chapter 10 Section 3.

105 Swedish Code of Judicial Procedure, Chapter 10 Section 8.

106 Swedish Code of Judicial Procedure, Chapter 10 Section 5.

107 Sw. Brottsbalken.

108 Sw. lag om internationell rättslig hjälp i brottmål.

109 Sw. lag om en europeisk utredningsorder.

110 Sw. Lag (1998:112) om ansvar för elektroniska anslagstavlor.

111 Sw. Yttrandefrihetsgrundlagen.

112 *Monroe v Hopkins* [2017] EWHC 433 (QB)

113 In *Chandler v O'Connor* [2019] EWHC 3181 (QB) (22 November 2019), the court awarded £10,000 in a summary disposal. The defendant, who in tweets had made defamatory allegations against the claimant that were serious and included alleging criminal money laundering and lobbying for a hard Brexit at the behest of a foreign state. If the case had been heard at a full trial, the court noted that £20,000 in damages would be reasonable.

114 *WXY v Gewanter* [2012] EWHC 496 (QB).

115 *GYH v Persons Unknown* [2017] EWHC 3360 (QB).

116 For example in *Hourani v Thomson (and others)* [2017] EWHC 432 (QB) the court awarded £30,000 in damages for harassment. The defendants were found to have accused the victim of murder and rape in person, via online posts, and the distribution of stickers. This was a co-ordinated campaign with a budget of US$500,000.

117 Inserted by section 111 Protection of Freedoms Act 2012.

118 *Hayes v Willoughby* [2013] UKSC 17.

119 Taken from: https://www.cps.gov.uk/legal-guidance/stalking-protection-orders.

120 *Connolly v DPP* [2007] EWHC 237 (Admin); [2008] 1 WLR 276.

121 https://www.bbc.co.uk/news/uk-england-derbyshire-53056165.

122 *Chambers v DPP* [2012] EWHC 2157.

123 *Director of Public Prosecutions v Smith* [2017] EWHC 359 (Admin).

124 *R. (on the application of Chabloz) v CPS* [2019] 10 WLUK 494.

125 *R. (on the application of Chabloz) v CPS* [2019] 10 WLUK 494.

126 *Weller & Ors v Associated Newspapers Ltd* [2014] EWHC 1163 (QB).

127 https://www.newburytoday.co.uk/news/news/30909/reading-crown-court-hungerford-man-avoids-jail-for-computer-hacking.html.

128 R v Mawji [2003] EWCA Crim 3067.

129 R v Furmage [2018] EWCA Crim 433.

130 R v Ireland [1997] 3 WLR 534.

131 R v Zain Qaiser [unreported] https://www.cps.gov.uk/cps/news/hacker-behind-ps500k-online-blackmail-campaign-jailed.

132 R v Blackshaw [2011] EWCA Crim 2312.

133 R v Andrew Coulson [2013] EWCA Crim 1026.

134 Merlin Entertainment LPC and others v Peter Cave [2014] EWHC 3036 (QB).

135 Norwood v the United Kingdom (2004).

136 Bowman v the United Kingdom (1982).

137 https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

138 422 U.S. 490, 511 (1975). See also, Havens Realty Corp. v. Coleman, 455 U.S. 363 (1982).

139 429 U.S. 252 (1977).

140 455 U.S. 363 (1982).

141 See, for example, Fair Hous. of Marin v. Combs, 285 F.3d 899, 905 (9th Circ. 2002).

142 432 U.S. 333 (1977).

143 uBID, Inc. v. GoDaddy Grp. Inc., 623 F.3d 421, 425-26 (7th Cir. 2010) (no general jurisdiction despite "extensive and deliberate" web-based contacts); Hayward, 2015 WL 5444787 at *6; Jackson v. Calif. Newspapers P'ship, 406 F. Supp. 2d 893, 895 (N.D. Ill. 2005) (California newspaper's website insufficient to confer jurisdiction in Illinois for defamation claim by Illinois resident).

144 uBID, 623 F.3d at 425; Bittman v. Fox, 2015 WL 5612061 at *3 (N.D. Ill. Sep. 23, 2015).

145 134 S. Ct. 1115 (2014).

146 Bittman v. Fox, 107 F. Supp. 3d 896 (N.D. Ill. 2015).

147 Apex Energy Group LLC v. Schweihs, 2015 WL 5613375, at *6-7 (S.D. Ind. Sep. 23, 2015) (maintaining a website that received visitors from Indiana did not show that alleged tortious conduct was expressly aimed at Indiana).

148 575 U.S. 723.

149 205 F. Supp. 2d 791 (N.D. Ohio 2002).

150 136 F. Supp. 2d 446, 448 (W.D. Pa. 2001).