

# Communication offences

Hate speech, harassment, stalking and more  
Dr Simona Ciobotaru  
[simona.ciobotaru@port.ac.uk](mailto:simona.ciobotaru@port.ac.uk)



# Definition

The Council of Europe defines hate speech as:

- The advocacy, promotion, or incitement, in any form, of the denigration, hatred or vilification of a person or group of persons, as well as any harassment, insult, negative stereotyping, stigmatization or threat in respect of such a person or group and the justification of all the preceding types of expression, on the ground of “race”, colour, descent, national or ethnic origin, age, disability, language, religion or belief, sex, gender, gender identity, sexual orientation and other personal characteristics or status
- (Council of Europe Commission against Racism and Intolerance, 2015, p. 3).

# Hate speech

- Inciting and condoning acts of violence and discrimination
- UK laws (Race Relations Act 1965 and Public Order Act 1986) prohibit the incitement of racial hatred and defamation on grounds of ethnic or national origin even without any likelihood of imminent lawless action following this incident.
- Religious hatred has also been added to the above
- Hate speech criminalisation is based on the social impact of such activity for supporting the development of violent behaviour against those it targets.

# Hate speech online

- Happens online particularly in fora of extremist political groups from Neo-Nazis, White Supremacists to Christian Fundamentalists and Anti-abortion groups
- Alt-Right and the move towards more mainstream platforms such as major social media like YouTube and Facebook
- Major impact since such platforms give a global, popular platform to hate speech groups – email distribution and sharing of content – but also perpetrating hate offences
- Relative anonymity or pseudonymity enables perpetrators (Yar and Steinmetz, 2019)
- [See video regarding Facebook challenges on hate speech](#)

# The weaponisation of memes and 'joking'

- [Extremist groups use memes in the form of jokes in order to propagate discriminatory/segregating views](#)
- Research by Woods and Ruscher (2021): The spread of memes, originating on extremist websites before appearing on mainstream platforms establishes a level of tolerance for these more extreme forms of “humour”, while also being effective at recruiting new members to those political causes, or radicalising them into further action
- Internet culture channels vs mainstream media
- [Incels](#), hate and misogyny – [calls for making misogyny a hate crime in UK](#)
- Muslim hate, xenophobia and racism

# Big challenges

- Different national standards – forum shopping
- The US will not sign the additional Protocol of the Cybercrime Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003) – 5 ratifications – very low
- [Political situation drifting towards the extremes](#) – Trump and Qanon and the [Russia/Ukraine war](#)
- The grey area of trolling: comments or behaviours online purposefully meant to annoy or disrupt

# COVID-19 and hate

- [Covid-19 and hate crime](#) – Anti-Chinese, xenophobic and ageist/ableist sentiment
- [Online hate speech rose 20% during pandemic in the UK and US](#)
- More time spent online, boredom and uncertainty fed abusive behaviours online – normalisation of trolling
- Polarisation due to COVID-19 lockdowns and vaccines – conspiracy theories
- [Secretary General of the UN highlighted the increase of hate in our societies](#)

# More big challenges

- Arbitrating and defining speech as hateful, degrading and discriminatory
- [Social media identification of prohibited speech and enforcement challenges](#) – banning of Qanon hashtags on TikTok
- Conflict between regulating hate speech and censoring political/journalistic speech
- Antidote to hate speech is not censorship but more speech in terms of education, positive messages and truthful information
- US 1<sup>st</sup> amendment protects free speech even if discriminatory/hateful unless specifically containing serious imminent threats of violence against identifiable persons or directly inciting other to commit specific criminal acts against those persons. (Yar and Steinmetz, 2019)
- [But Must taking over Twitter has changed the trend?](#)



# New Regulatory landscape for intermediaries

## E-commerce Directive adopted in 2000

- 'safe harbour' principle, online intermediaries hosting or transmitting content by a third party exempt from liability unless aware of the illegality and are not acting adequately to stop it
- They are subject to 'duties of care' and 'notice and take down' obligations to remove illegal online content
- **UK implementation: The Electronic Commerce (EC Directive) Regulations 2002**

## EU Digital Services Act:

- new mechanisms for users to flag illegal content online;
- platforms to cooperate with specialised 'trusted flaggers' to identify and expeditiously remove illegal content;
- Risk-based actions - new regulators - More transparency and safeguards for users
- Hate explicitly included in many ToS of big platforms

# A crazy example before we start with harassment: The LAMBDAMOO rape

- [Online harassment is not a new phenomenon!](#)
- [The LAMDA-MOO case](#)

# Harassment and stalking

- Harassment is a **behaviour intended to disturb or upset**
- **Stalking is an aggravated form of harassment**
- Usually victims are adults although it is possible to harass or stalk a minor
- Both behaviours are regulated as harassment and fall under the Protection from Harassment Act 1997 in the UK

# Importance of harassment and stalking

- Harassment links with trolling
- Stalking is mainly targeting women causing fear of violence
- Stalking became a big social issue through feminist/women's rights campaigning
- Social media facilitate stalking? How?
- First law in California related to stalking and murder of Rebecca Schaefer in 1991

# Council of Europe Convention on preventing and combating violence against women and domestic violence

- Brought changes from 2013 onwards
- the first European regional human rights instrument to specifically address violence against women as a form of gender-based violence:
- Art.34 calls for the criminalisation of stalking:
- *Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety, is criminalized*
- Recently, we had the first General Recommendation which is specifically devoted to the 'Digital Dimension of Violence against Women'.

# Harassment/Stalking and the Internet of Things

- IoT use and hacking of such devices can facilitate domestic abuse and harassment/stalking cases:
- <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>
- As IoT will become more prevalent, such uses can become more commonplace
- [Listen to this podcast](#) by my colleague Dr. Sugiura on technology and harassment

# Home Office report on tech-facilitated domestic abuse

- [Home Office](#) report highlights that domestic abuse perpetrators are increasingly using digital and online technologies to monitor, threaten and humiliate their victims.
- Children used to facilitate the abuse through exploitation of their devices such as phones, tablets and games consoles in order to monitor and maintain control over victims.
- From smart home abuse to spyware, revenge porn and unauthorised access
- [The newer cases of airtags and stalking](#)

# Protection from Harassment Act 1997

- S.1 provides that a person must not pursue a course of conduct (at least 2 occasions see s.7.3 – can include plain speech)
- a. Which amounts to harassment of another and
- b. Which he/she knows or ought to know that their course of action amounts to harassment of the other
- Criterion for knowing that action amounts to harassment: **if a reasonable person in possession of the same information would think so – common element for all harassment/stalking offences**
- Penalty: max 6 months or fine
- Can be issued with a restraining order under s.5
- If order breached up to 5 years



# Problems with restraining orders

- Sporadic enforcement by police – low arrest rates
- Ineffective deterrent for compulsive cases or people with mental health issues
- Alternatively it can overcriminalise protesters, overzealous journalists and others who demonstrate pestering behaviour, but not to the degree of stalking

# Fear of violence and harassment

- (s.4): If the harassment is of such a nature as to put the victim:
- **in fear of violence**
- **on at least two occasions** then
- offender may be charged with the aggravated offence of '**putting people in fear of violence**' entailing a penalty of up to 10 years
- It must be proven that the offender ought to know that the victim will fear that violence will be used against them
- **Cyberbullying here? There is no actual definition in law**
- **Alternative for cyberbullying/trolling: [Malicious Communications Act 1988](#)**

# New Stalking offence

- Protection of Freedoms Act 2012 adds to PHA 1997:
- s.2A: The person pursues a course of conduct in breach of section 1(1) (conduct amounting to harassment) and the course of conduct amounts to stalking.
- Section 2A provides a non-exhaustive list of relevant behaviours for example:
  - (c) publishing any statement or other material—
  - (i) relating or purporting to relate to a person, or
  - (ii) purporting to originate from a person,
  - (d) monitoring the use by a person of the internet, email or any other form of electronic communication
- Summary conviction up to 51 weeks and fine

# Stalking involving fear of violence or serious alarm or distress

- New offence (PoFA 2012)
- Course of conduct amounting to stalking and either:
  - (i) causes another (“B”) to fear, on at least two occasions, that violence will be used against B, or
  - (ii) causes B serious alarm or distress which has a substantial adverse effect on B's usual day-to-day activities
- A knows or ought to know that A's course of conduct will cause B so to fear on each of those occasions or (as the case may be) will cause such alarm or distress.
- More serious stalking offence
- Max penalty: 10 years
- If not guilty for this, maybe guilty for s.2 or s.2A

# Racially aggravated harassment

- S.32 of the Crime and Disorder Act 1998 ( CDA 1998) provides for two racially or religiously aggravated harassment offences, provided the racial or religious aggravation test in section 28 of the CDA 1998 is met.
- Under section 32(1) of the CDA 1998, a person is guilty of an offence under this section if he commits-
- a) an offence under s2 or s2A of the Protection from Harassment Act 1997 (offences of harassment and stalking); or
- b) an offence under s4 or s4A of that Act (putting people in fear of violence and stalking involving fear of violence or serious alarm or distress), which is racially aggravated for the purposes of this section.
- Penalty increases compared to PFHA 1997 Act regular offences (2 years for ss.2/2A and 14 years for ss. 4/4A)

# What is a racially or religiously aggravated offence?

- S.28 of CDA 1998:
- An offence is racially or religiously aggravated if—
- (a) at the time of committing the offence, or immediately before or after doing so, the offender demonstrates towards the victim of the offence hostility based on the victim's membership (or presumed membership) of a racial or religious group; or
- (b) the offence is motivated (wholly or partly) by hostility towards members of a racial or religious group based on their membership of that group.
- Disability hate crime offences also exist

# Tactics to mitigate cyberstalking

- Ignore and avoid - block
- Online presence management to reduce exposure
- Help seeking by victims
- Negotiation/threat and retribution
- Compliance and false excuses to placate the stalker
- Is it realistic to ask victims to disconnect?

# Cyberbullying/Trolling and the law

- S.1 Malicious Communications Act 1988: offence for any person to send a communication that is "indecent or grossly offensive" for the purpose of causing "distress or anxiety to the recipient"
- **Extends to false information where the offender knows or believes it to be false**
- S. 127 of Communications Act 2003: offence to send via any electronic communication network a message or other matter that is deemed "grossly offensive or of an indecent, obscene or menacing character".
- S.5 Public Order Act 1986: offence to use threatening, abusive or insulting words, behaviour, writing or any visual representations likely to cause harassment, alarm or distress within the hearing or sight of a person.
- Generally lower penalties than Protection of Harassment Act 1997
- Serious problem globally - suicides have prompted discussions for more hands on treatment of the problem. See the Lori Drew case in the US (Holt et al, 2019)
- See also case of the Starwars kid video



# **AMP v Person's Unknown**

- Unique application of Protection from Harassment Act 1997
- Claimant's mobile stolen/lost while at Uni
- Sexually explicit images in it (face visible)
- Blackmailing of claimant and family by the person that got the phone
- When that failed, blackmailer uploaded images via torrent
- Injunction served by court on blackmailer requiring desist and destroy
- The judge agreed that seeding the torrent was harassment, and that the claimant had a reasonable expectation of privacy under Article 8 of the Human Rights Act.
- Failure to comply: offence that can lead to a European Arrest Warrant

- Desist and destroy initially successful
- US-based free speech group claimed the decision was chilling speech and re-uploaded the photos
- Efforts to remove photos based on copyright now
- Valuable precedent for establishing that the **sharing of personal images = harassment**

# Revenge Porn

- S. 33 Criminal Justice and Courts Act 2015
- Offence of disclosing private sexual photographs or films **without the consent of** an individual who appears in them and **with intent** to cause that individual **distress**.
- Purpose must be to cause distress to the victim.
- If message is sent because it was thought to be funny would not be committing the offence
- Defences relate to assisting in crime investigations, journalistic publications in the public interest, previous disclosure for reward
- Max penalty: 2 years - Cases have mainly been lawsuits – big case in US with \$6.4 million in damages

# Upskirting offence

- It is estimated that one in ten women have already experienced a form of cyber violence since the age of 15.
- Voyeurism Act 2019 amends Sexual Offences Act adding s. 67A
- Whoever operates equipment or records an image beneath the clothing of another person
- To enable themselves or others to observe genitals, buttocks or underwear, when these would not be visible
- **Purpose:** obtain sexual gratification, humiliation, alarm or distress
- Does so without the victim's consent or reasonably believing there is consent
- Max penalty: 2 years
- Downblousing offence discussed as part of Online Safety bill...

# Virtual mobs

- En masse harassment on particular victims (dogpiling)
- From short bursts on social media to long-term complex campaigns.
- Character assassinations
- Useful for extreme groups to bring their arguments and hate to the mainstream
- [The gamergate case and harassment against women criticising sexist gaming](#)

# The Online Safety Bill

Duty of care: duty on all companies including search engines to protect users from illegal content

Must proactively prevent content from reaching users

Legal but harmful content to be blocked for children, but not for adults in latest iteration

[Senior manager liability added after long debate](#)

Failure to comply with the proposed rules will place organizations at risk of fines of up to 10% of global annual turnover or £18 million (US\$22 million), whichever is higher.

Ofcom will be the regulator

# The future

- [The rise of deepfake porn](#) – [efforts in the UK to criminalise it](#)
- Prosecutors would no longer need to prove they intended to cause distress.
- The metaverse has a harassment problem already - [Gang rape in the metaverse](#)
- Normalisation of such virtual behaviour can lead to more violence for our children in the offline environment as well.
- “Personal boundary” mode – helps dodge unwanted interactions
- [The report](#) revealed multiple types of abusive behaviour such as minors being exposed to graphic sexual content, bullying, harassment and abuse of other users, including minors, minors being groomed to repeat racist and extremist messages
- reporting tools were inefficient for reporting many of these issues