

XV. HATE SPEECH, CYBERBULLYING AND THE DIFFICULTY OF DETECTING CRIME IN ONLINE SPACE – THE EXAMPLE OF THE UNITED KINGDOM

ÁGNES JUHÁSZ

1. Regulation of hate speech

In the United Kingdom, freedom of expression is regulated by the Human Rights Act 1998 (hereinafter referred as to HRA)¹, by incorporating the rights set out in the European Convention on Human Rights (after this referred to as ECHR). According to Article 12(1) HCR, everyone has the right to freedom of expression. This right includes the freedom to hold opinions on the one hand, and to receive and impart information and ideas. On the other hand. Article 12(2) states that exercising of this freedom may be subject to such formalities, conditions, restrictions, or penalties. For instance, freedom of expression can be restricted to protect the reputation or rights of others.

The use of hateful expressions, as in other countries, is negatively perceived in the UK. Acts motivated by hate cover a wide range of acts including criminal offences (hate crimes) and non-criminal hate incidents. The term ‘hate speech’ is a broader expression that covers both criminal and non-criminal acts.

The existing set of rules on hate speech is the result of several centuries of evolution. It overarches the branches of law combining the provisions of constitutional law, criminal law, and civil law. In this development process, the last five decades have been particularly important, as the elaboration of the

¹ Available at <https://www.legislation.gov.uk/ukpga/1998/42/contents>

anti-discrimination rules and the development of the international regulation of human rights took place in this period.

Hate crimes are regulated by the rules on the protection of the public order. However, the applicability of the related provisions depends on the place where the given act was committed. Whereas similar rules are applicable to hate crimes in England, Scotland, and Wales, Northern Ireland adopted its regulation on hate crimes, even if these rules fully comply with the regulations of the other three parts of the UK.

In the following, provisions related to hate crimes are reviewed according to the parts of the UK.

1.1. England, Scotland, and Wales

Provisions aimed at treating the use of expressions inciting racial hatred appeared first time in 1965, during the fight against racial discrimination. The adoption of these rules was a sort of legislative response to the immigration waves of the 1950s and 1960s, and the incidents motivated by racial discrimination that became more and more common at that time.

Race Relations Act 1965 (referred to as RRA) was adopted to regulate different acts motivated by racial discrimination. Article 6(1) RRA provided on the incitement to racial hatred qualifying it as unlawful. Incitement to racial hatred could be committed by the publishing or distributing or written matter having a threatening, abusive, or insulting nature. Moreover, the offence of incitement to racial hatred is committed if a person uses in any public place or at any public meeting words which are threatening, abusive, or insulting. In both cases, it is required that the person committing the offence acts with intent to stir up hatred against any section of the public in Great Britain distinguished by colour, race, or ethnic or national origin, or the act is likely to stir up hatred against any section distinguished by the mentioned characteristics.

From the 1970s, provisions on racial hatred were highly debated which later resulted in the amendment of these rules.

Rules on racial hatred are contained by the Part III of the Public Order Act 1986 (hereinafter referred to as POA).² In 2023, a new Public Order Act was passed, amending the provisions of the POA 1986 in several places. However, the provisions on racial hatred remain unchanged.

At the beginning of Part III, the meaning of racial hatred is clarified. According to Article 17, racial hatred, in the application of Part III POA, means hatred

² Available at <https://www.legislation.gov.uk/ukpga/1986/64/contents>

against a group of persons defined by reference to colour, race, nationality (including citizenship), or ethnic or national origins. However, the interpretation of this article arises further questions regarding the term ‘race’.^{3,4} After this clarification of racial hatred, Part III POA provides rules on different criminal offences by which the person committing the act intends to stir up racial hatred or racial hatred is likely to be stirred up thereby.

According to Article 18(1) POA, the use of threatening, abusive, or insulting words or behaviour, or displaying any written material which is threatening, abusive, or insulting, is an offence, if the act intends to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. Similarly, the publishing or distributing of written material having the same features, i.e. it is threatening, abusive, or insulting, is also an offence provided that the person committing the act intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. (Article 19(1) POA)

The legislator also takes into consideration if threatening, abusive, or insulting words are used within the framework of a public performance. According to Article 20(1) POA, any person who presents or directs a public performance of play commits an offence, if the performance involves the use of threatening, abusive, or insulting words or behaviour and the person intends thereby to stir up racial hatred, or, having regard to all circumstances, and, in particular, taking the performance as a whole, racial hatred is likely to be stirred up hatred. In the lack of such intention, the person who presents or directs the performance can be revealed from the responsibility, if the fulfilment of either of the circumstances declared in points (a)-(c) of Article 20(2) can be proven by this person. For defence, the person presenting or directing the performance shall prove that he did not know and had no reason to suspect that (a) the performance would involve the use of the offending words or behaviour, or (b) the offending words or behaviour were threatening, abusive or insulting, or (c) the circumstances in which the performance would be given would be such that racial hatred would be likely to be stirred up.

According to Article 21(1) POA, distributing, showing, or playing any recording of visual images or sounds which are threatening, insulting or abusive, is a

3 Certain ethno-religious groups such as Jews and Sikhs have been recognised as racial groups in law in addition to being religious groups, while Roma, Romani Gypsies and Irish Travellers (‘GRT’) are also recognised racial groups based on their ethnic origins. Cf. *Mandla v Dowell Lee* [1983] 2 AC 548, [1983] 2 WLR 620; *Commission for Racial Equality v Dutton* [1989] QB 783, [1989] 2 WLR 17; *O’Leary v Punch Retail* (29 Aug 2000).

4 Neller, 2023, p. 285.

criminal offence if this act intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. In those cases when a given broadcasting or programme contains threatening, abusive, or insulting visual images or sounds, not only the person who provides the programme service, but those by whom the programme is produced or directed or by whom the offending words or behaviour are used, shall be guilty of committing criminal offence.) Article 22(2) POA) Nevertheless, the perpetration of the above-mentioned criminal offence can only be assessed if the person intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby.

Part III POA devotes a separate section for the racially inflammatory materials. The mere possession of written material or a recording of visual images or sounds which is threatening, abusive or insulting, is a criminal offence, if the written material is being displayed, published, distributed, the recording is being distributed, shown, played, or both kind of materials are included in a cable programme service, whether by himself or another. (Article 23(1) POA) Similarly to other acts, these acts can only be assessed as criminal offence if the act of the person committing is purposeful. By committing the act, the person intended to stir up hatred or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby.

It shall be noted that guilt of a legal entity (body corporate) also can be established in the case of committing the above-mentioned acts. In those cases when the act is committed with the consent or connivance of a director, manager, secretary or other similar officer of the body or a person purporting to act in any such capacity, both the person committing the act and the body corporate are guilty of the offence and liable to be proceeded against and punished accordingly. (Article 28(1) POA)

In October 2007, after countless failed attempts, incitement to religious hatred was criminalised and POA was supplemented with a new part (Part 3A).⁵ From March 2010, following a recent amendment of the POA and the heading of Part 3A as well, Part 3A covers other offences based on hatred against

⁵ Part 3A was inserted by the Racial and Religious Hatred Act 2006. For examples from the related literature, see Cumper, Peter: Outlawing incitement to religious hatred – a British perspective, In: *Religion and Human Rights*, Vol. 1 (2006) No. 3, pp. 249–268; Hare, Ivan: Crosses, Crescents and Sacred Cows. Criminalising Incitement to Religious Hatred, In: *Public Law*, 3/2006, pp. 521–538; Thompson, Simon: Freedom of expression and hatred of religion, In: *Ethnicities*, Vol. 12 (2012), Issue 2, pp. 215–232, McGuire, Kim-Salter, Michael: Legal Responses to Religious Hate Crime: Identifying Critical Issues, In: *Kings Law Journal*, Vol. 25 (2014) Issue 2, pp. 159–184.

persons on grounds of sexual orientation.⁶ These amendments of the POA were important milestones in the regulation of hate crimes since acts motivated by hatred against persons on religious hatred or grounds of sexual orientation were separated from racial hatred. Comparing these two branches of offences, some essential differences can be outlined. In the case of the former, either the conduct of the person or the material possessed by the person shall have a threatening nature, but the abusive or insulting character is not required. Moreover, acts stirring up religious hatred or hatred on the grounds of sexual orientation qualifies as a criminal offence only in those cases when the act of the person is intentional. Acts which are likely to stir up hatred cannot be assessed as a criminal offence.

Nevertheless, regarding the delimitation of racial and religious hatred, it shall be noted that the boundaries between them are sometimes blurred. While some religions are practised worldwide (e.g. Christianity, Islamism), other religions are specifically linked to a particular ethnic group, although their practice is not territorially defined (e.g. Judaism). In Britain, the judicial practice established the category of ‘mono-ethnic’ faith (e.g. Judaism, Sikhism).⁷ However, the distinguishing between ‘race’ and ‘religion’ is not always clear which makes difficult to assess if a certain act motivated by hatred should be deemed under the rules on racial hatred or religious hatred.⁸

The structure of Part 3A practically wholly complies with the Part III of the POA. Introductory provisions intend to make clear the basic expressions. According to Article 29A POA, in the application of Part 3A, the expression ‘religious hatred’ means hatred against a group of persons defined by reference to religious belief or lack of religious belief. The POA, however, does not define what amounts to a religion or a religious belief. In the absence of a specific legal provision, it is for the courts to determine whether a case involves religion or religious belief. It can be said that Article 29A can be applied in the case of widely recognised religions like Christianity, Islam, Hinduism, Judaism, Buddhism, Sikhism, and Rastafarianism, while branches or sects within a religion

6 For the comprehensive discussion of the problem of hatred against persons on grounds of sexual orientation see Goodall, Kay: Challenging hate speech: incitement to hatred on grounds of sexual orientation in England, Wales and Northern Ireland, In: *The International Journal of Human Rights*, Vol. 13 (2009), Issue 2-3, pp. 211–232.

7 Cf. *Mandla v Dowell Lee* [1983] 2 AC 548. The case is reviewed and analysed by Neller. See Neller op. cit. p. 287.

8 About this problem see in details Goodall, Kay: Incitement to Religious Hatred: All Talk and No Substance?, *The Modern Law Review*, Vol. 70, No. 1 (Jan., 2007), pp. 89–113, Neller op. cit. p. 285, Hare op. cit. 534.

can be considered as religious beliefs. The lack of religious belief also can be the ground for religious hatred.

‘Hatred on the grounds of sexual orientation’ means hatred against a group of persons defined by reference to sexual orientation whether towards persons of the same sex, the opposite sex, or both. (Article 29AB POA)

Among the hate crimes covered by Part 3A POA, the legislator first sets out various cases of incitement to hatred based on religious and sexual orientation, which are fully compatible with the situations set out in Part III POA. It is a criminal offence to use threatening words or behaviour, or display any written material that is threatening if the person committing the conduct intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation (Article 29B POA) It is important to note that the in this case, contrary to hate speech based on racial hatred, the offence can only be established if the conduct is purposeful, and the suitability of the conduct to incite hatred does not in itself provide a basis for criminalising the conduct. The act may be committed in a public or private place. However, the act is not a criminal offence if the place where the words or behaviour are used, or the written material is displayed, by a person inside a dwelling and is not heard or seen except by other persons in that or another dwelling.⁹

The publishing or distributing of written material that is threatening is an offence if the person committing the act intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29C(1) POA). Similarly, any person who presents or directs a public performance that involves the use of threatening words or behaviour, is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29D(1) POA) According to the POA, distributing, showing, or playing a recording of visual images or sounds which are threatening is an offence if the person intends to stir up religious hatred or hatred on the grounds of sexual orientation with his act. (Article 29E(1) POA) In those cases when a given programme containing threatening visual images or sounds is included in a programme service, the person providing the programme service, and any person by whom the programme is produced or directed, or by whom offending words or behaviour are used, is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29F POA)

9 In the application of Part III POA, a ‘dwelling’ means any structure or part of a structure occupied as a person’s home or other living accommodation (whether the occupation is separate or shared with others) but does not include any part not so occupied, and for this purpose ‘structure’ includes a tent, caravan, vehicle, vessel or other temporary or movable structure. (Article 29 POA).

In the case of criminal offences regulated by Part 3A POA, religious groups or grounds of sexual orientation are the target of the hate speech. However, there are other cases when religion is not the characteristic of why the group of persons are attacked, but the source of hate speech. These kinds of religiously motivated expressions are often critical and hostile towards same-sex relationships, therefore, a special dimension of the right to expression, i.e. the right to religious expression and the protection against hate speech (homophobic speech) is in conflict.¹⁰¹¹

After the regulation of the above-mentioned criminal offences which intend to stir up racial hatred, religious hatred, or hatred on the grounds of sexual orientation, Part 3A POA provides rules on the inflammatory materials. According to Article 29G POA, it is a criminal offence if a person possesses written material or recording of visual images or sounds that have a threatening nature, provided that the written material is displayed, published, distributed, or included in a programme service, or the recording is being distributed, shown, played, or included in a programme service, whether by himself or another. Likewise, both the intentional nature of the committing act and the purpose of stirring up hatred are required to deem the act as a criminal offence.

After the taxation of the different criminal offences, Articles 29J and 29JA declare the protection of freedom of expression and highlight separately the freedom of expression on sexual orientation. Article 29J POA, according to the Marriage (Same Sex Couples) Act 2013, states that the discussion or criticism of sexual conduct or practices or the urging of persons to refrain from or modify such conduct or practices shall not be taken of itself to be threatening or intended to stir up hatred. The same is true for marriage: any discussion or criticism of marriage that concerns the sex of the parties to marriage shall not be taken of itself to be threatening or intended to stir up hatred.

In 2021 the Scottish Parliament adopted the Hate Crime and Public Order (Scotland) Act¹¹² which prescribes the application of provisions other than the rules of POA in Scotland. On the other hand, the Scottish Act will amend or repeal several provisions of Part 3A of the POA.

Although the act maintains the existing legislative protections from crimes aggravated by prejudice towards race, religion, disability, transgender identity,

10 For the related case law, see *Hammond v Department of Public Prosecutions* (2004) EWHC 69

11 See in more detail: Edge, Peter W.: *Oppositional Religious Speech: Understanding Hate Preaching*, In: *Ecclesiastical Law Journal*, Volume 20 (2018) Issue 3, pp. 278-289; Foster, Steve: *Accommodating Intolerant Speech: Religious Free Speech versus Equality, and Diversity*, In: *European Human Rights Law Review*, No. 6/2019, pp. 609-625.

12 Available at <https://www.legislation.gov.uk/asp/2021/14/contents>

and sexual orientation, it introduces new protections against offences aggravated by prejudice towards a person's age. Moreover, it redefines the term 'transgender identity' by removing the term 'intersexuality' and adding the term 'variations in sex characteristics.'

The applicable provisions of the act were highly debated. Some authors expressly argued that the legislation threatens freedom of expression.¹³ Finally, after more than four years, the legislation was implemented on 1st April 2024.

1.2. Northern Ireland

In Northern Ireland, incitement to hatred has been a criminal offence since 1970 when the *Prevention of Incitement to Hatred Act* (hereinafter referred to as PIHA) was adopted. According to Article 1 PIHA a person shall be guilty of an offence if, with intent to stir up hatred against, or arouse fear of, any section of the public in Northern Ireland, he publishes or distributes written or other matter which is threatening, abusive or insulting, or uses in any public place or at any public meeting words which are threatening, abusive or insulting.

This act was replaced by the Public Order (Northern Ireland) Order 1981. The adoption of this act resulted in the insertion of the criminal offence of incitement to hatred into a wider public law regulatory framework. However, its life was quite short, since in 1987, a new Public Order (Northern Ireland) Order¹⁴ (hereinafter referred to as POO) was adopted which is still in force nowadays, even though it has been amended several times.

Part III of POO contains rules on stirring up hatred and, at the same time, on the act arousing fear.¹⁵ The separation of the expressions 'stirring up hatred' and 'arousing fear' is a basic element of the regulation of Northern Ireland. Moreover, the use of the expression 'arousing fear' is an important difference between POO and POA which is applicable in England, Scotland, and Wales since the latter act does not contain this expression at all.

At the beginning of Part III POO, the terms 'fear' and 'hatred' are explained. According to Article 8(1) POO, 'fear' means fear of a group of persons defined by reference to religious belief, sexual orientation, disability, colour, race, nationality (including citizenship), or ethnic or national origins, while 'hatred' means hatred against a group of persons defined by reference to religious belief, sexual orientation, disability] colour, race, nationality (including citizenship) or ethnic

¹³ Bechtold, 2022.

¹⁴ Available at <https://www.legislation.gov.uk/nisi/1987/463/contents>

¹⁵ It is worth noting that POO does not take the expression 'incitement to hatred' from the previous act of 1981.

or national origins. Sexual orientation and disability are a group-forming characteristic from 2004, when POO was amended.¹⁶ After the clarification of the terms 'fear' and 'hatred', POO declares that any discussion or criticism of marriage which concerns the sex of the parties to marriage is not to be taken of itself to be threatening, abusive or insulting, or intended to stir up hatred or arouse fear. (Article 8(2) POO).¹⁷

Article 9(1) POO declares that a person who uses threatening, abusive, or insulting words or behaviour, or displays any written material which is threatening, abusive, or insulting, is guilty of an offence if he intends thereby to stir up hatred or to arouse fear, or, having regard to all the circumstances, hatred is likely to be stirred up or fear is likely to be aroused thereby. However, the person is not guilty of the said offence if he did not intend to stir up hatred with his words or behaviour, or the written material, and he was not aware that his act might be, threatening, abusive, or insulting. (Article 9(4) POO)

The further articles of the POO, just as the provisions of the POA introduced in point (a) of this subchapter, state that the publishing or distributing of a written material, or distributing, showing or playing a recording of visual images or sounds is a criminal offence, if the written material or recording has threatening, abusive or insulting nature and the person committing the act intends thereby to stir up hatred or arouse fear, or, having regard to all the circumstances hatred is likely to be stirred up or fear is likely to be aroused thereby. (Articles 10(1) and 11(1) POO) Similarly, with the same characteristics, the inclusion of a programme having a threatening, abusive, or insulting nature in a programme service is also a criminal offence. In this latter case not only the person providing the programme service, but any person by whom the programme is produced or directed, and by whom offending words or behaviour are used are guilty of the mentioned offence. (Article 12(1) POO)

According to Article 13(1) POO, the possession of written material or a recording of visual images or sounds which are threatening, abusive, or insulting is a criminal offence, if the person committing the act intends or is likely to stir up hatred or arouse fear, and displays, publishes, distributes the written material, distributes, shows or plays the recording, or includes either the written material or the recording in a programme service.

16 The original text of Article 8 POO was supplemented by the terms 'sexual orientation' and 'disabled' in 2004 when the Criminal Justice (Northern Ireland) Order 2004 was adopted and amended the POO.

17 This provision was inserted by The Marriage (Same-sex Couples) and Civil Partnership (Opposite-sex Couples) (Northern Ireland) Regulations 2019. The provision is in force from 13th January 2020.

In 2020, a consultation was launched in the United Kingdom. The main goal of this consultation was to prepare the amendment of the existing regulation on hate crimes to harmonise the applicable legal consequences. The major reason for the consultation was the divergent treatment of hate crimes by criminal law. Regarding the weight of the applied legal consequences, these criminal offences were assessed differently which greatly depends on whether the offence was committed because of the belonging of the victim to a given racial group, or his disability. In practice, a demand has arisen for the extension of the criminal law regulation. According to this, beyond those characteristics that are the most common basis for hate crimes (e.g. ethnicity, racial or religious affiliation, sexual orientation, disability, transgenderism, etc.), several other personal features shall be protected which also evoke hatred within the society. Such a feature can be the person's gender (e.g. misogyny) or age (c.f. ageism), but the homelessness or the occupation (e.g. sex worker) of the person, as well as the philosophical conviction or the belonging to a subculture (e.g. gothic, punk, etc.) can also be the basis for the victimisation of hate crime.

Considering the results of the consultation, the British legislator intends to create a more efficient criminal law action against acts motivated by hatred. Acts based on discrimination on grounds of sex and gender, and racial hatred acts committed in football games would also be covered by criminal law provisions. After the close of the consultation process, the received opinions were evaluated, and a final report was published in 2021.¹⁸ The document contains detailed recommendations for the reform of hate crime offences. (E.g., among others, there is a recommendation on including the term 'asexual' into the definition of sexual orientation and replacing the term 'transgender' with the term 'transgender or gender diverse'. It is also recommended to add age as a protected characteristic in hate crime laws.)

2. Definition and regulation of cyberbullying

When researching the regulation on hate speech, the delimitation of hate speech and bullying is essential. While hate speech appears as an independent type of hate crime, bullying is not a criminal offence in the United Kingdom, even if it shows similar features. The term 'bullying' covers conduct where a person uses

¹⁸ Available at <https://assets.publishing.service.gov.uk/media/61ba053ed3bf7f055eb9b8cf/Hate-crime-report-accessible.pdf>

his power or strength to frighten or hurt someone, who is thought to be weaker. Bullying act is often performed over a longer period, and the person committing the act often forces the other person to do something he does not want to do. The scope of the victims of bullying is wide since bullying can be committed practically anywhere (e.g. school, workplace, etc.).

Compared to hate speech, which is regulated by law, the perpetration of bullying covers a much wider range of conduct. Bullying might appear in several forms of acts, independently or combined. In the case of verbal bullying, the perpetrator, the bully, uses words to hurt, harass, or scare the other person. One typical act is the use of a nickname (sobriquet) or making rude comments about the person or his family. Physical bullying always requires assault (e.g. hitting, pushing, physical abuse, aggression, etc.) Emotional abuse covers those cases where the bully wants to make an impact on the other person's emotions by using threats, making him uncertain, or displacing him from a given community (e.g. community of friends or workplace community) or a given activity (e.g. team sport).

The interception point of hate speech and bullying is discrimination since bullying also can appear as a form of discrimination when the bullying conduct (threatening or harassment) is based on the person's disability, racial or religious belonging, philosophical belief, sexual or gender identity.

As online platforms and technologies recently came to the fore, bullying appears more and more visibly in the online space, especially in social media. Bullying conduct committed in the online space is called cyberbullying by the literature. The term refers to the place of perpetration and, at the same time, distinguishes itself from the traditional, face-to-face bullying acts. Cyberbullying can be defined as an intentional aggressive behaviour involving a power imbalance between those involved, where the perpetrator, the cyberbully intends to harass, intimidate, and threaten the cyber-victim repeatedly over time using the internet (including social networking sites) and via electronic devices, such as sending text messages, emails, and video messages.¹⁹

Cyberbullying, by its nature, is particularly common among young people. According to a national survey in 2014²⁰, 42% of youth under age 25 have already felt threatened in the online space, while 56% of the asked persons have already witnessed online harassment.

The act can be committed either by computer, mobile, tablet, or game console. Cyberbullying can be realised not only via electronic correspondence (e.g.

¹⁹ El Asam and Samara, 2016, pp. 127–141; Marczak and Coyne, 2010, pp. 182–193.

²⁰ Cyberbullying: An analysis of data from the Health Behaviour in School-aged Children (HBSC) survey for England, 2014.

by sending threatening or harassing e-mails) or text messages but also by making offensive comments on social media platforms (e.g. Facebook, Twitter, Instagram, etc.) or by sharing embarrassing or smear photos or videos or making false profiles. Bullying also can take place in chat rooms, interactive video game communities (e.g. by sending messages, displacing from the game, etc.), and several other places in the online space.

Cyberbullying commonly appears not as an independent cyber act but as the supplementary or accompanying conduct of the personal, direct, and face-to-face bullying act. However, while bullying is limited to the time that the harmed person spends in the place of the commitment of the act (i.e. at school, workplace, or in another community), in the case of cyberbullying the harming conduct can be realised at any time of the day due to the unlimited availability of the Internet. A further difference is that cyberbullying, regardless of the intent of the perpetrator, typically takes place in front of a wider audience (e.g. a smear photo reaches much more people through multiple sharing). Nevertheless, proof of cyberbullying is easier in many cases since victims can take screenshots, save photos or videos, and deliver the website address to the investigating authorities. On the other hand, however, perpetrators may easily hide their identity by making themselves anonymous, and they often behave in such a way that they would never do in real life. Since in the online sphere, perpetrators do not see the reactions of their victims, they can remain emotionally almost fully independent because they are not aware of the emotional impact of their conduct, and therefore, it is more difficult for them to give up their harming activity.

As it was mentioned above, bullying including cyberbullying as a type of bullying regarding the place of perpetration, is not an independent criminal offence in the UK when finishing the manuscript of this chapter. Therefore, there is no specific law addressing conduct which can be deemed as cyberbullying. Nevertheless, due to the diversity of perpetrating conduct, various legislative provisions can be applied to both forms of bullying. In the following, these provisions are reviewed.

It also should be added that in the UK, the need for a single set of rules covering unlawful conduct committed in the online space has been growing over the last decade. In 2019, the UK Government launched a consultation²¹ on online harms to tackle internet-related risks, such as cyberbullying, and to develop a single regulatory framework that would provide a transparent set of requirements

21 The materials related to the consultation, including the White Paper on which it is based (Online Harms White Paper) and a summary of the government's responses to the consultation are available at: <https://www.gov.uk/government/consultations/online-harms-white-paper>

for ISPs to establish and maintain online safety and would ensure the protection of users' rights to free expression. The launching of this consultation was the first step in the process whose main objective was to amend and make more consistent and transparent the then-existing, rather fragmented legislation, which contains both public and private law provisions.

After the closing and the evaluation of the consultation, on 12th May 2021, the Government submitted the Draft Online Safety Bill.²² After its publication, the bill was highly criticised all over the UK and provoked debates from both theoreticians and practitioners.²³ Some critics argued that the bill was not strict enough, while others said it went too far. Some also questioned the practical applicability of some of the provisions of the bill. However, after numerous refinements, amendments, and additions, the bill was finally adopted during the parliamentary session 2022-2023. The new act entitled Online Safety Act 2023 (hereinafter OSA)²⁴ received Royal Assent on 26th October 2023. The provisions of the OSA will enter into force gradually.²⁵ Therefore, at the end of this point of the Chapter, the new criminal offences introduced by the OSA will also be reviewed, since these offences can also be committed electronically, i.e. in the online space.

According to Article 1(1) of the Protection from Harassment Act 1997²⁶, it is a criminal offence if a person pursues a conduct that amounts to the harassment of another, and which he knows or must know amounts to harassment of the other. In the online space, this conduct can be perpetrated by sending a mass of e-mails or messages with abusive content if the perpetrator intends to intimidate the other person or to cause pain and suffering for him.

Beyond the Protection from Harassment Act 1997, provisions of the Malicious Communications Act 1988²⁷ (hereinafter MCA) also can be applied to bullying. MCA declares that any person who sends to another person a letter, an electronic communication, or an article of any description that conveys a message that is indecent or grossly offensive, a threat, or information that is false and known or believed to be false by the sender, or any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature, is guilty of an offence. Furthermore, the perpetrator is required to intend by the sending of these items to cause distress or anxiety to the recipient or to any other

22 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

23 Coe, 2022, pp. 50–75; Trengove et al., 2022; Anderson, 2022.

24 Available at <https://www.legislation.gov.uk/ukpga/2023/50/enacted>

25 Regarding the commencement of the provisions see in detail Article 210 OSA.

26 Available at <https://www.legislation.gov.uk/ukpga/1997/40/contents>

27 Available at <https://www.legislation.gov.uk/ukpga/1988/27/contents>

person to whom the content or nature of the letter, electronic communication, or other article is communicated.²⁸ The term ‘sending’ shall be interpreted in a wide sense since it covers not only sending but delivering and transmitting.

It shall be noted that the content of the above-mentioned article will be amended by the Online Safety Act and the term used in Article 1(1)(a)(ii) and (iii), i.e. ‘threat’, and ‘information that is false and known or believed to be false by the sender’ will be repealed on 31st January 2024.

Regarding phone messages, the Telecommunications Act 1984²⁹ can be applied. Within the rules on the improper use of public telecommunication, Article 43 states that sending a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character. The sending of a message is also punishable if the person commits the act to cause annoyance, inconvenience, or needless anxiety to another, and he knows the message to be false or persistently makes use, for that purpose, of a public telecommunication system.

The Communication Act 2003³⁰ supplements the provision of the Telecommunications Act 1984 and contains rules on the improper use of public electronic communications networks. According to Article 127 a person who sends using a public electronic communications network a message or other matter which is grossly offensive or of an indecent, obscene, or menacing character or causes any such message or matter to be so sent, is guilty of an offence. The person is also guilty of an offence if, to cause annoyance, inconvenience, or needless anxiety to another, he (a) sends using a public electronic communications network, a message that he knows to be false, (b) causes such a message to be sent, or persistently makes use of a public electronic communications network.

Comparing the content of the last two pieces it can be concluded that Telecommunications Act 1984 and the Communications Act 2003 make similar provisions for communications. The main difference is how the offence was committed, i.e. whether the offence was committed using public telecommunications or a public electronic communications network.

The Obscene Publication Act 1959³¹ prohibits the publication of obscene matters. According to Article 2(1) of the act, any person who, whether for gain or not, publishes an obscene article or who has an obscene article for publication for gain (whether gain to himself or gain to another)] shall be liable. Regarding the interpretation of this provision, Article 1 clarifies the terms ‘article’, ‘publish’, and ‘obscene’.

28 Article 1(1) MCA.

29 Available at <https://www.legislation.gov.uk/ukpga/1984/12/contents/enacted>

30 Available at <https://www.legislation.gov.uk/ukpga/2003/21/section/127>

31 Available at <https://www.legislation.gov.uk/en/ukpga/1964/74>

According to Article 1(2) of this act, the term ‘article’ shall be interpreted broadly. It means any description of an article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures. For this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. (Article 1(1) Obscene Publication Act 1959)

The term ‘publication’ is also interpreted broadly. A person publishes an article who distributes, circulates, sells, lets on hire, gives, or lends it, or who offers it for sale or for letting on hire. Moreover, in the case of an article containing or embodying matter to be looked at or a record, a person who shows, plays, or projects it or, where the matter is data stored electronically, transmits that data shall be deemed as who publishes the article. (Article 1(3) Obscene Publication Act 1959)³²

Some of the provisions of the POA have already been described above in the section on hate speech (section 1.8.1). However, the legislation referred to may also be relevant to cyberbullying. Under Article 5(1) of the POA, a person commits an offence if he uses threatening or abusive words or behaviour, or disorderly behaviour, or displays any writing, sign, or other visible representation which is threatening or abusive, within the hearing or sight of a person likely to be caused harassment, alarm, or distress thereby. Article 4A of the POA considers as a separate offence when any of the above-mentioned conduct is committed with the specific intent to cause the other person harassment, alarm, or distress.

In the case of committing cyberbullying conduct, Article 5 POA typically can be applied when a mobile phone is used not only to send a text message or picture but as a camera to record a video.

Cyberbullying conduct often involves hacking into the computer or online account of the victim. After hacking into the computer or online account of the victim, the perpetrator has access to the victim’s personal data, correspondence, and pictures, and can copy them. Perpetrators typically copy all these data to use them to harass or humiliate the victim. Harassment or humiliation can take place either through the publication of personal data on a public website or by the perpetrator sharing the obtained data with third parties by electronic

³² For more on judicial practice concerning publications with indecent content, see: *R v Phillip James McGuigan* (1996) 2 Cr App R (S) 253, *R v Land* (1999) QB 65, *R v GS* (2012) 2 Cr. App. R. 14, *R v Peacock* (unreported, 6 January 2011, Southwark Crown Court, London, UK).

mail (e.g. by sending an attachment) or by telephone message. This also includes cases where personal data or images are obtained by hacking into a computer or online account but are not shared with third parties in the online space, but, for example, by the printing out of the victim's e-mails or images on paper.

Cyberbullying may also be considered as anti-social behaviour, in which case the provisions of the Anti-social Behaviour, Crime, and Policing Act 2014 (hereinafter referred to as ABCPA)³³ may apply.

Under Article 2(1) ABCPA a behaviour is anti-social if it has caused or is likely to cause, harassment, alarm, or distress to any person. The conduct also has an anti-social nature if it can cause nuisance or annoyance to a person concerning that person's occupation of residential premises (e.g. social rented housing or owner-occupied dwelling), or it can cause housing-related nuisance or annoyance to any person. Part 1 of ABCPA grants specified organisations (e.g. a local authority, a housing provider, the chief officer of police for a police area, etc.) to apply to the courts for a civil injunction against any person aged 10 or over the court is satisfied, on the balance of probabilities, that the person has engaged or threatens to engage in anti-social behaviour, and the court considers it just and convenient to grant the injunction to prevent the respondent from engaging in anti-social behaviour. (Article 1(1) ABCPA)

Provisions of the Defamation Act 1996³⁴ (hereinafter DA 1996) and Defamation Act 2013³⁵ (hereinafter DA 2013) can be applied to cyberbullying acts if the publication of a statement has caused or is likely to cause serious harm to the reputation of the aggrieved party. Although either a natural person or a legal person can be in the position of a victim, the assessment of the term 'serious harm' is different. As Article 1(2) DA 2013 clarifies, harm to the reputation of a body that trades for profit is not 'serious harm' unless it has caused or is likely to cause the body serious financial loss.³⁶

If the conduct causing serious harm to the reputation of a person was made via the publication on a website, the aggrieved party may contact the website operator and request the removal of the infringing material. Detailed rules on defamation of reputation for website operators are set out in The Defamation (Operators of Websites) Regulations 2013.

33 Available at <https://www.legislation.gov.uk/ukpga/2014/12/contents/enacted>

34 Available at <https://www.legislation.gov.uk/ukpga/1996/31/contents>

35 Available at <https://www.legislation.gov.uk/ukpga/2013/26/contents/enacted>

36 For an interpretation of serious harm, see: *Cooke & Anor v MGN Ltd & Anor* (2014) EWHC 2831 (QB), *Ames v Spamhaus* (2015) EWHC 127 (QB), *Lachaux v Independent Print Ltd* (2017) EWCA Civ 1334, *Lachaux v Independent Print Ltd & Anor* (2019) UKSC 27, *Brett Wilson LLP v Persons Unknown* (2015) EWHC 2628 (QB), *Euroeco Fuels (Poland) Ltd & Ors v Szczecin and Swinoujscie Seaports Authority SA & Ors* (2018) EWHC 1081 (QB).

Nevertheless, under Article 1 DA 1996, a person committing the act causing serious harm to the reputation has a defence if he shows that he was not the author, editor, or publisher of the statement complained of, he took reasonable care about its publication, and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement. This defence called ‘innocent dissemination’ is also available for ISPs, however relying on this defence is more limited for them.

Recently, new legal acts were introduced in Scotland and Northern Ireland. Until the adoption of these new acts, the law of defamation in these parts of the UK was substantially the same as the law in England and Wales was, before the introduction of the DA 2013.

Defamation and Malicious Publication (Scotland) Act 2021 was introduced to modernise and simplify the existing law of defamation. According to Article 1(2) of the act, a defamatory statement is only actionable if the statement has been published by the publisher to a person who is other than the person about whom the statement is, and the publication of the statement has caused or is likely to cause serious harm to the reputation the person about whom the statement is.

As to Article 1(4), a statement about a person is defamatory if (a) it causes harm to the person’s reputation, i.e. it tends to lower the person’s reputation in the estimation of ordinary persons), (b) a reference to publishing a statement is a reference to communicating the statement by any means to a person in a manner that the person can access and understand, and (c) a statement is published when the recipient has seen or heard it.

It is important to note that contrary to DA 1996, Defamation and Malicious Publication (Scotland) Act 2021 abolishes the common law defences of innocent dissemination and establishes new defences (defence of truth, defence of publication on a matter of public interest, defence of honest opinion).

In Northern Ireland, rules on defamation are contained by the Defamation Act (Northern Ireland) 2022 which reviewed and reformed previously existing defamation laws, to ensure the balance in the protection of the right to freedom of expression, the right to protection of good name and reputation, and the right of access to justice.

On 13 November 2023, a consultation opened Defamation Act (Northern Ireland) 2022 to review how the new act has been operating. The review was published in June 2024 by the Department of Finance.³⁷

³⁷ Available at <https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/Review%20of%20the%20Defamation%20Act%20%28NI%29%202022%20published.pdf>

In Part 10, the OSA contains criminal offences that relate to communication. These offences can be ranked into several groups.

The first group of offences includes false communication and threatening communication. A person commits the criminal offence of false communication if the person sends a message³⁸, the message conveys information that the person knows to be false, at the time of sending it, the person intended the message, or the information in it, to cause non-trivial psychological or physical harm to a likely audience, and the person has no reasonable excuse for sending the message. It is important that the provider of an internet service using which a communication is sent, transmitted, or published is not to be regarded as a person who sends a message, i.e. an ISP can not be the perpetrator of the criminal offence of false communication. (Article 179(1) OSA)

In the case of the criminal offence of threatening communication, the person also sends a message.³⁹ However, unlike the offence of false communication, the offence here also requires that the message conveys a threat of death or serious harm, and at the time of sending it, the person intended an individual encountering⁴⁰ the message to fear that the threat would be carried out (whether or not by the person sending the message) or was reckless as to whether an individual encountering the message would fear that the threat would be carried out (whether or not by the person sending the message). (Article 181(1) OSA) ‘Serious harm’ means serious injury amounting to grievous bodily harm, rape, assault by penetration (within the meaning of Article 2 of the Sexual Offences Act 2003) or serious financial loss. (Article 181(2) OSA)

In the next group, offences of sending or showing flashing images are included.⁴¹ These conducts, summarised as ‘cyber-flashing’, are a form of digital harassment or sexual misconduct. According to Article 183(1) OSA person commits

38 OSA provides for interpretation of the term ‘sends a message’. According to Article 182(2) OSA, a person ‘sends a message’ if the person (a)sends, transmits, or publishes a communication (including an oral communication) by electronic means, or (b)sends, or gives to an individual, a letter or a thing of any other description, and references to a message are to be read accordingly. Moreover, according to Article 182(3) OSA, a person also ‘sends a message’ if the person (a)causes a communication (including an oral communication) to be sent, transmitted, or published by electronic means, or (b)causes a letter or a thing of any other description to be sent, or given to an individual.

39 The term ‘sends a message’ is interpreted the same way as in Footnote 63.

40 According to Article 182(5) OSA, the term ‘encounter’, in relation to a message, means read, view, hear, or otherwise experience the message.

41 It is worth noting that until the adoption of the OSA, there was not clear regulation on the above-mentioned conduct in the UK. In contrast, however, the Sexual Offences (Scotland) Act 2009 includes the offence of ‘coercing a person into looking at a sexual image’ (Article 6) which can cover the cyber-flashing conduct. Cf. McGlynn and Johnson, 2021, pp. 183–184.

an offence if he (or she) sends a communication by electronic means which consists of or includes flashing images⁴², and at the time the communication is sent, it is reasonably foreseeable that an individual with epilepsy would be among the individuals who would view it, and the person sending the communication (hereinafter sender) sends it with the intention that such an individual will suffer harm as a result of viewing the flashing images. Sending a communication by electronic means which consists of or includes flashing images is also a criminal offence, if the sender believes that an individual whom the sender knows to be an individual with epilepsy, or whom the sender suspects to be an individual with epilepsy, will, or might, view it, and the sender intends that this individual will suffer harm as a result of viewing the flashing images. In addition to the fulfilment of one of these two conditions, the offence shall also be established if the sender has no reasonable excuse for sending the communication.

A person also commits an offence, he shows an individual (recipient) flashing images by means of an electronic communications device, and when showing the images he knows that recipient is an individual with epilepsy, or suspects that the recipient is an individual with epilepsy, and when showing the images, he intends that the recipient will suffer harm as a result of viewing them, and has no reasonable excuse for showing the images. (Article 183(8) OSA)

It is an important difference between the criminal offences regulated in Article 183(1) and 183(8) OSA that in the first case the exemptions listed in Article 180 (1)-(5) OSA are applicable, while it is not possible in the second case. Nevertheless, none of the above-mentioned criminal offences can be committed by a healthcare professional acting in that capacity. Another important provision is that a provider of an internet service by means of which a communication is sent, for the purposes of Article 183(1) OSA, is not to be regarded as a person who sends a communication.

According to Article 184(1) OSA, encouraging or assisting serious self-harm is a criminal offence. A person commits this offence if he does a relevant act capable of encouraging or assisting the serious self-harm of another person, and the act was intended to encourage or assist the serious self-harm of another person. A 'relevant act' can be for example a direct, in-person communication with the other person, sending, transmitting, or publishing a communication by electronic means.⁴³ It is important to note that intentionality is a prereq-

⁴² According to Article 183(13) OSA, the term 'flashing images' means images which carry a risk that an individual with photosensitive epilepsy who viewed them would suffer a seizure as a result.

⁴³ The listing of acts that can be deemed as 'relevant act' in the application of the referred article of the OSA see Article 182(2) OSA.

uisite for establishing the offence, i.e. the person committing the act intend to encourage or assist the serious self-harm of the other person. On the other hand, the offence is independent of the result of the act, since the person commits an offence whether the result, i.e. the serious self-harm occurs or not.

Regarding ISPs, it shall be noted that a provider of an internet service by means of which a communication is sent, transmitted, or published is not to be regarded as a person who sends, transmits, or publishes it. (Article 184(10) OSA)

The OSA also provides for two new offences, the sending etc photograph or film of genitals and the sharing or threatening to share intimate photograph or film to be inserted into the Sexual Offences Act 2003.⁴⁴ The supplementation of this act is particularly important, since the conduct of the perpetrator can also be carried out electronically.

According to Article 66A(1) of the Sexual Offences Act 2003, a person who intentionally sends or gives a photograph (including both the negative and the positive version) or film (moving image) of any person's genitals to another person commits an offence if he intends that the other person will see the genitals and be caused alarm, distress or humiliation, or he sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether the other party will be caused alarm, distress or humiliation. The sending or giving include, in particular the sending of the photograph or film to another person by any means, electronically or otherwise, showing it to another person, and placing it for a particular person to find. (Article 66A(2) of the Sexual Offences Act 2003)

In the case of the criminal offence of sharing or threatening to share intimate photograph or film, according to Article 66B(1) of the Sexual Offences Act 2003, a person commits the offence, if he intentionally shares a photograph or film which shows, or appears to show, another person in an intimate state, this person does not consent to the sharing of the photograph or film, and the person sharing the photograph or film does not reasonably believe that the person who is showed in an intimate state consents. The person also commits the offence if he shares the photograph or film with the same character and the person who is showed in an intimate state does not consent to the sharing of the photograph or film, and the person shares the content with the intention of causing the other person alarm, distress or humiliation. Thirdly, the person commits the offence as well if he shares the photograph or film with the mentioned character for the purpose of him or another person obtaining sexual gratification, and the person who is showed in an intimate state does not consent and the person sharing the photograph or film does not reasonably believe that the other person consents.

44 Cf. Article 66A-66D of the Sexual Offences Act 2003.

(Article 66B(2)-(3) of the Sexual Offences Act 2003) For each of the acts just mentioned, the result, i.e. the sharing of the photo or video, is realised. However, it is also a criminal offence, if the person does not actually share, but threatens the other person with the sharing of a photograph or film which shows, or appears to show, the other person in an intimate state, and he does it with the intention that the person who is showed in an intimate state or another person who knows him or her will fear that the threat will be carried out, or the person sharing the photo or film being reckless as to whether either of the mentioned persons will fear that the threat will be carried out. (Article 66B(4) of the Sexual Offences Act 2003)

In relation to the offences listed above, the legislation also sets out several exceptions, i.e. when the person does not commit a criminal offence with the sharing of a photograph or film which shows another person in an intimate state. These exceptions will not be reviewed in detail.⁴⁵

Considering the interpretation of the term ‘sharing’, Article 66D(2) of the Sexual Offences Act 2003 clarifies that a person ‘shares’ something if the person, by any means, gives or shows it to another person or makes it available to another person. Nevertheless, provider of an internet service by means of which a photograph or film is shared is not to be regarded as a person who shares it. (Article 66D(3) of the Sexual Offences Act 2003)

3. Regulation and prevention of bullying and cyberbullying at the workplace and at the school

3.1. Bullying and cyberbullying at the workplace

Since cyberbullying, as a specific type of bullying in the online space, can occur in many areas of everyday life, several additional sectoral laws may be applied in addition to those described above. One of the most common settings for bullying behaviour is the workplace, where online bullying is also becoming increasingly prevalent. According to a survey published in 2020, 23% of British employees have been bullied at work.⁴⁶

Although bullying including cyberbullying and harassment are two different categories, there are some similarities. e.g. both linked to the abuse of

⁴⁵ The exemptions are regulated in 66C of the Sexual Offences Act 2003.

⁴⁶ Cf. <https://www.smeloans.co.uk/blog/bullying-in-the-workplace-statistics-uk/>

power.⁴⁷ However, while harassment, whether based on a person's age, gender, gender identity, disability, marital status, pregnancy, race, religion, or sexual orientation, is dealt with by English law through complex regulation, bullying conduct disregarding the place of perpetration does not fall under the definition of harassment and therefore it is, in principle, not considered unlawful.

The need for a legal framework for harassment in the workplace has been expressed since the 1990s. In 1996, the Dignity at Work Bill was introduced in Parliament, which would have banned harassment in the workplace generally. The bill, however, was not passed.⁴⁸ In the UK, legislation that would contain explicit provisions for such offences or would allow for the prosecution of perpetrators still does not exist, but some special laws can be applied. Moreover, in the absence of an independent legal regulation on bullying in the workplace, the role of judicial practice is particularly important, especially for the development of the rules regarding this question.⁴⁹

Equality Act 2010 provides for harassment and victimisation and defines them as prohibited conduct. Article 26(1) of the act defines harassment as unwanted conduct related to a relevant protected characteristic (age, disability, gender reassignment, race, religion or belief, sex, sexual orientation), which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating, or offensive environment for that individual. According to the case law, the Equality Act 2010 may apply to workplace bullying.⁵⁰

Under Article 2 of the Health and Safety at Work Act 1974⁵¹, employers are required to provide a safe working environment for their employees. This duty of the employer shall be ensured as far as it is reasonably practicable. If an employee becomes a victim of harassment, bullying, or cyberbullying at work, using the computer infrastructure used there, the employer breaches this obligation. Rules of the Protection from Harassment Act 1997 already referred to also can be applied, although it lays down general rules on harassment and does not contain a specific provision on harassment in the workplace. This was confirmed by the court in 2006 in *Majrowski v Guy's and St Thomas's NHS Trust*.⁵² It was held that an employee could also base a claim for compensation for workplace harassment on the provision of the Protection from Harassment Act 1997.

47 For a comprehensive treatment of the topic, see Einarsen, Hoel, Zapf and Cooper, 2020.

48 For details on the process of preparing and negotiating the bill and the reasons behind its rejection, see: Harthill, 2008, pp. 286–289.

49 Hoel, 2013, p. 65.

50 Cf. *Yeboah v Crofton*, 2002, IRLR 634.

51 Available at <https://www.legislation.gov.uk/ukpga/1974/37/contents>

52 *Majrowski v Guy's and St Thomas's NHS Trust* (2006) UKHL 34.

Regulation of workplace harassment and bullying continues to be a demand in British society. In response to this demand, the Bullying and Respect at Work Bill was introduced in the summer of 2023. The Bill provides for a statutory definition of bullying at work and contains detailed provisions relating to bullying at work, including to enable claims relating to workplace bullying to be considered by an employment tribunal. At the time of writing, the 1st reading in the House of Commons was completed.

3.2. Bullying and cyberbullying at the workplace

A school environment is also a typical place for abusive behaviours like bullying and, with the growth in the use of smart devices, cyberbullying.

In these cases, the acquired data and images are shared through a Virtual Learning Environment (VLE) in the form of a chat message or chat wall. Cyberbullying also covers the conduct when, following the hacking of a computer or online account, personal data or images are not shared with third parties or the public, but the perpetrator deletes data or documents (e.g. homework, university assignments, etc.) stored or uploaded to a shared storage space used by others, causing inconvenience to that person. In the above cases, in addition to the application of the classic privacy, confidentiality, and data protection rules and legal consequences, it is also possible to deem the conduct in question as a criminal offence under the Computer Misuse Act 1990⁵³ and, therefore, to apply the criminal consequences.

In the UK, a comprehensive reform of education was introduced in 1998. The School Standards and Framework Act 1998⁵⁴ prescribed state schools as mandatory to develop anti-bullying policies. From 2003, this provision shall also be applied to private institutions.

Article 89(1)(b) of the Education and Inspections Act 2006⁵⁵ states that the head teacher at a relevant school must determine measures to be taken to encourage good behaviour and respect for others on the part of pupils and prevent all forms of bullying among pupils. The measures determined by the head of the institution, to such extent as is reasonable, include measures to be taken to regulate the conduct of pupils at a time when they are not on the premises of the school and are not under the lawful control or charge of a member of the staff of the school. It shall be noted that this provision this legislation does not apply to independent schools.

⁵³ Available at <https://www.legislation.gov.uk/ukpga/1990/18/contents>

⁵⁴ Available at <https://www.legislation.gov.uk/ukpga/1998/31/contents>

⁵⁵ Available at <https://www.legislation.gov.uk/ukpga/2006/40/contents>

As a disciplinary penalty, the legislation allows the staff of the educational institution to confiscate certain devices (e.g. mobile phones) from pupils. The teacher may also ask the pupil to reveal the contents of the message or even the mobile phone to detect the bullying. Disciplinary action may be taken against a pupil who refuses the request.

For private schools in England and Wales, the Education (Independent School Standards) (England) Regulations 2014⁵⁶ contain provisions. Part 3 of the legislation, on the welfare, health, and safety of pupils, states that the proprietor of a school shall ensure that bullying at the school is prevented in so far as reasonably practicable, by the drawing up and implementation of an effective anti-bullying strategy.

It is important to note that the above-mentioned legislation only applies to independent schools in England and Wales, i.e. in the other parts of the UK separate provisions have been made for independent schools.

In Northern Ireland, the Education Reform (Northern Ireland) Order 1989 was the first legal act that required schools in Northern Ireland to develop and implement discipline policies. Later, Article 3 of the Education (Northern Ireland) Order 1998⁵⁷ provided for the responsibility of the Board of Governors and principals for discipline including implementing discipline policies. According to the original text of Article 3(3)(a)(ii), the management of the grant-aided school was required to encourage good behaviour and respect for others on the part of pupils. In 2003, the text was modified⁵⁸ and completed with the phrase ‘in particular, preventing all forms of bullying among pupils.’ This modified text was in force until 2016 when the Addressing Bullying in Schools Act (Northern Ireland) 2016⁵⁹ (hereinafter referred to as ABSA) was adopted.

Bullying is a core notion of the act. However, the scope of the act is limited to bullying at schools, therefore the term ‘bullying’ is interpreted as ‘bullying at school’. According to Article 1(1) ABSA, bullying behaviour includes, but is not limited to, the repeated use of any verbal, written, or electronic expression or other act, or a combination thereof, by a pupil or group of pupils against another pupil or group of pupils with the purpose of causing physical or emotional harm to the latter. It is worth noting that under ABSA only those bullying conduct are covered which are committed by pupils and against pupils. ABSA does not cover

56 Available at <https://www.legislation.gov.uk/uksi/2014/3283>

57 Available at <https://www.legislation.gov.uk/nisi/1998/1759/contents/made>

58 Article 3(a)(ii) of the Education (Northern Ireland) Order 1998 was amended by Article 19(3) of the Education and Libraries (Northern Ireland) Order 2003.

59 Available at <https://www.legislation.gov.uk/en/ni/2016/25/contents>. Although the Addressing Bullying in Schools Act (Northern Ireland) 2016 was adopted in 2016, it came into force on 1st September 2021.

acts which are committed either by a pupil or a teacher (or any other member of the staff) against another teacher, or by a teacher against a pupil. These bullying conducts shall be assessed under laws other than ABSA.

The Addressing Bullying in Schools Act (Northern Ireland) 2016 prescribes for the Board of Governors of a grant-aided school to determine the measures to be taken at the school to prevent bullying involving a registered pupil at the school. The measures can be applied by the Board of Governors, the staff of the school, or other persons not only on the premises of the school during the school day, but while the pupil travels to or from the school during the school term, while the pupil is in the lawful control or charge of a member of the staff of the school, or while the pupil is receiving educational provision arranged on behalf of the school and provided elsewhere than on the premises of the school.

In case of the occurrence of bullying, the Board of Governors of a grant-aided school shall ensure that a record is kept of all incidents of bullying or alleged bullying involving a registered pupil at the school. This record shall state (a) what, from all the circumstances, appears to be the motivation of the incident, and (b) the methods of bullying (i.e. it is committed using verbal, written, or electronic communication, any other act, or a combination of those). Regarding the motivation of the incident, Article 3(3) provides examples to which the motivation can relate. According to this article, bullying can be motivated by differences in religious belief, political opinion, racial group, age, sex, sexual orientation, or marital status, and differences between persons with a disability and persons without, such as differences between persons with dependants and persons without, persons based on gender reassignment, and persons based on pregnancy.

Considering the record on the occurrence of bullying conduct, the act prescribes the record to include information about how the incident was addressed.

In Scotland, the Schools (Health Promotion and Nutrition) (Scotland) Act⁶⁰ 2007 requires schools to promote health, including the mental, emotional, social, and physical health and well-being of children. The Education (Additional Support for Learning) (Scotland) Act 2004 provides for support for children and young people with learning difficulties, including support for children and young people who are experiencing difficulties because of bullying.⁶¹

As it was previously mentioned, a new legislation of a comprehensive nature has been adopted in the UK in October 2023. A key concern for the legislator was to ensure the fullest possible protection of children in online spaces. The OSA requires ISPs to identify, mitigate and manage the risks of harm from content

⁶⁰ Available at <https://www.legislation.gov.uk/asp/2007/15/contents/2008-08-04>

⁶¹ Available at <https://www.legislation.gov.uk/asp/2004/4/contents/2014-08-01>

and activity that is harmful to children, and to regulate. Moreover, OSA seek to secure (among other things) that services are safe by design, and designed and operated in such a way that a higher standard of protection is provided for children than for adults. (Article 1(2)-(3) OSA).

Several measures are introduced by the OSA which aimed at ensuring the online safety for children. Establishing new criminal offences is of particular importance for the protection of children, as the victims of these newly criminalised conduct under the OSA were, in the vast majority of cases, children. This will certainly mean much stronger protection for children against abusive behaviour in the online space in the future.

The OSA requires ISPs to introduce age assurance and age verification to ensure that children cannot access such services which are not designed for them (e.g. porn sites). Although users including persons under the age of 18 have always had to answer the question whether or not they are over 18, but in the future age verification will have to be done in a different and more rigorous way. Operators of social media platforms also must prevent children accessing them before the minimum age. These ISPs are obliged to take action to prevent illegal and harmful content (including images or videos of child sexual abuse and exploitation) from being shared on their social media site and making sure that the content is quickly removed.

In practice, a major problem was that parents could not access their children's online data, such as their personal account in a social media platform in the event of their child's death. In the future, under the provisions of the OSA, parents will be able to do this. Moreover, OSA provides children and their parents with a more effective toolkit for reporting online infringements.

4. Crimes committed in the online space, cyberbullying, and the enforceability of the authorities' action against hate speech

In the case of hate crimes committed in the online space and explicitly criminalised by law, criminal law consequences are applied according to the criminal procedural rules. The victim of the crime also plays an important role in the activity of the investigating authority in collecting evidence, as his report and testimony serve as primary evidence in the case. On the other hand, however, in those cyberbullying conduct which are considered a criminal offence, the process of revealing the facts and proving them is often quite difficult. Recalling

cyberbullying is often very emotionally distressing for the victim, especially in those cases where the act took place over a long time and caused the victim serious psychological distress.

As the conduct of bullying and cyberbullying are not separate criminal offences in the UK, criminal sanctions can only be applied if the act also has elements of other criminal offences. In the lack of this, the victim of the bullying or cyberbullying can at most make a compensation claim against the perpetrator for the suffered harm.

As it was noted above, acts of bullying and cyberbullying most often take place in the workplace or educational institutions. Although English law obliges the employer to ensure proper working conditions including the mental and psychological well-being of employees, bullying conduct is mostly dealt with in the workplace secretly, 'behind closed doors.' Official action is only be taken if the bullying conduct can be classified as criminal or other legal offence under a legal act, for example, if the given conduct includes the elements of harassment or, constitutes defamation at the same time.

As noted above, in the case of educational institutions there are several legal provisions aimed at preventing bullying conduct in the school or dealing with the acts that have already taken place. However, as with bullying conduct in the workplace, such acts in schools and between pupils are primarily treated at the local level, i.e. by the educational institution. The educational institution records the behaviour, its background, its real or perceived reasons, and how it is dealt with (e.g. applied consequence, disciplinary action) and provides support (e.g. access to a psychologist) to the victim of the bullying conduct if he requests it.

The perpetrators of bullying and cyberbullying conduct in educational institutions, due to their age, often cannot be held criminally liable even if their actions are criminalised. Nevertheless, in cases where the conduct can be assessed as anti-social behaviour, the measures set out in the separate act (ABCPA) may be applied to a person over 10 years of age if it can be shown that the measure is necessary to protect the person or persons harmed by the anti-social behaviour from further anti-social behaviour.

Under English law, civil enforcement, provided that the bullying or cyberbullying conduct also amounts to a violation of privacy rights, is possible, but requires prudent consideration, since the costs of such claims are relatively high.

In those cases where the infringing conduct (e.g. defamation) takes place on the Internet, the aggrieved party may contact the operator (Internet service provider, hereinafter ISP) of the website and can request the removal of the infringing content. However, Article 1 of the DA 2013, cited above, allows the ISP to

rely on the so-called ‘innocent dissemination’, but only until he becomes aware that the content published on the website may be capable of causing damage to honour or reputation.

Where the aggrieved party chooses the civil enforcement and the proceeding results in a judgment in the case, The Defamation (Operators of Websites) Regulations, also mentioned above, provide the possibility for the court to oblige the defendant (infringing party) to publish a summary of the judgment. It is worth noting, however, that in judicial practice, this type of judgment is rarely handed down.⁶²

5. The liability of internet service providers and social media platforms

Nowadays, the number of online statements that damage the social image and reputation of a person is increasing in the UK due to the growing use of social media (e.g. Facebook, Twitter). This trend poses an increasing risk to online users. Expressing the opinion in the online space and the infringements relating to them, as well as the questions that arose on the treatment of these infringements, made ISPs a key player in the problem. The regulation of the liability of ISPs and social media service providers have long been the focus of both jurisprudence and legal attention. The provisions on the liability of ISPs appear in several pieces of legislation and will be briefly discussed below, including the relevant case law.

DA 2013 contains detailed rules on the liability of ISPs for the publication of infringing content and establishes new defences for ISPs.⁶³ The liability of the operator of an Internet website depends on the identity of the person who made the infringing statement.

Article 5 DA 2013 provides a new defence for website operators considering statements posted on their sites by third parties. By relying on this, an ISP can argue that it did not post the infringing statement on its website. Where a post is uploaded to a website by an identifiable person, the existing law provides that the host will have a defence only in the absence of knowledge on their part of the defamatory statement. The person who posted the statement can be identified

⁶² On the publication of the summary of the judgment see *Shakil-Ur-Rahman v ARY Network Ltd* (2016) EWHC 3110 (QB), *Turley v UNITE the Union & Anor* (2019) EWHC 3547., *Monir v Wood* (2018) EWHC 3525 (QB).

⁶³ Mullis et al., 2013.

if the aggrieved party has sufficient information to bring proceedings against that person.

Accordingly, the ISP cannot be exempted from liability, even if the defence was invoked, if the aggrieved party proves that (a) the person who posted the statement with the infringing content on the website was not identifiable, (b) he or she gave a notice of complaint to the ISP concerning the statement, (c) and the ISP failed to respond to the notice of complaint of the aggrieved party. Although the primary aim of the DA 2013 was to protect persons against defamation, the law tips the balance in favour of freedom of expression and protection against defamation.

Additional protection for ISPs can be found in Article 10 DA 2013, which states that a court has no jurisdiction to hear and determine an action for defamation brought against a person who was not the author, editor, or publisher of the statement complained of unless the court is satisfied that it is not reasonably practicable for an action to be brought against the author, editor, or publisher.

The previous but still existing law on defamation, i.e. DA 1996, also contains a defence by which the person can be exempted from liability. According to Article 1 of the DA 1996, a person has a defence if he proves that he was not the author, editor, or publisher of the statement complained of, he took reasonable care concerning its publication, and he did not know, and had no reason to believe, that his conduct would result in or contribute to the publication of a defamatory statement. Since there is no specific mention of an ISP in the DA 1996, it was the judicial practice that designed the framework of the defence for ISPs. (Relating judgments will be referred to in point c) of this subheading.)

In Scotland, the Defamation and Malicious Publication (Scotland) Act 2021 provides for ISPs. In Article 3, there is a restriction on proceedings against secondary publishers which provides that there is no right to bring defamation proceedings against a person about a statement in Scotland unless they are the author, editor, or publisher of the statement.⁶⁴ The act does not contain a corresponding defence specifically for ISPs in Scotland, though they can be protected by other defences. Therefore, defences in Scotland and England are not identical, but they will likely overlap in their operation.

⁶⁴ In the application of Article 3, ‘author’ means the person from whom the statement originated, but does not include a person who did not intend the statement to be published, ‘editor’ means a person with editorial or equivalent responsibility for the content of the statement or the decision to publish it, and ‘publisher’ means a commercial publisher (that is to say, a person whose business is issuing material to the public or to a section of the public) who issues material containing the statement in the course of that business.

The Defamation (Operators of Websites) Regulations 2013 also contains rules concerning the liability of ISPs. Regulation 3 and the Schedule provide for the actions to be taken by the operator in response to the notice of the aggrieved party to maintain Article 5(2) defence.

In 2002, the e-Commerce Directive of the European Union⁶⁵ was implemented by The Electronic Commerce (EC Directive) Regulations which contains the same rules on the liability of ISPs as Section 4 of the e-Commerce Directive. The Electronic Commerce (EC Directive) Regulations 2002 determines three cases, the so-called safe harbours (mere conduit, caching, and hosting) where the provider may be exempted from liability.

Regarding the case of mere conduit, Article 17(1) of The Electronic Commerce (EC Directive) Regulations 2002 states that in those cases where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or any criminal sanction as a result of that transmission where the service provider (a) did not initiate the transmission, (b) did not select the receiver of the transmission, and (c) did not select or modify the information contained in the transmission. The acts of transmission and provision of access include the automatic, intermediate, and transient storage of the information transmitted where this takes place for the sole purpose of carrying out the transmission in the communication network, and the information is not stored for any period longer than is reasonably necessary for the transmission.

Article 18(1) of The Electronic Commerce (EC Directive) Regulations 2002 provides about caching. Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or any other pecuniary remedy or for any criminal sanction as a result of that transmission where the information is the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request. Further requirements for the defence are that the service provider

- does not modify the information,
- complies with conditions on access to the information,

⁶⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, pp. 1–16.

- complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by the industry,
- does not interfere with the lawful use of technology, widely recognised, and used by industry, to obtain data on the use of the information, and
- acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

According to Article 19(1) of The Electronic Commerce (EC Directive) Regulations 2002, ISP shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction, if the information society service provided by the ISP consists of the storage of information (hosting) provided by a recipient of the service, and the ISP does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful, or upon obtaining such knowledge or awareness, ISP acts expeditiously to remove or to disable access to the information. A further requirement is for exempting from liability that the recipient of the service was not acting under the authority or the control of the ISP.⁶⁶

The liability of ISPs has been the subject of several judgments in English case law. In this respect, the assessment of ISPs is rather controversial. There have been cases where the liability of the ISP was established because the court did not see the applicability of the exemption under Article 1 of the DA 1996.⁶⁷ In other cases, the activity of the service provider was assessed as a simple data transfer (mere conduit) and therefore it was exempted from liability.⁶⁸ If an ISP appears only as a passive medium of communication, it cannot be considered as a publisher of data or information. This was also confirmed by the court in the Google case where it was considered that Google as a search engine is not a

⁶⁶ For case law on the application of the Article 19 exemption see *Karim v Newsquest Media Group* (2009) EWHC 3205 (QB), *Kaschke v Gray* (2010) EWHC 690 (QB), *Davison v Habeeb* (2011) EWHC 3031 (QB), *Tamiz v Google* (2012) EWHC 449 (QB), *McGrath v Dawkins* (2012) EWHC B3 (QB), *McAlpine v Bercow* (2013) EWHC 1342 (QB), *Cairns v Modi* (2012) EWCA Civ 1382.

⁶⁷ *Godfrey v Demon Internet Limited* (1999) EWHC QB 240. The case is described and analysed in detail by Michael Deturbide. See Deturbide, Michael: Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses, In: *The Journal of Information, Law, and Technology*, No. 3/2000.

⁶⁸ *Totalise Plc v Motley Fool Ltd.* [2001] EWHC 706 (QB), *Bunt v Tilley* (2006) EWHC 407 (QB).

publisher at common law. It merely provides the framework for people to search for information on the Internet but cannot filter out previously infringing content. Therefore, the liability of Google as a search engine was not established.⁶⁹ It is important to note that the search engine operator cannot be held liable even if it has already been notified about the existence of the infringing content. Similarly, the liability of the service provider for content that has already been archived and is in the fragmented list has also not been established.⁷⁰ To sum up, in English law, search engine operators enjoy complete immunity from the application of the rules on liability for internet content that negatively affects public perception.

Recently, the role of an ISP as a blog operator was also discussed in judicial practice. There is a judgment where the court did not accept Google's reference to Article 1 of DA 1996.⁷¹ In another case, the court took the opposite position and did not find Google liable for defamation.⁷² However, this decision was reversed by the Court of Appeal who held that Google knew about the publication of the defamatory statement, since it received the notice. Therefore, Google cannot successfully rely on the defence based on Article 1 DA 1996 and is liable for defamation.⁷³

Reviewing the English regulation and case law on the liability of ISPs, it can be stated that the question of determining liability remains rather uncertain; drawing the line between the mere transmission of data and the provision of content is still difficult. This is also reflected in the judgments given in the cases against Google. While the activity of Google as a search engine was considered by the court as a simple data transfer, and therefore, it was not found liable, its activity as a blog operator was found to be actionable after the notification of the infringing content.

The adoption of the OSA in October 2023, by the reshaping of their responsibilities, has significant impact on the regulation of the operation of ISPs. As it is declared in the introduction of the OSA, it provides for a new regulatory framework which has the general purpose of making the use of internet services regulated safer for individuals in the UK. To achieve this purpose, the OSA requires service providers to identify, mitigate, and manage the risks of harm from illegal content and activity, and content and activity that is harmful to children. Moreover, the OSA confers new functions and powers to the Office of

69 Metropolitan International Schools Ltd v Designtecnica Corp. (2009) EWHC 1765 (QB).

70 Budu v BBC (2010) EWHC 616 (QB).

71 Davison v Habeeb (2011) EWHC 3031 (QB).

72 Tamiz v Google (2012) EWHC 449 (QB).

73 Tamiz v Google (2013) EWCA Civ 68.

Communications (hereinafter OFCOM) which is the UK communications regulator, overseeing the broadcasting, telecommunications, and postal industries. (Article 1(2) OSA)

Provisions of the OSA, on the one hand, cover online service providers that allow people to create or share content or interact with each other. In the wording of the legislation, these are the ‘user-to-user services’ where the content is generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service and may be encountered by another user, or other users, of the service. (Article 3(1) OSA). Accordingly, these services include various social media services, photo- and video-sharing services, services facilitating chat, and other forms of direct communication, as well as online and mobile gaming services. On the other hand, ‘search services’, i.e. internet services that are, or include, a search engine, are also covered by the regulation. (Article 3(4) OSA) Beyond the providers of user-to-user services and service services, OSA regulates certain online pornographic content as well.

It is important to note that the regulation applies to all online service providers, regardless of their size, i.e. provisions of the OSA shall also be applied for individuals who provide an online service.

The duty of care of the ISPs is in the core of the new regulation. Part 3 OSA imposes duties of care separately on providers of user-to-user services (Chapter 2) and search services (Chapter 3). Certain duties of care relate to the content (illegal content) or activity of the service providers, while others are established regarding services which are likely to be accessed by children (Chapter 4), or relating to fraudulent advertising (Chapter 5). Moreover, the OSA clearly designates the borders within OFCOM can act free and, at the same time, requires OFCOM to issue codes of practice about the duties of care of the service providers (Chapter 6). In 2024, OFCOM published the Illegal content Codes of Practice for user-to-user services⁷⁴ and the Illegal content Codes of Practice for search services.⁷⁵ Depending on the completion of the Parliamentary process of these codes, from 17 March 2025, providers will have to take the safety measures set out in the Codes of Practice or use other effective measures to protect users from illegal content and activity.

⁷⁴ <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services.pdf?v=387711>

⁷⁵ <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-search-services.pdf?v=387710>

Bibliography

- Anderson, R., Gilbert, S. (2022) 'The Online Safety Bill. Policy Brief', October; <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/09/Policy-Brief-Online-Safety-Bill.pdf>
- Bleich, E. (2018) From Race to Hate: 'A Historical Perspective' in Brudholm, Thomas – Schepelehn Johansen, Brigitte (eds.): *Hate, Politics, Law: Critical Perspectives on Combating Hate*, Oxford University Press, Oxford, pp. 15–33
- Bleich, E. (2011) 'The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies', *Journal of Ethnic and Migration Studies*, Vol. 37, No. 6, July, pp. 917–934
- Bechtold, E. (2022) 'Scotland's New Hate Crime Act Imperils Freedom of Expression', *The Edinburgh Law Review*, Vol. 26, No. 2, pp. 250–257
- Coe, P. (2023) 'Assessing damages for intentional infliction of harm, misuse of private information and breach of confidence in 'image-based abuse' claims', *Professional Negligence*, Vol. 39, Issue 3, pp. 137–141
- Coe, P. (2023) 'Tackling online false information in the United Kingdom: The Online Safety Act 2023 and its disconnection from free speech law and theory', *Journal of Media Law*, Vol. 15, Issue 2, pp. 213–242
- Coe, P. (2022) 'The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora's box?', *Journal of Media Law*, Vol. 14, Issue 1: The regulation of hate speech online, pp. 50–75
- Cumper, P. (2006) 'Outlawing incitement to religious hatred – a British perspective', *Religion and Human Rights*, Vol. 1, No. 3, pp. 249–268
- Deturbide, M. (2000) 'Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses', *The Journal of Information, Law, and Technology*, No. 3
- Edge, P. W. (2018) 'Oppositional Religious Speech: Understanding Hate Preaching', *Ecclesiastical Law Journal*, Volume 20, Issue 3, pp. 278–289
- Einarsen, S. V., Hoel, H., Zapf, D., Cooper, C. L. (2020) 'The Concept of Bullying and Harassment at Work', in Einarsen, S. V. et al. (eds.): *Bullying and Harassment in the Workplace. Theory, Research and Practice*, CRC Press, Boca Raton, pp. 3–39
- El Asam, A., Samara, M. (2016) 'Cyberbullying and the law: A review of psychological and legal challenges', *Computers in Human Behaviour*, Vol. 65, December, pp. 127–141
- Foster, S. (2019) 'Accommodating Intolerant Speech: Religious Free Speech versus Equality, and Diversity', *European Human Rights Law Review*, No. 6, pp. 609–625

- Goodall, K. (2009) 'Challenging hate speech: incitement to hatred on grounds of sexual orientation in England, Wales and Northern Ireland', *The International Journal of Human Rights*, Vol. 13, Issue 2-3, pp. 211-232
- Goodall, K. (2007) 'Incitement to Religious Hatred: All Talk and no Substance?', *The Modern Law Review*, Vol. 70, No. 1, January, pp. 89-113
- Hare, I. (2006) 'Crosses, Crescents and Sacred Cows. Criminalising Incitement to Religious Hatred', *Public Law*, 3, pp. 521-538
- Harthill, S. (2008) 'Bullying in the Workplace: Lessons from the United Kingdom', *Minnesota Journal of International Law*, Vol. 17, Issue 2, pp. 247-302.
- Hoel, H. (2013) 'Workplace Bullying in United Kingdom', *Workplace Bullying and Harassment*, No. 2, pp. 61-76
- Johnson, V. R. (2016) 'Comparative Defamation Law: England and the United States', *University of Miami International and Comparative Law Review*, Vol. 24, Issue 1, pp. 1-97
- Marczak, M., Coyne, I. (2010) 'Cyberbullying at school: Good practice and legal aspects in the United Kingdom', *Australian Journal of Guidance and Counseling*, Vol. 20, No. 2, pp. 182-193.
- McGlynn, C., Johnson, K. (2021) 'Criminalising Cyberflashing: Options for Law Reform', *The Journal of Criminal Law*, Vol. 85, No. 3, pp. 171-188
- McGuire, K., Salter, M. (2014) 'Legal Responses to Religious Hate Crime: Identifying Critical Issues', *Kings Law Journal*, Vol. 25, Issue 2, pp. 159-184
- Mullis et al. (2013) A comprehensive description and analysis of the new defences established by DA 2013, pp. 1-97.
- Mullis, A., Scott, A. (2014) 'Tilting at Windmills: the Defamation Act 2013', *The Modern Law Review*, Vol 77, No. 1, pp. 87-109
- Neller, J. (2023) 'Race, religion, law: an intertextual micro-genealogy of 'stirring up hatred' provisions in England and Wales', *Critical Discourse Studies*, Vol. 2020, No. 3, pp. 282-293, p. 285
- Thompson, S. (2012) 'Freedom of expression and hatred of religion', *Ethnicities*, Vol. 12, Issue 2, pp. 215-232
- Trengove, M., Kazim, E., Almeida, D., Hilliard, A. Zannone, S. Lomas, E. (2022) 'A critical review of the Online Safety Bill', *Patterns*, Vol 3, Issue 8
- Vaughan, M. (2019) 'Accepting the 'D' word: discrimination in 1960s' UK academic discourse', *Race & Class*, Vol. 61, pp. 85-95