

©2016, Elsevier. Licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International <http://creativecommons.org/about/downloads>



# **Cyberbullying and the Law: A Review of Psychological and Legal Challenges**

**Aiman El Asam & Muthanna Samara\***

Department of Psychology, Kingston University London, Penrhyn Road, Kingston-  
Upon-Thames, KT1 2EE UK

\* Dr Muthanna Samara (correspondence author)

Associate Professor in Psychology

Department of Psychology

Kingston University London

Penrhyn Road

Kingston-Upon-Thames

KT1 2EE UK

Email: M.Samara@Kingston.ac.uk

Tel: +44 (0) 20 8417 2533

**Running head:** Cyberbullying: Psychological and Legal Challenges

**Authors' declaration:** The authors declare that there are no competing financial interests exist. The paper has not been published elsewhere and it has not been submitted simultaneously for publication elsewhere.

## **Cyberbullying and the Law: A Review of Psychological and Legal Challenges**

**Running head:** Cyberbullying: Psychological and Legal Challenges

### **Abstract**

Cyberbullying, in its different forms, is common among children and adolescents and is facilitated by the increased use of technology. The consequences of cyberbullying could be severe, especially on mental health, potentially leading to suicide in extreme cases. Although parents, schools and online social networking sites are encouraged to provide a safe online environment, little is known about the legal avenues which could be utilised to prevent cyberbullying or act as a deterrent to such. This article attempts to explore current laws, and the challenges that exist to establishing cyberbullying legislation in the context of the UK. It is arguable that a number of statutes may be of assistance in relation to cyberbullying, namely Education and Inspections Act 2006, Protection from Harassment Act 1997, Communications Act 2003, Telecommunication Act 1988, Public Order Act 1986, Obscene Publications Act 1959, Computer Misuse Act 1990, Crime and Disorder Act 1998, Defamation Act 2013. However, given the lack of clear definition of bullying, the applicability of these laws to cyberbullying is open to debate. Establishing new legislation or a modification to existing laws is particularly challenging for a number of reasons, namely: an absence of consistent bullying/cyberbullying definition, a difficulty in determining intention to harm or evidence of such, a lack of surveillance, a lack of general awareness, issues surrounding jurisdiction, the role of technology, and the age of criminal responsibility. These challenges are elaborated and discussed in this article.

**Keywords:** Cyberbullying; Victimisation; Psychological Impact; Cyberbullying Prosecution; Legal Challenges; Children and Adolescents

## **Introduction**

Historically, bullying has been part and parcel of childhood and regarded as an accepted and normalised experience (Limber & Small, 2003). As such, it has never raised any alarm until the last two decades whereby this view has been seriously challenged, eliciting a need for attention (McCarthy, Rylance, Bennett, & Zimmermann, 2001). This has led to worldwide recognition of cyberbullying (Campbell, 2005) as it has been experienced first-hand by many people during childhood, adolescence and for some it can even continue into adult life. Bullying, in its traditional form, has been defined as being an aggressive, intentional act or behaviour that is carried out by a group or an individual repeatedly and over time against a victim who cannot easily defend him or herself (Whitney & Smith, 1993; Olweus, 1999). Furthermore, bullying is explained as a form of abuse that is based on an imbalance of power; hence it can be defined as a systematic abuse of power (Smith & Sharp, 1994; Rigby, 2002).

In recent years bullying has taken a different form, often labelled as cyberbullying or online bullying. It is defined as intentional aggressive behaviour involving a power imbalance between those involved, where the cyberbully intends to harass, intimidate and threaten the cybervictim repeatedly over a period of time using the internet (including social networking sites) and via electronic devices, such as sending text messages, emails and video messages (Juvonen & Gross, 2008; Marczak & Coyne, 2010; Patchin & Hinduja, 2012; Smith et al., 2008).

Bullying was found to be prevalent amongst children. For instance, in the UK the NSPCC (2015) reported that in the past year 25,736 counselling sessions were provided to children who were concerned about face-to-face bullying and cyberbullying. Bullying has been perceived as a form of entertainment and a learning experience (Smith et al., 2008; Sabella, Patchin & Hinduja, 2013). However, evidence has accumulated showing that it has

psychological consequences for both the bully and the victim. The severity and the psychological consequences of face-to-face bullying and cyberbullying are well documented. Past research has shown that young victims of face-to-face bullying suffer various maladaptive outcomes (Beran & Li, 2007). Correlations between face-to-face bullying and psychiatric, psychosomatic and physical health issues have also emerged in empirical research (Arseneault et al., 2006; Kim et al., 2006; Gini & Pozzoli, 2009). Similarly, cyberbullying has severe consequences and could lead to depressive symptoms among the victims (e.g. Baker & Tanrikulu, 2010) and other psychological problems such as stress, loneliness, anxiety, low self-esteem (e.g. Katzer, Fetchenhauer, & Belschak, 2009; Ybarra et al. 2006), suicidal ideation (Katsumata, Matsumoto, Kitani, & Takeshima, 2008) and suicide (Feinberg & Robey, 2008).

Despite its prevalence and psychological consequences among children and adolescents, the laws governing cyberbullying within the legal systems of the UK (England & Wales, Scotland and Northern Ireland) are complex, both in terms of its definition and legal status, with existing legislation lacking in definition. The purpose of this paper is to review cyberbullying, looking specifically at its variations, risk factors and consequences, as well as critically reviewing the current legislation governing its legal status when taking into account the severe consequences that may arise as a result.

## **Cyberbullying**

People often pose the question “what did we do before we had the internet and mobile phones?” Technology is rapidly developing and enhancing education, employment and social interactions. It is part of our daily lives allowing us to connect with people around the world and keep in contact with friends and family. However, technology such as the internet and electronic devices are being used more frequently to cause emotional harm and distress to others in the form of online harassment, stalking and bullying.

Despite its advantages, modern technology has its risks and clearly cyberbullying is one of the main emerging challenges facing the society in this digital world (Walrave & Heirman, 2011). The continual use of technology means that cyberbullying is becoming a persistent problem that may eventually surpass the traditional form of playground bullying. As previously defined, cyberbullying is summarised as an intentional aggressive and repeated behaviour that intends to harass, intimidate and threaten the victim via electronic means characterised by imbalance of power (Juvonen & Gross, 2008; Marczak & Coyne, 2010; Patchin & Hinduja, 2012; Smith et al., 2008). The imbalance of power mentioned within this definition refers to anonymity (Butler, Kift, & Campbell, 2009) or the skill level the cyberbully has for using technology (Grigg, 2010) rather than only strength, age or popularity which is referred to in the definition of face-to-face bullying or traditional bullying. Cyberbullying can be more repetitive with continual viewing/involvement of many individuals over varying periods of time, and due to its nature is wider spread (Grigg, 2010). Also, it is easy to bully others in cyberspace; all that is required is access to an electronic device, such as a mobile phone or computer, and the details of the victim to whom the bullying will be directed, such as their mobile phone number, internet address or username. By using this method, the perpetrator does not have to face their victim and therefore can remain anonymous; the bullying can remain a cold attack on a person and the perpetrator does not have to witness directly the consequences of their actions. The perpetrator can be regarded as cowardly in conducting their actions in the cyberspace forum. The ease of cyberbullying enables those who may otherwise not bully in the traditional sense, to cyberbully others, as it is more convenient and anonymous (Poland, 2010). According to Vandebosch and VanCleemput (2008), definitions of cyberbullying often include behaviours not covered by traditional definitions of bullying. Indeed, much of the current research suggests that the majority of cyberbullying is a direct extension of face-to-face bullying.

That is, it is mainly carried out by youths who bully face-to-face and is directed towards the same victim within previously established social networks (Juvonen & Gross, 2008; Ybarra & Mitchell, 2004).

Despite a rich vein of research in this area, cyberbullying is not consistently defined. In fact, some surveys might not refer to bullying by its exact definition and it has been noted that there is an absence of a universal cyberbullying definition, and as such there is a need for consistent, conceptual and operational definitions of the term cyberbullying (Tokunaga, 2010). Further, Smith et al. (2013b) highlighted that a number of studies do not consider the repetition or imbalance of power in their definition of cyberbullying; hence such studies are considered to discuss and measure cyber aggression or cyber abuse. Repetition and imbalance of power are considered important when defining cyberbullying.

### ***Types of cyberbullying***

Similar to traditional bullying there are different types of cyberbullying which include flaming, harassment, impersonation, outing and trickery, exclusion and ostracism, denigration, defamation, cyberstalking (Department for Children, Schools, & Families [DCSF], 2007; Feinberg & Robey, 2009; Gillespie, 2006; Kowalski, 2009; Pearce, Cross, Monks, Waters, & Falconer, 2011; Willard, 2007). Cyberbullying is an umbrella for many online bullying activities; some are more severe than others. It is essential to distinguish between the different types of cyberbullying; a brief explanation of each type is given below. Furthermore, it is also important to distinguish between the different roles individuals play in a given act of cyberbullying.

*Flaming* relates to emails that contain negative content directed or exchanged between two or more individuals (Friedman & Curral, 2003). As explained by Turnage (2007) the consistent definition of “flames” is that the messages contain an aggressive, hostile, intimidating, insulting, sarcastic, unfriendly and uninhibited content. In addition,, such

flaming messages are characterised by the use of excessive punctuation marks, capital letters and profanity. Flaming is sometimes referred to as *Trolling* (an equally popular term), which signifies similar behaviours. *Harassment* is a type of cyberbullying that takes the form of repeated emails that are intentionally sent to upset the recipient; the repeated nature and the use of offensive words categorise such action as cyberbullying (Feinberg & Robey, 2009; Wolak, et al., 2007). *Impersonation* is another form of cyberbullying where the perpetrator pretends to be someone else and uses their new identity to communicate with others (Kowalski, 2009). The internet makes it easy for others to use a fake identity and to pretend that they are someone else. This can often be witnessed on social network websites such as Facebook and MySpace. This form of cyberbullying became recognised after Megan Meir, a 13 year old American girl, committed suicide following an online communication with a woman who pretended to be a boy that liked Megan. The woman later taunted Megan on a continuous basis by putting up hateful messages about her, which led her to commit suicide (Tresniowski, Truesdell, & Morrissey, 2008). The unfortunate consequence of this type of bullying may have been exacerbated due to the vulnerability that adolescents experience when seeking a socially approved identity and desiring to fit in amongst peers. *Outing* is a form of cyberbullying whereby individuals share embarrassing or personal information (through electronic means) about another individual, without his/her permission (Willard, 2007a), whereas *Trickery* is when an individual shares embarrassing information with another only to find that it is eventually shared with others without his/her permission. *Exclusion and Ostracism* can be another form of cyberbullying which involves intentionally excluding an individual from online groups, for example, games, messaging, chat, or social network groups (Siegle, 2010; Willard, 2007a; Kowalski, 2009). Furthermore, *Denigration* takes place when online information is posted or shared about an individual that constitutes hurtful lies, rumours or cruel gossip in an aim to harm or destroy one's friendships or to ruin their

reputation (Feinberg & Robey, 2009); this can be performed by creating fake online profiles, blogs or websites. Denigration is closely related to *Defamation* however the latter is a concept defined as online communication that aims to harm the reputation of a person by mainly spreading false information. Other forms of cyberbullying can be explained as *Cyberstalking*, which means following a person online or electronically with or without his/her knowledge. Cyberstalking can also include performing other types of cyberbullying, for example bullying via messages (Willard, 2007).

As with the advances of technology and technological skills, the trends of cyberbullying are changing over time and cyberbullies will change the ways in which they bully others. For example, recently, humiliating misuse of photographs and videos has become apparent and is enhanced and encouraged by many online applications although has not been thoroughly researched (Katz, 2014).

This typology signifies the diversity of cyberbullying and the various forms it can take. In the act of cyberbullying adolescents who socialize online have probably been involved in some form of cyberbullying (Trolley et al., 2006; Willard, 2005 as cited in Mason, 2008) in direct and indirect roles. Research highlighted six main roles that adolescents can take (Trolley et al., 2006; Willard, 2005). These include the *entitlement bully* who believes that s/he is superior and has the right to bully (e.g., demonise, harass) another person for any particular reason (e.g., being different); the *target of entitlement bully* to whom bullying is directed; the *retaliator* who responds to bullying using the same method (online); the *victim of retaliator* who receives cyberbullying as a result of their own initial cyberbullying act; and *bystanders* which could include those who are part of the problem and are involved in cyberbullying (e.g., through support and encouragement, assistants or reinforcers of the bully) and those who get involved to protest and support the victim and form part of the solution (the defender).

### ***Prevalence and Risk Factors***

According to a cyberbullying statistics report in the UK (ChildLine, 2014), it is of growing concern that 69% of young people aged between 13 and 22 have experienced cyberbullying and 20% of these cases have been classified as very extreme and two times more at risk to be bullied on Facebook compared to other sites. Furthermore, 4,500 young people contacted ChildLine in relation to online bullying in 2012-13 (ChildLine, 2013). It has also been reported that 47% of parents are concerned about their child being bullied online. The above figures suggest that cyberbullying is becoming more of a concern over time due to the expansion of technological advances and rapid developments of technology (Paul et al., 2012; Schneider et al., 2012; Slonje & Smith, 2008)

From an empirical perspective, Sabella et al. (2013) argue that “a precise measure of the prevalence of cyberbullying ... is impossible to determine” (p. 2705). The majority of studies found cyberbullying to be less prevalent than face-to-face bullying (Sticca et al., 2013). However, there is a huge variation regarding prevalence rates. For example, Juvonen and Gross (2008) found that 72% of participants had experienced at least one incident of cyberbullying compared to 77% who had experienced at least one incident of face-to-face bullying, whilst Schneider et al. (2012) found that 15.8% had experienced cyberbullying compared to 25.9% who had experienced face-to-face bullying. The lack of accurate findings into prevalence rates could be due to different research methodologies (Sabella et al., 2013), the lack of common definition for cyberbullying or by cases being underreported. It was found that cyber victims mostly told no one about their experiences online (Slonje & Smith, 2008). There could be several reasons for this including their belief that adults are incompetent to understand their experience and thus are not able to help (Smith et al., 2008), feeling that it is their responsibility to stop the cyberbullying (Juvonen & Gross, 2008) and that they would not be believed if they told an adult (DCSF, 2007; Campbell, 2005); and/or

their concern that they would be prevented from using the internet or electronic devices in the future (Campbell, 2005; Campbell et al., 2010; Juvonen & Gross, 2008). Research has also found that girls are more likely to report cyberbullying compared to boys (Juvonen and Gross, 2008; Schneider et al., 2012; Smith et al., 2008). Cyberbullying is also more prevalent amongst secondary school adolescents due to the limited availability of the necessary technology amongst primary school pupils (Campbell et al., 2010) who are more likely to be supervised whilst using the internet or electronic devices (Pearce et al., 2011). Furthermore, cyberbullying is more likely to occur outside of the school premises (Feinberg & Robey, 2009; Slonje & Smith, 2008), although it has a significant impact on school functioning such as the wellbeing and the academic achievement of students (Feinberg & Robey, 2009; Pearce et al., 2011).

A number of factors were found to contribute towards or cause cyberbullying, such as gender, pride, shame, anger, guilt, prejudice, envy, and religion (Hoff & Mitchell, 2009; Jones, Manstead, & Livingstone, 2011). Further, an association was found between cyberbullying and proactive aggression, exposure to violence, justification of violence, poor social support (Calvete, et al. 2010), face to face bullying (Juvonen & Gross, 2008; Schneider, O'Donnell, Stueve, & Coulter, 2012; Smith et al., 2008; Sourander et al., 2010), time spent online (Smith et al., 2008; Sticca, Ruggieri, Alsaker, & Perren, 2012) and poor digital/online skills (Livingstone et al., 2011).

### ***Behavioural and Mental Health Consequences***

Cyberbullying can have significant negative consequences on an individual's wellbeing (Smith et al., 2008) health (Dehue, Bolman, & Vollink, 2008) and can be potentially traumatising and should be included in adolescent mental health assessment (Sourander et al., 2010). Furthermore, Bauman, Toomey and Walker (2013) suggested that bullying should be dealt with as a mental health problem rather than as a disciplinary issue. Until 2005, the

effects of cyberbullying on victims had not been scientifically researched (Campbell, 2005) and existing knowledge on the consequences of traditional bullying was relied upon to provide a theoretical understanding of the impact of cyberbullying on the victims. In fact, several recent suicide cases involving cyberbullied adolescents have been reported (ABC News, 2007 as cited in Tokunaga, 2010; Hinduja & Patchin, 2010) which are contributing towards raising more awareness on the negative effects of cyberbullying victimisation (Agatston, Kowalski, & Limber, 2007; Baker & Tanrikulu, 2010; Patchin & Hinduja, 2010).

Based on recent literature, there is evidence pointing towards serious health issues faced by cyberbullied individuals such as depressive symptoms (Ybarra, Mitchell, Wolak, & Finkelhor, 2006; Baker & Tanrikulu, 2010), stress, feelings of loneliness and anxiety, nervousness, as well as lowered self-esteem (Ybarra et al. 2006; Katzer, Fetchenhauer, & Belschak, 2009). Additionally, emotional and mental health problems, anger and sadness (Beran & Li, 2005; Didden et al., 2009; Mishna, et al., 2010), increased distress (Juvonen & Gross, 2008), psychosomatic symptoms (Neary & Joseph, 1994; Roland, 2002), loss of self-confidence along with a negative impact on school life and academic performance (Feinberg & Robey, 2008) have also been reported.

Externalised violence in the form of suicidal ideation (Katsumata, Matsumoto, Kitari, & Takeshima, 2008), suicide (Feinberg & Robey, 2008; Finkelhor et al., 2007) and even death (Patchin & Hinduja, 2006) are equally major concerns associated with extreme cases of cyberbullying. Ybarra, West, and Leaf (2007) conducted a national cross-sectional online survey using 1,588 adolescents in the age group of 10-15 who were either cyberbullied victims or perpetrators. It was found that the participants engaged in substance abuse (i.e. alcohol and drug use), and befriended at least one delinquent peer. Delinquent behaviours have also been observed in cyberbullies (Hinduja & Patchin, 2008; Ybarra & Mitchell, 2004). Therefore, research has demonstrated that the negative outcomes of cyberbullying are faced

by both the victims and the bullies and hence requires further attention. Some studies found that most of the above psychological and emotional problems can be experienced over a long term basis (e.g. Kumpulainen, Rasanen, & Puura, 2001; Roth, Coles, & Heimberg, 2002).

There appear to be several elements of cyberbullying, which makes it more harmful than face-to-face bullying. Cyberbullying can happen anytime and anywhere (Campbell, Cross, Spears, & Sleep, 2010; Sourander et al., 2010) and it can involve a significant number of observers (Pearce et al., 2011). Victims can be anyone who has access to electronic devices and/or the internet (Paul, Smith, & Blumberg, 2012) and are no longer safe at home as their privacy is completely invaded (Grigg, 2012; Kift, Campbell, & Butler, 2010). There is an element of permanency about the internet where any act of online cyberbullying can potentially be kept online indefinitely (Butler et al., 2009; Feinberg & Robey, 2009).

By using the internet and electronic devices, cyberbullies perceive themselves to be anonymous and do not receive direct feedback on their actions and thus feel less responsible (Gillespie, 2006; Feinberg & Robey, 2009; Slonje & Smith, 2008; Sourander et al., 2010), less empathetic and show no understanding of the negative consequences of their actions. In addition, there is a loss of social inhibition (Davies & Lee, 2008) due to the physical distance between the cyberbully and the cybervictim (Vandebosch, Beirens, D'Haese, Wegge, & Pabian, 2012). Therefore, cyberbullying is not a completely new form of bullying. Instead, traditional face-to-face bullying has transformed and adapted to suit modern times.

When reviewing previous research into the potential risk and severity of cyberbullying, it highlights a requirement for protective measures to be considered. Schools are encouraged to increase awareness and adopt an anti-bullying policy; they are also required to teach children to be safe online. Despite the schools' efforts in combating bullying they cannot prevent it from happening; children are encouraged to report bullying based on which disciplinary actions might be taken against the perpetrator (Samara & Smith, 2008), however

if a victim opts to go to the courtroom what laws can be used to prosecute bullies or provide a deterrent to cyberbullying?

## **Cyberbullying and the Law**

The above review clearly highlights the prevalence and the psychological consequences of cyberbullying. Cyberbullying can take a number of forms, most of which are intended to harm an individual repeatedly. Despite such extensive research, there is no matching clarity about its legal status; it is an area of legal limbo. It is increasingly witnessed that online interaction, as well as its nature, is quickly changing. However, the law must adapt to such changes, especially when it comes to cyberbullying given its potential consequences.

Although statistics on cyberbullying are continuously pointing towards a growing trend of this phenomenon in the UK there is no specific law criminalising bullying, whether it be offline or online. In fact, as stated above there are a number of tragic cases of suicide resulting from cyberbullying. It is thought that Joshua Unsworth committed suicide as a result of months of frequent and anonymous cyberbullying on Ask.fm website (Dailymail, 2013). Another tragic example is Daniel Perry (17 years old) who took his life, in 2013, after being tricked to create an explicit video using Skype and later was blackmailed by online friends; following this video he was constantly blackmailed and had been bullied online on Ask.fm where anonymous online users urged him to kill himself (BBC, 2014a). His family appealed to Prime Minister David Cameron to consider taking measures to ensure online safety.

Similarly, another example in 2015 of suicide is the case of Ronan Hughes (17 years) from Northern Ireland; Ronan was tricked into posting online images and was later blackmailed on Skype leading to his suicide (The Telegraph, 2015). Although the later examples are of a blackmailing nature, this can fall under the trickery form of cyberbullying. A number of other cases are attributed to online abuse and cyberbullying, and there are more examples on an

international level. From the aforementioned tragic cases of cyberbullying, it is difficult to overlook the fatal consequence of cyberbullying, which is death.

Although there is no specific law criminalising bullying whether it is offline or online, cyberbullying prosecutions can be applied under a number of legislative provisions. Of equal importance, there is the need to highlight that all schools in the UK are required by law to have an anti-bullying policy in place that deals with bullying as well as cyberbullying against other pupils and teachers (Smith, Smith, Osborn, & Samara, 2008; Smith, Kupferburg, Mora-Merchan, Samara, Bosley, & Osborn, 2012). Before introducing these laws it is important to explain the stages of prosecution for a legal case.

### ***Stages of Prosecution***

According to the Crown Prosecution Service (CPS) a prosecution can proceed if it passes the two stage test as set out in the Code for Crown Prosecutors. The first stage of the test requires evidential sufficiency and the second stage requires a consideration of public interest. That is, in the first stage the prosecutor must be satisfied that there is sufficient evidence for a realistic prospect of conviction, i.e. there is evidence on which a reasonable jury could convict bearing in mind that the standard of proof in criminal cases is the need to be sure beyond a reasonable doubt that the perpetrator did the act alleged. This is an onerous task for the prosecutor to overcome in a court of law. If a particular case does not pass this stage then a prosecution cannot proceed regardless of the severity of the allegation. Once the first threshold has been met, prosecutors must go on to consider the second stage and assess whether a prosecution is in the public interest. If this stage is met, then a suspect may be charged with an offence (CPS, 2015).

The difficulty with cyberbullying is deciding which offence a suspect may be charged with, as there is no offence of 'cyberbullying' or indeed 'bullying'. Communication through social media may amount to a criminal offence; it is therefore important that prosecutors

make an initial assessment of the content and the conduct in order to consider the possible criminality and decide which offence has been committed. An offence may be made out if there is a credible threat to a person/property or communications that might be considered grossly offensive, indecent, false or obscene. However, given the absence of a specific offence, the prosecutor will need to decide which offence has been committed and charge accordingly. There are a number of Acts, which may be used to bring a charge relating to cyberbullying. The Acts set out below are generally linked to offences made through communication (and telecommunication) and are therefore relevant to cyberbullying.

### ***Education and Inspections Act, 2006***

Before proceeding with the legality for cyberbullying it needs to be highlighted that the Education and Inspection Act 2006 stipulates that it is the responsibility of the school to provide a safe and healthy environment to all pupils and it has to stand firmly against bullying in all its forms including cyberbullying. Within this statute, legal powers have been assigned to the teachers whereby they have a “reasonable” power to regulate pupil’s conduct even outside the school (off-site) or when not under the direct supervision or control of a school teacher. This serves well with regard to cyberbullying as it often occurs outside of the school’s borders (e.g. home). This Act also gives the school staff the power to confiscate items in pupils’ possession (section 3.8). For example, they have the right to retain and confiscate mobile phones or other communication devices that cause disturbance in class, or which are used as a source for cyberbullying (i.e., breach the anti-bullying policy). Teachers also have the right to search through the phone if the child displays any cyberbullying act or is seen as a suspect involved in cyberbullying. This statute makes it clear that there is a certain power/punishment to be exercised in schools when and if cyberbullying takes place; however there is no explanation as to whether or not such displayed behaviours can be prosecuted. It simply highlights the actions that the school/teacher can take within reason.

Empowering school teachers, as shown above, is significant enough to control and/or perhaps discourage cyberbullying but mostly within the school arena as such ‘powers’ are lost as soon as the pupil steps outside the school vicinity. The law does not specify how the teachers can act outside the school premises. This matter is further aggravated as there is no specific law combating cyberbullying and hence it is not considered to be a criminal offence. Those who seek prosecution can apply or choose from a variety of civil and criminal laws, which forbid forms of harassments and threatening behaviour and more specifically behaviour that is displaced through communications. Hence cyberbullying, in its forms, can be considered criminal under such laws. Nevertheless the questions as to whether these laws are sufficient or directly relevant still lurks in the legal arena. In this review we will consider laws such as: Protection from Harassment Act 1997; Communications Act 2003; Public Order Act 1986; Obscene Publications Act 1959; Computer Misuse Act 1990; Crime and Disorder Act 1998; Defamation Act 2013. All of these legislative provisions were retrieved from Legislation.gov.uk (Legislation.gov.uk, 2015) as the main reference point. Such laws can apply to children as young as 10, children above this age are deemed responsible for his/her criminal actions (age of criminal responsibility). However, they are treated different from adults (18 years and above) where they attend youth courts and sentenced differently from adults, and placed in secure centres separate from adults (Gov.uk, 2015).

### ***Protection from Harassment Act 1997***

Cyberbullying is repetitive in its nature and section 1 of the Protection from Harassment Act 1997 provides that a person is prohibited from pursuing conduct that amounts to harassment, which s/he knows or should know amounts to harassment in some way or the other. There are another three relevant sections within this Act, which may be applied depending upon the seriousness of the conduct. Section 2 is the less serious offence, which is punishable with up to 6 months’ imprisonment or a fine of up to £5000. By virtue of

section 3, harassment can lead to a civil remedy or civil proceedings by the victim leading to claiming damages for the anxiety caused as a result of harassment. Section 4 of this Act explains a considerably more serious offence in cases where the harassment conduct is conducted on at least two occasions, and thereby deemed to be a continuous course of conduct and that on all occasions such conduct entails fear of violence to be used against a person. In this case the offender must know or ought to have known the consequences of such conduct i.e. causing fear to another on all occasions. A person found guilty under this section may potentially be punished with up to 5 years' imprisonment, a fine or both. In addition, for an offence under either section 2 or 4, the Court may issue an ancillary order such as restraining orders to protect the victim from further contact by the perpetrator. There are defences to a charge under the Protection from Harassment Act 1997, which include conduct being carried out to detect or prevent a crime; for self or another person's protection; the conduct was pursued under a rule of law or an enactment. This Act also covers online and offline stalking in England and Wales along with Scotland and Northern Ireland which both have similar legislations. In the case of Brenda Leyland who took her own life after it was discovered that she sent nearly 50 tweets in one day about the parents of Madeleine McCann, it has been suggested that this Act could have been used in this case (BBC, 2014b).

Although the aspect of repetition, which is one of the criteria of cyberbullying, is present, this Act fails to include details about bullying. Further, it highlights that fear of violence should be the nature of the repetitive harassment. However in cyberbullying some bullying behaviour might not reflect fear of violence, yet they amount to significant psychological consequences and anxiety.

### ***Communications Act 2003***

Section 127 in the Communication Act 2003 has the potential to cover cyberbullying; this section covers all types of electronic public communications referred to as "improper use

of public electronic communications network”. Section 127(1) sets out the offence and its content and accordingly a person is deemed guilty of an offence when s/he sends, through electronic public communication networks, “a message or other matter that is grossly offensive or of an indecent, obscene or menacing character” or “being a cause for sending such message/matter”. Section 127(2) provides that it is an offence where communication is aimed to cause annoyance, inconvenience, needless anxiety, sending or causing to send a false message or using forms of public communication systems in a persistent way. Being found guilty under this section could lead to punishment by imprisonment of up to 6 months or a fine of up to £5000, or both.

Cyberbullying can occur using electronic means hence this Act can be applied; however it fails to include cyberbullying or even any of its conditions apart from the content (repetition and imbalance of power not included). Establishing the intention to harm or cause anxiety is difficult in an online scenario, however one could rely on the repetitive nature of cyberbullying (the amount of time a message was posted and shared) to establish the motive. Although the repetitiveness criterion is not explicitly included, it could be used to explain the intention behind the act. On the other hand, the content, referred to as grossly offensive, indecent, obscene or menacing is subjective and could be hard to understand (e.g., what might be grossly offensive to one person might not reflect the same meaning to another); these generic characters are to an extent vague and need clarity. This Act may be used to bring a prosecution although aspects of repetition and imbalance of power are lacking in order to state that this Act can fully cover cyberbullying.

### ***Malicious Communications Act 1988***

Similar to the previous Act, the Malicious Communication Act 1988 can be utilised based on section 1: the “Offence of sending letters [...] with intent to cause distress or anxiety”. It is explained that it is an offence for any person to send an electronic

communication, letter or an article that bears a threat (in whole or part), indecent or grossly offensive message, false or known to be false information. Such communication can occur orally or through other communications by means of a telecommunication system. A person might be found guilty if s/he sends, delivers, transmits or causes sending, delivering or transmitting such communications, as explained earlier. It is conditional that such communication is aimed to cause distress and anxiety to the recipient, i.e. the communicator intended to cause distress. It is not an offence if such communications were made to reinforce a demand or belief that the threat was a proper method of reinforcing a demand (on reasonable grounds). If found guilty a person could be subject to imprisonment to a maximum of 6 months or to a fine of up to £5000, or both. This Act is similar to the Communication Act 2003, and the same argument can be made regarding the lack of inclusion of bullying, and specifically cyberbullying, in its definition.

Following high profile *Trolling/Flaming* incidents in recent times, the Malicious Communication Act 1988 was amended by the Criminal Justice and Courts Bill (November, 2014) to consider a penalty of 2 years' imprisonment for offences that cover sending electronic communication/article, of any kind, to another person which entails indecent or grossly offensive content conveying a threat or false information that aims to cause distress or anxiety to its targeted recipient. The obvious change is the punishment, which increased from a possible of 6 months' imprisonment to two years. This signifies an important change, with the legal systems of England and Wales acknowledging that this form of behaviour is serious and should be met with equally serious punishment. But what remains is that the repetitive aspect of cyberbullying was not included and a lack of definition remains absent.

### ***Telecommunication Act 1988***

Section 43 of the Telecommunication Act 1988 refers to the "improper use of public telecommunication system". This section highlights that it is an offence for a person to use

any public communication system to send a message/matter that is considered grossly offensive, indecent, menacing or obscene. Further, it is also an offence if such a message/matter is aimed to cause annoyance, inconvenience and needless anxiety to another person; a message/matter that is known to be false or persistently used for such purpose using public communication system. If found guilty the offender can be liable to imprisonment (not exceeding six months) or a fine that does not exceed £5000, or both. One could say that this is one of the most related Acts to cyberbullying as it clearly includes the content, although generic, that is often portrayed in cyberbullying. Furthermore it includes the persistent nature of such Acts; this can cover the repetition condition when defining cyberbullying. That leaves the imbalance of power as the only condition not covered here, but in the cyberworld it is hard to know who is more powerful (the bully or the victim). However, the anonymous nature of the bullies in some cases makes them more powerful in initiating bullying.

### ***Public Order Act 1986***

Prosecution for cyberbullying can be based on the Public Order Act 1986. By virtue of section 5, (harassment, alarm or distress) it is an offence to use abusive, insulting, threatening or disorderly behaviour. Further, a person is also guilty of offence if s/he “displays any writing, sign or other visible representation which is threatening, abusive or insulting, within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby”. On the other hand, a person is not guilty if s/he displays a reasonable conduct with no reason to believe that there is a person within sight or hearing who might be caused harassment, distress or alarm. This applies to mobile phones, as the Act covers all forms of communication (writing and visible representation) that can apply even to video or camera communication. A guilty individual could face a fine not exceeding level 3 (£1000). Again this Act is similar to earlier ones in that it fails to include the repetitive nature of cyberbullying and the imbalance of power that are part of the cyberbullying definition.

### ***Obscene Publications Act 1959***

The Obscene Publication Act 1959 considers it an offence to publish an obscene article. Publishing in this case can be in the form of showing, circulating, transmitting, playing or projecting. This Act considers an article as 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” (Section 1).

Under some circumstances a person might not be found guilty. For example, a person is not guilty if s/he proves that he had not inspected the article or had no cause to believe that such article makes him/her liable to be convicted of an offence. When found guilty a person could be fined or imprisoned for up to 2 years or both. This Act stresses the nature of publications as being obscene only, which makes it less conclusive compared to the other Acts, mentioned above.

### ***Computer Misuse Act 1990***

At times cyberbullying can take the form of hacking into someone’s computer (e.g. hacking into someone’s Facebook account and publishing indecent material). In such cases the Computer Misuse Act 1990 can be relevant and thus applied. This act prohibits hacking into computer material, access with the intention to facilitate or commit a crime, modify materials, supplying, obtaining or making anything that can be used or lead to computer misuse. However this Act does not refer to the type of content (other than assuming it is private/personal/confidential information) and does not include the repetitive nature of bullying. Here one might assume that the hacker is the more powerful to explain the other condition of cyberbullying. But what about hacking into someone’s mobile phone? Can this be considered under the Computer Misuse Act? Again one can assume that it applies since the mobile phone can include the same information held in the computer.

### ***Crime and Disorder Act 1998***

This Act provides for the imposition of an Anti-Social Behaviour Order (ASBO), which can be used in cases of cyberbullying nature. This order prohibits a person from being involved in anti-social behaviour/acts and can be used when there is some form of evidence of behaviour causing or likely to cause harassment, alarm and distress and can be used when the order is needed to provide protection to an individual from further anti-social behaviour. The nature of such behaviour is measured through the effects and the consequences they might have on an individual or individuals within a community where such behaviour take place. The prohibitions within this order should be specific to the anti-social behaviour and aimed to protect the individual. It is considered a criminal offence to breach the ASBO and criminal penalties apply to such cases. Bullying can be viewed as an anti-social behaviour, which clearly distresses victims and causes harm. However, this Act also fails to mention the aspects of repetition and imbalance of power. Furthermore, aspects of online anti-social behaviour are not covered which could be problematic when applying it to cyberbullying specifically.

### ***Defamation Act 2013***

This new Act, which came into effect in January 2014, aims to create a balance between freedom of speech and comments that might cause serious harm to an individual. For any statement to be defamatory by nature it must lead to other people thinking worse of an individual to whom the statement was directed towards. Such statements could include dishonesty, allegations of criminality, lack of integrity or sharp practice, insolvency and personal morality; in other words, it has to cause real or probably serious harm to the claimant reputation. The statement will not be deemed defamatory if the author can prove that it is true, similarly if it is a genuine honest opinion or if it is a matter of public interest. If proven defamatory this might lead to a injunction to stop it being repeated or paying

damages to the claimant. The issue here surrounds the real harm to reputation, although cyberbullying can lead to that, in many other cases reputation might not be the main importance in cyberbullying. If the exchanged communication is true (expressing thoughts) does the victim have to accept it as such? The content of this Act focuses more on the reputation factor, hence cyberbullying can be condemned if it includes content that is untrue and has a serious negative impact on the receiver. Once found guilty a person is forbidden from repeating the defamatory act but similar to other legislation there is no focus on the repetition of communication and the imbalance of power, also there needs to be more clarification on what is defamatory.

#### ***Amendments to tackle revenge porn***

Cyberbullying can take the form of online publishing and sharing of explicit sexual images/videos. In February 2015 a new amendment was created to tackle 'Revenge Porn' due to its increased occurrence in social media in the UK. Revenge porn involves online sharing and posting of photos, video of sexual nature without the subject's consent. Hence the amendment makes it illegal to disclose explicit pictures or videos of sexual nature without the consent of the person depicted and with an intention to cause distress. This can be an offence under the Communication Act 2003 or the Malicious Communication Act 1988. If the offence was repeated then this could be an offence under the Protection from Harassment Act 1997. Offenders might face a punishment of up to two years' imprisonment in addition to a fine. In relation to cyberbullying this amendment makes it clear that it is illegal to bully others using revenge porn. However to cover the repetitive nature of cyberbullying one can combine that with Protection from Harassment Act 1997 which clearly stipulates repetition in its definition of harassment.

### *Appealing for a new law*

After explaining the above legislation and highlighting, as far as possible, the extent to which each is relevant and can be applied to cases of cyberbullying, it is worth emphasising that cyberbullying has always existed in society especially in developed countries. But with the rapid advances of technology in its varied forms, this phenomenon has the potential to be even more prominent. As such, there is a desperate need for various forms of interventions to emerge, whether it being inside or outside schools. At the moment the emphasis is on the sensitisation of the UK Government with regards to the seriousness of this issue and the pressing need to develop strict laws specific to cyberbullying in order to combat it. However, does cyberbullying merit a new law? If bullying in its tradition form has not had the benefit of a specific law to make it a specific offence, then why does society require a dedication to combat cyberbullying? All the Acts reviewed earlier do not refer to children specifically but apply to anyone who can be held criminally responsible (10 years old and above). Do children and adolescents require a form of protection over and above what the existing laws are providing in order to address cyberbullying, or is cyberbullying to be regarded as the modern day bullying which replaces or extends to that which took place in the school ground prior to the advances in technology and which there was no dedicated protection for? Is it the case that society needs to educate people from a young age that it is simply unacceptable without the need to legislate and criminalise? Since 1999 it has become a legal requirement that schools in England have an anti-bullying policy, which means that schools have the power to include legislation on bullying and cyberbullying and follow-up the implementation of these rules. Research has found that comprehensive anti-bullying policies are significantly related to a reduction in bullying. However, schools were less likely to mention cyberbullying in their anti-bullying policies (Smith et al., 2008, 2012).

One of the more significant appeals to introduce a general bullying law was made through what is known as “Ayden’s law”, although it is not directed at cyberbullying it is worth explaining why it was not successful. Ayden Olson (14 years) committed suicide (March-2013) as a result of brutal school bullying after admitting he is homosexual. Following his death, the Ayden’s Law campaign had started to put up a case for all child victims of bullying. The appeal, led by families of victims, BeatBullying charity and the Sun Newspaper were successful in introducing a Bill (July-2013) which emphasised community-based bullying prevention while giving way to the need for the introduction of a statutory requirement for the government to work actively towards the implementation of anti-bullying strategies for the UK (The Sun, 2013). This Bill went beyond its focus on the victims of bullying as it was also aimed at supporting families with children who are bullies to seek help and change their behaviour. This Bill introduced the following sections:

*Justice for victims:* “If a child was found to be acting in a way that could cause physical or mental harm to another person, they could be charged and prosecuted”. As far as sentencing would be concerned it would be based on out-of-court measures.

*Community Protection:* An attempt would be made to provide anti-bullying training to all social workers while they are following their course. In doing so, they would be better equipped to work hand in hand with their community to limit bullying, support victims of bullying and their families, as well as helping bullies to change their maladaptive behaviour.

*Government action:* To convince the government from a legal stand point to publish ‘A Children and Young People’s Annual Anti-Bullying Strategy for the UK’ with the Prime Minister accountable for reporting progress to Parliament on a yearly basis.

*Family support:* Under Ayden’s Law, all families who have a child involved in bullying and intimidation will have to enrol in a compulsory family intervention programme.

This Bill was not passed by the UK Parliament. The exact reasons of its rejection are not known but one can speculate and argue a number of possible reasons. If this law regarding traditional bullying was not passed what chance is there for a new cyberbullying law to be established in the future. It can be argued that criminalising cyberbullying is an even harder task (since traditional bullying is not criminalised). By reviewing earlier research (e.g. Campbell & Završnik, 2013) a number of challenges might come to mind when thinking of a cyberbullying legislation that might explain why it is hard to introduce such law. Such challenges are presented below.

### ***Challenges and Obstacles***

The first challenge facing a cyberbullying criminal law is its *definition*; bullying in general and specifically cyberbullying are not directly defined or mentioned in UK laws (Marczak & Coyne, 2010). To pass legislation there needs to be a consistent and clear definition; different studies have defined or referred to it differently (e.g., cyberbullying, cyberstalking, cyber-harassment, and cyber-victimisation) (Campbell & Završnik, 2013). This clearly poses a challenge and therefore a unified term is needed.

*Lack of awareness* is another issue and according to Paul, Smith and Blumberg (2012a) young people are unlikely to be affected by cyberbullying laws mainly for their impulsive nature and naivety regarding their misuse of technology with an unintended consequence of causing harming to the other. Moreover they also hold the belief that they can maintain anonymity and not be caught. Furthermore with their better understanding and use of technology (generally) as compared to adults they feel that they can ‘get away’ with cyberbullying and in fact looking at the number of unaddressed cases of cyberbullying so far, such a belief on their behalf can certainly be reinforced to some extent. Finally, their lack of awareness of existing laws also put them in a situation whereby they can claim that they were not even informed of the meaning and consequences of cyberbullying. They may also be

unaware of the distress that they are causing their victim, given the lack of face-to-face contact.

*Intention to harm* is one of the main criteria in criminal laws and this is often problematic in written text, as some would refer to it as an indirect intent. As a consequence prosecution might not proceed in some cases of cyberbullying due to the judgement of intent (Lievens, 2012) but one might explain that the repetitive nature of cyberbullying can easily suggest the intentions. With regards to young cyberbullies this issue might be more prominent given their lack of maturity and their awareness of whether or not some behaviours are deemed illegal. This could be combatted by addressing it within the school curriculum, which would increase the awareness of pupils on bullying. It is complex to comprehend the full intention of children who are not legally aware of the consequences of their actions. Robinson and Darley (2004) argue that a criminal law can have a deterrent effect only if the potential offender is aware of the law (directly or indirectly) and the implications for breaking it. However it is commonly acknowledged that people generally lack knowledge of the law.

One major hurdle is the *lack of surveillance*; how would it be possible to follow and control cyber communication? Legislators would often ask themselves whether they possess the means to reinforce a particular law, making it a major ingredient in its success. In the context of cyberbullying, surveillance is particularly difficult. There could be a lack of extensive surveillance in order to fully enforce a cyberbullying law or, it may also lack the necessary sanctions to deter cyberbullying (Svensson & Larsson, 2012). Therefore it could be said that given the complexity of technological advances in today's society, effective surveillance techniques can be difficult to apply and hence detecting cyberbullying and more importantly, tracking and identifying the cyberbully can indeed be an ordeal.

*Establishing Evidence* in cases of cyberbullying or any other cybercrime is particularly challenging. It is difficult to rely on digital evidence; computers relies on zero and one (0,1)

as the basis of any online representations (coding). Such information is considered fragile and can be easily changed or lost (e.g. hacked); professional cybercriminals can set up their computers to destroy evidence and in some cases they can even use different IP numbers (Internet Protocol address). Hence such possible online manipulations do pose themselves as a major obstacle in providing accurate evidence in the court room. Cooperation with internet providers and social networks (Facebook, MySpace, Twitter and so on) is often tricky; although they have policies against cyberbullying they do not verify a user's true identity. Do the laws therefore need to be changed to ensure that people who set up social media identities have age verification prior to the identity being accepted? Would it go some way to limit the risk or children using these forums to bully others? Hence even when they cooperate they might not have the correct information apart from the IP address.

*Anonymity and identity* is another challenge. Online social networks are easily accessed using fake names and email addresses, hence a child could be bullied by others without actually knowing their true identity. Does this raise the issue that parents need to be educated to take responsibility for the media sites that their child accesses? Should they conduct checks as to which sites their child accesses? In fact, there are many ways to hide identity when using computers and, if required, the IP address can be masked using some available paid services; this makes it difficult to track the perpetrator and know their true identity (Campbell & Završnik, 2013). As a result, cyberbullies feel 'protected' behind their screen as well as powerful in terms of victimising their target without being accountable for the action. That said, not all bullies have the capacity of hiding their details, but even then such cyber details can be easily disputed.

Supposing that a law is passed against cyberbullying how about the *jurisdiction*? Bullies can be from everywhere in the world, prosecutors will have to check whether they have jurisdiction to proceed. It is problematic to prosecute a perpetrator from a foreign

country. Generally the main focus in such cases is on the jurisdiction of the perpetrator or author (Kift et al., 2010; Lievens, 2012). There are different legal systems across countries (e.g. common vs. civil laws), and the age of criminal responsibility could be different too. In Europe, in cases that involve cybercrimes or internet offences, there is a support through the computer emergency support team in the EU (CERT-EU) and through the Cyber-Crime centre (EC3) which were established by the Europol in 2013. Furthermore there is a 24/7 contact line for international cybercrime prosecution established by the Council of Europe (CoE) (Kerr, 2005). While considering jurisdiction it is important to highlight that different countries have different terms reflecting cyberbullying. For example, in Spain, the term used to define cyberbullying is ACOSO; in Germany it is commonly referred to as cyber-mobbing, while in Italy, it is known as BULLISMO VIRTUALE and this further stipulates jurisdiction as a challenge (Campbell & Završnik, 2013).

Some might see cyberbullying as a form of *free speech* and view it to be within their right. Surely freedom of speech is a major principle of any democratic society. However it does have its limits as set by international human rights law and other case laws. According to Campbell and Završnik (2013) a cyberbullying law should be tailored in such a way that it does not infringe current laws concerning freedom of speech. Constantly there is a debate around what distinguishes cyberbullying from freedom of speech or expression. One would need to distinguish between this term and cyberbullying and a number of researchers think that the connection between both is delicate (King, 2010; Lievens, 2012; Ruedy, 2008). In fact, it can be said that there exists a fine line separating each and thus this needs to be considered when assessing a case of potential cyberbullying.

If the government does criminalise cyberbullying behaviours by bringing the *age of criminal responsibility* to 10 years of age, this would also mean that children and adolescents between 10-17 years could be easily criminalised. However this would carry some

implications in relation to the extent to which it would be reasonable to criminalise individuals as young as 10 years of age and if so, what would be the rehabilitation outcomes for this age group. In addition, for a young child it is an obstacle for his/her future career to have a criminal file that cannot be wiped of the system even if regret and rehabilitation have taken place. These could be sticking points before passing a relevant Bill. It should be noted that although children could be criminal responsible by the age of 10 they do attend a youth court and there are secure facilities if found guilty, while the sentence is not as severe as that of an adult.

Although bullying and its associated adverse consequences on the wellbeing of young people have been in the limelight of research for many years now, there is still a debate pertaining to its *severity* and more specifically, those related to cyberbullying. The question is whether it is severe or prevalent enough to merit a law? Or is it just a normal accepted and normalised experience (Limber & Small, 2003). It has to be acknowledged that, in recent years, cyberbullying has led to severe outcomes (e.g., the suicide of Daniel Perry) and the recent amendments to the Malicious Communication Act 1988 further stressed that trolling (a form of cyberbullying) is a serious problem following high profile cases (adults).

### ***The Role of technology***

While there is no specific law covering cyberbullying in the UK, current laws could be and often are, applied to cyberbullying despite the challenges and limitations. When considering legal options for addressing cyberbullying there is a threshold of severity and requirements for evidence that are needed to satisfy the law. In such cases, electronic evidence and a trail of calls or messages could prove crucial in court, particularly to prove harassment or stalking, or sharing of illegal images. However, other actions can be taken, such as having material removed from a site, having a user banned from the site and retrieving images, all without recourse to law. These steps can be of enormous importance to

victims and are usually taken directly by the Social Networking Sites (SNS). There are electronic reporting tools, filtering tools, search tools and screen-prints or photographic evidence trails which can be immensely useful even in cases that do not pass the threshold of amounting to a crime.

A number of studies have looked at the role of computer-based technology in identifying cyberbullying, especially when considering SNS. SNS can deploy such technology, in order to ensure a safe environment (e.g., identifying perpetrators in severe cases and deleting harmful messages) (Vandebosch, 2014). Various forms of parental controls claim to be able to identify cyberbullying using technology, some with alerts to parents and controls on the sites a child can visit, the length of time they are allowed to spend on the site and some even claim to measure the mood of the user. The European Commission and SNS are committed to applying 'Safer Social Networking Principles' to safeguard young users (EC Social Networking Task Force, 2009). Such principles include the delivery of educational messages, ensuring privacy, and empowering users while installing reporting tools. Also some SNS providers apply strategies to detect inappropriate content at early stages to take the necessary actions. Content on SNS can be reviewed by different mechanisms, human or computerised (automated) monitoring methods (Staksrud & Lobe, 2010; Cited in Van Royen, Poels, Daelemans, & Vandebosch, 2014).

Cohen et al. (2014) proposed an example of such technology in the form of a multi-faceted computer based solution to cyberbullying aiming to mitigate its impact by offering assistance to the victims of bullying and the bullies. Following a series of group projects, they have developed a technology that is able to detect the occurrence of cyberbullying, to report incidences, with an option to integrate a third party once cyberbullying is detected. Finally, the technology offers facilities to manage online social networks and take actions in cases of bullying. The proposed technology aims to rate messages either positively or negatively, with

the audience or the receiver having the ability to rate a message with a score indicating how malicious it is (smaller or bigger than 1). A person will have this score in his records, thereby accumulating a reputation score. This research highlighted the possibility of fake reporting and privacy, and has proposed protection methods using artificial intelligence. This system allows filtering of messages and allows classification of messages (by users) as either positive or negative (abusive or non-abusive). A trusted third party selected by a user (e.g., parent or a friend) can check the messages and delete it if abusive/negative or keep it if judged non-abusive/positive. Highly abusive messages might require police intervention and should be kept as evidence. The filter also allows the grouping of people under two categories based on the content of their communication, one for those whose communication is welcomed and those whose communication is not. Other features allow the technology to detect messages and filter them based on pre-selected words (e.g., of abusive nature). The sender's information is also kept in the records once recognised or filtered as abusive. The proposed technology also offers sentiment analysis, often used in social media that aims to analyse the emotional content of texts (Pang & Lee, 2008). The system offers a reporting option, where a victim or a third party can report an abusive message (reporting the URL source). In a case where the victim of cyberbullying is not identified, a procedure is conducted to identify/confirm the victim and to communicate with him/her, as well as determining the bully/perpetrator. The victims are then provided help based on the nature of the communication (e.g., privacy leaking, harassment). Thereafter the victim is offered possible solutions and education on how to deal with the abusive communication/message. The perpetrators are also offered education. The system monitors messages sent by the perpetrators and sends frequent warnings that could lead to legal actions (if perpetrator does not stop the abuse). Further to the automated tools, it is suggested that there should be a more

centralised platform monitored by the authorities (e.g., police), who can closely work with administrative teams of various online social-networks or websites (see Cohen et al., 2014).

Cohen et al. (2014) clearly proposed a technological approach to detect cyberbullying, filter such behaviour and educate individuals involved. It can be argued that this technology can reduce cyberbullying and identify victims and bullies, although the accuracy of identification is not clearly discussed. Moreover, it can be used to establish evidence (records of cyberbullying) while involving a third party who can act as a potential witness if needed or as a way to protect against future cyberbullying by reporting it. However, the article failed to provide an accurate definition of cyberbullying (e.g., the repetitive nature, imbalance of power and the intention to harm). If an incident happens on one occasion it might be considered abuse or harassment but not necessary bullying. Albeit an interesting and useful technology, it needs to differentiate between cyberbullying and other forms of online harassment/abuse, although all merit attention. Also, it will be interesting to see how technology verifies true identities, especially young Internet users who can create multiple online identities.

Technologies can also be used to reduce the occurrences of cyberbullying. Bosse and Stam (2011) proposed an automated technology, which allows for beliefs, desires and intention (BDI) based normative agents that are physically present in the virtual society. A number of intelligent techniques are installed for the normative agent to allow detection of norm violation (e.g., abuse) then to apply a reward and punishment to maintain the desired behaviour. They have tested this system amongst 6-12 year old children, logging and analysing all of the behaviour, and the system was shown to be effective in reducing norm violation (cyberbullying) in the long term. Although this system uses artificial intelligence it is still far from perfect according to the authors, who have indicated that further research is needed before it is fully successful. This study mainly looked at reducing cyberbullying,

however it will be interesting to see how BDI-based normative agents can be extended to allow for reporting incidences, gathering evidence and identify bullies/victims while monitoring behaviour. Such features can surely enhance the appeal of this system and perhaps offer evidence in cases of cyberbullying, keeping in mind that establishing a law against cyberbullying is hindered (amongst other challenges) by the difficulty of establishing evidence. If such programmes are effective in limiting cyberbullying this can easily save many from resorting to seek legal intervention.

Further research by Ochoa et al. (2011) suggested the use of multi-agent systems to understand cyberbullying. This approach argues for the need to understand the social and cultural implications of cyber-technologies. They argue the use of an Artificial Society, which is a synthetic representation of the online society; it stimulates cooperation and competition among other social phenomena. Artificial Society seeks to understand how the societies work by synthetically creating them and understanding their complex processes, it also consider how the society interacts with the environment while understanding relevant cognition and intelligence. This complex multi-agent system, based on algorithms, seeks to understand different online global behaviours and patterns in order to understand cyberbullying. Although this is a novel approach, it was not the subject of experiment. There is a clear need to go beyond this theoretical proposal. Cyberbullying is a complex phenomenon and tackling it online is particularly problematic. Technology based proposals can certainly contribute to limiting cyberbullying, understanding it better and establishing evidence to provide for prosecution when needed.

It is almost impossible to manually monitor SNS content, hence there is increasing need for automated efficient technologies to provide quick content screening and detection of cyberbullying from large user-generated content (Van Royen et al., 2014). Automatic detection tools of cyberbullying use similar technologies, which categorise text (e.g., topic

detection, spam filtering and email routing) (Sebastiani, 2002). These tools are rule-based, unlike machine learning approaches, which are argued to be easier to use and provide better accuracy and efficiency as they are trained on labelled examples. Delort et al., (2011) explains that obtaining labelled data is particularly time-consuming and is expensive; the use of semi-supervised learning techniques can reduce manual data labelling. Van Royen et al., (2014) explained that it is simple to detect unwanted text such as racist language or spam, however cyberbullying is more complex. For that reason complex document representations are utilised while recording information about cyberbullying victims and bullies, this is achieved using words that are deemed insulting, profane or typical words used in cyberbullying. Machine-learning models can incorporate these words along with other characteristics such the personality and the gender of those involved which can be automatically determined (Schwartz et al., 2013). A challenge an automated system might face is the difficulty in determining the nature of the relationship between sender and recipient and the context, which makes it almost impossible to arbitrarily decide whether or not it is cyberbullying. During the day, in other parts of their life, children and adolescents might happily be together in school and then have an argument that is extended online. Context is crucial and cannot always be detected, unless recipients report abuse using other suitable methods (e.g., report abuse button). SNS reporting systems could be improved, the extensive use and the amount of text involved in SNS makes it harder to identify cyberbullying in a timely manner, especially those that need human intervention. Also the frequent use of new acronyms is proving to be challenging too, as often they are not included in filtered lists in SNS.

Cyberbullying detection technologies (automated) are low in precision; however it is useful in assisting human moderators to look at a lower number of cases. Technological advancements aimed to enhance automatic cyberbullying detection; this technology is

desirable and should be implemented, however there should be follow up strategies while ensuring privacy for adolescents and maintaining their self-reliance (Van Royen et al, 2014). Automated models detecting cyberbullying are developing, however there is a clear need to work with law enforcement agencies and to legally protect internet users against cyberbullying; although this is particularly challenging (e.g. establishing evidence and intent) it will be interesting to see how this can be incorporated into automated technologies that aim to protect against cyberbullying. The legal obligations of SNS providers regarding cyberbullying have not been explored. Although the majority require their users to be above the age of 13 years and warn against the use of all forms of abuse (terms and conditions), this is often bypassed. A lot can be learnt from current technologies combating cyberbullying, however more needs to be done to establish evidence (in cases of cyberbullying) and accurately identify perpetrators. SNS can play a major role in combating cyberbullying (e.g., by adopting suitable technologies), however more clarity is needed about their legal responsibilities, and if a law is to be established then surely they will play an integral part.

### ***Should cyberbullying be criminalised?***

Should we actually have a specific law against cyberbullying? There are several arguments that could be raised in an attempt to answer this question. There is an urgent need for the protection given by the law in this area as this would pave the way to more clarity in terms of identifying and classifying the different types of cyberbullying. Moreover, implementing a law against cyberbullying could largely contribute towards raising awareness with regards to the prevalence and severity of this phenomenon in the current UK society. Hence, altogether this could potentially lead to better protection for young people who are seen as vulnerable bearing in mind their ongoing reconciliation with the critical phase of adolescence. Conversely, it could be suggested that in some way or the other, most, if not all,

of the aforementioned legislation already cover the nature of cyberbullying therefore simply indicating a need to make adjustments to existing legislation.

Cyberbullying is prevalent in our society and it could potentially lead to fatal consequences. The fact that the Ayden's Law Bill was not passed highlights the difficulty in passing an anti-bullying law let alone one in relation to cyberbullying. Surely a law or any form of legal prohibition can limit this phenomenon whether it is off or online; ultimately this could lead to a safer cyberspace for children in a fast growing digital age. Enacting a law can be a way of educating people and influencing their social norms, hence having a cyberbullying law with punishment and sanctions might lead people to accept that such behaviour are wrong (Droback, 2006; cited in Smith & Steffgen, 2013). This can be a positive influence amongst young people, leading them to understand that cyberbullying is an unacceptable behaviour. According to the Social Development Model (Cleveland et al., 2008), young people usually need to have clear rules and regulations inculcated in them in order to engage in socially desirable behaviours. This model posits that the skills, attitudes and values pertaining to anti-social behaviours are learned through the social learning process (Catalano & Hawkins, 1996; Catalano et al., 2005). Hence having such law will provide new social norms condemning cyberbullying, which will include more clarity and increase their awareness.

The community, teachers and parents are hoping for legislation that provides a legal protection against cyberbullying in schools (Kift et al., 2010). However researchers (e.g. Jager, Amado, Matos, & Pessoa, 2010) think that monitoring online activities is not enhanced by many mechanisms and there is a common perception amongst experts that there is an essential need for more adequate mechanisms, rules and sanctions in order to combat cyberbullying. Hinduja and Patchin (2010) explain that parents often claim that they do not have the requisite skills to monitor their children's online activities, while teachers are often

reluctant to deal with problems outside of the school's environment, and more importantly legislators want to see clear evidence that cyberbullying poses a significant threat to individuals in order to provide a law against it. While King (2010) states that cyberbullying could be combated with educational measures and non-disciplinary actions, there are times this might not be sufficient on its own and a law would provide a stronger deterrent and prohibition which could have a greater effect due to resulting punishment. However, King (2010) further stressed that cyberbullying is best dealt with in classrooms and not in the courtroom, placing emphasis on the role of schools and teachers. The law can play a role in this awareness and education, and could lead to bullies/perpetrators being deterred from conducting any actions amounting to bullying.

It has been noted that cyberbullying is a social issue, which is experienced on an international level regardless of differences pertaining to boundaries and jurisdictions in many cases. Nonetheless taking into account the uniqueness of the legal system of each country, it would be wiser and perhaps more effective if cyberbullying is combatted on a national level (Davies & Lee, 2008). While there are voices in support of establishing a new cyberbullying law, others argue that current legislation exists in the UK to cover cyberbullying but there needs to be a stress on the major challenges facing their full implementation. As discussed earlier, there is no one piece of legislation in the UK that accurately describes cyberbullying or even bullying. Cyberbullying is characterised by its content referring to a repeated intentional aggressive act (harassment, intimidation and threat) using a telecommunication medium (e.g., mobile phones, computers), and it is also characterised by the imbalance of power between the bully and the victim. Taking this definition into consideration, there is an absence of legislation covering these points. Prosecution in any bullying case must arise from one of the aforementioned Acts of Parliament, and prosecutors must establish the nature of a cyberbullying case and then apply

the existing legislation; this is challenging for prosecutors and others involved in the court process.

By reviewing the legislation, it can be summarised that the various Acts (especially the communication related Acts) refer to content/action that is grossly offensive, menacing, obscene, false, indecent, causing needless anxiety, annoyance or inconvenience. The Protection from Harassment Act 1997 refers to harassing and violently threatening behaviour on at least two occasions. The Crime and Disorder Act 1998 refers to behaviour that causes harassment alarm or distress. While the Public Order Act 1986 refers to abusive, insulting, threatening or disorderly behaviour. The Computer Misuse Act 1990 refers to computer hacking and access to private personal information while the Defamation Act 2013 refers to false allegations that intend to harm someone's reputation.

It can be argued that in terms of content, cyberbullying can be partially covered by combining a number of statutes. Its repetitive nature is covered in the Protection from Harassment Act 1997, which refers to harassment on at least two occasions, and in the Telecommunication Act 1988 which refers to persistent behaviour. The imbalance of power can be translated based on the anonymous nature of cyberbullying (e.g. anonymity of the perpetrator) and by the inability of the victim to defend him/herself. It is clear that existing legislation does not provide sufficient clarity in respect of bullying and cyberbullying and it is accepted that including any definitions within the legislation is very challenging. One of the more critical issues of establishing a cyberbullying law is generating evidence. Online evidence is very problematic, requires huge cooperation (involving websites, companies internet provides etc.). Furthermore it is hard to establish the intention of a suspect to harm and their true identity. A moral challenge could be that since the age of criminal responsibility is 10 years old then children as young as this age can be criminalised and have a criminal record. There is a higher chance of them being criminalised in cyberbullying cases

as they are less likely to be aware of legislation and the implications of their actions. Others might argue that cyberbullying is not a significant problem that requires legal attention, and there is always the argument that cyberbullying is a normal behaviour and part of a child's development. Jurisdiction is another major problem; the cyberworld knows no borders and bullies or victims can be from anywhere across the world hence prosecutions across jurisdictions and/or establishing evidence from abroad is also problematic. The definition of cyberbullying in the legal systems of the UK is inconsistent, and other countries might not label such behaviour as criminal. Another main challenge is that the police say that they are overwhelmed with child exploitation cases and currently have a three months backlog; if a law against cyberbullying was passed they would be inundated and would not have the manpower to address it.

Technology is advancing fast, and it is understandable that the law is not keeping up with the pace. Indeed establishing a cyberbullying law would be very challenging and perhaps the challenges far exceed the benefits. However if one simply wants to adopt a medium approach, perhaps the Government could commence this by making the necessary amendments to existing legislation in order to effectively accommodate the intricate nature of cyberbullying. An alternative measure to combat cyberbullying could involve disciplining schools, parents and bullies/perpetrators using intervention schemes that would be powerful enough to bring about any anticipated positive outcomes.

While suggesting amendments to existing legislation to include bullying and cyberbullying, it is worth starting with a school-home approach. Schools should understand that bullying and cyberbullying can amount to illegal offences, and with sufficient evidence bullying can lead to warnings, fines and imprisonment; it is not known whether schools, parents or indeed children are aware of this fact. The law can serve as a strong deterrent, or even enhance (if incorporated) other bullying prevention methods/intervention. Children as

young as 10 years' of age are criminally responsible for their action. If cyberbullying is incorporated into current legislation then there is an increased likelihood that more children will be criminalised; and that could significantly and negatively affect their future. An offence and a caution stay on record for periods of 5.5 years and 2 years respectively, during which time both offences and cautions must be declared in certain situations. Where the line should be drawn is a challenging question. Perhaps the law can be applied if and when all other methods of prevention were exhausted (e.g. school and parents involvement).

Before applying the law the schools' anti-bullying policies should be revised to accommodate any amendments to legislation concerning bullying and cyberbullying. Schools should increase awareness amongst pupils of the legal consequences of their actions as they relate to bullying and cyberbullying. The law can only serve as a deterrent if children are aware of it. Hence legal education should be incorporated within schools' anti-bullying policies. Schools should frequently be made aware of their legal responsibility and parents should also bear some responsibility. The prevention of bullying and cyberbullying should start from home and school; hence parents should also be educated about the legal consequences. An amendment to legislation to incorporate an offence of cyberbullying will serve as a major deterrent; however the matter should be dealt with within schools initially. Schools and parents should be equally involved and held responsible, and if and when mediating solutions occur between schools and parents the targets of bullying should resort to the legal system. This article aims to provide a review of challenges that are facing the society on tackling cyberbullying. Policy makers should start fully incorporating bullying and cyberbullying in the law. Although this might not be achievable due to different challenges, an educational programme should be implemented to set out and explain the health impact of bullying.

## **Conclusion**

According to many studies, bullying and cyberbullying can have devastating consequences on a child's mental and physical health; hence the punishment should equal the impact. Technology has offered some solutions to reporting and reducing cyberbullying, although it might not be judged as fully efficient at the moment, especially that many of the SNS are international and issues of jurisdiction can, amongst other factors, prove to be challenging. Schools and parents should be the first to tackle the problem but the legal system should provide an alternative in severe cases and a platform to facilitate that. Defining what is severe could be challenging, what affects one person might not affect the other and what is viewed as a minor incident could have more impact. It is the consequences that might explain the severity at times. Although the law is not yet proven to be a deterrent, it ought to be tried and researched. Some current laws can be applied; however greater clarity is needed as well as legal awareness among schools, parents and children. Empirical research is essential in demonstrating the impact of a legal intervention on cyberbullying. It is not known how much children are aware of the legal system and current laws. Future research should design and test bullying/cyberbullying interventions that involve legal education, and legal consequences. Only then can scientific evidence enhance opinion among policy makers as to whether or not a law is needed. Moreover inspiration could be drawn from research in the USA where bullying and cyberbullying is made illegal in a number of states (Hinduja & Patchin, 2015). Also lessons can be learned from Canada (province of Nova Scotia), where a specialised cyberbullying investigative unit was first established. This unit aims to provide support to families and victims with legal protection, while giving school principals clear authority to tackle bullying and cyberbullying. Court or legal orders can include confiscating computers, smartphone and tablets (or any electronic mean) while banning contact between bullies and victims. Families are also held responsible in cases involving minors (Premier's

Office, 2013). Although many might view this as a radical approach in the UK, it may work as a deterrent and reduce cyberbullying.

## References

- ABC News. (2007). Parents: Cyber bullying led to teen's suicide retrieved July, 13<sup>th</sup>, 2015 from: <http://abcnews.go.com/GMA/story?id=3882520&page=1>
- Agatston, P.W., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health, 4*(6), S59-S60.
- Arsenault, L, Milne, B.J., Taylor, A., Adams, F., Delgado, K., Cadpi, A., & Moffitt, T.E. (2008). Being bullied as an environmentally mediated contributing factor to children's internalizing problems. *Archives of Pediatrics and Adolescent Medicine, 162*(2), 145-150.
- Baker, O.E., & Tanrikulu, I. (2010). Psychological consequences of cyber bullying experiences among Turkish secondary school children. *Procedia Social and Behavioral Sciences, 2*(2), 2771-2776.
- Bauman, S., Toomey, R.B., & Walker, J.L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence, 36*(2), 341-350.
- BBC News. (2014a). Daniel Perry's death sparks cyber-blackmail probe. Retrieved June, 20<sup>th</sup>, 2015 from: <http://www.bbc.co.uk/news/uk-scotland-24428437>
- BBC News. (2014b). Who, what, why: What laws currently cover trolling? Retrieved June, 21<sup>st</sup>, 2015 from: <http://www.bbc.co.uk/news/blogs-magazine-monitor-29686865>
- Beran, T., & Li, Q. (2005). Cyber-Harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277.
- Beran, T., & Li, Q. (2007). The relationship between cyber-bullying and school bullying. *Journal of Student Wellbeing, 1*(2), 16-33.

- Bosse, T., & Stam, S. (2011). A normative agent system to prevent cyberbullying. In IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology (pp.425–430).
- Butler, D.A., Kift, S.M., & Campbell, M.A. (2010). Cyber bullying in schools and the law: is there an effective means of addressing the power imbalance. *eLaw Journal*, *16(1)*, 84-114.
- Calvete, E., Orue, I., Estévez, A., Villardón, L., & Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior*, *26(5)*, 1128-1135.
- Campbell, M., & Završnik, A. (2013). Should cyberbullying be criminalized? In P Smith P, G Steffgen (eds). *Cyberbullying through the New Media: Findings from an International Network* (pp. 3-19). London: Psychology Press.
- Campbell, M., Cross, D., Spears, B., & Slee, P. (2010). *Cyberbullying: Legal implications for schools*. Occasional Paper 118. Melbourne: Centre for Strategic Education.
- Campbell, M.A. (2005). Cyber bullying: An old problem in a new guise? *Australian journal of Guidance and Counselling*, *15(1)*, 68-76.
- Catalano, R., Fleming, C., Haggerty, K., Abbott, R., Cortes, R., & Park, J. (2005). Mediator effects in the social development model: An examination of constituent theories. *Criminal Behaviour and Mental Health*, *15(4)*, 221-235.
- Catalano, R.F., & Hawkins, J.D. (1996). The social development model: A theory of antisocial behavior. In *Delinquency and Crime: Current Theories*, edited by J.D. Hawkins (pp. 149–197). New York, NY: Cambridge University Press.
- ChildLine. (2013). ChildLine annual review: Can I tell you something? Retrieved January, 15<sup>th</sup>, 2015 from: <https://www.nspcc.org.uk/globalassets/documents/research-reports/childline-review-2012-2013.pdf>

- ChildLine. (2014). ChildLine annual review: Under pressure. Retrieved May, 10<sup>th</sup>, 2015 from: <https://www.nspcc.org.uk/globalassets/documents/annual-reports/childline-review-under-pressure.pdf>
- Cleveland, M.J., Feinberg, M.E., Bontempo, D.E., & Greenberg, M.T. (2008). The role of risk and protective factors in substance use across adolescence. *Adolescent Health*, 43(2), 157-164.
- Cohen, R., Lam D.Y., Agarwal, N., Cormier, M., Jagdev,J., Jin,T., Kukreti, M., Liu,J., Rahim,K., Rawat, R., Sun,W., Wang, d., & Wexler, M. (2014).Using computer technology to address the problem of cyberbullying. *Computer and Society*, 44(2), 52-61.
- Communications Act. (2003). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/2003/21/contents>
- Computer Misuse Act. (1990). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/1990/18/contents>
- Crime and Disorder Act. (1998). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/1998/37/contents>
- Crown Prosecution Service. (2015). Code for Crown Prosecution. Reprieved June, the 13<sup>th</sup>, 2015 from: [https://www.cps.gov.uk/publications/code\\_for\\_crown\\_prosecutors/codetest.html](https://www.cps.gov.uk/publications/code_for_crown_prosecutors/codetest.html)
- Daily Mail. (2103). Schoolboy, 15, bullied to death by trolls on the internet. Retrieved December, 15<sup>th</sup>, 2015 from: <http://www.dailymail.co.uk/news/article-2305332/Joshua-Unsworth-15-bullied-death-trolls-internet.html>
- Davies, M.R., & Lee, B.A. (2008). The legal implications of student use of social networking sites in the UK and US: current concerns and lessons for the future. *Education and the Law*, 20(3), 259-88.

- Defamation Act. (2013). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from:  
<http://www.legislation.gov.uk/ukpga/2013/26/contents>
- Dehue, F., Bolman, C., & Vollink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *CyberPsychology and Behaviour*, 11(2), 217-225.
- Delort, J.Y., Arunasalam, B., Paris, C., (2011). Automatic moderation of online discussion sites. *International journal of Electronic Commerce*. 15(3), 9–30.
- Department for Children, Schools & Families [DCSF]. (2007). Cyberbullying: A whole-school community issue. Retrieved June, 19<sup>th</sup>, 2015 from:  
<http://old.digizen.org/downloads/cyberbullyingOverview.pdf>
- Didden, R., Scholte, R. H. J., Korzilius, H., De Moor, J. M. H., Vermeulen, A., O'Reilly, M., et al. (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. *Developmental Neurorehabilitation*, 12(3), 146-151.
- EC Social Networking Task Force. (2009). Safer Social Networking Principles for the EU. European Commission, Luxembourg. Retrieved July 15<sup>th</sup>, 2016 from:  
[https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn\\_principles.pdf](https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf)
- Education and Inspection Act. (2006). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from:  
<http://www.legislation.gov.uk/ukpga/2006/40/contents>
- Feinberg, T. & Robey, N. (2008). Cyberbullying. *Principal Leadership*, 9(1), 10-14.
- Feinberg, T. & Robey, N. (2009). Cyberbullying: Intervention and prevention strategies. *National Association of School Psychologists*, 38(4), 1-5.
- Feinberg, T., & Robey, N. (2009). Cyberbullying: School leaders cannot ignore cyberbullying but rather must understand its legal and psychological ramifications. *The Educational Digest*, 74(7), 26-31.

- Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007). Poly-victimization: A neglected component in child victimization. *Child Abuse and Neglect*, 3(1), 7-26.
- Friedman, R. A., & Currall, S.C. (2003). Conflict escalation: Dispute exacerbating elements of e-mail communication. *Human Relations*, 56(11), 1325-1347.
- Gillespie, A.A. (2006). Cyber-bullying and harassment of teenagers: The legal response. *Journal of Social Welfare and Family Law*, 28(2), 123-136.
- Gillespie, A.A. (2006). Offensive Communications and the Law. *Entertainment Law Review*, 17, 236-239.
- Gini, G., & Pozzoli, T. (2009). Association between bullying and psychosomatic problems: A meta-analysis. *Pediatrics*, 123(3), 1059–1065.
- GOV.UK. (2015). Age of criminal responsibility. Retrieved September, 3<sup>rd</sup>, 2015 from: <https://www.gov.uk/age-of-criminal-responsibility>
- GOV.UK. (2015). Criminal justice and the law. Retrieved September, May 20<sup>th</sup>, 2015 from: <https://www.gov.uk/age-of-criminal-responsibility>
- Grigg, D.W. (2010). Cyber-aggression: Definition and concept of cyberbullying. *Australian Journal of Guidance and Counselling*, 20(2), 143-156.
- Grigg, D.W. (2012). Definitional constructs of cyber-bullying and cyber-aggression from a triangulatory overview: a preliminary study into elements of cyber-bullying. *Journal of Aggression, Conflict and Peace Research*, 4(4), 202-215.
- Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206-221.
- Hinduja, S., & Patchin, J.W. (2008). Personal Information of adolescents on the internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, 31(1), 125-146.

- Hinduja, S., & Patchin, J.W. (2015). A brief review of state cyberbullying laws and policies. Cyberbullying research centre. Retrieved May 5<sup>th</sup>, 2015 from:  
<http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf>
- Hoff, D.L., & Mitchell, S.N. (2009). Cyberbullying: Causes, effects, and remedies. *Journal of Educational Administration*, 47(5), 652-665.
- Jager, T., Amado, J., Matos, A., & Pessoa, T. (2010). Analysis of experts' and trainers' views on cyberbullying. *Australian Journal of Guidance and Counselling*, 20(2), 169-181.
- Jones, S.E., Manstead, A.S.R., & Livingstone, A.G. (2011). Ganging up or sticking together? Group processes and children's responses to text-message bullying. *British Journal of Psychology*, 102(1), 71-96.
- Juvonen, J., & Gross, E.F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *The Journal of School Health*, 78(9), 496-505.
- Katsumata, Y., Matsumoto, T., Kitani, M., & Takeshima, T. (2008). Electronic media use and suicidal ideation in Japanese adolescents. *Psychiatry and the Clinical Neurosciences*, 62(6), 744-746.
- Katz, A. (2014). The Suffolk Cybersurvey. Retrieved on December, 15<sup>th</sup>, 2015 from:  
[http://www.suffolk.gov.uk/assets/suffolk.gov.uk/Your%20Community/e-Safer%20Suffolk/2015-02-09%20Cybersurvey%202014\\_FINAL.pdf](http://www.suffolk.gov.uk/assets/suffolk.gov.uk/Your%20Community/e-Safer%20Suffolk/2015-02-09%20Cybersurvey%202014_FINAL.pdf)
- Katzer, C., Fetchenhauer, D. & Belschak, F. (2009). Cyberbullying in Chatrooms: Who are the victims? *Journal of Media Psychology*, 21(1), 25-36.
- Kerr, O.S. (2005). Digital Evidence and the new criminal procedure. *Columbia Law Review*, 15, 279-318.
- Kift, S.M., Campbell, M.A., & Butler, D.A. (2010). Cyberbullying in social networking sites and blogs: legal issues for young people and schools. *Journal of Law, Information and Science*, 20(2), 60-97.

- Kim, Y.S., Leventhal, B., Koh, Y., Hubbard, A., & Boyce A. (2006). School bullying and youth violence: Causes or consequences of psychopathology? *Archives of General Psychiatry*, 63(9), 1035-41.
- King, A. (2010). Constitutionality of cyberbullying laws: Keeping the online playground safe for both teens and free speech. *Vanderbilt Law Review*, 63(3), 883.
- Kowalski, R.M. (2009). Cyber Bullying. Unpublished manuscript.
- Kumpulainen, K., Rasanen, E., & Puura, K. (2001). Psychiatric disorders and the use of mental health services among children involved in bullying. *Aggressive Behavior*, 27, 102-110.
- Lievens, E. (2012). Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour? *International Journal of Law, Crime and Justice*, 42(3), 251-270.
- Limber, S.P., & Small, M. A. (2003). State laws and policies to address bullying in schools. *School Psychology Review*, 32(3), 445-455.
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online.
- Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. *Australian Journal of Guidance and Counselling*, 20(2), 182-193.
- Mason, K.L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45(4), 323-348.
- McCarthy, P., Rylance, J., Bennett, R., & Zimmermann, H. (2001). *Bullying: From backyard to boardroom*. (2<sup>nd</sup> ed.). Sydney, Australia: The Federation Press.

- Mishna, F., Cook C., Gadalla T., Daciuk J., & Solomon S. (2010). Cyber bullying behaviours among middle and high school students. *The American Journal of Orthopsychiatry*, 80(3), 362-374.
- Neary, A., & Joseph, S. (1994). Peer victimization and its relationship to self-concept and depression among schoolgirls. *Personality and Individual Differences*, 16, 183-186.
- NSPCC. (2015). Always there when I need you: ChildLine review: what's affected children in April 2014 - March 2015.
- Obscene Publications Act. (1959). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents>
- Ochoa, A., Ponce,J., Jaramillo, R., Ornelasa,F., Hernández, A., Azpeitiab, D., Eliasa, A., & Hernándezd, A. (2011). Analysis of Cyber-Bullying in a Virtual Social Networking. 11th International Conference on Hybrid Intelligent Systems (HIS) (pp.229-234).
- Olweus, D. (1999). Sweden. In P.K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano & P. Slee (Eds.), *The nature of school bullying: A cross-national perspective* (pp. 7-27). London & New York: Routledge.
- Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval*, 2(1-2), 1-135.
- Patchin, J.W. & Hinduja, S. (2012). *Cyberbullying prevention and response: Expert perspectives*. New York, NY: Routledge.
- Patchin, J.W., & Hinduja, S. (2006). Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148-169.
- Patchin, J.W., & Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of School Health*, 80(12), 616-623.
- Paul, S., Smith, P.K., & Blumberg, H.H. (2012). Revisiting cyberbullying in schools using the quality circle approach. *School Psychology International*, 33(5), 492-504.

- Pearce, N., Cross, D., Monks, H., Waters, S., & Falconer, S. (2011). Current evidence of best practices in whole-school bullying intervention and its potential to inform cyberbullying interventions. *Australian Journal of Guidance and Counselling*, 21(1), 1-21.
- Poland, S. (2010). Cyberbullying continues to challenge educators. *District Administration*, 46(5), 55.
- Premier's office. (2013). Cyberbullying Investigative Unit a First in Canada. Retrieved from: <http://novascotia.ca/news/release/?id=20130425001>
- Protection from Harassment Act. (1997). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/1997/40/contents>
- Public Order Act. (1986). Legislation.gov.uk. Retrieved July, 1<sup>st</sup>, 2015 from: <http://www.legislation.gov.uk/ukpga/1986/64/contents>
- Rigby, K. (2002, September 30-October 1). *How successful are anti-bullying programs for schools?* Paper presented at The Role of Schools in Crime Prevention Conference convened by the Australian Institute of Criminology in conjunction with the Department of Education, Employment and Training, Victoria, and Crime Prevention Victoria, Melbourne.
- Robinson, P.H., & Darley, J.M. (2004). Does criminal law deter? A behavioural science investigation. *Oxford Journal of Legal Studies*, 24(2), 173-205.
- Roland, E. (2002). Bullying, depressive symptoms and suicidal thoughts. *Educational Research*, 44(1), 55-67.
- Roth, D.A., Coles, M.E., & Heimberg, R.G. (2002). The relationship between memories for childhood teasing and anxiety and depression in adulthood. *Journal of Anxiety Disorders* 16(2), 149-164.

- Ruedy, M. (2008). Repercussions of a Myspace teen suicide: Should anti-cyberbullying laws be created? *North Carolina Journal of Law and Technology*, 9(2), 323-346.
- Sabella, R. A., Patchin, J.W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior*, 29(6), 2703-11.
- Samara, M. & Smith, P. (2008). How schools tackle bullying, and the use of whole school policies: Changes over the last decade. *Educational Psychology*, 28(6), 663-676.
- Schneider, S., O'Donnell, L., Stueve, A., & Coulter, R. S. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *American Journal of Public Health*, 102(1), 171-177.
- Schwartz, H.A., Eichstaedt, J.C., Kern, M.L., Dziurzynski, L., Ramones, S.M., Agrawal, M., Shah, A., Kosinski, M., Stillwell, D., Seligman, M.E., Ungar, L.H., (2013). Personality, gender, and age in the language of social media: the open-vocabulary approach. *PLoS One* 8(9), e73791.
- Sebastiani, F. (2002). Machine learning in automated text categorization. *ACM Computer Surveys*, 34(1), 1-47.
- Siegle, D. (2010). Cyberbullying and sexting: Technology abuses of the 21st century. *Gifted Child Today*, 33(2), 14-65.
- Slonje, R., & Smith, P.K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, 49(2), 147-154.
- Smith P.K., Steffgen, G., & Sittichai, R.R. (2013b). The nature of cyberbullying, and an international network. In Smith P.K., & Steffgen G. (Eds.). *Cyberbullying through the New Media: Findings from an International Network* (pp. 3-19.). London: Psychology Press.

- Smith, K.P., Smith, C., Osborn, R., & Samara, M. (2008). A content analysis of school anti-bullying policies: Progress and limitations. *Educational Psychology in Practice, 24*, 1-12.
- Smith, P., Kupferburg, A., Mora-Merchan, J. A., Samara, M., Bosley S., & Osborn, R. (2012). A content analysis of school anti-bullying policies: a follow-up after six years. *Educational Psychology in Practice, 28*(1), 47-70.
- Smith, P., Steffgen, G. (2013). *Cyberbullying through the New Media: Findings from an International Network*. London: Psychology Press.
- Smith, P.K., & Sharp, S. (1994). *School bullying: Insights and perspectives*. London: Routledge.
- Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376-385.
- Sourander, A., Klomek, A., Ikonen, M., Lineroos, J., Luntamo, T., Koskelainen, M., Ristkari, T. & Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Arch Gen Psychiatry, 67*(7), 720-728.
- Staksrud, E., & Lobe., B. ( 2010). Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report. European Commission Safer Internet Programme, Luxembourg.
- Sticca, F., Ruggieri, S., Alsaker, F., & Perren, S. (2013). Longitudinal risk factors for cyberbullying in adolescence. *Journal of Community and Applied Social Psychology, 23*(1), 52-67.
- Svensson, M. & Larsson, S. (2012). Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms. *New Media and Society, 14*(7), 1 147-1 163.

- The Sun Newspaper. (2013). Stop child torment. Retrieved February, 25<sup>th</sup>, 2015 from:  
<http://www.thesun.co.uk/sol/homepage/news/justice/4915742/aydens-law-bullying-petition.html>
- The Telegraph Newspaper. (2015). Online trick 'led to teenage boy's suicide'. Retrieved December, 15<sup>th</sup>, 2015 from: <http://www.telegraph.co.uk/news/uknews/law-and-order/11661272/Online-trick-led-to-teenage-boys-suicide.html>
- Tokunaga, R.S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277-287.
- Tresniowski, A., Truesdell, J., & Morrissey, S. (2008). A cyberbully conviction. *People*, 70(24), 73-74
- Trolley, B, Hanel, C., & Shields, L. (2006). *Demystifying and deescalating cyber bullying in the schools: A resource guide for counsellors, educators and parents*. Book Locker, Bangor, ME.
- Turnage, A.K. (2007). Email flaming behaviors and organizational conflict. *Journal of Computer-Mediated Communication*, 13(1), 43-59.
- Turnage, A.K. (2008). Email flaming behavior and organizational conflict. *Journal of ComputerMediated Communication*, 13(1), 43-59.
- Van Royen, K., Poels, K., Daelemans, W., & Vandebosch, H. (2014). Automatic monitoring of cyberbullying on social networking sites: from technical feasibility to desirability, *Telematics and informatics*, 32(1), 89-97.
- Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology and Behavior*, 11(4), 499-503.
- Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D., & Pabian, S. (2012). Police actions with regard to cyberbullying: The Belgian case. *Psicothema*, 24(4), 646-652.

- Vandebosch, S., (2014). Addressing cyberbullying using a multi-stakeholder approach: The Flemish case. In S. Van der Hof, B. Van den Berg & B. Schermer (Eds.) *Minding minors wandering the Web: Regulating online child safety* (pp.243-260). The Hague; Asser Press.
- Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. *Children and Society*, 25(1), 59-72.
- Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research*, 35(1), 3-25.
- Willard, N. (2005). I can't see you, you can't see me: How the use of information and communication technologies can impact responsible behavior. Retrieved January 30<sup>th</sup>, 2015 from: <http://www.cyberbully.org/cyberbully/docs/disinhibition.pdf>
- Willard, N. (2007). *Cybersafe kids, cyber-savvy teens: Helping young people learn to use the Internet safely and responsibly*. California: Jossey-Bass.
- Willard, N. (2007, April). Educators guide to cyberbullying and cyberthreats. Retrieved June 12<sup>th</sup>, 2015, from: <https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx>
- Willard, N. (2007a). Cyberbullying and cyberthreats: Effectively managing Internet use risks in schools. Retrieved June 12<sup>th</sup>, 2015 from: [https://www.occhd.org/system/files/1041/original/Cyberbullying\\_and\\_Cyberthreats.pdf?1281106034](https://www.occhd.org/system/files/1041/original/Cyberbullying_and_Cyberthreats.pdf?1281106034)
- Willard, N. (2007b). Cyberbullying legislation and school policies: Where are the boundaries of the "schoolhouse gate" in the new virtual world? Retrieved June 12<sup>th</sup>, 2015 from: <http://www.embracecivility.org/wp-content/uploadsnew/2012/10/cblegislation.pdf>

- Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Does online harassment constitute bullying? An explanation of online harassment by known peers and online-only contacts. *Journal of Adolescent Health, 41*(6), S51-S58.
- Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety Survey. *Pediatrics, 118*(4), 1169-77.
- Ybarra, M., Diener-West, M., & Leaf, P. (2007a). Examining the overlap in Internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health, 41*(6 Suppl 1), S42-S52.
- Ybarra, M.L., & Mitchell, K.J. (2004). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, 45*(7), 1308-1316.