

Bullying prevention and intervention strategies under UAE law

Intervention
strategies
under
UAE law

1237

Tareq Na'el Al-Tawil

*Business Law and Ethics, College of Business Administration,
Abu Dhabi University, Abu Dhabi, United Arab Emirates, and*

Salam Abdallah

*MIS, College of Business Administration, Abu Dhabi University,
Abu Dhabi, United Arab Emirates*

Abstract

Purpose – The purpose of this paper is to examine the nature of cyberbullying and corresponding strategies being used under the New United Arab Emirates (UAE) Cybercrimes Law.

Design/methodology/approach – The analysis begins with a review of the nature of cyberbullying, focusing primarily on key concepts, underlying risk factors, forms of cyberbullying and adverse effects. Background information about the nature of cyberbullying will then lay the foundation for the subsequent sections of the analysis, which will focus on preventive strategies and legislative measures. The second section of the analysis will entail a review of the legislative framework for cyberbullying in the UAE. The goal here is to examine how the UAE is responding to the emerging threat of cyberbullying in its jurisdiction. The next section will then shift gears to interventions and strategies being implemented at the global level. A global perspective is central to comparing practices in the UAE to international standards and regulations.

Findings – Findings from the analysis have shown that the UAE has the most robust and comprehensive cyberbullying laws internationally. Nonetheless, the New Cybercrimes Law is ambiguous, and it is not expressively specific to cyberbullying. The law does not have a clear definition of cyberbullying, as well as the scope of its application to specific cases involving students. A comparative analysis across jurisdictions has revealed that most countries neither have specific cyberbullying laws nor explicitly define the phenomenon in existing laws. Thus, cyberbullying is a gray area in the UAE national law, requiring a clear definition and scope of application. The courts will establish case law that will finally address the current definitional challenges and extend of applying the New Cybercrimes Law.

Originality/value – The analysis concludes with the application of international best standards and practices to the UAE context, focusing specifically on how to strengthen laws and procedures in the UAE.

Keywords Cyberbullying, Cybersecurity, Cybercrimes, New UAE Cybercrimes Law

Paper type Research paper

Introduction

Cyberbullying is an emerging and concerning problem in the United Arab Emirates (UAE). For instance, the 2019 Cartoon Network MENA Survey revealed that at least 85% of school children in the UAE had experienced bullying, mostly on online platforms, with only 50% of parents aware of this fact (Masudi, 2019). According to the survey, cyberspace is increasingly changing the landscape of bullying because most cases are psychological and take place online rather than inside schools (Masudi, 2019). Moreover, 56% of Emirati parents identified cyberbullying as a pressing concern for their children based on findings from the “Responsible Digital Parenting” survey, which Intelligent CIO conducted in 2021



Journal of Financial Crime
Vol. 31 No. 5, 2024
pp. 1237-1251
© Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-07-2023-0171

(Banda, 2021). Cases of cyberbullying significantly increased during the global COVID-19 pandemic. Notably, the pandemic increased the use of technological devices in the wake of widespread lockdowns and school closures. Increased exposure to the internet subsequently exposed children to cases of online harassment, bullying and victimization. A combination of these issues highlights the need for proactive measures that will prevent future exposure and harm from cyberbullying.

The purpose of this analytical paper is to examine the nature of cyberbullying and corresponding strategies being used in the UAE. The analysis begins with a review of the nature of cyberbullying, focusing primarily on key concepts, underlying risk factors, forms of cyberbullying and adverse effects. Background information about the nature of cyberbullying will then lay the foundation for the subsequent sections of the analysis, which will focus on preventive strategies and legislative measures. The second section of the analysis will entail a review of the legislative framework for cyberbullying in the UAE. The goal here is to examine how the UAE is responding to the emerging threat of cyberbullying in its jurisdiction. The next section will then shift gears to interventions and strategies being implemented at the global level. A global perspective is central to comparing practices in the UAE to international standards and regulations. Finally, the analysis concludes with the application of international best standards and practices to the UAE context, focusing specifically on how to strengthen laws and procedures in the UAE.

Cyberbullying: ambiguity in definition

The concept of “cyberbullying” is particularly complex and challenging considering its relationship with traditional forms of bullying. Hence, a clear definition of cyberbullying is necessary to minimize legal ambiguity (Notar *et al.*, 2013, p. 2). Such clarity will be useful when examining the effectiveness of UAE’s cybersecurity laws.

An enduring question confronting researchers and policymakers is whether bullying and cyberbullying are the same concepts. The issue often arises because perpetrators of the traditional form of bullying are the same in the case of cyberbullying. Additionally, there is a strong, positive relationship between being a victim of both bullying and cyberbullying. Psychological effects are also the same in both cases, although victims of cyberbullying report severe outcomes than those who experience the conventional form of bullying (Englander *et al.*, 2017). However, there is no definitive evidence to support the assertion that the psychological impact of cyberbullying is greater than that of traditional bullying. Three features that define bullying, namely, intent, repetition and power imbalance, are not always transferrable to digital behaviors. Digital environments where cyberbullying occurs have unique qualities that render both bullying and cyberbullying distinct in terms of motivations, circumstances and outcomes (Englander *et al.*, 2017, p. 149). Consequently, it is necessary to begin this section with a conceptual definition of cyberbullying versus bullying.

Traditional bullying versus cyberbullying

There is no consensus about the definite definition of cyberbullying. However, the use of digital technology or electronic means to bully or repeatedly inflict harm is a crosscutting definition. For example, Lee, Abell and Holmes define cyberbullying as an aggressive behavior committed using information and communication technology with the intention of harming others (Lee *et al.*, 2017). Similarly, Tokunaga defines cyberbullying as an intentional and repeated act of hurting someone through the internet (Tokunaga, 2010). The two definitions reinforce the relationship between bullying and the use of digital media. The definitions also align with the three criteria included in the definition of traditional bullying: intent, power imbalance and repetition. The three characteristics of an aggressor/perpetrator are important because they

predict the negative impact of bullying on the target. An important observation from most of the definitions is the distinction between the two forms of bullying based on setting. Traditional bullying is specific to the school environment, while cyberbullying takes place on the internet or through digital media (Englander *et al.*, 2017, p. 149).

Traditional bullying and cyberbullying usually interact with in-school interactions between perpetrators and targets. Events that happen at the school can trigger cyberbullying, which then causes problems at school. Cyberbullying involving children and adolescents usually involves peers who know each other from the school setting. Consider the case where targets of cyberbullying usually identify their perpetrators as school peers or classmates (Tokunaga, 2010, p. 278). As such, it can be argued that cyberbullying could be another form of traditional bullying. Notably, cyberbullying could be conceptualized as an extension of bullying from the school playground or environment. Bullying is no longer confined to the schoolyard and classrooms following the rapid expansion and use of electronic and internet-based communication among school-aged children and adolescents. The anonymity and privacy of the internet has now made cyberbullying more appealing than the traditional forms of bullying. Cases of cyberbullying are also increasing because the internet and digital media give cyberbullies a false sense of courage unlike face-to-face encounters (Slonje *et al.*, 2013).

The school playground and hallways have always been important venues for traditional forms of bullying. Nevertheless, cyberbullies are now using the internet, specifically social media and mobile phone applications, to cause psychological harm to their targets. Cyberbullies are now harassing, disrespecting, teasing, or isolating their classmates by sending text messages, instant messages, e-mails, photos and videos via smartphones, computers, tablets and other digital mediums. The use of diverse digital modalities to perpetrate acts of psychological violence makes cyberbullying an insidious form of traditional bullying (Notar *et al.*, 2013, pp. 1-9). A notable observation is that cyberbullies continue to inflict harm even when their targets are in the comfort and safety of their homes. Moreover, it is much easier to identify bullies on the playground than it is on the internet, social media and other digital platforms. The privacy afforded by the internet also makes it hard for parents and teachers to find out whether children are being bullied or bullying their peers. The two examples exemplify how it is difficult to assess intent, repetition, and power imbalances between cyberbullies and their targets (Englander *et al.*, 2017, p. 149).

Intentionality. Intentionality is an important element of cyberbullying because it establishes the grounds for legal action. Bullies usually have different reasons for bullying others, but the intention is always to cause harm and inflict fear. Nonetheless, judgment of intentionality becomes problematic in cases of cyberbullying. A case of cyberbullying can be either direct or indirect, general or specific, which makes it difficult to establish intentionality. A notable example is when an individual shares an offensive message, photo or video on the internet where third parties transmit the same on their social media accounts (Slonje *et al.*, 2013, p. 28; Notar *et al.*, 2013, p. 3). A practical challenge here is determining whether the intention of the primary perpetrator was to have the message or video/photo distributed to a large audience. Thus, cyberbullying suffers the challenge of differentiating general from specific intention. General intent is easy to determine because there is intentionality to engage in bullying and cyberbullying behavior. In contrast, specific intention requires proof that the intention of the perpetrator was to achieve a particular outcome by engaging in cyberbullying behavior (Slonje *et al.*, 2013, p. 28).

The difference between general and specific intention questions the type of intent to include in the definition of cyberbullying and corresponding laws. General intention is the most appropriate standard for defining cyberbullying and associated laws since the quest

for specific intent could be unfair or too harsh in its application. Specific intent is particularly difficult to prove if a cyberbullying case involves people with intimate or close relationship. An example is when a person repeatedly sends text messages or shares intimate photos to woo another one into an intimate relationship. A general intention standard requires the target to simply prove that the intention of the perpetrator amounts to sexual harassment. Conversely, a specific intent standard is difficult to determine because the perpetrator could argue that the purpose was to express love and affection rather than harass, cause fear or inflict pain. The situation means that it would be much easier to institute action based on the general intent standard and not the one for specific intent (Navarro, 2016). Thus, the outcome of cyberbullying, which entails reasonable harm to the target, becomes more important than the intention.

The issue of general and specific intention calls for revisiting the criterion for assessing intentionality in cyberbullying. Specifically, the definition of cyberbullying should not be confined to only intentional behavior. On the contrary, unintentional but negligent and reckless use of social media or the internet should be part of the definition of cyberbullying. For example, sending or sharing humiliating messages about a person does not fit into the definition of general intent of cyberbullying if the actions are either unintentional or indirect. General intentionality of nondeliberate forms of cyberbullying can be legally null and void since the perpetrator is not targeting an intentional target. Nevertheless, general intentionality becomes plausible if the definition of cyberbullying includes the failure to reasonably foresee that unintentional behavioral or actions could reach an intentional target and subsequently cause irreparable harm (Díaz and Fite, 2019). The technical application of the general intent standard may be different in this case, but the focus shifts from intention to personal responsibility and outcomes to the target.

Repetition. Repetition is a precursor of severity in both traditional bullying and cyberbullying. Thus, there is a strong correlation between repetition and the severity of outcomes of bullying, regardless of the type. For instance, long-term exposure to cyberbullying is more likely to cause severe psychological outcomes. Nonetheless, the repetition criterion is also problematic in the definition of cyberbullying. The problem with the repetition criterion is the possibility of discounting a single episode of cyberbullying as not reaching the threshold of causing severe outcomes. In essence, the repetition criterion may lead to a situation where authority could dismiss the first episode of cyberbullying even when it amounts to clear violation (Slonje *et al.*, 2013, pp. 29-30). Therefore, repetition may not count as a definitional element of cyberbullying but rather a gatekeeper determinant of whether an incident is severe or less severe. Effectively, repetition can be conceptualized as an index of severity, like in the case of intention, instead of an element that defines cyberbullying itself (Aliyev and Gengec, 2019).

Moreover, repetition can potentially have multiple meanings in the context of cyberbullying. A charge of traditional cyberbullying stands when a perpetrator targets their victims with repeated aggression and distressful actions. An example is where a specific student gets bullied everyday along the hallways or on the playground. Harassment then occurs more than once in this case. The same situation can be replicated in cyberspace, whereby a cyberbully constantly sends offensive or threatening messages to their targets. Thus, the repetition criterion emphasizes the number of episodes or incidents of cyberbullying. On the other hand, there is another definition of repetition that is unique to cyberbullying. The second form of repetition entails a single incidence of cyberbullying that repeatedly transmits offensive materials against a target to often an unknown and ever-expanding audience. This form of repetition effectively extends the duration of a single cyberbullying incident or gives it a multiepisodic character (Beghin, 2020). Thus, repetition is more than the temporal duration of the cyberbullying incident.

Power imbalance. A key question that emerges is about the kind of power that a bully has. The power can be either physical or psychological within the context of traditional bullying. For example, the physical appearance of a perpetrator is always intimidating to their targets. Students with a large body frame are more likely to bully those who are petite or appear to be physically weak. Physical power can also have a direct bearing on psychological power. Well-build students normally garner respect, admiration and popularity among peers, which are key attributes of psychological power. The defining characteristics of psychological power include having more prestige and status, more friends and greater access to valued resources (Beghin, 2020, p. 19). As such, psychological power imbues a sense of superiority that aggressors exploit to torment or intimidate those perceived to be weak or helpless. However, the power imbalance is visible when there is physical interaction or contact between perpetrators and targets.

The need for physical contact between aggressors and targets of bullying questions whether the domain of power imbalance is applicable to cyberbullying. The question is important because the goal of any law is to offer redress to those who feel victimized because of their inherent powerlessness. The law then becomes the only recourse for the weak and defenseless. Thus, an important issue to consider is the meaning of power imbalance in the context of cyberbullying. Cyberbullying presents additional implications for understanding power imbalance from the perspective of traditional bullying (Beghin, 2020, p. 20; Slonje *et al.*, 2013, p. 30). Social status is perhaps the first place to start when examining the balance of power in cyberbullying. Cases of cyberbullying are undoubtedly higher among adolescents because of the critical phase of their development. Adolescents often crave for social status and recognition as they navigate through the challenging developmental stage. Unlike traditional bullying, social status becomes invisible in cyberbullying given the disempowering consequences (Slonje *et al.*, 2013, p. 30).

The invisibility of social status exemplifies how it is difficult to define power imbalance in cyberbullying context. The absence of physical contact between the cyberbully and victim further amplifies this problem. Some researchers have conceptualized power imbalance in cyberbullying based on the technological savviness of cyberbullies. A recurrent conceptualization is that cyberbullies use their advanced knowledge of and expertise in technology to perpetrate acts of aggression against those perceived to know nothing about technology. A notable example is where victims of cyberbullying may not know how to block or stop the spread of offensive content on social media or the internet. Consequently, cyberbullies take advantage of their targets' technological naivety to inflict harm while remaining anonymous (Englander *et al.*, 2017, p. 150). An argument that arises is that the mere fact of anonymity establishes power imbalance between the cyberbully and target. Nevertheless, anonymity is only sufficient to establish the threshold of power imbalance if cyberbullying is indeed anonymous (Slonje *et al.*, 2013, p. 31; Englander *et al.*, 2017, p. 150).

Three observations emerge from the foregoing discussions. First, the use of digital media differentiates cyberbullying from traditional bullying. Second, cyberbullying is a form of bullying that extends beyond the confines of the school setting. The first two factors demonstrate the potential difference between bullying and cyberbullying based on six factors. First, cyberbullying is ubiquitous in the sense that the presence of an electronic device makes one susceptible to cyberbullying. Second cyberbullying is anonymous, whereby the identity of the perpetrator can be a mystery to the targets. Third, cyberbullying can be universal in terms of the physical distance between the aggressor and target. Fourth, it is difficult for teachers and adults to detect cases of cyberbullying especially if they are not technological savvy. Fifth, cyberbullying is of variable duration given that offensive content can stay on the internet for longer or leave an indelible trail. Sixth, cyberbullying has an

unknown, infinite audience that can worsen the experience for affected individuals (Englander *et al.*, 2017, p. 150).

The third observation is that cyberbullying aligns with the three features of traditional bullying: intentionality, repetition and power imbalance, as presented beforehand. The third point is important to this discussion because intention, repetition and power imbalance are definitional principles used in most definitions of cyberbullying. However, ambiguities arise when applying the three definitional principles to both bullying and cyberbullying (Englander *et al.*, 2017, p. 150). For instance, an intentional act, such as a bad joke, may unintentionally harm a recipient. A pertinent question that arises is how to assess and quantify an intent to harm. Specifically, it is difficult to determine whether an intent to harm has the same threshold as an awareness of harm. The subjective nature of intent then makes it hard to legislate cyberbullying because it becomes difficult to differentiate bullying and cyberbullying from playful teasing and similar cases. Repetition and power imbalance are also problematic in the context of cyberbullying. An important concern is whether cyberbullying should constitute a single event that causes significant harm, repetitive exposure to a specific form of cyberbullying, or both cases (Slonje *et al.*, 2013, p. 30).

Ambiguities inherent in the three definitional principles have blurred the conceptualization and legislation of cyberbullying. The use of “banter” brings into perspective definitional ambiguities. Banter, which is a common concept on Twitter, involves friendly and playful exchange of teasing remarks. Banter does not constitute all the elements of bullying since the intention is not to cause harm. There is also no power imbalance considering that banter usually involves acquaintances on social media. An issue that emerges is whether banter should be an acceptable form of interaction on social media simply because it does not encompass all the components of bullying (Englander *et al.*, 2017, p. 150). How then should the law navigate these ambiguities, like in the case of banter? The question is critical to avoid ambiguous application of the law or the possibility of over-legislation. A notable observation across jurisdictions is when citizens view anticyberbullying laws as an attempt to curtail free speech. Thus, it is necessary to understand these ambiguities when examining the scope and application of cyberbullying laws.

The effectiveness of cyberbullying laws is as good as the definition of this concept. Existing evidence has drawn parallels between bullying and cyberbullying, describing cyberbullying as an extension of the traditional form. Such conceptualization then complicates the scope of application of cyberbullying laws. The main concern is whether cyberbullying laws should be confined to schools or the general population. The issue is important considering that cyberbullying is a public issue despite being pervasive among school and college students. Schools have established policies and regulations to combat cases of traditional bullying (Englander *et al.*, 2017, p. 150; Tokunaga, 2010, p. 278). As such, a key question is whether cyberbullying laws are necessary considering the parallels with traditional bullying. An enduring argument is that cyberbullying laws should be school- or institutional-based rather than embedded in national laws since cases of cyberbullying are unique to school children and young people. Nonetheless, national laws are also necessary to address cases of cyberbullying that involve adults, such as sexual harassment, stalking, revenge porn and sharing of intimate photos/videos without consent.

A brief comparative analysis shows that countries have taken different approaches to combat cases of cyberbullying. For example, the United States (US) and the United Kingdom (UK) have adopted laws that are specific to cyberbullying. These laws have primarily arisen from high profile cases of cyberbullying reported in the media. Comparatively, other countries have rather adopted general laws and regulations that govern online crimes. For instance, most of the countries in the Gulf region, including the UAE, have enacted general

cybercrime laws with the goal of punishing different types of crimes committed online or through electronic means. Therefore, the next section shifts focus to the presentation of cyberbullying laws in the UAE. An examination of the UAE legislative and regulatory landscape will lay the foundation for determining the effectiveness of existing laws to combat escalating cases of cyberbullying. The goal of the analysis is to find out if the ambiguity inherent in the definition of cyberbullying has extended to the current laws in the UAE.

Cyberbullying law in the UAE

The UAE Government recently published in the Official Gazette the Federal Decree-Law No. 34 of 2021 Concerning the Fight Against Rumors and Cybercrime (the New Cybercrimes Law) on 26 September 2021. The New Cybercrimes Law was a repeal of the Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes (the Cyber Crimes Law). Therefore, an analysis of the Cyber Crimes Law is necessary to establish the foundation for reviewing the effectiveness of the New Cybercrimes Law. The primary objective of the Cyber Crimes Law was to criminalize persons who gained unauthorized access to an electronic information system, computer network or website. The Cyber Crimes Law also penalized individuals who indulge in omitting, destructing, copying, deleting, modifying, altering, deteriorating or publishing any information or data ([Saleem, 2023](#)).

The Cyber Crimes Law divided cybercrimes into multiple categories: unauthorized access to an electronic site, forgery, medical data, bank account data, activities that prejudice public morals, defamation, invasion of privacy, human trafficking and terrorist activity. Other categories included collection of donations without authority, state security and reputation, narcotics and money laundering, deportation, state security and exemptions [1]. Thus, the Cyber Crimes Law was a comprehensive legal framework to combat rising cases of cybercrimes. Cyberbullying fell under two categories: defamation and invasion of privacy. The Cyber Crimes Law defines defamation as the use of a computer network to accuse or insult another person of a punishable matter. Offenders were liable for imprisonment and a fine of 250,000–500,000 AED or either of the two penalties. On the other hand, the penalty for invasion of privacy entailed at least six months in prison and a fine ranging between 150,000 AED and 500,000 AED, or either of the two penalties ([Mazhar, 2019](#)). The purpose of the stringent laws was to ensure deterrence against cybercrimes, including cyberbullying.

The Cyber Crimes Law established the foundation for strengthening cybersecurity laws and regulations in the UAE. For instance, Cybercrime New Amendment Number 2 of 2018 amended the Cyber Crimes Law increasing the range of sanctions and financial penalties under Articles 26, 28 and 42. Consequently, the Cybercrime New Amendment elaborated cybercrimes by emphasizing the negative effects that the misuse of social media, websites and other online platforms could have on national security, social stability and cohesion among persons from diverse backgrounds ([Agarib, 2018](#)). The Cybercrime New Amendment specifically introduced new measures that include restrictions and probation on the use of electronic mediums, obligatory deportations and other punitive/hefty sanctions. The amended law also broadened the scope of incidents involving serious electronic crimes ([Agarib, 2018](#)). Therefore, the New Cybercrimes Law should be examined in line with both the Cyber Crimes Law and Cybercrime New Amendment to determine its effectiveness in combating cases of cyberbullying. Findings from the evaluation will then establish the basis for future reforms and best practices.

The New Cybercrimes Law has come into effect at a time when the UAE is experiencing a rapid increase in cases of cybercrimes. The UAE has assumed a leading role in digitizing government functions and operations. The unified smart city concept that was enshrined in

the UAE Vision 2021 illustrates how the development and adoption of advanced technologies has been UAE's national priority. Vision 2021 was UAE's national agenda that exemplified the country's commitment to becoming one of the world's innovative/smart cities. Consider the example where Abu Dhabi and Dubai are among the top ten smartest cities in the world, illustrating UAE's quest of becoming the "smartest" nation on the global level. Conversely, the frequency and risk of cyber threats have increased drastically with the country's technological revolution (Mazhar, 2019). Both the Cyber Crimes Law and Cybercrime New Amendment focused on protecting institutions and businesses from cybercrimes. The New Cybercrimes Law has now expanded these protections to residents and citizens by recognizing the ever-growing threats in the digital era.

The New Cybercrimes Law has key amendments that cover a wide range of areas. Common ones include criminalization of keeping or disclosing the geographical location of a third party without his/her consent, cyberbegging, spreading rumors, promoting adverts that mislead consumers, fake news, conducting surveys without a license and capturing photos of third parties without their consent. These amendments touch on cyberbullying because they have introduced new offences that regulate social media use, such as dissemination of misinformation and fake news (Chandra *et al.*, 2019). The scope of the New Cybercrimes Law has expanded to include cybercrimes that have been planned, prepared, supervised, directed and financed in the UAE or those that otherwise undermine the interests of the country or its citizens and residents. The New Cybercrimes Law has also replicated in similar terms most cybercrimes from the amended law while others have been reintroduced to suit specific sectors or have broader definitions. Banking, health, media and scientific institutions have been identified in the New Cybercrimes Law as essential sectors in the country (Chandra *et al.*, 2019).

The New Cybercrimes Law has received both applause and criticism across the board. Proponents of this law have argued that the addition of new offenses and broadening of existing ones will ensure responsible use of social media, which has become a source of fake news and hate crimes. Conversely, an analysis from a personal perspective shows that the New Cybercrimes Law has ambiguous and vague definitions on first impression. The question of ambiguity is inevitable, considering that the New Cybercrimes Law is still a nascent legislation that has been in operation for slightly over a year. Courts in the UAE will ultimately clarify the current ambiguity as the law becomes fully operational. Specifically, court cases and resulting judgments will establish jurisprudence for the New Cybercrimes Law, laying a clear mapwork for application. The next step is to examine how the New Cybercrimes Law applies specifically to cyberbullying by exploring its strengths and weaknesses, as well as potential gaps that could inform future amendments.

Cyberbullying within the confines of the new cybercrimes law

The New Cybercrimes Law has several provisions that are specific to cyberbullying. Invasion of privacy is the foremost criminal offence included in the New Cybercrimes Law. The New Cybercrimes Law criminalizes anyone who uses an information network to infringe on the privacy of another person's familial or private life without their consent. Cyberbullying exists in many forms, but they all involve the abuse and misuse of online technologies (Chandra *et al.*, 2019, p. 2805). Thus, the New Cybercrimes Law has established a comprehensive legal framework to address the concerns relating to the misuse and abuse of online technologies. The overarching goal of the New Cybercrimes Law is to strengthen the scope of protection from online crimes committed using information networks, technology and platforms (Bano, 2022). The breach of another person's online privacy is an important provision to consider when examining how the New Cybercrimes Law affects

cyberbullying. Ongoing discussions about the merits and demerits of the new law focus mostly on taking, posting and sharing pictures of other people on social media networks without their permission or consent.

Article 44 of the New Cybercrimes Law expressly prohibits and sanctions related to the violation of privacy and disclosure of secrets. Taking photographs of other people either in private or public is one of the five offenses included in this Article. Therefore, it is necessary to consider all the five provisions to avoid the tendency of reducing Article 44 to taking and posting pictures on social media. The first offense under Article 44 is eavesdropping, interception, recording, communication, transmission or disclosure of conversations, communications or audio or video materials. The second one is taking photographs of others at any public or private place or preparing, communicating, exposing, copying or keeping electronic images thereof. The third one is spreading news, electronic images, photographs, footages, comments, data or information, even if true and correct, to harm such person. The fourth one is taking, communication or publication of photographs of the casualties, dead persons or victims of accidents or disasters without permission or consent of the concerned persons. The fifth one is tracking, detecting, disclosing, exposing, copying or keeping data of geographical sites of third parties (Abou Assy, 2022).

Article 44 has broad provisions and offences that have a direct bearing on cyberbullying. Two conditions are necessary for the five activities to become criminal offences: intention and consent. First, the use of a computer network, electronic information system or information technology is a criminal offence under Article 44 if the intention of the perpetrator is to attack another person's privacy or the sanctity of an individual's family or private life. Second, the New Cybercrimes Law considers these activities to be criminal if perpetrators commit them without the consent or permission of the affected targets (Bano, 2022). An emerging question is how the provisions under Article 44 aligns with the offence of cyberbullying. Article 44 explicitly mentions the use of an electronic information system or any other channels of information technology with the intent of manipulating or modifying an image, recording or scene. The intention of the manipulation/modification is to offend or defame another person (Abou Assy, 2022). Thus, Article 44 provides a broad definition of cyberbullying by emphasizing three conditions: the use of electronic media, intention to harm and lack of consent.

Cyberbullying causes adverse psychological effects when people use technology in a wrong manner. Technology, as captured in Article 44, becomes a medium of abuse and violation of privacy in two ways. The first way entails using technology to bully people who may not even be aware of the damage being done. There is a growing trend where people are shocked when they find their private videos or photos posted on the internet without their knowledge, a phenomenon called revenge porn or nonconsensual pornography. Revenge porn is devastating because social media makes it convenient to share private photos and videos to millions of people across the globe. The targets are usually powerless because they can neither stop the spread nor delete them from the online footprint. The second means involve deliberately abusing technology to commit acts of cyberbullying and take advantage of others. A notable example is when a third-party gains unauthorized access to people's private data through hacking or similar activity. The perpetrator then uses the information to blackmail the affected targets for financial gain, sexual favors or other intentions (Saleem, 2023).

Defamation is a serious crime that demonstrates how the New Cybercrimes Law navigates the issue of cyberbullying. In fact, defamation is at the core of the New Cybercrimes Law, which underscores the importance that the UAE places on cyberbullying. The New Cybercrimes Law covers the offense of defamation under Article 20, which cites

two incidents where an electronic site can be used to defame others. The first instance entails insulting others using an electronic channel. The second one involves slandering others by attributing to them to incidents that lead to either the punishment or public contempt (Abou Assy, 2022). The example of revenge porn is a clear demonstration of the second incident of defamation. Thus, the offense of defamation broadens the scope of the New Cybercrimes Law. For example, defamation, which includes insult or slander, was only applicable to the state and state officers in the repealed law. However, the scope has now extended to citizens and residents of the UAE. The New Cybercrimes Law is now much broader, and it seems to be emphasizing the use of social media networks to insult and/or slander others (Bano, 2022).

Fake news and misinformation are other offences enshrined in the New Cybercrimes Law. Dissemination of fake news and other forms of miscommunication have a broader scope in the New Cybercrimes Law compared to the repealed law. As in the case of defamation, the New Cybercrimes Law does not confine to false information involving the state or state officials. The COVID-19 pandemic marked a new wave of fake news and misinformation. The problem was pervasive across social media networks. Accordingly, the New Cybercrimes Law included the new offence of fake news and misinformation as part of a broader package in the fight against cyberbullying. The new law now makes users responsible for the content and information that they create and publish online. Additionally, the new law also obligates social media platforms and internet service providers to ensure that their sites are not safe havens for cybercriminals and bullies. The New Cybercrimes Law specifically imposes explicit penalties on persons in charge of companies although there is need for evidence to prove that they were complicit in preventing commission of cybercrimes (Bano, 2022; Saleem, 2023).

From the foregoing discussions, cyberbullying is an illegal activity in the UAE under the New Cybercrimes Law. The new law explicitly criminalizes the use of technology to defame, harass, and insult others, imposing hefty penalties that include imprisonment, fines or both. The new law has maintained the same trend of setting minimum and maximum penalties depending on the type of crime committed. For example, sanctions for spreading fake news or misinformation include at least one year of imprisonment, a fine of not less than AED 100,000, or both. A defamation charge carries a fine of not less than AED 250,000 and not exceeding AED 500,000. Courts in the UAE have the discretion to make independent decisions and establish the jurisprudence for the New Cybercrimes Law. The fines and penalties serve as a guidance for courts when ruling on cases before them. There are currently no court cases and decisions related to the New Cybercrimes Law. However, a recurrent trend based on decisions under the repealed law shows that courts are applying the maximum penalty for cybercrimes and related crimes.

Scope of application and legal ambiguities. An analysis of the New Cybercrimes Law reveals two important issues that are central to its application, relevance and effectiveness in the context of cyberbullying. First, the New Cybercrimes Law does not explicitly define cyberbullying, including its forms and characteristics. Thus, cyberbullying can only be implied rather than certain in the New Cybercrimes Law. Second, the New Cybercrimes Law is indeed comprehensive and covers broad areas, but provisions therein are ambiguous. Ambiguity is important in this case because a law or piece of legislation is as good as the language used to define it. Ambiguous and unconcise laws/legislation cannot achieve the desired goals or outcomes. As mentioned, the courts will have an opportunity of clarifying ambiguous clauses and provisions as they apply them to case law, as well as establish jurisprudence. Case law is still nascent considering that the New Cybercrimes Law came into effect in the last quarter of 2021. However, the absence of robust case law does not in any way nullify a critical analysis of the New Cybercrimes Law. The analysis will focus on two issues: lack of definitional clarity and ambiguity.

The absence of a clear definition of cyberbullying and ambiguous provisions are key features of the New Cybercrimes Law. An analysis of the two elements is critical because of the profound impact that they could have on the application of the law to cases of cyberbullying. The two elements are important considering that the New Cybercrimes Law, as it currently exists, has been crafted to deal with other forms of cybercrimes. The law does not specifically target cyberbullying as a specific area of focus. Hence, the New Cybercrimes Law has overlapping and confused provisions within it. A practical challenge arises when cyberbullying becomes a mere act of committing a crime that is already in an existing law or legislation. For example, one could argue that cyberbullying is merely traditional bullying propagated through a different medium. Thus, legislative intervention becomes immaterial because existing laws can cover acts of cyberbullying. The New Cybercrimes Law aligns with this argument because it acknowledges crimes committed via electronic media but fails to expressly mention cyberbullying.

The New Cybercrimes Law does not provide an explicit definition of cyberbullying, posing a significant challenge. The definition of cyberbullying is unclear in research literature, as explored earlier in the paper. The issue has also spilled over to the New Cybercrimes Law. A pressing challenge for both researchers and policymakers is to conclude whether cyberbullying and traditional bullying overlap or are different. Discussions herein have shown that the definition of traditional bullying based on intentionality, repetition and power imbalance creates some fundamental tensions in the context of cyberspace. The tension then makes it hard to define cyberbullying, specifically locating the nexus between intentional and unintentional behavior (Englander *et al.*, 2017, p. 151). The New Cybercrimes Law has effectively identified specific forms of misusing the internet, which can fall within the purview of cyberbullying. However, the question of intentionality remains unclear in the absence of a concise and explicit definition of cyberbullying. A key concern that researchers and policymakers could encounter is whether cyberbullying is synonymous with or an element of cybercrime.

Moreover, cyberbullying is a murky area from a legislative perspective because of the uniqueness of social media. Cyberbullying indeed takes many forms, but social media has been central in propagating cases. Social media has gained prominence and acceptance among young people because it allows them to exercise freedom of speech and association. Young people also rely on social media to establish social connections and engage in captivating activities, such as creating and sharing content (Tokunaga, 2010, p. 278). Social media has now evolved to become a powerful tool of communication with unique interactions and codes of dialogue. Consider the case where jokes and banter are commonplace and acceptable in the context of social media communication. The same language is unacceptable in other forms of social interactions and communication outside social media. Consequently, content posted online could potentially fall under the confines of a personal statement of opinion and not harassment (Tokunaga, 2010, p. 278). A legal dilemma emerges when banter and offensive comments are acceptable in the context of social media but unintentionally reaches millions of unintentional audiences.

Cyberbullying presents a potential gray area in the New Cybercrimes Law given the uniqueness of online or internet-based communication. Banter and jokes once again illustrate the peculiarity of social media communication and dialogue, aligning with the challenge of intentionality. As discussed earlier, banter and jokes are acceptable forms of communication and interaction on social media. A dilemma arises when banter meant for a specific person or group within social media reaches millions of unintended audiences. The New Cybercrimes Law is ambiguous on this issue because the law only recommends blanket penalties for cybercrimes. The new law does not foresee a situation whereby some of the outline cyber offenses could be acceptable and justified in social media circles. A notable example is where a perpetrator escapes responsibility for an unintentional banter that goes viral and causes distress to the aggrieved party. Thus, the New Cybercrimes Law has a gray

area in this respect because the law does not draw a clear line between intentional and unintentional behaviors in cyberspace.

Comparative analysis

A comparative analysis is of the essence to identify best global practices and their application in the UAE context. The USA does not have a formal federal law that applies specifically to cyberbullying. Consequently, local and state authorities have the express mandate of legislating cyberbullying. In total, 48 US states had electronic harassment laws that explicitly included cyberbullying, as of January 2021 ([Cyberbullying Research Center, 2023](#)). Forty-four of these states included criminal sanctions in their cyberbullying laws. State policies, laws and regulations are diverse and continue to evolve in the USA. Nonetheless, laws and policies promulgated at the local and state levels have common components. All state legislations include definitions and defining features associated with bullying behaviors ([Cyberbullying Research Center, 2023](#)).

A notable observation across the USA is the key roles that school districts and school administration play in addressing cyberbullying. Local and state legislators have enacted laws that require school districts to develop cyberbullying policies and regulations. States also require that all schools have a formal policy for identifying and combating cases of bullying, including cyberbullying. Comparatively, the UAE has a comprehensive federal legislation for cyberbullying, unlike the case of the USA. The New Cybercrimes Law is the most comprehensive legislation in the region and globally, highlighting the government's tough stance on cyberbullying. However, Abu Dhabi and Dubai also have specific, local laws to combat cyberbullying, which align with federalism in the USA. An observation here is that devolved systems of government have express authority to legislate cyberbullying based on local circumstances. The UAE also acknowledges the role of school authorities in dealing with cases of cyberbullying. For example, the UAE Ministry of Education released guidelines in the wake of the pandemic to outline the roles and responsibilities of all schools' community members ([UAE Ministry of Education, 2023](#)).

Federalism is also visible in Canada and Australia. Canada addresses issues of cyberbullying under the Criminal Code. Criminal elements of cyberbullying are consistent across Canada because criminal law is federally regulated in the country. However, provinces and territories have their own regulations and guidelines. Furthermore, court decisions also vary across the provinces and territories. The Canadian Education Act has specific guidelines for schools to follow when handling cases of bullying and cyberbullying. For instance, perpetrators of cyberbullying face school suspension while repeat offenders may face a jail term or expulsion ([Government of Canada, 2023](#)). The Canadian Criminal Code uses the same language as the one in the New Cybercrimes Law with respect to publication of a libel that is either false or causes injury, ridicule, contempt or hatred to the affected person. On the other hand, cyberbullying laws vary across territories in Australia under the Federal Nature of Law. Laws in each Australian territory fall under three categories: Articulate of Industry Codes, Actions by State and lawsuit by victims ([Taylor, 2023](#)).

The European Union (EU) does not have a legal framework for regulating issues related to cyberbullying both directly and comprehensively. Some countries in the EU have adopted specific cybersecurity laws that apply to the local context while others do not have them. For example, Poland has designated cyber stalking as an illegal activity while the UK's Malicious Communications Act has specific penalties for cyberbullying, including six months or more in prison and a fine. However, the Convention on Cybercrime and European Data Protection Legislation is an international law being applied to address problematic areas in the EU. The European Commission has also partnered with 17 of the global leading

social media networks, including MySpace and Facebook, to protect young people from cyberthreats and stop online bullying. The UAE has adopted a different approach from the one in the EU. Specifically, the New Cybercrimes Law includes penalties for social media companies found to be implicit in identifying and stopping the spread of fake news and misinformation (Bano, 2022; Saleem, 2023).

Countries are also acknowledging and reinforcing the role that social media networks must play to protect children from cyberbullying. Notably, China has taken a similar approach to the one in the UAE by requiring service providers to implement necessary measures against cyberbullying. Parents and guardians of cyberbullied minors have a right to compel service providers to block, delete or disconnect link under the Chinese law. The Chinese legislation is as broad as UAE's New Cybercrimes Law. Just like the Chinese law, the New Cybercrimes Law demands that owners of websites, social media networks, digital platforms and marketing managers be aware of and remove illegal content immediately upon discovery. Thus, the New Cybercrimes Law has an explicit provision that imposes a penalty on owners or those responsible for running a company. However, evidence is needed to prove that company managers and owners knew about the existence of illegal content and that their complicity contributed to the commission of a crime (Saleem, 2023). The Chinese and UAE laws illustrate the shifting focus to companies that could be abating cyberbullying and other cybercrimes.

Companies, especially social media companies, have traditionally enforced cyberbullying policies through self-regulatory mechanisms. However, the addictive nature of social media among children and adolescents, as well as the growing risk of cyberbullying, is raising questions about the effectiveness of self-regulation. There have been numerous calls for governments to regulate social media platforms, but such discourses often raise concerns over censorship. Lawmakers in the USA and other jurisdictions have also toyed with the idea of developing stringent laws that will hold social media companies responsible for exposure of school children to dangerous content. Regulation of social media companies is indeed an emotive issue elsewhere, but the UAE is already addressing the problem through the New Cybercrimes Law. The new law recommends imposing a fine of up to AED 10,000,000 on a party that operates a website or electronic account where an offence has been committed. The fine applies when the party "refuses to remove the illegal content or block access to such content or refuse to comply with an order from the regulator or competent authorities without an acceptable excuse" (Wilkinson, 2022).

Conclusion

Countries reviewed in this discussion, including the UAE, have adopted two primary means of regulating cyberbullying. The first approach entails enacting special laws that specifically combat cyberbullying. This trend is notable in the USA where state and local legislators have drafted specific laws that target cyberbullying. In contrast, the second strategy is embedding cyberbullying regulations within the existing laws, such as the penal code. Countries that have adopted the second strategy do not have laws that are specific to cyberbullying. On the contrary, cyberbullying is addressed as one of the offenses under existing laws. The UAE is among those countries that have used the second approach whereby cyberbullying is part of the broader national legislation against cybercrimes. In fact, the UAE does not explicitly mention cyberbullying in both the repealed and new cybercrimes laws. The UAE undoubtedly has the most robust and extensive cyberbullying legislation at the global level. Nevertheless, the New Cybercrimes Law has inherent ambiguities that will have a profound effect on its application.

The UAE has a robust legislative framework for combating all forms of cybercrime, including cyberbullying. The new law has broadened offenses and penalties related to

cybercrimes to deter the abuse of information technologies and associated devices. The new law does not expressly target cyberbullying, but instead conceptualizes the offence under cybercrimes. Defamation or libel of social media is notable offence in the New Cybercrimes Law, which directly relates to cyberbullying. Effectively, the new law criminalizes any insult or defamatory statement posted online or on social media networks. The use of modern technology to modify a photo, recording or video of a person is also criminalized under the New Cybercrimes Law if the intention is to defame or abuse. Nonetheless, the new UAE law on cybersecurity emphasizes online privacy, which is only an aspect of cyberbullying. Consider the case where the New Cybercrimes Law mandates companies, particularly social media providers, to safeguard the safety of personal data. Thus, the new law lacks clarity on how to navigate definitional aspects of cyberbullying.

The New Cybercrimes Law has established the framework upon which the UAE can combat emerging threats of cyberbullying. The UAE has effectively set precedence in the region by acknowledging the threat of cybercrime. The new law may not explicitly apply to cyberbullying but it broadened application to cybercrimes that constitute misuse of electronic means to defame or harm others. However, the question of intentionality remains unresolved under the New Cybercrimes Law. For example, there is no mention of jokes and banter in social media conversations. Instead, the new law has blanket provisions for defamation or incel on social media. Thus, the legal ambiguity makes it difficult for courts to determine whether defamatory content is intentional or normal banter and jokes that are acceptable in the context of social media. The issue of intentionality draws attention back to the lack of a clear definition. The main concern is that neither cyberbullying nor cybercrimes have explicit definitions under the New Cybercrimes Law. Therefore, it would be difficult to directly apply provisions of the new law to cybersecurity.

In conclusion, the New Cybercrimes Law and similar regulations in the UAE and elsewhere address cyberbullying from a general standpoint. The approach ignores that cases of cyberbullying are disproportionately higher among students. The UAE currently has school-based policies aimed at addressing cyberbullying, requiring each public school to have an antibullying policy. The school is perhaps the best place to deal with students considering the punitive nature of the new law, which may not apply to adolescents who perpetrate cyberbullying. Thus, a probable conclusion is that cyberbullying does not need a national law but a school-level policy with a clear definition and preventive measures.

Note

1. Saleem, 2023. See also Elhais, "United Arab Emirates."

References

- Abou Assy, R. (2022), "UAE'S new federal law on countering rumors and cybercrimes– key amendments", The Legal 500, available at: www.legal500.com/developments/thought-leadership/uaes-new-federal-law-on-countering-rumors-and-cybercrimes-key-amendments/
- Agarib, A. (2018), "Deportation made optional in UAE cybercrime law", available at: www.khaleejtimes.com/nation/dubai/deportation-made-optional/-in-uae-cybercrimelaw
- Aliyev, R. and Gengec, H. (2019), "The effects of resilience and cyberbullying on Self-Esteem", *Journal of Education*, Vol. 199 No. 3, pp. 155-165.
- Banda, M. (2021), "Survey: 56% of Emirati parents name cyberbullying as concern", Intelligent CIO, available at: www.intelligentcio.com/me/2021/02/23/survey-56-of-emirati-parents-name-cyberbullying-as-concern/
- Bano, S. (2022), "New UAE cybercrimes law federal law no. 34 of 2021 ('cybercrimes law')", IR Global, available at: www.irglobal.com/article/new-uae-cybercrimes-law-federal-law-no-34-of-2021-cybercrimes-law/

- Beghin, H. (2020), "The effects of cyberbullying on students and schools", *BU Journal of Graduate Studies in Education*, Vol. 12 No. 2, pp. 19-22.
- Chandra, G.R., Sharma, B.K. and Liaqat, I.A. (2019), "UAE's strategy towards most cyber resilient nation", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 8 No. 12, pp. 2803-2809.
- Cyberbullying Research Center (2023), "Bullying laws across America", available at: www.cyberbullying.org/bullying-laws
- Díaz, K.I. and Fite, P.J. (2019), "Cyber victimization and its association with substance use, anxiety, and depression symptoms among Middle school youth", *Child and Youth Care Forum*, Vol. 48 No. 4, pp. 529-544.
- Englander, E., Donnerstein, E., Kowalski, R., Lin, C.A. and Parti, K. (2017), "Defining cyberbullying", *Pediatrics*, Vol. 140 No. Supplement_2, pp. 148-151.
- Government of Canada (2023), "Cyberbullying can be against the law", available at: www.canada.ca/en/public-safety-canada/campaigns/cyberbullying/cyberbullying-against-law.html
- Lee, J., Abell, N. and Holmes, J.L. (2017), "Validation of measures of cyberbullying perpetration and victimization in emerging adulthood", *Research on Social Work Practice*, Vol. 27 No. 4, pp. 456-467.
- Masudi, F. (2019), "UAE survey reveals 'shocking' result: 85 % children bullied, mostly online", *Gulf News*, available at: www.gulfnews.com/uae/education/uae-survey-reveals-shocking-result-85-per-cent-children-bullied-mostly-online-1.67306786
- Mazhar, F. (2019), "UAE to roll out new laws to combat cybercrimes", *Gulf News*.
- Navarro, R. (2016), "Gender issues and cyberbullying in children and adolescents: from gender differences to gender identity measures", *Cyberbullying across the Globe: Gender, Family, and Mental Health*, pp. 35-61.
- Notar, C.E., Padgett, S. and Roden, J. (2013), "Cyberbullying: a review of the literature", *Universal Journal of Educational Research*, Vol. 1 No. 1, p. 2.
- Saleem, S. (2023), "New UAE cyber crime law combating information technology crimes in the UAE: types, penalties and punishment of cyber crimes", Al Tamini and Co., available at: www.tamimi.com/law-update-articles/new-law-combating-information-technology-crimes/
- Slonje, R., Smith, P.K. and Frisén, A. (2013), "The nature of cyberbullying, and strategies for prevention", *Computers in Human Behavior*, Vol. 29 No. 1, pp. 26-32.
- Taylor, J. (2023), "How will new laws help stop Australians being bullied online?", *The Guardian*, available at: www.theguardian.com/media/2022/jan/23/how-will-new-laws-help-stop-Australians-being-bullied-online
- Tokunaga, R.S. (2010), "Following you home from school: a critical review and synthesis of research on cyberbullying victimization", *Computers in Human Behavior*, Vol. 26 No. 3, pp. 277-287.
- UAE Ministry of Education (2023), "Student behavior management distance learning 2020", available at: www.moe.gov.ae/Ar/Legislation/Documents/Student%20Behaviour%20Management_Distance%20Learning%202020_English.pdf
- Wilkinson, D. (2022), "UAE updates cybercrime law", Clyde and Co., available at: www.clydeco.com/en/insights/2022/03/uae-updates-cybercrime-law

Corresponding author

Tareq Na'el Al-Tawil can be contacted at: dr.tareqaltawil@yahoo.com

For instructions on how to order reprints of this article, please visit our website:

www.emeraldgrouppublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com