Cyberbullying in the UAE: A Snapshot of Cyberbullying Laws in the UAE

Fiona Robertson - Senior Counsel, Head of Media - Digital & Data - Dubai International Financial Centre

Amna Qureshi - Associate - Digital & Data - Dubai International Financial Centre

August 2017

However, there are also concerns emerging from parents and teachers that this technology can be used for harm as much as it can be used for positive educational purposes. It is becoming increasingly important for schools to educate students about the legal and appropriate use of the internet and to have policies which are clearly communicated to both staff and students. If pupils are engaging in cyberbullying activities, there could be consequences under a school's disciplinary and code of conduct procedures. If a school is aware of these types of activities, but does not take action, there could be reputational, regulatory, and potentially even legal implications for that school. Under the new Dubai Schools Law (Executive Council Resolution No. 2 of 2017) schools have an obligation to have in place a 'student safety and protection policy' approved by Dubai's Knowledge and Human Development Authority and must take all necessary measures to care for and protect their students' rights.

There are two ways in which technology may become a medium for abuse rather than education. Firstly; when children themselves are targeted in a way that they may not properly understand. The second is when children abuse technology to take advantage of, or persecute, others in their peer groups. In this article the authors focus on issues arising from the second category. Attention is given to potential legal ramifications for young people and children who misuse online resources and, in particular, social media.

Underage Access to Social Media

An important consideration is a child's minimum age before he or she is granted social media access. Firstly, it is important to note that there are no laws specifically governing minimum age requirements. There are certain guidelines and regulations that may apply to content (most visibly in relation to the censorship of films, television, and to a lesser extent magazines). Some of these guidelines also extend to online content. In this regard, telecommunications carriers have the right to block content they consider breaches Annex 1 of the Telecommunications Regulatory Authority's Internet Access Management Policy, for instance; 'internet content containing pornography and nudity' and 'gambling internet content.' These regulations, however, do not provide minimum age requirements for generic social media sites.

To fill this vacuum, which exists in most countries that permit access to global social media, pressure has been applied to the operators of social media sites to place age restrictions on users. Facebook, for example, requires all account holders to be at least thirteen years old before they can create an account. Not only is it not permitted to create an account if you are underage, but it is also not permitted to create an account for another person that is underage. Parents can request deletion of accounts that have been created in beach of this rule. More importantly, Facebook provides a form that allows third parties to report accounts that are held by underage users, which are then immediately deleted.

What Role Do Facebook Restrictions Play?

Platforms such as Facebook have reacted to parental concerns about access to unrestricted content – they have implemented bespoke rules designed to provide a sense of security to their users. However, these are not legal restrictions, and so breaching these rules does not carry any legal consequences. Should a child breach the minimum age restrictions for any social media site and then accesses adult content, there is little that can be done about it from a legal perspective.

Interestingly, in the United Kingdom the National Society for the Protection of Cruelty to Children has requested that there be a statutory code of practice to ensure children are adequately protected online. If the UK does take this to the next step, we can expect other countries to follow suit. This may mean that, in the future, there will be legal repercussions for online publishers who do not properly control or prohibit access to inappropriate content by children.

What is Cyberbullying?

Cyberbullying occurs when technology is used to convey the bullying message to the victim and to those around the victim. Mobile phones are the preferred medium for these acts, and the proliferation of apps such as WhatsApp as well as app based social media platforms make it increasingly easy to spread negative messages much further than was possible before. In addition, secondary perpetrators can readily forward and share the negative material, resulting in its rapid and widespread dissemination. The message may be viewed multiple times by a larger and more diverse audience – it could be sent to the victim's siblings, teachers, neighbours, and broader social groups.

Insights from the Child Rights Law in the UAE

The UAE's Child Rights Law (Federal Law No. 3 of 2016) affirms that all children have the right to education and basic protection in the UAE. Bullying has always been difficult to punish. It is suggested that the increased use of technology may aid bullying. Equally, such technology may assist with tracing its source.

Cybercrime Law and Penalties

Defamation, which is often at the core of cyberbullying, is potentially a criminal offence in the UAE. Not only does the UAE have extensive provisions within its Penal Code (Federal Law No. 3 of 1987), but it also has the benefit of the Cyber Crimes Law (Federal Decree No. 5 of 2012 on Cyber Crimes). For example, Article 138 of the Penal Code stipulates that a punishment of jail and a fine (determined at the discretion of the judge) "*shall be inflicted on any person who publishes through any means of publicity news, pictures or comments pertaining to the secrets of people's private or familial lives even if the same is true.*" The UAE has traditionally considered defamation to be a serious criminal offence.

As is often the case, it is the Cyber Crimes Law that provides the most practical recourse for victims of crimes involving technology. Article 20, for example, deals with slander in the broadest of terms:

Without prejudice to the provisions of slander crime prescribed in Islamic Sharia, any person who insults a third party or has attributed to him an incident that may make him subject to punishment or contempt by a third party by using an Information Network or an Information Technology Tool shall be punished by imprisonment and a fine not less than (AED 250,000) and not exceeding (AED 500,000) or by any of these punishments.

Note that the prescribed fine is a minimum of AED 250,000. Imprisonment is also possible, although a minimum sentence is not prescribed. For some offences the Juvenile Law (Federal Law No. 9 of 1976)

specifically dictates that children under the age of eighteen may be sentenced to no more than half of the prescribed detention period.

Article 16 of the Cyber Crimes Law states that a perpetrator of an action that could be considered to be extortion '*shall be punished by imprisonment for a period of two years at most and a fine not less than AED 250,000 and not in excess of AED 500,000, or either of these two penalties*'. Accordingly, threatening to bully someone unless money is received may lead to severe penalties – the act of bullying does not have to eventuate, it can simply be threatened. If the extortioner uses the threat of bullying (eg; "I'll tell everyone that you…") in order to extract money or something of value from the victim, they may be found guilty under this law.

Of course, the standards that are applied to defamation can be high – as is generally the case globally. The statement must, first and foremost, do harm to someone's reputation, and must do so in a manner that makes people consider that person in a negative light.

Additionally or alternatively, the parents of a victim may wish to consider civil action through court. This does present a more difficult case, requiring assessment of the damages arising from the offence, and should accordingly be discussed with a competent lawyer before proceeding.

Distributing and Sharing Pictures Without Consent

Cyberbullying can be, and often is, undertaken by using images of the victim in a way that is not authorised or otherwise without their consent. This could include images taken of the victim with consent at the time, but on the understanding of confidentiality. They may have, for example, been provided during the course of a relationship. Images may otherwise have been provided as a result of persistent bullying behaviour – eg; "if you don't give me photos, I will tell everyone that you…".

In the UAE, using images without consent can be a serious issue (which we have covered in previous Law Update articles). In this article we address common issues concerning the creation, retention, and/or circulation of pornographic images, as are commonly used in cyberbullying cases.

The Cyber Crimes Law prescribes harsh penalties for any use of material that is considered to be pornographic. Article 17 states;

Any person who established or operated or supervised an Electronic Site or transmitted, sent, published or re-published through the Information Network pornographic materials … and anything that may prejudice public morals shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

Any person, who produced, prepared, sent or saved pornographic materials … and anything that may prejudice public morals for the purpose of exploitation, distribution or displaying for a third party through an Information Network shall be punished by the same punishment.

The Article penalises several actions relating to a qualifying image's utilisation – including its transmission and sending. In addition, the Cyber Crimes Law imposes further penalties if the pornographic material concerns subjects younger than eighteen years old – so the vast majority of school pupils, stating:

If the subject of the pornographic content was a juvenile not exceeding eighteen years of age or if this content was designed to tempt juveniles the perpetrator shall be punished by imprisonment for a period not less than one year and a fine not less than (AED 50,000) and not exceeding (AED 150,000).

This is followed by Article 18:

Any person who intentionally acquires Juvenile Pornographic Materials by using an Electronic Information

System, Information Network, Electronic Site or any of the Information Technology Tool shall be punished by imprisonment for a period not less than six months and a fine not less than (AED 150,000) and not exceeding (AED 1,000,000).

Again, this covers situations where a person is seeking pornographic materials from anyone younger than eighteen. The fine is significant, as is the minimum jail term.

In addition, Article 16 of the Cyber Crimes Law (above) may also apply. If, for example, a teenager threatened to bully or defame a fellow student unless they provided a sexual image of themselves, then not only are they guilty of inciting contempt, receiving and distributing pornography, and child pornography, but they are also guilty of extortion. A court has discretion to apply all of the above penalties. As far as penalties are concerned, the Cyber Crimes Law also requires a judge to order the deportation of any perpetrator that is not a UAE national.

Reputation Management in the Online Environment

Undoubtedly it is imperative to take action against any person that is bullying another – and any adult that has to deal with a child that is being bullied has reason to wish it to stop as soon as possible. Unfortunately, the disadvantage of taking legal action is that the victim may be required to disclose aspects of their lives they may be ashamed of, or do not wish to make public. Under the Juvenile Law, court hearings in relation to children under eighteen will not be made public and may only be attended by certain persons (eg; lawyers, custodians, Ministry of Social Affairs) or with a court's permission. A court may even excuse a child's attendance during witness testimony if considered to be in the child's interests.

In all of the above, it is important to remember that, from a practical perspective, online publications often remain accessible for a long time, if not forever. Even when content is taken down from a site, or deleted from a particular device, it may be cached or may have been forwarded or saved to other devices. It may be dormant for some time and then re-surface, affecting the reputation of not only the victim, but inevitably the perpetrator and their cohorts. In teaching children, and young adults, about their use of social media, the importance of maintaining their reputation should be stressed at all times. A bullying post, a semi-naked photograph, a political rant – these can all come back to haunt them later. There is only one chance to emphasise this to all young people; it cannot be remedied later.

Al Tamimi & Company's Technology Media and Telecommunications team regularly advises on issues arising from media and content issues and on regulatory matters and disputes. For further information please contact Fiona Robertson (f.robertson@tamimi.com).