Online Harassment in Bangladesh

Sabbir Mahamud Chowdhury*
Chevening Scholar with the Foreign and Commonwealth Office of the UK
Studying LL.M in Criminal Justice at Queen Mary University of London.

The increased connectivity of online environment with the emergence of social media has given rise to a long range of communication crimes. To combat these crimes committed in cyberspace Bangladesh passed a new statute named Digital Security Act 2018 (hereinafter DSA).[1] Prior to enactment of DSA, communication offences through online were dealt with section 57 of the Information Technology and Communication Act 2006 (ICTA)[2] which criminalized publication of fake, obscene and defamatory information in the electronic form. The new law has repealed[3] section 57 of ICTA and enacted several sections for communication crimes which included online harassment[4], improper communication[5], online defamation[6], hate speech[7] etc. This paper is outlined to examine the scope of DSA to combat abusive and offensive communication through online which may cause harassment to a person.

Use of digital technology has provided new ways of commission of old crimes like harassment and stalking by overcoming the "traditional obstacle of offending" both physically and psychologically.[8] An act of abusive and offensive online communication may rise several interrelated communication crimes. Due to structural constrains this paper will only examine communication offences so far it relates to offence of harassment.

The difficulties of evaluating online communication crimes in Bangladesh is that, no real authoritative argument has been developed in this area of jurisprudence. Even though ICTA was enacted in 2006 hardly any case law can be found which has identified the basic features of online harassment law in Bangladesh. Therefore, this paper will conduct a comparative evaluation with contemporary UK laws that has been used for online harassment.

It must be mentioned that like most Jurisdiction[9] the UK has adopted their existing harassment law to prosecute crimes committed in online environment. In the UK major law relating to harassment is Protection from Harassment Act 1997 (hereinafter PHA). Individual act of harassment may be prosecuted under Malicious Communication Act 1988 (hereinafter

---

* Current version of the piece is an initial draft of a larger project the author is currently developing on Online Harassment regime in Bangladesh.

[1] ডিজিটাল নিরাপত্তা আইন ২০১৮, available at<https://ictd.gov.bd/site/view/law accessed 3 January 2019

[2] তথ্য,যোগাযোগ ও প্রযুক্তি আইন ২০০৬, available at <https://ictd.gov.bd/site/view/law accessed 3 January 2019

[3] DSA 2018, s 61

[4] ibid, S 25

[5] ibid, s 25

[6] ibid S 29

[7] ibid S 28

[8] Jonathan Clough, *Principles Of Cybercrime* (2nd edn, Cambridge University Press 2015) at 417

[9] Ibid, at 425

MCA), Communication Act 2003 (hereinafter CA).[10] Apart from these, prosecution of harassment can also be brought under some other UK laws.[11] This paper will only study nature of harassment offences that can be prosecuted under PHA, MCA and CA,

The aim of this paper is to find out how the online harassment law under DSA can be catered effectively for prosecuting and adjudicating. It will try to identify the conduct element and fault element of online harassment offence in Bangladesh. While doing so two other vital elements of the offence namely 'means of communication' and 'receipt of the conduct by the victim' will also be explored. Finally, it will be argued that lack of express provision in certain aspect in the DSA essentially gives more freedom to the prosecutors to indict a person for online harassment.

Conduct:

Section 25(1) DSA criminalizes sending or publishing offensive, false or intimidating information by a person. According to the section

> If any person through any website or other digital means intentionally or knowingly sends any information which is offensive or intimidating; or sends, circulates or publishes any information which is known to be false with an intention to annoy, defame, disgrace or insult a person…such act will an offence.[12]

So, the conduct must be either offensive and intimidatory or false. Question may arise on what conduct should be called offensive and intimidatory. The definition of criminal intimidation can be found in Penal Code 1860 (hereinafter PC). According to section 503 of PC criminal intimidation includes 'threatening a person to cause injury to his person, reputation or property etc' or 'to cause alarm to that person'. The definition of criminal intimidation is very relevant in identifying nature of act in offence of harassment. Still question remains what the legislature meant by 'offensive' conduct.

The UK laws have criminalized similar kind of conducts. Under MCA the conduct should be either indecent, grossly offensive, threatening or false. Section 127 of CA covered four proscribed character; grossly offensive, indecent, obscene, or menacing. In an online environment apart from sending grossly offensive or threatening massage sending of image, drawings, video or recording can be an offence under MCA if the article is of grossly indecent in nature.[13] In *DPP v Collins*[14], the House of Lords held that in determining the communication grossly offensive the court must take into account of 'the context and all relevant circumstances.' According to Bakalis[15] the threshold of 'grossly offensive' is very high to attract all behaviors that may constitute harassment; thereby not suited to harassment cases. For prosecuting harassment, the PHA has lesser threshold than MCA or CA. Under PHA 'alarming the person' or 'causing distress to the person' will cause harassment[16]. Again,

[10] 'Abusive and Offensive Online Communications | Law Commission' (law Com no 381) para 8.127, available at <https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/> accessed 3 January 2019,
[11] Ibid, at 8.23.
[12] DSA, S25(1)(a).
[13] Law Com no 381 (n 10) para 4.32.
[14] [2006] UKHL 40 at [8].
[15] Chara Bakalis, 'Rethinking Cyberhate Laws' (2017) 27 Information & Communications Technology Law.
[16] PHA, s 7(2).

under PHA there must be more than one conduct (course of conduct) by the offender[17] whereas one conduct is enough to constitute offence under MCA or CA. According to PHA if the victim is one there should be more than one conduct against him and if the victim is more than one there must be at least one conduct against each victim.[18] The course of conduct also include speech.[19] It is not necessary that all of these conducts must be committed online.[20] Sometimes a conduct if considered separately seems innocent may form course of conduct and cause considerable distress to the victim.[21] A prosecution under MCA or CA does not need more than one conduct. So, based on the circumstances and the nature of conduct the prosecutors have option to choose under which act a conduct of harassment should be prosecuted.

Under DSA, a single conduct of offensive communication can cause harassment. The intention of the accused should be to annoy, defame, disgrace or insult the victim. This law sets a lower threshold for determining nature of the conduct and number of the conduct than the contemporary UK laws. However, while interpreting offensive conduct under DSA the Bangladeshi courts can use 'context and relevant circumstances' as suggested by the Collins[22] case.

Means of Communication:

To constitute an offence under section 25 of the DSA the communication must be through 'website or any other digital means.' ICTA has a definition of website which includes 'data and information saved in computer or web server that can be viewed or browsed through internet'.[23] This definition identifies internet as the medium of communication. There is no explanation of 'digital means' in any law of Bangladesh. However, a relative definition of 'digital devise' can be found in DSA.[24] Under this act 'digital devise' includes 'Any digital or computer device connected with computer network and communication apparatus including…software with advantage of communication'. If we take the essence of these two definitions, we will find that "website or any other digital means" necessarily indicates communication through internet or computer network.

Since there is no separate law for online communication offences in the UK, they have no relative definition for 'online environment'. The Law Commission has used the term online to refer 'communication which takes place over the computer'.[25] It may include online games, emails, text massage, social media, blog or instant messaging service.[26] The CA has a definition of 'electronic communication network'.[27] It is not clear whether this definition

[17] PHA, s 7.
[18] Ibid.
[19] Ibid.
[20] Law Com no 381 (n10) para 8.38.
[21] 'Stalking and Harassment | The Crown Prosecution Service' (*Cps.gov.uk*, 2019) <https://www.cps.gov.uk/legal-guidance/stalking-and-harassment> accessed 3 January 2019.
[22] Collins, n16.
[23] S 2(12).
[24] S 2(1)i .
[25] Law Com no 381 (n 10) para 1.4.
[26] Ibid.
[27] CA, s 32.

includes communication through internet or not. This actually gives the courts flexibility for using its discretion.

The distinction the between two jurisdictions is the certainty versus flexibility. Bangladesh has taken more certain approach by prescribing means of communication which will help the prosecutors and judges to identify the means of communication for online crime instantly. Still the definition itself is so broad that it can include wide spectrum of communication offences.

Sends or Delivers?

Question may arise whether the victim has to receive the offensive communication to hold the defendant liable for harassment. Under section 1 of MCA it is enough to send the communication and no need for proving the receipt of such communication.[28] It will still be considered as sent if the communication was not received by the intended person due to technical or software error[29] or interception[30] by the enforcing agencies. Causing another person to send the communication by tricking him (sender) will also be treated as 'sending' under this section.[31] No specific provision of receipt of the communication can be found in CA. In *DPP v Collins*[32] it was observed that whether the victim has received the massage has no bearing on the allegation as the offence was completed when the massage sent. Deleting a massage of proscribed character posted in the social media even before anybody sees will not exempt the perpetrator from criminal liability under this section.[33] Under the PHA communication of the course of conduct to the victim is necessary. The Phrase 'amounts to harass another' necessarily indicates the receiving or knowledge of the victim of his course of conduct. Difficulties may arise when posting of the conduct is intended not to be received by the victim or the victim is unaware of the conduct. Even this kind of harassing conduct can be prosecuted for malicious prosecution.[34]A communication without any targeted recipient can be also prosecuted under section 127 of CA. [35]

Section 25 of DSA only included intentionally or knowingly 'sending' or 'publishing' or 'circulating' offensive communication. It did not insert any provision of delivery to the recipient. The ICTA has a definition of the term 'addressee'.[36] It means the person to whom a "data massage'[37] has been sent. Despite having the choice, the legislature did not insert the word 'addressee' in section 25. It may be argued that the legislature had avoided to do so because they did not want 'delivery' as one of the conditions of the offence. Therefore, mare proving 'sending' or 'publishing' or 'circulating' is sufficient for prosecuting a case of harassment. Hence, a post in a private blog or closed group which is not accessible by the

[28] Poison Pen Letters (1985) Law Com No 147, para 4.4.
[29] Law Com no 381, (n 10) para 4.19.
[30] Law Com No 147, (n 29).
[31] Law Com no 381, (n 10) para 4.20.
[32] [2006] UKHL 40.
[33] Law Com no 381, (n 10) para 4.72.
[34] Clough (n 8) at 444.
[35] Law Com no 381, (n 10) para 4.29.
[36] ICTA, S 2(22).
[37] Ibid.

intended person may constitute the offence under the act. This has made the offence conduct crime like CA or MCA as opposed to result crime.

Fault Element:

Under MCA the purpose of the communication must be causing distress and anxiety to the victim. It is not necessary that actual distress or anxiety was caused to the victim.[38] In *Collonny vs DPP*[39] the Queen's Bench Division held that 'nature of the communication may shed light on the defendant's *mens rea*'. It further held that without intention of causing distress or anxiety an indecent or grossly communication will not make a person liable for criminal offence.[40]

Section 127 of the CA does not have any express fault element. In *DPP v Collins*[41] the court referred Lord Reid's observations in *Sweet v Parsley*[42] where it was held that the court must 'read in words appropriate to require *mens rea*'. It is not material whether the recipient receives the massage, rather it is sufficient that the sender of the massage knows that the intended recipient will regard the massage peculiarly offensive. In *Chambers v DPP*[43] it was held that *mens ria* will be satisfied if it can be proved that either the defendant had intended to use the word of menacing character or he was aware of or to have recognized that the act will scare a reasonable person of the public who reads it.

Fault element in harassment can be viewed from subjective or objective test. Because of the difficulties to prove subjective fault element defense may be taken that the accused was unaware of result of the conduct some jurisdiction imposes objective test in addition to subjective fault element.[44] In *R v Colohan*[45] the court has adopted objective test to identify the fault element without considering the defendant's mental state of hypothetical reasonable schizophrenic. In this case the crown court convicted the accused with an observation that mental illness of the accused was not a defense. In appeal House of Lords held that the accused 'ought to have known that what he was doing amounts to harassment by the objective test of what a reasonable person would think'.[46]

The 'ought to have known' test is also applicable for cases under section 25 of DSA. For the purpose of this act the offensive and intimidatory or fake nature of the conduct should have been known to the perpetrator. It is immaterial to see whether the victim has sustained actual harm. Rather only test is relevant whether the accused knew the offensive nature of the conduct. Here the word Knowingly and intentionally should be read conjunctively. The word 'intentionally' qualifies the word 'knowingly'. Thus, objective fault element gives broad scope of criminalizing the conduct.

[38] Law Com no 381, (n 10) para 4.19.
[39] [2007] EWHC 237 (Admin).
[40] Ibid.
[41] [2006] UKHL 40.
[42] [1970] AC 132, 148.
[43] [2012] EWHC 2157 (Admin).
[44] Clough (n 8) at 431.
[45] [2001] EWCA Crim 1251.
[46] Ibid.

Conclusion

The discussion above has demonstrated that the crime of online harassment in Bangladesh has given wide range of discretion to the prosecutors and the judges. The comparative evaluation with the UK laws reveals that the biggest advantage of DSA is that it is enacted to deal with online offences only. It definitely gives more certainty of bringing a charge against an offender. It is not necessary to prove the impact of the conduct on the victim, which means it sets a lower threshold for the prosecutors. Further, adoption of objective fault element ensures more obligation to the online user to be careful about what he is doing. However, the wide scope of interpretation may cause over criminalizing of a conduct. To avoid this cautious application of the law taking into account of 'context and all relevant circumstances'[47] is required from the prosecutors and the judges.

[47] See (n 16).