International Journal of Human Rights Law Review

Volume 2 | Special Issue Art. 36

2023

ETHICAL REFLECTIONS ON CYBERSTALKING

Aditi Raj & Himanshu

Recommended Citation
Aditi Raj and Himanshu, 'Ethical Reflections on Cyberstalking' (2023) 2 IJHRLR S.I. 227-234.
Available at www.humanrightlawreview.in/vol-2-special-issue/.

ETHICAL REFLECTIONS ON CYBERSTALKING

Aditi Raj[1] and Himanshu[2]

THE EMERGENCE OF CYBERSTALKING & ASSOCIATED DILEMMAS

Stalking as it stands, being a deeply engraved issue of society, has reached a virtual sphere with the introduction of information technology in communication between people. If this virtual stalking, known as Cyberstalking, is to be defined in simple terms, it can be categorised as a behaviour wherein certain kinds of stalking activities, which used to occur in physical space, extends to the online world. The criminal aspect of stalking or Cyberstalking is, in its most basic explanation, can be understood to be the one in which the stalker secretly and illicitly keeps a watch on the movements of the stalkee with a particular goal in mind. A Cyberstalking act can range from identity theft to online impersonation, identity deception & threats to hostile posting. Moreover, posting of "revenge porn" by jilted lovers and ill-intentioned groups of online teens bullying victims into suicide also comes under the purview of Cyberstalking. As far as the physical world is concerned, there is no clear demarcation of lines for which activities and behaviour would constitute stalking, and this further makes it even more challenging to categorise activities in the virtual world.

Another issue with the categorization of stalking activities in the cyber-realm is that cybercrimes are often confused with a graver term, "*harassment crimes*". Grodzinsky illustrates two real-life instances to draw the fine line between cybercrimes and harassment crimes. The first is the case of a teen Christian Hunold who used computer technology to terrorize the principal of a high school by constructing a

[1] Law Student, 3rd Year, B.A. LL.B. (Hons.), National University of Study and Research in Law, Ranchi.
[2] Law Student, 3rd Year, B.A. LL.B. (Hons.), National University of Study and Research in Law, Ranchi.

website that published a hit list of teachers and students of the school. The research work behind this stalking or maybe harassment was done online via communicating with several students of the same school who were completely unaware of the circumstances. Grodzinsky questions, whether it should be termed as an act of cyberstalking or it should be more appropriately be called cyber harassment, based upon the graveness of the act.

In another case, the man wanted to get into a relationship with the woman however she spurned his advances. Following that, the stalker assumed the identity of the woman in various Internet chat rooms when soliciting "*kinky sex*." The incident that followed was that the women began to receive telephone solicitations from men, ultimately ending up seeing a solicitor appear at her door. The same question arises in this case too, whether it is mere cyberstalking or online harassment using computer technology, as the man didn't himself stalk the woman but engaged others to do so. The noteworthy point in both these cases is that no physical harm was caused to the victims, and there was evident non-separation of certain harassment activities from stalking behaviour. Moreover, the second case in which the solicitor even came to the residence of the victim, cannot be purely regarded as a case of only cyberstalking as it took place in both the worlds, i.e. physical and virtual.

THE AMY BOYER CYBERSTALKING CASE: AN ANALYSIS FROM THE LENS OF ETHICS

Twenty-year-old Amy Boyer was killed by her stalker who stalked her through the internet. Her stalker hosted two websites on the internet, one describing her personal information with her picture and the other explaining how he plans to murder Amy in detail. The research behind his work was solely based upon online search facilities and other tools provided by Internet Service Providers (ISPs). Among various other

questions that are raised in Amy's case, like whether her privacy was violated, or was she a victim of online defamation, or whether her stalker had a protected right to free speech, Tavani and Grodzinsky choose the more ethical concern surrounding the issue, i.e. has cyber technology made a moral difference?

Tavani presents two sets of arguments, one in favour and the other against the affirmative answer to the question. While denying any relevant difference in the stalking case due to Internet technology, Tavani contends that internet tools are irrelevant from an ethical point of view as far as execution of murder is concerned, as "a murder is a murder". Moreover, his contention extends to further argue that since the stalking activities had been a part of the offline world for a very long time already, there is nothing special about one of its forms called cyberstalking, irrespective of whether or not those incidents led to the death of the victim.

While justifying the relation of morality and cyber technology, the author argues that the advent of the ecosystem has primarily led to the raised concerns of scale and scope. The scale can be illustrated as to how a cyberstalker can stalk multiple victims simultaneously, while the scope can be explained as the potential penetration of victims, that is how a stalker sitting in the States can stalk a victim living in India. The author however has not addressed in particular how cyber technology concerns morality differently. Stalking whether in the physical space or in the virtual sphere, whether on a single person or multiple people, if has any effect on morality, then has it in the same way.

Further, as far as Amy Boyer's case is concerned, Grodzinsky and Tavani raise two questions of moral responsibility, first, whether the two ISPs that hosted the websites should be held morally accountable? And second, do ordinary users who come across the website have a moral responsibility to inform the potential victim?

MORAL RESPONSIBILITY: A DUAL FACET THEORY

The first question, whether an ISP should be held legally or morally responsible or not for hosting the two websites draws attention to the word responsible. The responsibility has to be understood both in the legal and moral context to answer the question. Further consideration has to attend, to whether such responsibility can be attributed to an organization or collectively such as an ISP. The court's ruling suggests that if an organization has claimed to have editorial control over the contents, it would be considered similar to a newspaper in which case the standard of strict legal liability used for original publishers could be applied. The counter contention of ISPs is that they should not be understood as "original publishers," but rather as "common carriers," as they only provide the "conduits for communication but not the content." In the same line, the legislation provides that these organizations or providers should not be treated as the publisher of any information provided by another information content provider, hence are not legally liable for the content on their websites.

The dilemma of whether ISPs should be made morally responsible for the behaviour of their customers has been explained with illustrations of Spinello's and Vedder's views. Spinello suggests a threefold mechanism to tackle the issue, where an ISP should not be held strictly liable just because it has presented an "occasion for defamation". Rather, it should be considered whether the ISP had the control to do something about it and whether it failed to do so or not. According to Spinello, his theory considers both the faces where ISPs are not brutally persecuted for their customers' deeds while they are also being subjected to reasonable accountability. Spinello's theory also takes into account the incapability of ISPs to pre-screen content hence strict liability should not be put.

Vedder's argument on the other hand, while being consistent with Spinello's views differs in the reasoning for its contention. Vedder suggests two kinds of responsibility, retrospective and prospective. His contention, primarily based on a notion of moral responsibility, argues that applying strict legal liability to ISPs will deter harm to ISP users in the future. Moreover, his theory suggests that if a collectivity can be subjected to accountability, it should be in both prospective as well as retrospective manner. While Vedder's contention on the accountability issue seems just, his notion about retrospective accountability is unique. The purpose behind the retrospective approach can be attributed to evaluating the past behaviour cycle to understand the extent of responsibility and accountability that can be put on the said collectivities more amicably.

The discussion of the two perspectives was to answer the question raised in Amy's case, thus we can now apply Spinello's and Vedder's views to the case. The ultimate conclusion, if these two views are to be taken as correct, pens down to reasonably holding these ISPs morally accountable if it also could be shown that the two ISPs were capable of limiting the harm that resulted to Boyer. However, the law does not recognise it as something for which legal action should be initiated, hence it is evident that legal and moral aspects differ quite a lot in this debate. Moreover, the debate about whether ISPs should be held accountable or not has settled with another question to ponder, that is whether there exists any sense of moral responsibility at individual levels.

For instance, in the Amy Boyer case, an issue can be raised that is the moral responsibility of the users who came across the two websites to inform Amy about the potential threat to her and whether such regulation, if admitted, should be based solely on self-regulation or strictly by law? The moral obligation can be understood from two

different perspectives, namely a minimalist sense of moral obligation and an ethic of care. The believers of the former theory argue that all morality demands from an individual are that he or she should do no harm and his moral obligation ends there. There is no requirement per se to prevent harm or do good to others, however, this concept seems somewhat flawed. Consider pondering over the question of whether the "do no harm" policy is sufficient on one's part as a moral agent or aren't we obliged to prevent the harm if it is in our hands to do so? The answer lies in one's belief i.e., if an individual thinks, that the purpose of morality is to alleviate human suffering and to promote human flourishing, whenever possible, then clearly we would seem obligated to prevent harm in cyberspace. The author counters himself when he contends that moral behaviour depends upon the belief of an individual. If that's so, moral behaviour cannot be put as an obligation on any individual.

The second perspective, which is the care of ethics, on the other hand, argues that individuals should assist one another whenever it is in their power to do so. One of the ideas behind this perspective is that the traditional theories of morality tend to engender a sense of individualism while care ethic creates a sense of community in people. If such an idea is to be adopted, the author contends, ordinary Internet users would be prone to assist others whenever they can help to prevent harm from coming to them. Thus, even if there are no specific laws in place, individuals would tend to assist one another out of a moral obligation. Ultimately, we can understand the ethical implications of cyberstalking behaviour more clearly.

The moral responsibility stands questionable on the part of what should be its sphere to which it should expand. The question arises due to the incidents concerning Genovese Syndrome. The syndrome got its name from a lady who was murdered by continuously stabbing her for 35

minutes when 38 of her neighbours watched the incident but none of them called the police. Grodzinsky questions whether they were obliged in any way to notify the police in the absence of any law prescribing such action? The answer needs a consideration towards the potential harm that could come to members of the online community if we fail to act to prevent harm when it is in our power to help and when doing so would neither cause us any great inconvenience nor put our safety at risk.

An analogy can be drawn with all the previous cases, about how the individuals associated with the case cooperated to help. However, in the case of Amy Boyer, no one actually informed her about the potential threat that ultimately led to her death. Similarly, Genovese also did not receive any assistance from the neighbours, which ultimately resulted in her death. The conclusion that can be drawn suggests that there exists a sense of morality even in the absence of any formal law in place, be it the physical world or the virtual community. If the contention has to be denied, it has to be denied together that no person on the planet can be held liable to any other individual without a law. Since the online world has not been explored much, we'll cite an instance from the physical realm to understand the idea better. For instance, if a jeweller's shop is looted, the neighbouring shop who has installed a CCTV outside his shop will not be obligated to provide the recording for finding out the thief, or in more grave situations, a man witnessing an incident of teasing on the streets would not have to bother to rescue the victim. This will give rise to a potentially harmful society altogether, with the extinction of community hood as there will be only individualism and no ethic of care towards others.

REFERENCES

- Frances S Grodzisky and Herman T. Tavani, *Ethical Reflections on Cyberstalking*