Imran Alam[*]
Naveed-ur-Rahman[**]
Muhammad Mumtaz Ali Khan[***]
Mr. Zahid Farooq, [****]

The Internet Services Providers (ISPs) Liability in Online Defamatory Contents with Reference to Specific Actual Knowledge Clause in Pakistan

Abstract

Internet Service Providers (ISPs) regulatory law is based on the principles of common law in Pakistan under "The Prevention of Electronic Crimes Act 2016" especially the specific actual knowledge clause. As per the clause, ISPs can be held liable for online defamatory contents as soon as they acknowledge them, and they do not remove them in reasonable time from the website. The famous case Byrean v Dean [1937]1 K.B. 1818 was decided on the same principle of acquaintance. On the other hand, the situations in developed nations like the UK or USA have become absolutely different as they have enacted moderate laws to govern ISPs on modern needs and requirements, hence, by leaving behind common law principles of dissemination of defamatory material.

The paper examines the approach adopted by Pakistan on ISPs in the context of specific actual knowledge clause. Furthermore, following questions have been tried to sort out.

- *What is actual knowledge when is it deemed to have been acquired by the ISPs regarding defamatory online material?*
- *Can the ISP edit online objectionable contents on its own motion without being declared as co-publisher by the courts?*
- *Whether specific actual knowledge is not attained by the ISPs after editing the online defamatory contents?*

The legal approaches adopted by the USA and UK have also been examined for better understanding of the law in Pakistan.

Key Words: Cyber defamation, ISPs, EU, CDA, Liability, Cyber Crimes Bill, Limitations.

Introduction

Since the inception of the Internet, the position of ISPs and their possible liability for posting contents on Internet, especially concerning infringement of copyrights and posing contents of defamatory nature, is being questioned in the courts of law, and different courts of law have arrived at different outcomes about the status of ISPs. There appeared a serious requirement for legal conviction which may lead many countries including Pakistan to legislate or rather give a concrete legal covering and may fill the gap that purposefully is left in the law as the regulatory bodies may prepare certain rules and regulations in this regard.

ISPs are basically Internet Service Providers; they may be also called as intermediaries or online service providers to the cyber world. The ISPs or intermediary may be defined as the entities which provide internet based technology services to the public.[1] Such services may comprise social forums, internet e-mails, websites like Twitter, Facebook, online communication services and online bulletin boards etc.[2] Section 2(r) of the Electronic Transaction Ordinance, 2002 defines the word "intermediary" which means an entity or a person who is engaged as a service provider for sending, receiving, storing or transmitting electronic communications or other interrelated services. The same definition of service provider has also been given under Section 2(z)(b) of the Prevention of Electronic Crimes Act, 2016.

Keeping in view the functions and duties of ISPs, the same may be categorized as under:-

[*] Imran Alam Assistant Professor, University Law College, University of the Punjab, Lahore.
[**] Naveed-ur-Rahman, Lecturer, University Law College, University of the Punjab, Lahore.
[***] Muhammad Mumtaz Ali Khan Director (Administration), Punjab Higher Education Commission
[****] Mr. Zahid Farooq, Advocate, High Court Lahore.

[1] Muhamad Saeh, *Online Defamation and Intermediaries' Liability: International*, (2012) p 2 Faculty of Law, Queensland University Of Technology
[2] Ibid

(i) ISPs providing Access.

(ii) ISPs providing Content, and

(iii) Conduits

Access providers and conduits usually do not have control over their users. They only provide a forum for mutual communication between them. Live television programs, telephone or mobile phone communications, communications over Skype or WhatsApp are the examples of access provider ISPs and conduits. Law is very clear in respect to these technologies. They cannot be declared liable for defamatory speeches delivered by users. However, there is an issue in respect to the content provider ISPs. If they are authors or publishers of the uploaded online contents, they may be held liable for such online defamatory material. There is no ambiguity in it. If they merely disseminate the information uploaded by online users, they cannot be liable. Only if they fail to fulfill required obligations as per law. Their functions and duties may be changed. So, their liability is subject to change as per their functions and duties. Google, Facebook, YouTube, Yahoo, Wikipedia etc are examples of content providers. They have certain obligations towards law. They can only avoid liability if they fulfill their obligations as set out by each nation or country. These obligations and laws in respect to ISPs may vary from one country to another.

To deal with the liability of an ISP, two approaches can be found. First is known as a vertical approach, wherein diversified regimes of liability spread over to diversified areas of law.[3] The United States exactly adopted this approach. Here, the copyright issues are tackled through 'The Digital Millennium Copyright Act'. On the other hand, the liability derived from violations of other laws is covered through the Telecommunications Act of 1996[4]. The second approach is called a horizontal approach, wherein one liability regime is applied to an infringement irrespective of the area of law. Therefore, the same regime is applied to an infringement of any type, it may be defamation, or violation of privacy rights or may be infringement of a copyright.[5] The horizontal approach proved to be most favorable on the ground that here ISPs are not required to have a check over the content of the material which is published by their customers. If a vertical approach is adopted, it may have applied diversified legal liability regime upon the data which is flowing through the system. In that case, the ISPs will be required to decode the bits that arrange data and before posting, it will also have to scrutinize the other content e.g., images, music, etc. All this will result in causing exceptionally heavy burden over the shoulders of ISPs, which may lead to convert them into censorship agents.

(i) Position in USA

In the USA, a famous case titled, *Oakmont Inc. vs. Prodigy Services*[6] caused the enactment of Communication Decency Act (CDA), 1996. The case was also decided according to the principles of the common law regarding dissemination of defamatory statements. The facts of the case were that some defamatory material was posted by a third party on the website, "the Money Talk" being hosted by the defendant. It was argued by the plaintiff that the Director of the Market Programs & Communication (the defendant) wrote a number of articles on the point and in this way has tried to grip himself in online service causing control of editorial nature over the contents of messages which were online, and the online users posted the same on the system. The defendant employed a software program to prescreen all these offensive and unwanted material available on the website,[7] The defendant was held responsible by the court for posting defamatory contents by the online users. Following grounds were mentioned fixing the liability: -

(i) The defendant was exercising control of editorial nature over the material posted online,

(ii) The defendant used a software program to prescreen all the offensive and undesired material,

(iii) The defendant was efficiently enforcing some online content guidelines through its board leaders.

The case was decided by the court on the principle that an ISP would get the status of 'publisher' on having 'editorial control' and 'knowledge' of the defamatory contents.[8]

---

[3] Rosa Julia-Barcelo, *Liability for Online Intermediaries: A European Perspective*, **CENTRE DE RECHERCHES** INFORMATIQUE **ET** DROIT, *at*http://www.eclip.org/eclip_l.htm., **7, 10.**

[4] Telecommunications Act of 1996, Pub. L. No. 104-104, Title V, 110 Stat. 56, 133-43 (1996).

[5] Julia-Barcelo, *supra*

[6] Oakmont Inc v Prodigy Services Company N.Y. Sup. [1995] WL 323710

[7] Muhammad Saeh, online defamation, and intermediaries' liability: international, (2012) 15 (2), Faculty of Law, Queensland University of Technology

[8] Ibid 16(1,3)

In another case, *Cubby Inc. vs. CompuServe*[9], the defendant, an ISP Company, was saved from being liable as publishers of the online defamatory material posted by third parties on the basis that it had no editorial control as well as knowledge regarding dissemination of online defamatory contents was posted by third parties.

After the decisions made by different courts of law in the above-mentioned cases, the Congress of United States showed serious concern about the issues of ISPs and intermediaries. Consequently, the Congress successfully voted for a bill so as to create immunity for the ISPs absolving all kinds of liability of criminal & civil nature which may arise as a result of cybercrimes.[10] This legislation is known as 'the Communication Decency Act (CDA), 1996' aiming at to ensure that ISPs would be saved from all kinds of litigation in the country provided if they act as "good Samaritans" towards the public good. However, if they act with malicious intention or if they are publishers of the material then they have to face the fate of their acts as per law. Section 230(c) of CDA Law, 1996 declares that the internet service providers will not be responsible for providing access, blocking or amending in any way the offensive/obscene contents available on the internet if the same were posted on the internet for just and good determinations. Similarly, if online contents are provided by third parties, no Internet Service Provider or intermediary shall be considered the publisher or speaker of the same. [11]

Judicial approach of the United States absolutely changed after the incorporation of CDA Law, 1996. In another case, titled as '*Zeran vs. America Online*',[12] some defamatory advertising material was posted by some unknown subscribers on the website. The posts showed that the plaintiff was in possession of some 'T-shirts' meant for sale regarding bombing of a place known as Alferd P. Murrah which was situated in the city of Oklahoma. The user also posted the home address and the telephone number in the posts. Resultantly, the plaintiff started to receive obnoxious calls and threats. In this case, the ISP, known as AOL, immediately removed posts from the website when it came into the knowledge of the plaintiff. The posts again started to appear on the website after some time. The plaintiff sued the defendant on the ground that as to way he did not remove the posts of defamatory nature which were posted by a third party. In this case, the Court refused to incur the liability on the defendant merely on the ground that the defendant did not remove defamatory material posted online by users within reasonable time. So, the court overruled the principle of 'reasonable care' which was to be followed under the common law principles of dissemination of defamatory material. The court also did not follow notice-based liability which is applicable in the UK and Pakistan.

In another case, *Doe vs. AOL*[13], the plaintiff, on the ground of negligence brought an action against the defendant arguing that it had failed to block that objectionable material on the website which was posted by a third party. The court, while following the '*Zeran vs. AOL*' case[14] in which it was declared that the ultimate object of the law is to protect the ISPs and intermediaries guaranteeing them from self-regulation of laws regarding defamatory material available on the website. The court further posed a question that as to whether the ISPs can be subjected to the principles of negligence as contained in the common law and in other laws of contemporary nature in the wake of CDA Law, 1996. The court finally declared that in order to protect ISPs from all kinds of liabilities, the CDA Law, 1996 preempts all other laws.

Section 230 of the CDA Law, 1996 provides immunity to all of the providers of Interactive Computer Services, a term which has been interpreted by the US courts in a very broader sense. Even, the public libraries which provide internet facility to the public were declared eligible to seek immunity in case titled Kathleen *R. vs. City of Livermore*[15]. In another case, titled *Finkel v Facebook Inc 2009*[16], the social websites were declared eligible by the court to seek similar kind of immunity being users of such websites while acting as third parties who post comments in the boxes meant for the purpose. Similarly, OLX, Amazon.com, Alibaba and alike websites which are considered as marketing websites were also declared to fall in the domain of "Interactive Computer Services".

In the case of *Barret vs. Rosenthal*[17]the common law principle of 'redistribution and republication of defamatory contents' was overruled by the US SC by not considering them 'authors' and 'publishers' of the web-contents.

Thus, the ISPs enjoy immunity under Section 230 of CDA law for having editorial control over the website contents. However, prior to the enactment of the CDA law, the ISPs could be declared as liable for having editorial control. It was firmly declared by the US courts that after editing or changing the original contents by the Internet Service Providers, they cannot be held as

[9] Cubby Inc v CompuServe [1991] SDNY 776 Federal Supplement 135
[10] Muhammad Saeh, online Defamation and Intermediarie`s liability: international, (2012) 16 (3), Faculty of Law, Queensland University of Technology
[11] Section 230 (C), The CDA 1996
[12] Zeran v America Online [1997] 4th Cir. 129 F.3d (327)
[13] Doe v America Online [2001] Southern Reporters 2nd 783 (1010)
[14] Zeran v AOL [1997] 4th Cir. 129 F.3d 327
[15] Kathleen R. Vs City of Livermore (2001) No. A086349, First Dist. Div. Four
[16] Finkel v Facebook Inc [Feb. 24, 2009] N.Y. Supreme Ct. 2009102578-09
[17]Barret v. Rosenthal [2006] Cal. 4th 33 40

'publishers'.

In the case of *Zeran v AOL*[18], the court went on to say that the relevant law does not create a bar on immunity after service of notice by the plaintiff to the ISP. Whereas, before the enactment of CDA law, the situation was completely changed.

The immunity which is provided under this law is not only meant for civil litigation. Immunity was also immunity to the ISPs in criminal proceedings as well, as appears from the *Craigslist case*[19].

It is concluded that the approach of the US Congress is comprehensive enough. ISPs enjoy absolute immunity/privileges under the CDA Law, 1996 in the USA. Now, the ISPs may engage in any kind of business in the USA devoid of any fear of litigation at the legal forums for acting as "Good Samaritans" towards the public good. However, if they act with malicious intention or they are the publishers of the defamatory material then they cannot claim immunity under the CDA law 1996.

(ii) Liability of ISPs in UK

In the United Kingdom, the defamation cases were dealt with under 'The Defamation Act, 1996' which was replaced by the Defamation Act, 2013 with certain amendments. Now, this law has provided various safeguards and immunities to the ISPs and intermediaries from unwanted litigation in defamation cases.[20] This law pays a homage to the common law principles on defamation.

The common law principles on dissemination of defamatory statements are:

(i) That the defendant was not the editor, publisher or at least author of the statement in dispute,

(ii) That the defendant was unaware about the defamatory statement in issue before disseminating the same,

(iii) That the defendant took reasonable care in respect to the statement in issue before dissemination.

The Defamation Act, 1996 was not containing any provision over the ISPs issues. It was only the common law principles wherein dissemination of defamatory material was applicable on ISPs to limit their liability in defamation cases under cyber laws. The Common Law principles on defamation considers ISPs as 'publishers' of the defamatory content only when the plaintiff had notified about the defamatory material. Some of cases of ISPs which were decided under The Defamation Act 1996 during common law regime, are mentioned as under:-

In the case titled as *Godfrey vs. Demon Internet*[21], a newspaper called "*Soc Culture Thai*" was being hosted by the defendant. A third party created a message in the news group which was posted by the defendant. That post was containing derogatory remarks against the *Thai* women. Therefore, the plaintiff made a request to the defendant for removing the said content from the website. However, the defendant did not bother to abide by the request and failed to remove the post before its automatic expiry. The court held the ISP responsible for dissemination of defamatory remarks after it received the notice by the plaintiff.

In another case *Davison v Habeeb*[22], the plaintiff brought an action against the editor of the Palestine Telegraph for publishing some defamatory material on the "the blogger website" against him. Through that material, the plaintiff was allegedly shown as involved in some criminal activities. The plaintiff had also notified to the Google Corp. regarding defamatory contents appearing on the blog being hosted by it (Google Corp.). *Justice Richard Parkes* while deciding the remarked that evidently the blog was being hosted by the Google Corp. who was acting as a "gigantic notice board" in the matter. In this way, the Google corporation was aware of the defamatory information appearing on the blog and that the continuous visibility of the defamatory contents on the website brought a defame for the plaintiff. It was also evident that the defendant did not employ reasonable care as envisaged U/S 1 of the Defamation Act, 1996. Therefore, the court declared the Google Corp. as responsible for the reason that it did not remove the defamatory material in spite of the fact that he was already notified by the plaintiff. Google Corp. can take the defense of innocent dissemination only if the notice regarding defamatory contents was not served to it by the plaintiff.

[18] Zeran v AOL [1997] 4th Cir. 129 F.3d 327
[19] Craigslist-A Case for Criminal Liability for Online Service Providers; Barkley Technology Law Journal; Article 23, Issue 1 Volume 25 (Radbod T. Shahrzad, Jan 2010).
[20] Section 2, The Defamation Act, 2013 [commencement (England and Wales Order)]
[21] Godfrey v Demon Internet [2001] Q.B 201, [2000] 3 WLR 1020
[22] Davison v Habeeb [2011] Q. B EWHC 3031

In *Metropolitan International School vs. Designtechnica Corp*.[23] the court observed that the user carried out search through Google Engine. In that mechanism, the search was performed automatically with the help of already installed programs. During that span of time, the Google did not stop the clip appearance on that website resulted from the online search made by the users. While relying on the case titled *Bunt v Tilley,*[24] *Justice Eady J.* formulated that the role of Google Corp. merely emerged as a facilitator. In those circumstances, it becomes very difficult for the Google Corp. to immediately remove defamatory material with original authorization. The plea 'innocent dissemination' taken by the defendant need not be proved.

Now, the Defamation Act, 2013 is explicitly dealing with the ISPs liability towards defamation as it contains specific provisions to deal with internet intermediaries. Under this law, we find consolidation of common law principles and European Union Directives (EUD) 2000/31/EC. Now, the ISPs can be made more cautious, moderate, and responsible in the course of their business in the cyber world with the entry of few novel amendments.

Sec. 5 of the Act, 2013 grants immunity to ISPs for online defamatory material appearing on the website by the third party. Sec.5(2) of the Act, 2013 declares that Internet Service Providers may not be considered 'authors' of the defamatory contents appearing on the website. This section emphasizes that ISPs shall not be held responsible considering them 'authors' of the website contents. However, if the complainant notifies them about the defamatory statement appearing on the website and the same is not removed by the ISPs within a reasonable time, only then they can be precluded from claiming immunity as guaranteed by the relevant law. In that way, they could be declared as 'authors' or 'publishers' of the defamatory material.

Sec. 5(12) of the Act, 2013 provides express immunity for content moderation by the ISPs in the website contents uploaded by the users. ISPs have been given editing right in the online contents authored by users. They cannot be declared as authors of the material merely on the ground of editing it. ISPs can block, edit, or amend the online objectionable contents under the moderation clause. Moderation or editing must be in the public interest. The clause is equal to the CDA Law, 1996 of USA that empowers the ISPs for providing access to, for amending or blocking any obscene material available on the website for good and just purposes. The law encourages the ISPs for suggesting appropriate amendments in the material available online without fearing to be associated as 'publishers' of the contents. In case titled as *Kaschke V Gray*,[25] the Internet Service Provider while exercising editorial control over the website amended and corrected the language appearing on that website about the defamatory content posted on it by some of his users. The ISP was precluded from liability.

The law also obligates the ISPs regarding identification of their online users. They are required to point out the publisher or the author of the online material as and when required by legal forums. Sec. 5(3)(a) of the Defamation Act, 2013 provides that if the ISP does not produce the required data at the legal forum for the purpose of identification of the author, then he will not be in a position to claim immunity as provided under the law. In that case, he will be held as author of such online content.

In the *Oriental Press Groups Ltd vs. Fewaworks Solution Ltd*[26], the Hong Kong Court of Final Appeal based its judgment on the principle of "Knowledge and Control" criteria, according to which the Internet Service Providers cannot claim the defense of 'innocent dissemination' if they had knowledge and exercise control over the material posted on the website. The court determined that the ISP is subject to liability on the basis of having knowledge and control over the contents uploaded by its users on its website. The judgment was based on the common law principle of defamation. The brief facts of the case were that some defamatory statements were posted on the forum in years 2008 and 2009. The claimant brought those statements into the notice of the administrators of the forum and requested them to delete them immediately. The administrator of the website removed the statements appeared on the website in the year 2009, however, the statements of the years, 2008 remained there for a reasonable time and the administrator failed to remove them during that period. The court declared the forum responsible on the basis of having knowledge of the statements of the year 2008 and for not removing the same within reasonable time frame.

In another famous case *Byrean v Dean* 1937[27], the Court decided the case on the principle of acquaintance and held the defendant liable for the defamatory remarks written on the notice board which remained there for several days besides the fact that the defendant had knowledge about it.

In the same way, if some sort of defamatory material appears on the website which is uploaded by its online user and the ISP having knowledge about it does not remove the same within reasonable time then it stands on the feet of as publishers of the defamatory statements.

[23] Metropolitan International School v Designtechnica Corp. [2009] EWHC 1765 (Q.B)
[24] Bunt v Tilley [2006] EWHC 407 (Q. B)
[25] Kaschke Vs. Gray [2010] EWHC 690(QB)
[26] Oriental Press Groups Ltd v Fewaworks Solution Ltd 2013 HKEC (1025)
[27] Byrne v Dean [1937] 1 K.B. 818

The term Specific actual knowledge includes the gist of 'actual knowledge' which denotes the meaning of 'direct and clear knowledge', which is perceptibly different from the 'constructive knowledge', or awareness of such type of information which may persuade a sensible person to further inquire into the matter."[28]

No immunity will be given to the ISPs for the defamatory material appearing on the website if found working with malicious intention against the complainant.

(iii) Liability of Internet Service Providers– Position in Pakistan

Before the year 2002, a comprehensive law about the concept of 'cyber defamation' was not available under any Statute in Pakistan. The very first legislation was 'The Defamation Ordinance, 2002' which provided some governing laws to regulate the cases about defamation in Pakistan. This Ordinance was based on the common law principles of defamation. Before that, the remedy against defamation could be obtained either in the form of pecuniary damages from the civil court under the provisions of CPC, 1908 or by bringing an action before a criminal court of law under relevant sections of Cr.P.C. 1898 which was prescribing punishment of some imprisonment to the culprit along with award of damages to the victim. With the passage of time, this old criminal justice system proved inadequate and was found not well equipped to deal with sophisticated online threats.

To regulate effectively the cybercrimes law in Pakistan, the National Assembly of Pakistan promulgated the Prevention of Electronic Crimes Act (PECA), 2016. Although, at the time of its promulgation, the law was hotly debated in Pakistan, however, it paved a way to prevent cybercrimes and thus started to contribute in the national security of Pakistan.

Section 35 of "The Prevention of Electronic Crimes Act, 2016[29]" prevents all types of criminal as well as civil litigation against the ISPs in the country. If the ISP has Specific actual knowledge, actual notice given by the claimant or malice behind not removing the defamatory online material from the website then it may not claim immunity as per the law. However, the burden of proof is on the complainant that the ISP had the actual knowledge, actual notice or was nurturing some malice against him due to which he did not remove the defamatory contents.

Further, the conduct of intermediaries is also regulated under Section 35 of the Act ibid when online users commit cyber defamatory acts. In this case too, the ISPs find exemption from facing from all kinds of civil or criminal proceedings, however, they are under certain limitations under the new law, e.g., ISPs will not disclose any information about the investigation or procedure to the public except about those facts which are allowed to be disclosed by law. Moreover, under the new law, the ISPs are not under any obligation to proactively monitor the website contents. Their function starts only when a notice is served upon the ISPs by the claimant informing them of some defamatory content appearing on the website. In that case, they fall under obligation to remove such defamatory material from their website that too within a reasonable time. Thus, as per this law, now, an ISP can be held responsible for defamation when he fails to remove that reported obscene content from the website within reasonable time. Another condition precedent to bring action against an ISP is to establish the fact that he has actual knowledge of the obscene material on the website. The concept of actual knowledge has been taken from the common law principles. Lastly, the victim is required to establish malicious intent on the part of ISP.

Thus, a service provider cannot be subjected to a civil or criminal liability in Pakistan unless and until it is proved that he certainly had specific knowledge about the obscene material on the website and was indulged in willful intent to do so. In other words, he is required to proactively and positively commit that defamatory offence. Just omission to have a check over the alleged defamatory content on the website or failure on his part to remove the content without receiving any notice, does not entitle him to be prosecuted under the law. Moreover, the burden of proof will be on the shoulders on the person who is alleging defamation content on the website which is damaging his repute. All such developments are of positive nature which now provide protection to the ISPs and the same were not existing in the earlier law.[30].

Conclusion

[28] The Black`s Law Dictionary, 8th Edition.

[29] Section 35 of the Prevention of Electronic Crimes Act 2016 states that no service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not through merely omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, …
Clause 2 of the same section states that no provider shall under any circumstances are liable under this Act or under any other law for the time being in force for provision of services in good faith.

[30]Here's what you need to know about Prevention of Electronic Crimes Bill 2016 by Yasser Latif Hamadani @ the Real YLH, August 12, 2016.

As for conclusion, we can say that the developed countries are towards the trend of self regulation of online contents by the ISPs. For them, ISPs should be independent in their decisions of viewing, blocking, giving access or amending the online material provided by online users. They are legally assured that no litigation of any kind whatsoever in nature shall be conducted against them for doing so. The phenomenon may be called self regulation of online material by ISPs. The purpose behind is that ISPs would do so for public good only. However, it is inherently required to set up a fair mechanism to the said purpose, limiting the ISP's liability. Seemingly, there are some drawbacks in that targeted plans which portray an unfeasible future. When methodological developments are applied, these advance internet industry practices and also show discrepancies at national level combined with malpractices. These loopholes need to be highlighted with plausible resources to control it.

If the defamatory material comes into the notice of complainant, it will create an obligation upon the ISPs to remove that defamatory contents from the relevant website within a reasonable time. In case, they fail to do the same and that too within a period of reasonable time, only then they will be admitted as the authors of the content. Time period within which the defamatory contents are required to be removed by the ISPs has not been specified in the law. In this regard, the court is supposed to determine the reasonable time period by keeping in view the circumstances of each case. Pakistan and the UK law is in line in respect to the notice based liability. The USA law has offered immunity to ISPs even after notice is served by the complainant regarding online defamatory contents under the CDA Law 1996. In *Zeran v AOL*[31], the court observed that ISPs may not be held responsible just on the basis of notice-based-liability. In *Barrett v Rosenthal*[32], the court ruled that the ISPs are under obligation to evaluate the nature of contents which may be true or false, keeping in view public interest under the notice-based system before taking it down.

After examining the law on ISPs set out in "The Prevention of Electronic Crimes Act 2016" and the conventional common law principles of dissemination of defamatory statements, one may attribute similarity between the two i.e., ISPs liability is based on "Knowledge and Control based criteria".

Suggestions

There are few suggestions which are required to be put in "The Prevention of Electronic Crimes Act, 2016"

Provisions for editing rights by the ISPs in the website contents which are uploaded by the users may be incorporated through legislation. The ISPs may be ensured that that merely editing and changing the website contents does not entitle them to be authors or publishers. For just and absolute causes, editing and removing data from the website in the given circumstances must be allowed.

Some provisions must be framed for 'notice procedure' for the aggrieved person/complainant fixing some time limit for the ISPs to remove the undesired material from the website. This will facilitate not only to the complainant but also will ease the ISPs. At the same time, the notice procedure should be trouble-free in a way that the complainant may serve notice directly to the respective ISP. For that purpose, technicalities like court`s permission may not be conditioned.

ISPs should be given opportunities to identify the users and provide their identity along with obscene material as and when required by the law enforcing agencies. In such matters, the users must be facilitated through the legal process in the country. In cases, if the ISPs could not identify the original authors of the obscene material, the state should cooperate with them to identify the original author of the obscene material.

Encouragement must be given to the ISPs and intermediaries to monitor and vigilantly watch the websites to observe the online activities of their users. It may be made subject to the right of privacy and law. Moreover, just on the basis of knowledge, the ISPs may not be treated as authors and publishers of the obscene material. At the same time, the ISPs must act as "Good Samaritans" striving for public good.

To declare the obscene material as defamatory, some criteria must be prescribed through legislation on the point. For the purpose, the concept of Cyber defamation should be clearly placed amongst the category of cyber crimes and must be declared as a criminal act under the penal laws.

In order to prevent and block defamatory material on the website, the ISPs may be allowed to use screening programs in their websites. At the same time, if these screening programs do not spot online obscene material which may be because of certain technicalities involved in the internet technology. In those cases, the ISPs who are operating the website be protected against undesired litigation.

There is no disagreement that the cybercrimes of comprehensive nature are need of the hour. Cyber attacks and data leaks are rampant now-a-days. The existing laws, in certain cases fail to cater the newly emerging cyber crimes. Therefore, it is imperative for the legislature that the provisions of this law must be drafted in conformity with the international treaties like ICCPR and may not compromise the freedoms and rights of the people at the same time.

[31] Zeran v AOL [1997] 4th Cir 129 F.3d 327
[32] Barrett v Rosenthal [2006] 40 Cal. 4th 33