ANDHRA LEGAL DECISIONS

2000 (2) JOURNAL ALD

CYBER LAWS THE NEED OF THE HOUR

By

—A. SANTHOSH KUMAR

ADVOCATE

As the world enters the new millenium, if we take a glance at the past centuries the most effective invention affecting the very lives of the people has been the computer. Today every aspect of man's life has been more often than not controlled by artificial intelligence. If computer has made life more easier, the dawn of the internet has drastically reduced the boundaries of the world. Now the planet earth seems to have acquired the name of a "global village", with the communication system becoming more and more advanced and also cheap. The internet has thrown wide open the doors for computer based commerce, telephony, mail services and a lot of other areas thus shrinking the world to a entity which no historian nor a prophecy maker would have have thought of.

Technology brings with it both good and bad things, history has been witness to many a thing which would have been essentially been made for the good of the people, but ultimately the negative side of technology assuming preponderance over the positive. Here comes into picture the element of control over the negative side and here assume the greatest importance the Courts of law and the Legislature. One community which is registering exponential growth is that of the internet users due to its diverse benefits to a wide range of people. In this backdrop it is prudent to expect perpetration of crimes ranging from on-line defamation, on-line breach of contracts, bank frauds, on-line torts. This situation calls for a growth in understanding of the digital manipulations and the electronic communication systems on the part of the Legislature, the bar and the judiciary. Disputes relating to domain names, infringement of trademarks, breaching the security of systems, manipulating data, violation of copyright, violation of software patents, fraudulent electronic money transfer could be some of the crimes that could be perpetrated in the realm of cyberspace.

JURISDICTION IN CYBER SPACE

Since the nature of the internet has no boundaries the question of jurisdiction becomes very ephemeral and at the same time the most important issue. Hypothetically if A has been defamed by B by sending mail to C who happens to be A's neighbour but B lives in another country and the mail itself originated there, the question arises as to where the grievance has to be redressed. In the real world a person can usually locate the person or entity with whom it is interacting; this tends to facilitate identification of partners and validation of transactions. This process is far more difficult in cyberspace, when the parties in a transaction may be in adjoining rooms or half the world away, and the network offers no way to tell the difference. To add to the problem it is nearly impossible to screen the internet resources by a country. In some cases however the request and reply sequence may be used by the country which wants to screen requests originating from a hostile country but internet protocols were not designed to facilitate geographic documentation, they ignore it. Internet machines do have addresses but these locate the machine on the network and not in real space. Thus, the user may be accessing materials at a particular site, or he may be accessing copies of those materials located on a different machine half a world away. This means that not only is it impossible

to be certain of an Internet user's physical location, it is equally impossible to be certain of an Internet resource's physical location. Indeed, given that the network lends itself to distributed computing applications, an Internet resource may well have no discrete physical location — portions of the resource may be resident on many different machines around the world, to be transparently and seamlessly assembled as needed when called for.

DOMAIN NAME DISPUTES

The first case in India raising a dispute in relation to a domain name dispute was recently filed in the Delhi High Court. *Titan Industries Ltd. v Prashant Kooapati*, Delhi High Court *C.M. Nayar*, J. Unreported.

The domain name in question was 'Tanishq', in respect of which trade mark applications had been made by the plaintiffs in several countries around the world. The plaintiff had also obtained registrations in at least 23 countries in respect of jewellery, watches and clocks. An application for registering the trade mark in India was pending.

The defendants registered "www.tanishq.com" with the intention of operating a home page. The plaintiffs, who had been using the trade mark since the last 4 years, sued for passing off and alleged that the use of the domain name by the defendants would lead to confusion and deception and damage the goodwill and reputation of the plaintiffs.

The Delhi High Court held that there is a *prima facie* case in favour of the plaintiffs for grant of an *ex-parte* ad-interim injunction. The Court accordingly restrained the defendants from registering a name or operating any business, and making, selling, offering for sale, advertising and in any manner dealing in any goods under the name 'Tanishq' or any other name which is identical or deceptively similar to the plaintiff's trade mark TANISHQ or containing the said work as an essential or dominant feature thereof, on the internet or otherwise and from doing any other thing as is likely to lead to passing off of the business and goods of the defendants as the business and goods of the plaintiff.

The said injunction speaks about restraining the defendants from registering the said domain name, but the said injunction has to be directed to the firm which has actually registered the domain name for which the Indian Courts lack jurisdiction. The remedy for the plaintiffs to actually remove the domain name is to approach the firm registering the domain name and then would arise another round of litigation and complexities. Some well publicised examples of these types of domain names disputes are:

candyland.com: Both *Hasbro* and an adult entertainment provider desired the candyland.com domain name. *Hasbro* was too late to register the name itself, but it is never too late to sue (well, almost never). The domain name is now in suspension until the resolution of the lawsuit.

mcdonalds.com: This domain name was taken by an author from Wired magazine who was writing a story on the value of domain names. In his article, the author requested that people contact him at **ronald@mcdonalds.com** with suggestions of what to do with the domain name. In exchange for returning the domain name to McDonalds, the author convinced the company to make a charitable contribution.

microsoft.com: The company Zero Micro Software obtained a registration for micros0ft.com (with a zero in place of the second 'o'), but the registration was suspended after a protest was filed by Microsoft.

mtv.com: The MTV domain name was originally taken by MTV video jockey *Adam Curry*. Although MTV originally showed little interest in the domain name or the Internet, when *Adam Curry* left MTV the company wanted to control the domain name. After a Federal Court action was brought, the dispute settled out of Court.

peta.org: An organisation entitled "People Eating Tasty Animals" obtained the peta.org domain name, much to the disgust of the better know People for the Ethical Treatment of Animals. This domain name is also suspended pending resolution of the dispute.

roadrunner.com: When InterNIC threatened to suspend the roadrunner.com domain name after a protest by Warner Brothers, the New Mexico Internet access provider who was using the domain name filed suit to prevent the suspension.

taiwan.com: The mainland China news organisation Xinhua was allowed to register the domain name taiwan.com, much to the disgust of the Government of Taiwan.

There are many more domain name disputes which have arisen in the last year, a list of which is being maintained at Georgetown University.

InterNIC:

When a dispute over a domain name occurs, such as those described above, the parties usually turn to two places simultaneously: the Courts and InterNIC. InterNIC, as explained above, is responsible for the registration of second level domain names for these top-level domains: .COM, .EDU, .NET, .ORG, and .GOV. Since InterNIC does not handle registrations relating to other top-level domains, it does not become involved with disputes over names in those other top-level domains. However, since the vast majority of new domain names are under one of these top-level domains (most commonly .COM), InterNIC has become the focal point of disputes over these names.

InterNIC is not so much of an organisation as it is a co-operative activity between three organisations: the National Science Foundation, Network Solutions, Inc., and AT&T. The National Science Foundation has a supervisory role. AT&T manages the domain name directories and databases. Network Solutions Inc. (NSI) manages the actual registration of domain names, and therefore is the real organisation that is attempting to manage domain name disputes.

While Courts and Judges have the authority to award control and ownership over domain names (just as they have authority to award control and ownership over any other property), the judicial process is notoriously slow. Consequently, the control and ownership of disputed domain names while a Court case is pending can be a very important issue.

VIRUSES

Computer viruses are increasingly of concern—both for operators of computer information systems and for users of the systems. But what is a virus? A virus refers to any sort of destructive computer programme, though the term is usually reserved for the most dangerous ones. Computer virus crime involves an intent to cause damage, "akin to vandalism on a small scale, or terrorism on a grand scale". Viruses can be spread through networked computers or by sharing disks between computers. Viruses cause damage by attacking another file or by simply filling up the computer's memory or by using up the computer's processor power. There are a number of different types of viruses, but one of the factors common to most of them is that they all copy themselves (or parts of themselves). Viruses are, in essence, self-replicating very famous virus in India was discovered in India called the "JOSHI" virus in the year 1990. The virus displays on every January 5 "Type happy Birthday Joshi" and when typed everything returns to normal,system memory decreases by 6 KB when the virus is resident.

Computer crime is an ever-present area of concern for operators of networked computer systems. Operators continuously find themselves needing to devote substantial resources to avoid falling victim to system-crackers and the like. The term "computer crime" covers a variety of offenses, including: unauthorised access to and use of computer resources, data theft, damaging stored data, engaging in service attacks, trafficking in stolen passwords, spreading computer viruses, and a number of other related offenses. All of these activities are often referred to as "hacking". Hackers can get into other systems *via* internet and can do a host of things like reading e-mails, transferring accounts, and filling the system with pornographic material. Legislation making these things punishable is the need of the hour.

DEFAMATION : The issue raised here is that can a person sue for defamation that occurred to a fictitious name or a persona that appears on a computer? If user's real name, is not used while communicating through the internet could the real user (the actual person being defamed) sue the person sending the communication for defaming the user's persona on the internet. In the internet community, unless users know each other in real life away from the computer, the only impression one user gets of another is from how he or she appears on the computer screen. The user in real life may not even be the same sex as the person he or she portrays on the screen of the computer.

INDIAN LEGISLATIONS ON CYBER RIGHTS AND CRIMES

In India, the Intellectual Property Rights (IPR) of computer software are covered under the Copyright Law. Accordingly, the copyright of computer Software is protected under the provisions of Indian Copyright Act, 1957. Major changes to Indian Copyright Law were introduced in 1994. These changes came into effect from 10th May, 1995. This has made the Indian Copyright Law, one of the toughest in the world. The amendments to the Copyright Act introduced in June, 1994 were a landmark in the copyright regime of India. For the first time in India, the Copyright Law clearly explained the rights of copyright holder, position on rentals of software, the rights of the user to make backup copies and most importantly, the amendments imposed heavy punishment and fines for infringement of copyright of software and fines for infringement of copyright of software. Software creates unique problems because it is so easy to duplicate and the copy is usually as good as original (although many a times plagued with computer virus). The fact, that the copy is as good as original, however, does not legitimate piracy. The Copyright infringer may be tried under both civil and criminal law.

Sec 2(ffb) defines a computer as - "computer" includes any electronic or similar device having information processing capabilities;

Sec 2 (ffc) defines " computer programme" as a set of instructions expressed in words, codes, schemes or in any other form , including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular result.

Sec 2(o) defines "literary work" as including computer programmes, tables and compilations including computer databases;

According to Section 14 of the Copyright Act, it is illegal to make or distribute copies of copyrighted software without proper or specific authorisation. The only exception is provided by Section 52 of the Act, which allows a backup copy purely as a temporary protection against loss, distribution or damage to the original copy.

Section 14 of the Copyright Act, 1957: Meaning of copyright : For the purposes of this Act, "copyright" means the exclusive right subject to the provisions of this Act to do or authorise the doing of any of the following acts in respect of a work or any substantial part thereof, namely-

a) in the case of a literary, dramatic or musical work not being a computer programme,—

i) to reproduce the work in material form including the storing of it in any medium by electronic means

ii) to issue copies of the work to the public and not being copies already in circulation;

iii) to perform the work in public , or communicate it to the public ;

iv) to make any cinematograph film or sound recording in respect of the work ;

v) to make any translation of the work ;

vi) to make any adaptation of the work ;

vii) to do in relation to a translation or an adaptation of the work, any of the acts specified in relation to the work in sub-clauses (i) to (vi);

b) in the case of a computer programme—

(i) to do any of the acts specified in clause (a);

(ii) to sell or to give on hire, or offer for sale or hire, any copy of the computer programme, regardless of whether such copy has been sold or given on hire on earlier occasions

Relevant portion of Section 52

Section 52 : Certain acts not to be infringements of copyright : (1) The following acts shall not constitute an infringement of copyright, namely:-

"(aa) the making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme, from such copy—

(i) in order to utilise the computer programme for the purpose for which it was supplied: or

(ii) to make up backup copies purely as a temporary protection against loss, destruction or damage in order only to utilise the computer programme for the purpose for which it was supplied;"

The 1994 amendment to the Copyright Act also prohibits the sale or to give on hire, or offer for sale or hire, any copy of the computer programme without specific authorisation of the Copyright holder. A civil and criminal action may be instituted for injunction, actual damages (including infringer's profits) or statutory damages per infringement *etc*. Moreover, with the amendments to Indian Copyright Act in 1994, even the criminal penalties have substantially increased. Section 63-B, stipulates a minimum jail term of 7 days. The jail term could be extended up to three years. The Act further provides for fine ranging from Rs. 50,000 to Rs.2,00,000, and jail term up to three years for such an infringement.

Section 63 B : Knowing use of infringing copy of computer programme to be an offence : Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable with a term of imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees:

Provided that where the computer programme has not been used for gain or in the course of trade or business, the Court may, for adequate and special reasons to be mentioned in the judgment, not impose any sentence of imprisonment and may impose a fine which may extend to fifty thousand rupees.

Agencies of Government of India have been very actively participating in protection of the rights of Copyright holder. Both Department of Electronics and Ministry of Human Resource Development have been active in incorporating amendments to the Indian Copyright Act. These agencies are now helping the law enforcing agencies *e.g.*, the Police to enforce the law.

THE PROPOSED INFORMATION TECHNOLOGY BILL, 1999

The proposed IT Bill '99 draws from the model law on electronic commerce as framed by the UN Commission on International Trade Law (UNCITRAL) as well as from the US State Laws of Utah and Ilinois on electronics and digital signatures and the Electronics Transactions Act passed by Singapore in June, 1998. Some of the main features of the proposed law which will cover e-commerce include the setting up of an elaborate machinery for licensing, monitoring and certifying authorities (Part V Sections 18 to 37). For this, a controller is to be appointed. Contravention of the regulations will be adjudicated by adjudicating officers who would be empowered to impose penalty. (Part VIII Section 46 to 49)

A Cyber Regulations Appellate Tribunal (Part IX from Section 50 to 65) is also proposed to hear appeals on the decisions of the adjudicating officers. It is also proposed that any department or Ministry may accept the filing, creating and retention of documents in form of electronic record. There will be liability of pay compensation for unauthorised access to computer, computer network and computer data base. Any document which

under the law requires a signature, a digital signature would satisfy that requirement. Such a Legislation would also amend existing Acts like the Indian Evidence Act and Indian Penal Code. It is felt that framing of cyber laws in the country has become absolutely necessary to facilitate international trade within a global IT environment.

The Preamble provides to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and for matters connected therewith or incidental thereto; Whereas the General Assembly of the United Nations by resolution A/RES/51/162 dated 30th January, 1997 has adopted the Model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law ;

AND Whereas the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper based methods of communication and storage of information;

AND Whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records;

BE it enacted by Parliament in the Fiftieth Year of the Republic of India as follows:-

The relevant portion addressing to the issue of computer crimes in part XI is being reproduced below :

Tampering with computer source documents :

66. Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with a fine which may extend up to rupees two lakhs or with imprisonment up to three years, or with both.

Explanation :—For the purposes of this section computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Publishing of information which is obscene in electronic form

67. Whoever publishes or causes to be published in the electronic media any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprive and corrupt persons who are likely having regard to all relevant circumstances to read, see or hear the matter contained or embodied in it shall be punished on first conviction with imprisonment of either description for a term which may extend to two years and with fine which may extend to twenty five thousand rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to fifty thousand rupees.

Penalty for misrepresentation :

68. If any person makes any misrepresentation or suppresses any material fact to the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Breach of confidentiality :

69. Save as otherwise provided in this Act or any other law for the time being in

force if any person who, in pursuant to any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty for publishing Digital Signature Certificate false in certain particulars :

70. (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty for failure to furnish information, return, etc.

71. If any person, who is required under this Act or any rules or regulations made thereunder fails to,—

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a fine not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding give thousand rupees for every day during which such failure continues;

(c) maintain books of accounts or records, fails to maintain the same, he shall be liable to a fine not exceeding ten thousand rupees for every day during which the failure continues.

Offences by companies

72. (1) Where an offence or contravention under this Act has been committed by a company, every person who at the time the offence or contravention was committed was in charge of, and was responsible to the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence or contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act, if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

(2) Notwithstanding anything contained in sub-section (1), where an offence or contravention under this Act has been committed by a company and it is proved that the offence or contravention has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence or contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section,—

(a) "company" means any body corporate and includes a firm or other association of individuals; and

(b) "director", in relation to a firm, means a partner in the firm.

Publication for fraudulent purpose

73. Whoever knowingly creates, publishes or otherwise makes available a Digital

Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Act to apply for offences committed outside India

74. (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any contraventions and offences committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1) this Act shall apply to an offence committed outside India by any person if the Act constituting the offence involves a computer, computer system or computer network located in India.

Protected system

75. (1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network system to be a protected system.

(2) The appropriate Government may, by order in writing authorise the persons who are authorised to access protected systems.

(3) Any person who secures access or attempts to secure access to a protected system in contravention of this section shall be punished with imprisonment for a term which may extend to ten years.

Confiscation

76. Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act or regulations made thereunder has been or is being contravened, shall be liable to confiscation :

Provided that where it is established to the satisfaction of the Court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act or regulations made thereunder, the Court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person guilty of the breach of the provisions of this Act or regulations made thereunder as it may think fit.

Compensation and Confiscation not to interfere with other punishments

77. No award of any compensation under Part IX shall prevent the infliction of any punishment to which the person affected thereby is liable under the provisions of this Act or under any other law.

Power to investigate offences

78. Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (1 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence or contravention under this Act.

AMENDMENTS :

Indian Penal Code, 1860 : Sections 29, 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 469, 470, 471, 477-A

Indian Evidence Act, 1872 : Sections 3, 22, 34, 35, 47, 59, 65, 73, 81, 85, 88, 90, 131

Amendments are also sought to be made to the Banker's Book Evidence Act,1891 & Reserve Bank of India Act,1934.

Conclusion : Only time would tell how these issues relating to the cyber world can be resolved with the law addressing these aspects is only in its nascent stage. India which is growing as a major consumer of the software market and as a major user of the internet has to see that the Information Technology Bill, 1999 is passed as soon as possible and the provisions implemented with impunity complementing the Copyright Act, 1957.