

THE HINDU Business Line

INTERNET EDITION

Financial Daily from THE HINDU group of publications

Wednesday, Sep 10, 2003

- Home
- News
- News Update

eWorld

- Columns
- eWorld
- Index
- Archives

Features

- Investment World
- eWorld
- Catalyst
- Mentor
- Life
- Canvas
- Praxis
- Urban Pulse
- Brand Quest

Stocks

- Quotes
- SE Diary
- Scoreboard
- Open-End Mutual Fund

Port Info

- Ships in Ports

Archives

- Yesterday
- Datewise
- Resources

Group Sites

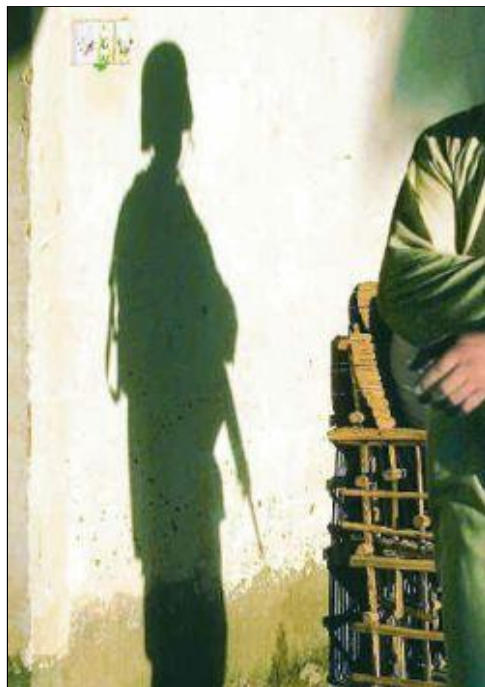
- The Hindu
- Business Line
- The Sportstar
- Frontline
- The Hindu eBooks

eWorld - Security

Dark deeds remain in the dark

Vipin V. Nair

It's not the law but the attitude that is flawed when it comes to tackling cyber crime, say experts. And as long as this sort of indifference continues, such acts of felony will remain shrouded in mystery.



IN May 2000, at the height of the dot-com boom, India enacted the IT Act and became part of a select group of countries to have put in place cyber laws. Three years down the line, is the Internet a better place to live in? Are those cyber criminals behind bars? Are we shopping mad online?

Well, not really. The Internet is still a dirty place to hang out; beware those viruses and spam mails. Cyber hooligans are growing in numbers and are very much at large. And we are still wary of using our credit card online.

Despite the enactment of cyber laws and their existence for three years, a lot more needs to be done, both online and offline, as well as within the judiciary and law enforcement agencies, experts feel. However, a number of right steps have also been taken to make the IT Act more relevant in today's context.

The problem areas

Stories in this Section

New, but for how long?

One pillar too many?

Under the hammer, and thriving

Setting up a message folder

Problems in receiving messages

Printing problems

The mind of a VC

Dark deeds remain in the dark

Purely for the fun of it

Caught copying

Quiz

A new tribe in the making

Standing the test of a test

Cartoon

In all these years, despite the growing crime rate in the cyber world, only less than 25 cases have been registered under the IT Act 2000. And no final verdict has been passed in any of these cases as they are now pending with various courts in the country.

"Although the law came into operation on October 17, 2000, it still has an element of mystery around it. Not only from the perception of the common man, but also from the perception of lawyers, law enforcing agencies and even the judiciary," says Pavan Duggal, Supreme Court lawyer who specialises in cyber laws.

Duggal says the prime reason for this is the fact that the IT Act is a set of technical laws. "By nature, we prefer to stay away from technicalities," he says. Another major hurdle is the reluctance on the part of companies to report the instances of cyber crimes, as they don't want to get negative publicity or worse get entangled in legal proceedings.

"We had a problem not with the law but with the attitude. In the last three years we have actually seen an under reporting of cyber crime cases," Duggal says. Even the government departments whose websites have been hacked left, right and centre by Pakistani hacker groups, have not bothered to register a case. The only case against hacking was filed by the Centre Board of Direct Taxes (CBDT) when its website was hacked on April 1, 2002.

According to Kiran Karnik, President of National Association of Software and Service Companies (Nasscom), the association is encouraging member companies to come out and report instances of cyber crimes. "We are conducting workshops for our members on this issue," Karnik says. Besides, Nasscom is also doing awareness campaigns and workshops for police and other enforcement agencies across the country.

A major hurdle in cracking down on the perpetrators of cyber crimes such as hacking is the fact that most of them are not in India. The IT Act does give extra-territorial jurisdiction to law enforcement agencies, but such powers are largely inefficient. This is because India does not have reciprocity and extradition treaties with a large number of countries.

What India needs to do in this backdrop, is to be a part of the international momentum against cyber crime. The only international treaty on this subject is the Council of Europe's Convention on Cyber Crime, formulated primarily by the European Union. By signing this treaty, member countries agree on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals.

At the last count, there are 43 member countries, including the US and South Africa. India is not yet a part of this group and being a member would go a long way in addressing this issue of cross-border cyber terrorism.

The Indian IT Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crime and criminals. "We are now beginning to see new

categories and varieties of cyber crimes, which have not been addressed in the IT Act. This includes cyber stalking, cyber nuisance, cyber harassment, cyber defamation and the like," Duggal points out.

Another glaring omission in the Act, which contradicts the very objective of passing such a law - encouraging e-commerce by giving it legal validity — is the fact that the IT Act does not cover electronic payment. However, some steps such as amendments to the Negotiable Instruments Act have been taken to address this issue. Also in the making is a law on data protection.

The right side of law

The shortcomings of the law notwithstanding, there have been positive developments as well. "We have made progress. We have actually seen crystallisation of public opinion and the awareness has been rising about cyber law and cyber crime," says Duggal.

The legal validity of the electronic format such as emails is one of the major outcomes of enactment of the IT Act. E-mails and their print outs are now accepted as legal evidence by courts. In fact, in the Parliament attack case, the Special Judge has given the due evidential value on e-mails and electronic data contained in the seized laptop of terrorists.

Although there is paucity in numbers, a wide range of cases is now booked at the IT Act, ranging from theft of Internet hours to cyber defamation to pornography to hacking to cheating. In fact, Asia's first case of cyber defamation is filed in India in the case of SMC Numatics Ltd. Vs Jogesh Kwatra. Defamatory emails were allegedly sent to the top management of SMC Numatics by the defendant, who has since been restrained by the Delhi High Court from sending any form of communication to the plaintiff.

A case has even been filed against the 419 cheaters from Nigeria. A person in West Bengal was duped by e-mails and he sent his notebook across, only to realise that he was cheated.

Perhaps the most notorious case filed till date under the Indian IT Act is that of Dr L. Prakash, a well-known orthopaedist in Chennai. On charges of alleged pornography, he was arrested and has been in jail for 23 months now, as the courts refused to grant him bail. "It is very difficult to get bails under the IT Act because of the extent of media attention on such cases The Media almost conducts a parallel trail," Duggal points out.

Another positive aspects are the increasing awareness among law enforcement agencies on the need to set up special cells to handle cyber crime. The CBI has a well-established cyber crime cell. The first cyber crime police station has also come up in Bangalore. But the challenges for the cops are rising by the day as they are dealing with crimes committed by vicious brains rather than brawn.

vipin@thehindu.co.in

[Article](#) [E-Mail](#) :: [Comment](#) :: [Syndication](#)

The Hindu Group: [Home](#) | [About Us](#) | [Copyright](#) | [Archives](#) | [Contacts](#) | [Subscription](#)
Group Sites: [The Hindu](#) | [Business Line](#) | [The Sportstar](#) | [Frontline](#) | [The Hindu eBooks](#) | [Home](#) |

Copyright © 2003, The Hindu Business Line. Republication or redissemination of the contents of this screen are expressly prohibited without the written consent of The Hindu Business Line
