Corporate criminal liability: the case of Baazee.com

By Priti Suri and Rohan Jhusiwala, PSA, Legal Counsellors

PSA
Legal Counsellors
14A & 14B Hansalaya, 15 Barakhamba Road
New Delhi - 110001, India
Tel: +91 11 4350 0500
Fax: +91 11 4350 0502
www.psalegal.com
Email: p.suri@psalegal.com

Corporate criminal liability is an important item on the agenda of legislators and legal practitioners, yet it has not been defined under any statute, rule or regulation in India. In general terms, it refers to the imposition of criminal liability on a company or its employees for an illegal act. The Indian law on corporate criminal liability is not confined to the general criminal law under the Indian Penal Code (IPC), 1860, but is scattered across several statutes, including the Negotiable Instruments Act, 1881, and the Information Technology (IT) Act, 2000.

Broadly speaking, the IT Act categorizes cyber crimes in three groups. The first category includes wrongs such as damage to computers and computer systems. These acts or omissions are not subject to criminalization and *mens rea* (criminal intent) does not apply; but they are subject to the liability principle, attracting penalties in the form of fines. The second category covers tampering with computer source documents and hacking, in which *mens rea* is an integral part of the offence. The third category deals with acts or omissions such as breach of confidentiality and privacy, which incur criminal liability under the vicarious liability principle.

The IT Act requires all Indian companies to have an IT security policy which covers a range of areas including the role and responsibility of employees, security parameters, authorized data access and retention and authentication of electronic records. Further, both a company and its officials can be made liable for contravention of the provisions.

Accountability requirements are outlined in section 85 of the IT Act. These impose liability on every person who was in charge of and responsible to the company when an offence was committed, and on any director, manager, secretary or other officer who consented to it. In this way section 85 allocates collective and vicarious responsibility to every person directly responsible for an offence, and also on the employer for employees' wrongful acts.

The IT Act underwent an important test when it was discussed by Delhi High Court in *Avnish Bajaj vs State*, which was decided on 29 May 2008. The plaintiff was the managing director of an auction website, Baazee.com, who had been arrested and charged under sections 67 and 85 of the IT Act (which relate to the transmission of obscene material through electronic media) and various provisions of the IPC, following the posting of an obscene video on the website by a third party. The plaintiff filed a petition before the court, asking for the criminal proceedings to be quashed on various grounds.

The case instigated a debate on the application of section 292 of the IPC (which deals with the sale of obscene books), and of section 67 of the IT Act. The charges under the IPC were quashed by the court, but the court allowed prosecution under the IT Act to continue before the trial court. The court recognized "deemed criminal liability" of the directors of the accused company, which meant it was not necessary for the company itself to be a party to the case in order to proceed against its directors.

Several important findings have emerged from the Baazee.com case. Firstly, a company disseminating information about products online will be deemed to be advertising and causing the products to be sold. This means that companies posting advertisements on their website which are in breach of any Indian law will be held liable under the IT Act. Accordingly, there is an increased burden on companies which use online advertisements to generate revenue to perform detailed checks on the content of the advertisements.

Furthermore, websites allowing users to sell or purchase goods must ensure that these transactions are not illegal. There is a need for a protocol that clearly sets out the guidelines website companies should follow when allowing such transactions.

Finally, the impossibility of checking every online listing due to a high volume of online transactions does not constitute a defence. Failure to adhere to the restrictions on the listing of illegal material may result in criminal liability for the company maintaining the website.

Several steps would enable a more potent implementation of corporate criminal liability. Defining "due diligence", and limiting the powers of the police to arrest suspects without warrant under section 85 (which occurred in the Baazee.com case), would enable the police to exercise restraint at the preliminary stage – that is, before arresting a suspect.

In addition, network service providers – including employers providing internet access to their employees – should not be made liable for all third-party information or data made available by them. However, employers must incorporate the cyber law compliance requirements of the IT Act in their business processes, and follow a strict monitoring regime. There is also a need to establish a regulatory framework to deal with corporate criminal offences under the IT Act.

As the first cyber crime case to go through the courts in India, the Baazee.com case was a watershed in the nation's cyber law history. The criminal provisions under the IT Act have drawn a lot of criticism, mainly from within the IT industry. However, it is imperative that these provisions be retained, while the issues highlighted by the case are addressed through judicial precedents and by fine-tuning relevant sections of the IT Act.

Priti Suri is the proprietor of PSA where Rohan Jhusiwala is an associate.