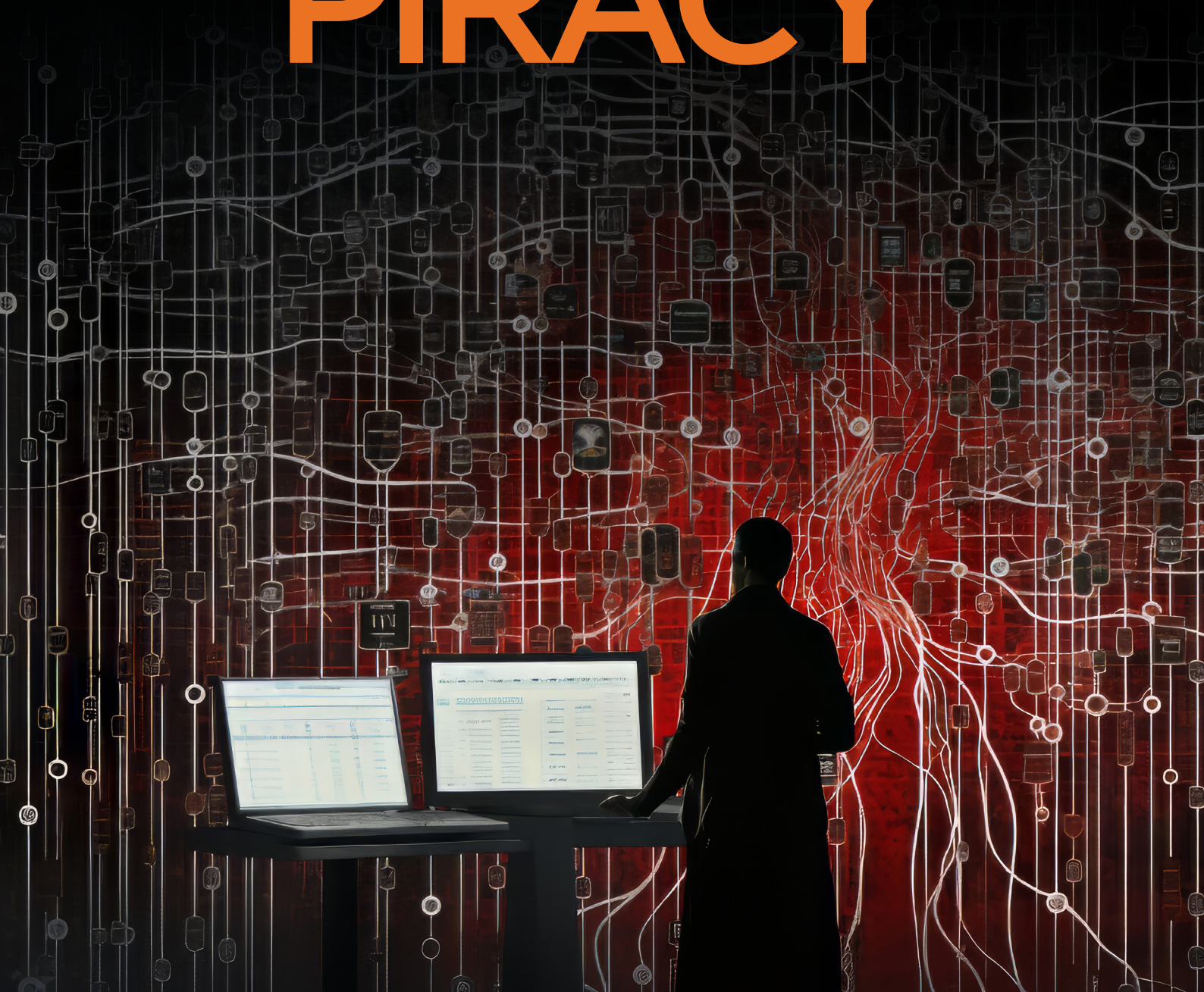


Fight Against PIRACY



LawPickle

www.lawpickle.com

Like the oceans, the internet was under the siege of pirates, engaging in digital piracy!

There is no denying that digital piracy leads to significant revenue loss for both the content producers and the for the government.

Initially, Courts combated digital piracy by directing the Internet Service Providers (“ISPs”) to block access to URLs storing infringing content. However, it was soon realized that the infringer operating the URL can create a new one within a few seconds. For the first time the Hon’ble Delhi High Court passed a judgment in Department of Electronics and Information Technology v. Star India Pvt. Ltd., FAO (OS) 57/2015, directing the ISPs to block access to the domain name, thereby moving forward from URL blocking to website blocking.





To battle it out with the ongoing piracy, the Hon'ble Delhi High Court delivered its most comprehensive judgement in 2019, i.e., *UTV v 1337x.to*, CS(COMM)724/2017 ("UTV Judgment"). The UTV judgment was significant because it provided:

- **Website Nature Assessment:** The Hon'ble Court established the factors for determining whether a website is "rogue";
- **Dynamic Injunction:** The Hon'ble Court recognized that rogue websites are "Hydra-Headed", you cut off one head, two more would grow back. To tackle the menace of hydra-headed websites, the Hon'ble Court fashioned the remedy of 'Dynamic Injunction'. Right owners could extend the blocks to newly found redirects / mirrors / alpha-numeric variations of the already blocked rogue website by filing impleadment applications before the Ld. Joint Registrar.
- **Test for Rogue Websites:** The Hon'ble Court conclusively held that the test for examining the Rogue nature of website is a qualitative approach and not quantitative. It has to be established that the primary purpose of the website is to engage in copyright infringement and/or disseminate the copyrighted content;
- **ISP Obligations:** The UTV judgment reiterated that as ISPs are intermediaries, they are bound to take down the infringing domains communicated to them by right-owners as court orders constitute actual knowledge;
- **Digital Piracy as a crime:** The Hon'ble Court held that digital piracy is equivalent to physical piracy;
- **Necessary and Proportionate Blocking:** The website blocking order should be passed if the Hon'ble Court is satisfied that it is 'necessary' and 'proportionate.'

ORDERS ADOPTED BY THE HON'BLE COURTS TO TACKLE ONLINE PIRACY



The UTV Judgment was the springboard for passing innovative orders against the ever-evolving forms of piracy:

- a. Global Blocking of Rogue Websites:** Orders directing Domain Name Registrars (“DNR”) to lock and suspend infringing domain names has led to a global shut down of rogue websites. This proves more effective than ISP blocking as this is effective only in the concerned country and there are technical means available (e.g. through VPNs) to access the rogue websites. Further, any website which is suspended by DNRs is not shown as part of index published in the Google search engine.
- b. Pirate brand orders:** Many sites have become well-known for making available pirated content such as ThePirateBay or KickAssTorrents. In such cases, third parties, unassociated with the main operator have also started copy-cat rogue domains under the same brand. By way of such ‘Pirate Brand’ orders, Courts have permitted right owners to extend the original blocking order to such new online locations that are associated with the original ‘rogue’ website on the basis only of “its name, branding or identity of its operators”.
- c. Blocking Cyberlockers :** Cyberlockers are online data hosting services that provide remote file storage space with a secure storage architecture and file sharing services. They act as sophisticated uploading and streaming platforms that disseminate pirated content to and from their servers on devices connected to the Internet. Courts have directed blocking of ‘rogue’ cyberlockers and their servers thereby not just the access to the road is blocked, but also the warehouse.
- d. ‘Dynamic+’ injunction:** Orders have been passed by Courts to protect works generated during the pendency of the suit as also works that will be created in the future .

- e. Blocking of Telegram channels / WhatsApp groups :** Noting that large scale piracy is occurring through organized Telegram channels or WhatsApp groups, Courts in such instances have passed the following directions:
- i. Directed the suspension of such Telegram channels and WhatsApp groups;
 - ii. Directed the disclosure of the details of the group admins operating such channels / group to enabling the right owners to take appropriate actions.
 - iii. Directed Telecomm Service Providers to disclose KYC details of individuals to whom the impugned phone numbers are registered.
- f. Quia-Timet Actions:** The Hon'ble Court has on numerous occasions passed orders blocking websites for protecting copyright content which is yet to be released . For instance for movies which are to yet to be released in theatres or on a OTT Platform.
- g. Blocking of Rogue Mobile Applications:** In the case of Rogue mobile applications hosting primarily infringing content, the Hon'ble Court passed the following directions for effective blocking:
- i. Direct blocking of the source User Interfaces used by the mobile applications to connect with the server which stores the infringing content.
 - ii. Blocking orders against the websites which provides .apk files (software) for downloading these rogue mobile applications.
- h. Tackling Real-time piracy of live sports broadcast:** The Courts noted that during the short duration of a live broadcast of a sporting event, new rogue websites emerge with the sole aim of broadcasting the same. To address this issue, Courts have permitted right owners:
- i. to directly communicate the list of rogue websites to ISPs impleaded in the suit so that these can be blocked on real-time basis.
 - ii. Further, Dept. of Telecommunications and Ministry of Electronics and Information Technology are also directed to issue blocking orders to ISPs immediately upon receipt of right owners' communication.
 - iii. Domain Name Registrars are directed to lock and suspend the websites within 72 hours of being provided with the Court order.