LAW AND ETHICS

IN

INFORMATION SECURITY.

Adm: SCII/01342/2018.

Name: NELIUS MUKAMI.

HOW SOFTWARE LICENSE INFRIGEMENT, ILLICIT USE AND MISUSE OF CORPORATE RESOURCES ARE HANDLED IN KENYA, INDIA, US AND ENGLAND.

In Kenya:

Infringement is defined by the Kenyan Copyright Act as an act that violates a right protected by the Act. Software infringement is the unauthorised reproduction or copying of someone's original work without their authorization. The taking of the whole or major portion of software, like other literary works, is a kind of infringement. Where there is a substantial reproduction of the original, copyright covers selective, changed, summarized, and otherwise varied versions of the work. This is commonly referred to as adaptation, and if done without permission, it is clearly defined as an act of infringement. Many infringement accusations are based on straightforward incidents of piracy where the copying is clear. Others, on the other hand, are more difficult to resolve because copyright protection does not apply only to exact copies.

Software protection.

Local legislation as well as multilateral accords such as the Universal Copyrights Convention and the Berne Convention on Literary Works give protection. The Berne Convention is administered by the World Intellectual Property Organization (WIP0), a specialized entity of the United Nations. Since June 1993, Kenya has been a signatory to the Berne Convention on Literary and Artistic Works. The Convention ensures that copyrighted works are protected in member states.

Methods adopted to prevent copying.

Copy protection and digital rights management approaches, which include addition of software or hardware to prevent software from unlawful copying, have been employed by software developers. Software owners have devised a variety of gadgets and methods to secure their software.

Coding software in such a way that it triggers faults in copying programs while remaining legible for normal use is one of the approaches used to safeguard it against copying.

Large software development companies have begun to include dongles in their products. Dongles are used to ensure that only authorized users have access to specific software applications. When an application that comes with a dongle is loaded, it checks the dongle for verification. If the application is unable to locate the dongle, it simply exits. This indicates that without the dongle is present, the program will not operate on the PC. The dongles are usually provided by software manufacturers along with the product's media at the time of purchase, but they may also be offered if the purchaser wants to make updates to the software with the owner's consent.

Product activation keys or codes are yet another way employed by software development companies. This strategy renders a software product useless or severely limits its functionality until it is registered with a publisher using a unique identification or activation number. The method frequently hashes information about the specific configuration of the hardware on which the software operates with the product's license identification number. Workarounds to bypass the product activation mechanism have been created, reducing the system's capacity to prevent software from copying significantly.

Some software developers choose to scramble the program code on the magnetic disk where the software is stored or to change the disk directory. This is done to prevent the application from being copied from the disk. There are additional technologies that degrade the quality of software copies made from the original.

Infringers and those who make infringement feasible can be prosecuted by software owners. This prohibits the offender from infringing again and acts as a deterrence to future infringers.

In India:

Cybercrime has evolved into a major menace to humanity. Cybercrime protection is critical for a country's social, cultural, and security aspects. To combat cybercrime, the Indian government passed the Information Technology Act of 2000. The IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 are also revised by the Act. Cybercrime can originate anywhere in the globe and go across national borders via the internet, complicating both the technological and legal aspects of detecting and prosecuting these crimes.

"The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000) that was notified on October 17, 2000," according to Wikipedia. It is India's most important law dealing with digital crimes, often known as cybercrimes, and electronic trade. To combat cybercrime, worldwide harmonization efforts, coordination, and cooperation among diverse states are essential.

In United States:

In the United States, intellectual property is considered a protected asset. Copyright rules in the United States extend this protection to the printed word, including electronic formats. Fair use of copyrighted works includes using them to support news reporting, teaching, scholarship, and a variety of other related activities, as long as they are used for educational or library purposes, are not commercial, and are not excessive. It is perfectly acceptable to use portions of someone else's work as reference as long as due recognition is given to the original author of such works, including a clear description of the location of source materials (citation), and the work is not represented as one's own.

U.S. laws protecting privacy include the Federal Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and the Health Insurance Portability and Accountability Act of 1996.

England:

The Copyright, Designs and Patents Act of 1988 is the main legislation controlling copyright (CDPA). To update the CDPA and apply the EU copyright directives, several acts and regulations have been passed.

European Council Cyber-Crime Convention.

In 2001, the European Council adopted the European Council Cyber-Crime Convention. It establishes an international task force to supervise a variety of security functions related to Internet activities in order to establish harmonized technology regulations across international borders. It also aims to improve the efficacy of international investigations into technological law violations.

References.

1. Gichuid, F. (2010). Software copyright protection in Kenya the law and practice.
2. Legal, Ethical and Professional Issues in Information Security (n.d). *University of Arkansas Grantham Website*. Retrieved June 13th, 2022, from https://content.grantham.edu/at/IS211/ch03.pdf
3. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cybercrime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 1633-1640.
4. WARREN, E. (2018). Legal, ethical, and professional issues in information security. *Retrieved 31st January*, 89-116.