# Chapter 21
# Digital Ethics


## ABSTRACT

*The purpose of this chapter is to discuss strategies that can be applied in the domain of cyberlaw. The chapter begins by distinguishing between ethics, morality, and law. It then focuses on the relation between ethics and digital technologies. The chapter then examines proposals for what should be included in codes of ethics as well as examples of codes of ethics for IT companies. The examples include the British Computer Society, the Association for Computer Machinery, and the Data Processing Management Association. Next, ethical codes for regulating automation, computerization, and artificial intelligence are summarized. The chapter then discusses ethical issues surrounding privacy, anonymity, and personal data, including the EU's right of access by data subjects as well as issues connected with big data. The chapter then focuses on crimes caused by digitization and the protection of intellectual property. The chapter concludes by considering recent laws of ecommerce as well as social and international legal challenges of regulating cyberspace.*


## INTRODUCTION

Ethics is the study of proper professional action based on morals and applicable laws. In the field of information technology, some of the major ethical concerns include automation, ICT, robotization, and the Internet. The specialization that studies ICT and law—also known "cyberlaw" or "IT law"—aims to regulate the digital dissemination of information on a variety of media, such as video/film, software, e-commerce, and other forms. This field also considers issues relating to intellectual property, contract law, privacy, freedom of expression, and jurisdiction.

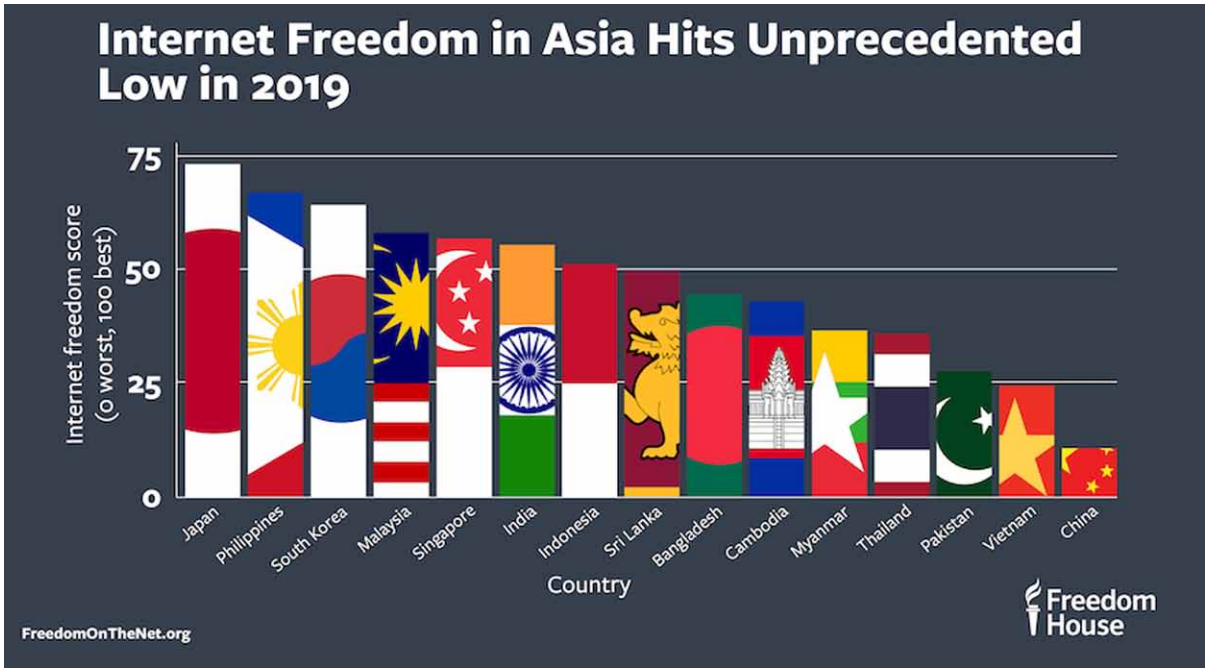
One of the predominant issues in IT law is net neutrality, which is the principle that Internet service providers (ISPs) must treat all Internet communications equally and not discriminate or charge different rates depending on the user, content, website, platform, application, type of hardware, source address, destination address, or method of communication (Easley et al., 2018).

Another major concern has been freedom of expression on the Internet (e.g., see Figure 1). Article 19 of the Universal Declaration of Human Rights calls for the protection of freedom of expression in all media. This includes the right to have an opinion without interference and to seek, receive, and

DOI: 10.4018/978-1-7998-8036-3.ch021

communicate information and ideas through any media, regardless of borders. Compared to traditional print media, the availability and relative anonymity of cyberspace have lifted the conventional barriers between a person and their ability to publish. Anyone with an Internet connection can potentially reach millions of people (Zittrain, 2013).

*Figure 1. Freedom of expression on the Internet in Asia (Funk, 2019)*




One of the more well-known laws of information technology is the Sarbanes-Oxley Act of 2002, which was a response to financial scandals in the early 2000s involving companies such as *Enron, Tyco International,* and *WorldCom.* Such high-profile frauds shook investor confidence in the credibility of company financial statements and prompted many to demand a review of multi-annual regulatory standards. The law introduced strict new rules for accountants, auditors, and corporate officials and imposed more stringent record-keeping requirements. The law also added new criminal penalties for securities violations. For example, the head of a company cannot offer as a defense the argument that he has not read a digital report on the state of the company if he has signed it.

Crime in cyberspace develops very quickly and can multiply its range at the speed of light. Hence, cyberlaw often lags behind these kinds of crime. To be successful, it requires effective international cooperation. These issues will be briefly discussed in this chapter, but in strategic terms, for the full characterization of these rights would require a book of its own.