Unit 1: The Law and Legal Systems

Welcome to Week 1.

Reflection:

What is Law? In general, law may be described as "a system of rules developed and enforced by social or political groups to regulate conduct" Despite the fact that the precise concept of law has been the topic of fierce debate for a very long time (Chaniotis, A., 2002), the debate continues (Willis, H. E., 1925). It has variously been considered both a science (Spooner, L., 1882) and an art of justice (Cohen, M. L., 1992). State-enforced laws may be produced by a group legislature or a single legislator, resulting in legislation; by the executive branch through decrees and regulations; or, most often in common law nations, by judges via the creation of precedent. Private parties may construct legally binding contracts, including arbitration agreements that provide alternatives to the customary court action for resolving disputes. It is conceivable for a written or unwritten constitution and the rights it enshrines to influence the lawmaking process itself. In addition to serving as a moderator in interpersonal interactions, the law has several consequences on politics, the economy, history, and society (Wikipedia., 2022).

Cyberlaw, a subfield of computer law, examines the Internet's relationship to various technical and electronic aspects, such as computers, software, hardware, and information systems (IS). Cyberlaw is sometimes also referred to as "cyber law" or "Internet law" (Techopedia., 2020).

Cyberlaws protect information access, privacy, communications, intellectual property (IP), and free speech in relation to the use of the internet, websites, email, computers, cell phones, software, and hardware, such as data storage devices, thereby preventing or minimizing large-scale damage resulting from cybercriminal activities. This can be accomplished by restricting the extent of potential damage (Techopedia., 2020).

The rise in Internet traffic volume has contributed to an increase in the proportion of legal issues on a global scale. It is challenging to enforce cyberlaws because the laws governing the internet vary from jurisdiction to jurisdiction and country to country. The penalties for violating these regulations range from fines to solitary confinement (katharina.kiener-manu. 2018).

Implication and Limitation to Cyber Law:
Here below we are defining the some of the implication and limitations concerning to cyber law:

- **Ambiguous Terms:** Important legal terms lack definite meanings, resulting in ambiguity within the legal system. This is dangerous since it could have other conceivable meanings. For instance, internet libel does not specify whether certain events constitute libel. [Bibliography needed] There is a potential that the provision for gathering real-time data, among other provisions, contains unclear language (Ochoa, M., 2014).

- **Threatens freedom of speech:** The vagueness of the legislation, particularly those dealing to online libel, can cause people to be hesitant in their online speech, which can be detrimental to the right to free expression. The simple communication of the facts could be considered libelous, depending on how it is presented. In a nutshell, the law holds individuals back without their knowledge. Even though freedom of expression does not have an unrestricted reach, the law nonetheless restricts the ability of those who wish to express themselves. Widespread fear exists that even constructive criticism and negative feedback could be misconstrued as an "attack" and used against the person providing it (Ochoa, M., 2014).
- **Maintenance of the law**: The implementation and enforcement of the Cybercrime Law would incur additional annual expenses of P 50,000,000.00 for the Philippines. Not to mention the court proceedings themselves. For the law against cybercrime to be effective, it must be treated with moderation and objectivity, as it addresses delicate issues (Ochoa, M., 2014).

Cyber Forensics in context of law enforcement: Since its inception and subsequent widespread use in the late 1980s, computer forensics has become an indispensable component of practically every law enforcement investigation. As a result of the adoption, investigators and enthusiasts now have access to more useful and reasonably priced tools for extracting data from devices. Law enforcement organizations began to see the necessity for computer forensics when technology began to progress and communication between users (or criminals) began to migrate to technology as a way of plotting illegal acts. Computer forensics is used not only to track criminals through their digital footprints, but also to investigate criminal conduct to comprehend their goals, methods of operation, and other factors that led to their capture or incarceration (Crager, R. 2021).

Given what we know about the history of the development of computer forensics up to this point, it is not far from the truth to assert that computer forensics is deeply ingrained within the framework of the judicial system. [Bibliography needed] The major use of computer forensics is in the sphere of law enforcement, making it the application utilized most frequently in real-world circumstances. This is related to the fact that law enforcement is responsible for apprehending criminals. Digital forensics allows law enforcement to discover the digital fingerprints of offenders, which can provide investigators with information about the criminal's whereabouts as well as his or her motivations, hobbies, and weaknesses. The most important question to ask in any investigation into this topic is, "How has law enforcement utilized digital forensics to locate criminals?" This is since this is the most important question to ask. This is the case regardless of the conditions (Flory, T., 2016).

How likely is it that the discovered evidence will be admissible in court, considering the various ways it could have been gathered? Even though it may not cover as much space as forensic science in its more comprehensive form, computer forensics has a very broad range of applications. Despite this, it is possible to focus in on extremely specific aspects of the numerous subfields and problems it handles. However, one of the most typical reasons law enforcement organizations utilize computer forensics is to follow a criminal's steps after leaving a crime scene, which ultimately leads to their apprehension and incarceration. This is one of the most prevalent instances in which law enforcement

authorities utilize computer forensics. In the instance of the BTK Killer from Wichita, Kansas, law enforcement, who believed the serial murderer to be deceased, was able to obtain a hard drive from the serial killer in the early 2000s, proving that he was still alive. The serial killer wanted investigators to follow the trail he left behind on a hard drive. The facts surrounding this case are publicly recognized. On the other hand, the planned trail included a floppy disk drive that had been wrongly formatted or wiped. This allowed the investigators to have access to the device's stored meta data. After doing open-source intelligence analysis, the detectives were able to trace the connection back to Dennis Rader, the church council president at the time who eventually confessed to over 200 killings. The username shown on the drive's metadata contained the words "Christ Lutheran Church and Dennis," allowing police to identify Rader. (Rivera 2018). If digital and computer forensics had not been widely established, supported, and utilized since the early 2000s, it is probable that the BTK Killer would have been able to avoid punishment for his irresponsible and cruel actions.

Academics Argument:
Initially, members of a group who were interested in computer and digital forensics as a hobby had no idea what would become of the field. Initially, they were created largely by law enforcement professionals interested in collecting data from a range of computers and information systems. To solve crimes, collect intelligence, and punish offenders, however, they swiftly became a requirement among the law enforcement community. In response to the massive uproar and demand for computer forensics specialists in the late 1990s and early 2000s, law enforcement agencies, government agencies, and other organizations began offering classes, developed specialized tools, and eventually developed an entire profession for computer forensics. All of this was a result of the rising demand for computer forensics expertise. Computer forensics enables law enforcement organizations to not only catch criminals, but also study specific offenders to construct profiles based on their actions and predict their future activities. In this age of advanced technology, law enforcement agencies use computer forensics to find evidence that can be used to prosecute a criminal, track the criminal's movements (via digital fingerprinting), and ultimately present evidence in court that proves beyond a reasonable doubt that the criminal in question committed the crime in question.

References:

Chaniotis, A. (2002). An Annotated Translation of'Crimes Against Humanity'(Chapter 11) by Geoffrey Robertson. Submitted in 2002 in Gent.

Cohen, M. L. (1992). Law: The art of justice. Scribner.

Crager, R. (2021). Computer Forensics in Law Enforcement. Www.academia.edu. Retrieved from https://www.academia.edu/61078853/Computer_Forensics_in_Law_Enforcement.

Flory, T. (2016). Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies. Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2016.1374.

katharina.kiener-manu. (2018). Cybercrime Module 3 Key Issues. Retrieved from www.unodc.org website: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/intro.html.

Ochoa, M. (2014). Cybercrime Law Advantages and Disadvantages. Retrieved from Scribd website: https://www.scribd.com/doc/217423947/Cybercrime-Law-Advantages-and-Disadvantages.

Spooner, L. (1882). Natural Law, Or, The Science of Justice: A Treatise on Natural Law, Natural Justice, Natural Rights, Natural Liberty, and Natural Society: Showing that All Legislation Whatsoever is an Absurdity, a Usurpation, and a Crime. A. Williams.

Techopedia. (2020). What is Cyberlaw? - Definition from Techopedia. Retrieved from Techopedia.com website: https://www.techopedia.com/definition/25600/cyberlaw.

Wikipedia. (2022, January 14). Law. Retrieved January 17, 2022, from Wikipedia website: https://en.wikipedia.org/wiki/Law#cite_note-ReferenceB-2.

Willis, H. E. (1925). Definition of Law, A. Virginia Law Review, 12, 203. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/valr12&div=25&id=&page=.