International Journal of Judicial Law

Analysis of the rule of law in corruption

Yashika Nagpal
Amity Law School, Delhi, India

* Corresponding Author: **Yashika Nagpal**

Article Info

ISSN (online): xxxx-xxxx
Volume: 01
Issue: 05
September-October 2022
Received: 25-09-2022;
Accepted: 10-10-2022
Page No: 07-08

Abstract
The importance of the Internet and computer systems in modern life cannot be overstated. Although the growth of networks and cyberspace has greatly benefited the general public, there are others who use these advances to gain illicit advantages. Recent social media users have seen different ways of being hacked. Both impersonation scams involving the Internal Revenue Service (IRS) and those involving technical assistance are the most common types of tactics attackers use to steal money from their victims. This study focuses on the rule of law and technology, international cybercrime, and types of Internet-related crimes. This study will provide detailed information on the legal order in corruption and international legal standards for privacy protection.

Keywords: Rule of Law, Technology, International

1. Introduction

Information and Communication Technology (ICT) criminal law identifies acceptable standards of behavior on the Internet, establishes socio-legal sanctions for cybercrime, generally protects ICT users and mitigates or prevents harm to people, data, systems, services and infrastructure, in particular; protects human rights; enables the investigation and prosecution of online crime (outside the traditional real-world environment); and facilitates cooperation between law enforcement agencies (UNODC, 2013, p. 52). The Cybercrime Act provides guidelines and standards of behavior and conduct for the use of the Internet, computers and related digital technologies and for the activities of government and private organizations, as well as for the rules of evidence and criminal procedure and other criminal justice matters in cyberspace. It also regulates risks and/or mitigates damages to individuals, organizations and infrastructure in the event of cybercrime. For this reason, legislation in the field of computer crime includes substantive, procedural and preventive aspects. Cybercrime

Substantive law

Illegal activities require specific definitions and prohibitions by law. A person cannot be punished for an act that was not prohibited by law when it was committed, according to the moral concept of nullum crimen sans lege (Latin: "no crime without law") (UNODC, 2013, p. 53). Legal entities such as natural persons, organizations and governments have rights and obligations defined by substantive law. Laws and regulations enacted by local, state, and federal legislatures (statutes), United States and state constitutions, and court decisions are all sources of substantive law.

Procedural law

Rulemaking is governed by procedural law, which sets standards for the enforcement of rulemaking. Criminal procedure is an important part of procedural law because it contains detailed rules and guidelines for how the criminal justice system and its agents should treat and process suspects, accused and convicted persons (Maras, forthcoming, 2020; criminal procedure general information , see LaFave et al., 2015; for information on international criminal proceedings, see Boas, et al., 2011). Finally, cybercrime procedural law includes provisions on jurisdiction and investigative powers, evidence and criminal proceedings relating to data collection, interception, search and seizure, retention and retention (which are further described in Cybercrime Module 4 on Introduction to Digital Forensics, Module 5 on Cybercrime Investigation, Module 6 on Practical Aspects of Cybercrime Investigation and Digital Forensics and Cybercrime Module 10 on Privacy and Data Protection, see also UNODC, 2013, pp. xxii-xxiii). In terms of process, cybercrime presents a number of unique challenges, particularly with respect to jurisdiction, investigation and digital evidence.

Preventive law

Regulation and risk mitigation are the primary objectives of preventive legislation preventive law focuses on cybercrime to either prevent it or at least reduce the harm that results from the commission of cybercrime (UNODC, 2013, 55). Cybercrime Module 10 on privacy and data protection covers data protection laws such as the EU General Data Protection Regulation 2016 and the African Union Convention on Cybersecurity and Data Protection 2014, which aim to reduce the material damage caused by crime breach of private data in case of cybercrime occur and/or mitigate such damages. As a result, criminal justice agents are equipped with the tools necessary to investigate and punish cybercrime. This includes facilities such as the infrastructure of telecommunications and electronic communications service providers that enable interception and data storage.

Types of Internet-related crimes

Cybercrime and cyberattacks have no agreed definition at the global level. For the most part, crimes fall into one of four categories: I crimes against the confidentiality, integrity and availability of computer data; ii) computer-related offences; ii3) content-related offences; and finally iv) infringement of copyright and related rights.

In general, cybercrime can be divided into three categories: cybercrime, cybercrime and online sexual exploitation and abuse of children, which is a different type of crime.

- Malware, ransomware and attacks on critical national infrastructure (such as a cyber-takeover of a power plant by an organized crime group) are examples of cybercrime that depends on ICT infrastructure. Another example would be overloading a website with data to shut it down (DDOS attack).
- Criminal activity that can take place both offline and online is known as cybercrime. Online fraud, drug transactions and money laundering are examples of this.
- Sextortion is the exploitation of self-created images by extortion and is becoming increasingly common on the open internet and darknet forums.

The rule of law in corruption

Corruption has a well-deserved reputation as one of society's most pernicious ills. Those who belong to underrepresented or oppressed groups, such as minorities, people with disabilities, refugees, migrants and convicts, are disproportionately affected by erosion of trust in government institutions and, as a result, are an obstacle to economic progress. It affects women, children and the poor the most, preventing them from accessing basic social needs including health care, housing and education.

When it comes to fighting corruption, investigative journalists and whistleblowers are critical. Two recent murders, one in Malta and one in Slovakia, illustrate the danger journalists face when they go after corrupt politicians and the money they receive from organized crime. Three years since then it had been since Daphne had been brutally murdered and no one had been able to determine who or what had ordered it or why. In September 2020, two and a half years after the death of Jan Kuciak and his fiancée Matina Kunrová, the murderers were found guilty; however, those who organized the crimes were not found guilty. As a result of the court decision, I believe that justice must be ensured in Slovakia and impunity avoided. In 2018, attempts were made on the life of Montenegrin journalist Olivera Laki, and the perpetrators of this crime have not yet been caught; she is known for her investigations into political corruption in her newspaper Vijesti. Since the violent beating of Serbian investigative journalist Ivan Nini in 2015, the crime and corruption reporting network KRIK has received death threats and been targeted for smears. Investigative journalist Khadija Ismayilova, who was jailed for criticizing government officials and their families over allegations of corruption and illegal business operations, is another illustrative example. Although the European Court found many violations of the Convention in her case – including a violation of Article 18 – it concluded that this was done to punish and silence the journalist for her work as a journalist. Another danger to journalists investigating misconduct (SLAPP) is what are known as strategic public participation lawsuits. These are frivolous lawsuits initiated by wealthy individuals or corporations in an attempt to intimidate journalists into abandoning their investigations and refraining from using the court system. So, for example, before she was killed, Daphne Caruana Galizia was already the target of more than 40 civil and criminal libel suits in Malta, some of which were brought against her family even after she died.

Conclusion

The Cybercrime Act provides guidelines and standards of behavior and conduct for the use of the Internet, computers and related digital technologies and for the activities of government and private organizations, as well as for the rules of evidence and criminal procedure and other criminal justice matters in cyberspace. It also regulates risks and/or mitigates damages to individuals, organizations and infrastructure in the event of cybercrime. For this reason, legislation in the field of computer crime includes substantive, procedural and preventive aspects. Cybercrime A person's right to privacy or reasonable expectation of privacy is taken into account when enacting privacy legislation. With today's technical capabilities, it is possible to have as much privacy as you want, and these technologies can enable a growing number of contractual practices. Regulation and risk mitigation are the primary objectives of preventive legislation. When it comes to cybercrime, the Prevention Act aims to make it harder for criminals to commit crimes, or at least reduce the damage they do.

References

1. Oliver Diggelmann, Maria Nicole Cleis (7 July 2014). "How the Right to Privacy Became a Human Right". Review of human rights. 14 (3): 441–458. doi:10.1093/hrlr/ngu014.
2. "Introduction: Privacy and Surveillance in Transatlantic Perspective", Surveillance, Privacy and Transatlantic Relations, Hart Publishing, 2017, doi:10.5040/9781509905447.ch-001, ISBN 978-1-5099-206 October 0501
3. Jump up to:a b Greenleaf, Graham (2009). "Five Years of the APEC Privacy Framework: Failure or Promise?". Computer Law and Security Report. 25:28–43. doi:10.1016/j.clsr.2008.12.002. S2CID 62198335. SSRN 2022907.
4. Jump up to:a b c Marvin, Lynn M.; et al. (2015). “Implementing the U.S. Discovery in Asia: An Overview of e-Discovery Laws and Asian Privacy Laws”. Richmond Journal of Law & Technology. 21 – via HeinOnline.

5. Jump up to:a b c d Reidenberg, Joel R. (2000). "Resolving Conflicting International Privacy Rules in Cyberspace". Stanford Law Review. 52 (5): 1315–1371. doi:10.2307/1229516. JSTOR 1229516.
6. Jump up to:a b Victor, Jacob M. (November 2013). "The EU General Data Protection Regulation: Towards a proprietary regime for protecting data privacy". The Yale Law Journal. 123(2):513–528. JSTOR 23744289.
7. Jump up to:a b Tene, Omar (2013). "The Midlife Crisis in Privacy Law: A Critical Assessment of the Second Wave of Global Privacy Laws". Ohio State Law Journal. 74 – via HeinOnline.
8. "OECD Recommendation on Cross-Border Cooperation in the Enforcement of Privacy Laws - OECD". www.oecd.org. Retrieved March 21, 2018.
9. Greenleaf, Graham (2012). "Independence of Data Protection Authorities (Part 1: International Standards). Computer Law and Security Review. 28: 3–13. doi:10.1016/j.clsr.2011.12.001.
10. "III.V.7 UN GENERAL ASSEMBLY RESOLUTION 68/167 (ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE)". International Law and World Order: The Essential Papers of Weston and Carlson. doi:10.1163/2211-4394_rwilwo_com_033375.
11. "UN Principles on Personal Data Protection and Privacy". January 4, 2019.
12. Grosse v Purvis [2003] QDC 151, District Court (Qld, Australia).
13. Jump up to:ab Giller vs. Procopets [2008] VSCA 236 (10 December 2008), Court of Appeal (Vic, Australia).
14. Jane Doe v Australian Broadcasting Corporation [2007] VCC 281, County Court of Victoria
15. "Invasion of Privacy: Penalties and Remedies: Review of the law of privacy: stage 3" (2009) (Issues paper 14), New Zealand Law Commission, ISBN 978-1-877316-67-8, 2009 NZIP 14 access August 27, 2011