Page 107 - 123 **DOI:** *https://doij.org/10.10000/IJLSI.112067*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 4

2024

Law Relating to Cyber Crimes: International Perspective

SAHELI GORAI[1]

ABSTRACT

The latest trends promoting digital sovereignty are increasingly freeing us from the complexities and challenges of international law in cyberspace. The complexities and challenges of digital sovereignty lie in the ability to control and direct international actors through the use of digital technologies such as the Internet, social media, and other digital media.Although international law is still in its beginning there is an urgent need to determine how it will be applied in this area, but that is a long way to go and it is still in its infancy. This chapter is divided into two parts a brief overview of the existing challenges for international cyber law and a discussion on the impact of these challenges on the future of cyber security with the help of Human Rights.

The lack of effective international legal instruments in cyberspace is widely debated in theoretical and political debates. The complexity of cyberspace makes it difficult for parties to reach agreements, let alone enact acceptable and binding laws. The contentious academic debates primarily divide those who believe that states should play a more influential role in formulating international cyberspace law and those who argue that cyberspace should remain a free and distributed domain.

Keywords*: Cyber law, Human Rights, Cyberspace, Cyber security.*

I. INTRODUCTION

Beyond academic textbooks, more dynamic discussions are taking place among stakeholders and international organizations. International law is a set of legally binding norms for independent sovereign states in their collective relations. It is in the form of agreements, protocols, conventions, etc. That rules are not only meant for the States but also for International Organizations and Individuals international law intends to regulate the extent to which one State's enforcement jurisdiction impinges or conflicts with others. International law may be public international law 'or' private international law. Public International Law 'governs the relationshipbetween States. In this case,a private dispute settlement mechanism is increasingly being provided by private international law. Private International Law is that body of law, which comes into operation whenever a domestic court is faced with a claim that

[1] Author is an Advocate in India.

 [ISSN 2581-9453]

contains a foreign element. The resolution of such private dispute is resolved through the law of 'conflict of laws' It is that part of the private law of a country, which deals with cases having a foreign element in practice it is the application of 'statutory elements of both the State and International Laws which help the domestic courts to arrive at a decision. All these debates lead to a point of convergence: the lack of an international legal regime in cyberspace is due to the complexity and competence of the actor in cyberspace. To make matters worse, in recent years several international, mostly state, actors have promoted the idea of digital sovereignty to further their interest in regaining control over information, communications, data, and infrastructure related to the Internet. It thus poses greater challenges for a possible future international cyber security law.[2]

International jurisdiction on the internet is not treated. United State law provides a guideline by which separate State courts may base their decision, and States can reference decisions achieved through other State court cases as a basis for their decision. In other words, while a Texas state court can use a Wisconsin court order to decide an Internet case, there is no higher authority to regulate individual countries. In such cases, each country typically takes its laws into Thomas Aquinas in his magnum opus Summa Theological mentioned, "law is an ordinance of reason for the common good, made by those who care about the community". Unfortunately, this adage does not necessarily resonate with international law on cyberspace. The future of international law in cyberspace would also have little impact on state behavior due to the growing trend to promote digital sovereignty standards. Sovereignty is one of the indispensable guidelines that ensure the security of the country.Sovereignty allows us as a nation to withstand pressure from others. It is crucial to our economic independence. As information technology plays an increasingly important role in the Indian economy, it becomes imperative to identify digital sovereignty issues and formulate appropriate policies to ensure our digital sovereignty. The threat to India's digital sovereignty mainly comes from two areas viz.i.e. digital standards and the internet.[3]Digital standards are often used to provide an unfair economic advantage to emerging markets such as India, where a company or group of companies, usually based in the West, creates the standard and files numerous intellectual property lawsuits, such as patents on the standard. The standard is then taken through one or more international standardization bodies and is turned into an international standard which is then forced onto the users in emerging economies. Users of the standard are therefore forced

[2]Dr. S.R.Myneni , Information Technology, Asia Law House, Hyderabad, p.14, 1st Edition, 2017.
[3]Wadje Ashok, "Cyber Obscenity Issues and Challenges" (2018), Ph.D. thesis, Symbiosis National University, http://hdl.handle.net/10603/223082

to pay disproportionate royalties, directly or indirectly, by paying a higher price for the final products, and manufacturers are forced to pay unfair royalties.

II. HISTORY

International law's applicability to cyberspace and cyber activities has been a source of debate. The highly contested topic was whether cyberspace provides a new 'Wild West' in which current international law standards, if not international law itself, would be inapplicable and therefore would not govern actions taking place in this 'space'. Both scholarly research and state practice have agreed that international law extends to cyberspace and cyber operations. The latest trends promoting digital sovereignty are increasingly freeing us from the complexities and challenges of international law in cyberspace. The complexities and challenges of digital sovereignty lie in the ability to control and direct international actors through the use of digital technologies such as the Internet, social media, and other digital media. As a result, the focus shifted to deciding how international law principles could be interpreted and applied to cyberspace and cyber operations. This does not, however, imply that applying international law norms is straightforward. On the opposite, there are significant concerns over how to perceive and enforce several standards. In this regard, there are two key challenges: on the one hand, due to cyberspace's special characteristics, interpreting international law's application to cyber operations may necessitate any adaptation. On the other hand, international law topics, especially States, may have differing, if not divergent, views of basic international law norms.[4]The first thing to understand about international law is that it bears just a passing similarity to the law that most people are familiar with. In most nations, domestic laws are enacted by a sovereign body after careful thought. Statutes are meticulously designed to ensure that the legislation has a specific effect. This does not apply to international law. Treaties are not the principal means of defining international law, contrary to common opinion. International law is a jumble of historical experience and history and negotiated treaties between countries. Under this patchwork of rules, customary international law - rather than laws or conventions - takes precedence in emerging areas of the law. When states adopt their general and compatible practices out of a sense of moral responsibility, customary international law evolves. When this happens, nation-states deem customary law to be legally binding. Nations can take measures they consider necessary in situations where there is no existing consensus on what constitutes lawful conduct. The Lotus philosophy, so named after the International Court of Justice decision in which it was created, is based on this. Just a few

[4] Rallan, Nirmal,Impact of Information Technology on the Legal Concept of Obscenity, (2020), Ph.D. thesis, Amity University, http://hdl.handle.net/10603/336440.

acts are called peremptory conventions of international law, meaning they are generally considered to be wrong and illegal. Piracy, child trafficking, and hijacking are examples of exemplary regions. The international legal system's very existence is one of the reasons there are so few widely recognized standards. It is determined by what nations do and feel they are obligated to do, which makes reaching a consensus impossible.[5] Except in seemingly simple situations like torture, there is no rule without agreement. Many states regard 'torture or unfair, inhuman, or degrading treatment or punishment' as a violation of human rights norms that have become customary international law. Nonetheless, acts resembling torture occur, and states that support them are rarely condemned, so it is impossible to claim that there is full international consensus on the subject. Although the few prohibitions accepted as peremptory norms do not apply to war, this does not mean that armed conflict is unregulated.

(A) Background

A universally recognized and well-understood customary law reflects the comprehensive and practically uniform behavior of nation-states in traditional warfare: the law of war.Unfortunately, enforcing the laws of war in cyberspace is problematic because the actions and effects available to states and non-state actors in cyberspace do not necessarily conform to the rules of armed conflict. Cyberspace offers new opportunities for nation-states, allowing them to take non-kinetic measures that may not have been available before.Using cyber methods, actions that once might have necessitated the use of physical force in armed conflicts can now be carried out without it. States can also take actions in cyberspace that would be consistent with the use of armed force, but it is easier to evade responsibility for such actions: they can act "without attribution" in cyberspace. In the absence of a specific legal order for cyberspace, the logical approach is to take existing guidelines for more conventional warfare and see if they can be applied to cyberspace activities. The following brief discussion is a general examination of how national practices become binding on all nations as Customary International Law. A more detailed discussion follows the general discussion of how customary international law might apply to nation-state cyber actions. Countries' diplomatic affairs are gradually taking place in cyberspace.This contribution aims to raise evidence in favor of the idea that international law analysis should be expanded to cover cyberspace. Due to the absence of treaty law in this field, one must turn to a secondary source of international law, namely tradition, as noted by one eminent researcher: 'Customary law still regulates various branches

[5] International Law and Human Rights, Dr. S.K. Kapoor, Central Law Agency, Allahabad, India, 3rd Edition, 2018.

of international law, and, more importantly, new rules of that law are emerging.'[6]

States can also take actions in cyberspace that would be consistent with the use of armed force, but it is easier to evade responsibility for such actions: they can act 'without attribution' in cyberspace. In the absence of a specific legal order for cyberspace, the logical approach is to take existing guidelines for more conventional warfare and see if they can be applied to cyberspace activities. The following brief discussion is a general examination of how national practices become binding on all nations as customary international law, victims anywhere in the world. It is now essential that all those persons, who deal with the cyber world, must have some idea about what acts constitute a cybercrime in the different countries of the world. Therefore, entire countries of the world have prepared cyber laws as per their need and ability to execute them. Since the impact of cybercrime is unbounded, any effort made at the national level has to meet international coverage forthe sake of effective containment of cybercrime and protecting the interest of society. Such a situation necessitatess understanding of global legal response relating to cybercrime. The discoveries and the inventions both constructive and destructive are very rapid all around the world. In the absence of international cooperation, it will not be possible for any country to know the recent advances in the other country. A country victim of any kind of latest cybercrime shall have the opportunity to intimate other countries in time so that it may plan its defense well in advance.Therefore international communication and cooperation for effective cyber law is necessary, for an effective operation against cybercrime. Considering the nature of cybercrime, the international community has tried to bring international cooperation by implementing cyber law's various conventions to deal with cybercrime. The legal responses to cybercrimein various countries of the world are varied. Such laws are still intheir gestation period.[7]

The U.N. is a forum of 191 member states and is active in the field of cyber security protection and cybercrime prevention. United Nations General Assembly in 1985. In 1985, the United Nations General Assembly decided in its Resolution of 11th December called upon governments and internationalorganizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, to ensure legal security in the background of the broadest possible use of information processing in international transactions.[8]

In 1990, the UN's General Assembly adopted the Guidelines Concerning Computerized

[6]Supra Note 2 at.35.
[7] Dr. S.R. Myneni, Human Rights Asia Law House, Hyderabad, India, p. 48 1st Edition, 2018.
[8]Supra Note 5.

Personal Data Files. It proposed taking appropriate measures to protect the files against natural and artificial dangers. The guidelines extended the protection of governmental international organizations Part – B.

The International Review of Criminal Policy, United Nations Manual on the Prevention and Control of Computer-related crime which is called for further international work and presented a proper statement of the problem. It stated that further activities could be undertaken at the international level, including harmonizing substantive law and establishing a jurisdictional base. The background paper for the workshop on crimes relating to the Computer network at the 10th Congress on Prevention of Crime and Treatment of Offenders proposed two levels of the definition of cybercrime. In the narrow sense, that is, computer-related crime denoted, any illegal behavior committed using or about, a computer system or network, including such crimes as illegal possession offering, or distribution of information usinga Computer system or network. The United Nations General Assembly called on States to consider measures to combat the misuse of information systems for criminal purposes in their efforts and agreed to keep information technology issues on the agenda of future sessions.[9]

III. BUDAPEST CONVENTION ON CYBER CRIME, 2001 ADOPTED BY THE COMMITTEE OF MINISTRIES OF THE COUNCIL OF EUROPE ON 8TH NOVEMBER, 2001[10]

The Budapest Convention on Cyber Crime was opened for signature in Budapest (Hungary) on 23rd November 2001 and it entered into force on 1st July 2004. It was the first-ever international treaty on criminal offenses committed against or with the help of computer networks such as the Internet. As on 28th October 2010, thirty states had signed, ratified, and acceded to the convention, whisk a further sixteen states had signed the convention but not ratified.The convention wassigned by Canada, Japan, the USA, and the Republic of South Africa on 23rd November 2001. The US Senate ratified the convention unanimously in August 2006 and became the 16th Nation to ratify the convention. The convention entered into force in the USA on 1st January 2007. Further accessions from other non-European countries are expected States are planned. India is still not a signatory to the cybercrime convention and the bilateral extradition treaties, which it has signed with around 50 countries so far, do not mention 'cyber crime' as extraditable offenses but it may not deter the Indian Government from granting extradition.In March 2006, the Additional Protocol to the Convention on Cybercrime came into

[9]Supra Note.7.
[10]Supra Note 2, p.522.

force. Those states that have ratified the additional protocol are required to criminalize, the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic motivated threats and insults.

The convention contains 48 Articles in total and the Convention deals in particular with offenses related to infringement of copyright, computer-related fraud, child pornography, cyber obscenity, and offenses connected with network security. The Convention includes a list of crimes that each signatory State must transport into their law. The following offenses are defined by the convention illegal interception, data interference, system interference, misuse of devices, computer-related frauds, computer-related forgery, offenses related to child pornography, and offenses related to copyright and neighboring rights.The treaty also includes a clause on a particular kind of cross-border access to computer data storage that does not require mutual help and calls for the creation of an ongoing network to guarantee prompt assistance among Signatory parties. Its fundamental goal is to promote a common criminal policy that protects society against cybercrime, particularly through the adoption of suitable laws and the promotion of international collaboration.[11]

It is significant to note that almost every kind of cybercrimehas been made extraditable under the convention. Moreover, the Convention has the force of International law behind it. In other words, a suitable legal framework is already in place to investigate, search for, seize, arrest, try, and extradite cybercriminals for cybercrimes.The main objective of the Convention has been set out in the preamble.

IV. THE SPREAD OF HUMAN RIGHTS

From Babylon, the idea of human rights quickly to Greece and eventually Rome.The concept of "natural law" arose from observing the fact that people tend to follow certain unwritten laws throughout their lives.Roman law is based on rational considerations derived from the nature of being. The City – the State of Greece gave its citizen equal freedom of speech, equality before the law, the right to vote, the right to be elected to public office, the right to trade, and the right to access justice. Similar rights were granted to the Romans by the Roman Civil Code.Therefore, the origin of the concept of human rights is found in the Greco-Roman law of Stoicism, the doctrine that universal power pervades all creation so that human behavior must be judged according to natural law. Natural laws are so basic for a decent, civilized, and orderly life.

[11]International Law and Human Rights, Dr. S.K. Kapoor, Central Law Agency, Allahabad, India, p.78, 3rd Edition, 2018.

Middle Ages – Magna Carta (1215)[12]

Magna Carta is an English charter that was first published in 1215. Magna Carta required the king to give up certain rights, respect certain courts, and agree to obey the law. It explicitly protected certain rights of the King's subjects to own and inherit property and to be protected from excessive taxes. It stressed the right of the Church to be free from Government interference. It establishes the right of property-owning widows to choose not to remarry. It also establishes the principles of due process and equality before the law. Magna Carta is considered the right of habeas corpus, allowing appeal against unlawful imprisonment. The Magna Carta was a significant turning point in the fight for freedom and is widely considered one of the most significant legal instruments in the growth of modern democracy.Thus, the magnum opus Magna Carta was the earliest influence in the broad historical process that led to the rule of constitutional law in the English-speaking world today.

Petition of Rights (1628)[13]

The Petition for Rights, which the British Parliament drafted in 1628 and sent as the Declaration of Civil Liberties, is the next significant advance in the history of human rights. Arbitrary arrest and imprisonment for opposing this policy provoked intense hostility in Parliament against the 1st Duke of Buckingham.John Locke developed the concept of natural rights, the idea that people are naturally free and equal. Although Locke believed that natural rights were derived from God because people were created by God, his ideas were important in the development of modern legal concepts.[14] Locke's natural rights are not based on citizenship or state law and are not necessarily limited to certain ethnic, cultural, or religious groups.

United States Declaration of Independence (1776)[15]

On July 1776, the United States Congress approved the Declaration of Independence, which consists, On July 4, 1776, United States Congress approved the Declaration of Independence, which consists, "We hold these truths to be self-evident that all men are created equal endowed by the creator with certain unalienable rights: among them are life, liberty, and pursuit of happiness." Its primary author, the main author was Thomas Jefferson. He wrote the Proclamation as an official explanation of Congress' vote to declare independence from Great

[12]Sanjeev Kumar, "Cyber Crime in India: Trends and Prevention", (2021), (2021) Vol. 9, Issue– 5, pp. 370.
[13]Supra Note 7.
[14] Mark Cartwright, Petition of Right, World History Encyclopedia, (June 13, 2024, 10:00 p.m.) https://faculty.chass.ncsu.edu/slatta/hi216/documents/hrhist.html.
[15]Raj Singh Deora and DhavalChudasama, "Brief Study of Cybercrime on an Internet" Vol. 11, Issue – 1, pp.7 (2011).

Britain on July 4, more than a year after the start of the American Revolutionary War, and declared that the Thirteen American Colonies were no longer part of the British Empire. Congress issued the Declaration of Independence in various forms. It was originally published as a printed spreadsheet that was available and read by the public. PPhilosophically, the manifesto emphasized two issues: rights and rights to revolution.These ideas became widely held by Americans and also spread internationally, notably influencing the French Revolution.

The Constitution of the USA (1987) and the Bill of Rights (1791)[16]

The United States Constitution, written in Philadelphia in the summer of 1787, is the basic law of the federal government of the United States and an important document in the Western world. The oldest national constitution used to define the main organs of government, their jurisdiction, and the basic rights of citizens. Constitution - The first ten amendments to the Bill of Rights, first enacted on December 15, 1791, limit the powers of the United States federal government and enshrine the rights of all citizens, residents, and visitors to United States territory protected. The law protects freedom of speech, freedom of religion, the right to keepand bear arms, freedom of assembly, and freedom of petition. It also prohibits unreasonable searches and seizures, cruel and unusual punishment, and self-incrimination. The Bill of Rights prohibits Congress from passing any laws relating to the religious establishment and prohibits the federal government from depriving people of their right to life, liberty, or property. Federal criminal cases require an indictment by a grand jury for any felony or heinous crime, a speedy trial by a fair jury where the crime occurred, and double jeopardy. In 1920, the 19th Amendment was enacted, stating that the right to vote should not be abridged or denied because of race.

The French Revolution: Declaration of the Rights of Man and the Citizen (1789)[17]

The Declaration of the Rights of Man and the Citizen proclaimed that men were born free and equal in their rights. The usual aim of civil associations was the preservation of the natural and imprescriptible rights of man, which consisted of ‘liberty, property, security, and resistance to oppression’. The exercise of these natural rights should be restricted only to the extent it was necessary to secure the enjoyment of their rights by other individuals. Law was considered to be the expression of the general will. Every citizen had a right to participate personally, or through his representative, in its formation. It must be the same for all. It ought to prohibit only those actions which were harmful to society. Every person was entitled not to be accused,

[16]Ibid.
[17]Supra Note 7, P.108.

arrested, or imprisoned except by the procedure prescribed by law. The right to religious liberty and freedom of expression was also recognized. Since the right to private property was considered inviolable and sacred no one could be deprived of it except for public necessity and on payment of legally ascertained just compensation. The sovereignty resided in the people and all authority in the state was derived from them.

The First Geneva Convention (1864)[18]

In 1864, Sixteen European countries and several American states attended a conference in Geneva, at the initiative of invitation of the Swiss Federal Council, on the initiative of the Geneva Committee. The diplomatic conference was held for adopting a convention for the treatment of wounded soldiers in combat. The main principles laid down in the later Geneva Convention and maintained by the Conventions provided for an obligation to extend care without discrimination to the wounded and sick military personnel and marking of medical personnel transports and equipment with the Red Cross on a white background.

The Universal Declaration of Human Rights (1948)[19]

Though the UN could not incorporate Human Rights in its Charter, it was realized by the members that it should be an obligation of the international community to promote human rights. By 1948, the UN's new Human Rights Commission had captured the world's attention under the dynamic chairpersonship of Eleanor Roosevelt - President Franklin Roosevelt's widow, a human rights champion in her rights and the US delegation to the UN -the Commission set out to draft the document that became the Universal Declaration of Human Rights. He was credited with giving the Declaration its impetus and referred to it as the "International Magna Carta" for all of humanity. On December 10, 1948, the UN ratified it as a non-binding declaration. The statement was the first international legal attempt to constrain state behavior and impose obligations on them to their population based on the rights-duty duality approach. The document was structured to include the basic principles of dignity, liberty, equality, and brotherhood in the first two articles, followed successively by rights about individuals; rights of individuals about each other to groups; spiritual, public, and political rights; and economic, social, and cultural rights. The final three paragraphs define rights in terms of their scope, obligations, and the social and political framework in which they must be implemented.

[18]Supra Note 15.
[19]Supra Note 5, p.95.

International Covenant on Economic, Social and Cultural Rights, 1966 (ICESCR)[20]

The Universal Declaration of Human Rights, 1948 (UDHR), which is a milestone in the history of human rights, and the International Covenant on Civil and Political Rights,1966 (ICCPR) which represents the 'Second Generation' of Human Rights are the three International human rights law. They are referred to as the "International Bill of Rights" collectively. Each of these instruments enumerates specific rights inherent in each human being.A significant international human rights pact, the ICCPR offers several civil and political rights guarantees. The International Covenant on Economic, Social, and Cultural Rights and the Universal Declaration of Human Rights are collectively referred to as the International Bill of Human Rights. By the ICCPR, nations that have ratified it are required to defend and uphold fundamental human rights like the right to life and human dignity, equality before the law, freedom of speech, assembly, and association, the right to privacy, freedom from torture and other cruel treatment, gender equality, the right to a fair trial, and rights for minorities. The Covenant compels governments to take administrative, judicial, and legislative measures to protect the rights enshrined in the treaty and to provide an effective remedy. The U.N. General Assembly adopted the Covenant in 1966, and it went into effect in 1976. As of December 2013, the Covenant had been ratified by 167 nations.

V. INTERNATIONAL HUMAN RIGHTS INSTRUMENT

It means the treaties and other international texts that serve as legal sources for international human rights law and the protection of human rights in general.

Regional

Regional human rights systems, which are made up of regional instruments and mechanisms, are becoming more and more crucial to the advancement and defense of human rights. Regional human rights instruments (such as treaties, conventions, and declarations) aid in the localization of international human rights standards by highlighting the specific human rights issues that the region is concerned about. Following that, regional human rights mechanisms (such as commissions, special rapporteurs, and courts) assist in putting these tools into practice locally. Africa, the Americas, and Europe currently have the three most established regional human rights regimes.

Europe

The regional arrangements for protecting human rights in Europe are extensive, involving the

[20]Supra Note 5, p.141.

Council of Europe, the European Union, and the Organization for Security and Cooperation in Europe. Each of these intergovernmental organizations has its own regional human rights mechanisms and instruments. The European Convention on Human Rights (ECHR), the European Social Charter, and the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, as well as the corresponding mechanisms of the European Court of Human Rights, the European Committee of Social Rights, and the European Committee for the Prevention of Torture and Inhuman The European system also has a Commissioner for Human Rights and a Commission against Racism and intolerance.The European Court of Human Rights, which is located in Strasbourg, has jurisdiction over the Council of Europe member States that have opted to accept the Court's optional jurisdiction. All court rulings concerning a state that has made this determination are conclusive. The Court hears applications from both individuals and States alleging human rights abuses.[21]

The Americas

Within the Organization of American States (OAS), an intergovernmental body, there is a regional human rights agreement for the Americas (the inter-American system for the protection of human rights). The inter-American human rights system, like the United Nations (UN) human rights system, includes a statement of principles (the 1948 American Declaration on the Rights and Duties of Man adopted seven months before the Universal Declaration), a legally binding treaty (the American Convention on Human Rights, which went into effect in 1978), as well as Charter-based and treaty-based implementation mechanisms (the Inter-American Commission on Human Rights and the American Convention on Human Rights (the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights respectively). The Charter-based system applies to all member states of the OAS, while the Convention system is legally binding only on the States parties to it. The two systems overlap and engage in numerous interactions. It is made up of seven independent Commissioners who act in their capacities. It accepts individual petitions, keeps tabs on the state of human rights in member states, and deals with pressing thematic concerns. The Inter-American Commission has created several Rapporteurships, one Special Rapporteurship, and a Unit to monitor OAS States' compliance with inter-American human rights treaties. This includes a Rapporteurship on the Rights of Women, a Rapporteurship on the Rights of the Child, a Rapporteurship on Rights of Indigenous Peoples, a Rapporteurship on the Rights of Persons Deprived of Liberty, a Rapporteurship on Migrant Workers and their Families, a

[21] European Journal for Security Research (June 16, 2024 10:00a.m.) www.paperity.com/cybersecuirityissuse.

Rapporteurship on the Rights of Afro-Descendants and against Racial Discrimination, a Special Rapporteur on Freedom of Expression as well as a Rapporteurship on Human Rights Defenders. This last position is the only Special Rapporteurship at the IACHR, meaning that the mandate-holder is dedicated full-time to the job (all other mandates are held by Commissioners). A Unit on the Rights of Lesbian, Gay, Trans, Bisexual, and Intersex Persons was created in 2011. The Inter-American Court of Human Rights (based in San Jose, Costa Rica) has two main responsibilities. First, to hear cases submitted to it by the Commission or a State Party to the Convention and judge whether or not a violation has been committed. The sentence is binding and cannot be appealed, but the system does not provide for means of enforcement. Second, the Court gives advisory opinions interpreting the American Convention or other international agreements relevant to the protection of human rights in the Americas.[22]

Africa

The intergovernmental body known as the African Union has built the regional human rights framework for Africa. The 1981 African Charter on Human and Peoples' Rights is the primary regional human rights document in Africa, and the African Commission on Human and Peoples' Rights and the recently founded African Court on Human and Peoples' Rights are the primary instruments. The African Charter (which entered into force in 1986) incorporates universal human rights standards and principles but also reflects the virtues and values of African traditions. Thus, the African Charter is characterized by the concept of a reciprocal relationship between the individual and the community, linking individual and collective rights. The African Commission for Human Rights was founded by the African Charter and is based in Banjul, Gambia. It is an eleven-member quasi-judicial body tasked with promoting and defending collective (peoples') rights and human rights across the African continent (by receiving regular reports from States Parties on how the Charter's provisions are being implemented) as well as interpreting the African Charter and considering individual complaints of violations of the Charter. Several Special Mechanisms have also been established by the African Commission, including eleven working groups, committees, or study groups, six Special Rapporteurs, who monitor and investigate allegations of violations in African Union member states, and six Special Rapporteurs. The Special Rapporteur mandates cover Extra-judicial, Summary, or Arbitrary Execution; Freedom of Expression and Access to Information; Human Rights Defenders; Prisons and Conditions of Detention; Refugees, Asylum Seekers, Migrants, and Internally Displaced Persons; and Rights of Women. The Working Groups cover

[22] UN trade and development (June 17, 2024 11:00 a.m.) https://unctad.org/.

specific issues related to the work of the African Commission; Indigenous Populations/Communities in Africa; Economic, Social, and Cultural Rights; Rights of Older Persons and People with Disabilities; the Death Penalty; Extractive Industries, Environment, and Human Rights Violations; Fair Trial; and Communications. And finally, there is a Committee for the Prevention of Torture in Africa; a Committee on the Protection of the Rights of People Living with HIV; and a Study Group on Freedom of Association. A Protocol to the African Charter on the Establishment of an African Court on Human and Peoples' Rights came into effect in 2004, which led to the establishment of the African Court on Human and Peoples' Rights. Regarding the interpretation and application of the African Charter, the Protocol, and any other pertinent human rights document ratified by the States in question, the Court has jurisdiction over all issues and disputes that are brought before it.[23]

Australia

The Cybercrime Convention is an international response to the borderless nature of cybercrime. For example, a criminal based in Eastern Europe can steal Australian credit card data from the website of an online business based in South-East Asia.

In August 2012, the Australian Government passed the *Cybercrime Legislation Amendment Act, 2012* (CLAA). The purpose of the CLAA was to enable Australia to accede to the Council of Europe Convention on Cybercrime (Cybercrime Convention), the only international treaty on cybercrime. The vast bulk of cybercrime, particularly targeting Australian companies, originates off-shore and is often the result of well-organised resourced organizations. Many of these criminal organizations are based in or utilize Information and Communication Technologies facilities based in, states with poor legislative or enforcement frameworks. This makes it virtually impossible for any state acting alone to locate or apprehend the responsible parties, or even to gather evidence about what occurred, and how. The stated aim of the Cybercrime Convention is "to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation".[24]The Cybercrime Convention encompasses offenses against computer data and systems, computer-related forgery and fraud, content-related offenses, and infringement of intellectual property rights. The Cybercrime Convention also requires member states to provide mutual assistance to other member states.[25]

[23] Ibid.
[24]Ibid.
[25]Nuruddin Khan and Dr. Shobha Gulati "International Legislative Framework Of Cybercrimes- A Comparative Study Of India, Israel, And USA", Vol. – 7, Issue – 1, p. 785 (2023).

United Kingdom

Computer Misuse Act 1990, this act is the codified Act that deals with cyber crimes in the United Kingdom and criminalizes several acts, including accessing data without authorization (i.e. hacking) and installing malware (e.g. computer viruses, spyware, ransom ware, etc.). Computer unauthorized use protects an organization's personal information from unauthorized access or alteration. The following acts are illegal under the law.

Unauthorized access to computer material. It is an unauthorized intrusion (hacking) into a computer system. Unauthorized access to computer material to commit another crime. It refers to infiltrating a computer system to steal data or destroy a device or network (e.g. introducing a virus).Unauthorized modification of data refers to modifying or deleting data and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information), Manufacturing, supplying, or procuring items that may be used in computer exploitation crimes. These four main clauses cover a wide range of crimes such as hacking, computer fraud, extortion, and viruses.

Canada

The government's proposed Critical Cyber Systems Protection Act (CCSPA) presents significant reforms to Canada's regulatory approach to cybersecurity for federally regulated private sector industries. The law will set minimum standards for cyber due diligence for actors in many major economic sectors. Under Canadian law, cybercrime is protected by the Canadian Penal Code 1985. The Penal Code defines various cybercrimes and provides various prison sentences for various criminal acts committed using computer resources and technology. Under the prescribed laws, hacking is a criminal offense with a prescribed imprisonment of a maximum of five years. However, in some cases of significant degree, the maximum imprisonment is for ten years. Denial of service that restricts lawful access to and use of your computer data is considered fraud under Canadian criminal law and carries a penalty of 10 years in prison.Similarly, Criminal law provides for various cyber crimes including phishing, infection of IT Systems with Malware, Spyware, Ransom ware, Worms, etc. which are also considered Mischief, and for the same ten-year imprisonment is prescribed. It also provides protection and regulation against identity theft and fraud by imposing imprisonment of up to 10 years. The Copyright Act protects and regulated electronic theft which includes breach of confidentiality by the employees or copyright infringement. Violation of the Copyright Act brings up a fine of up to 1 Million or five years of imprisonment or both.Canadian cybercrime laws apply to all Canadian citizens regardless of where they live. If a Canadian citizen is

 [ISSN 2581-9453]

assaulted by a foreigner, it is considered a crime committed in Canada and will be prosecuted under the Penal Code.Besides criminal law, there are also competition laws, personal data protection laws, electronic document laws, and telecommunications laws that regulate various cyber activities that undermine civil rights in the form of national security, interests, and privacy.[26]

California

The most detailed privacy law in the United States is the California Consumer Privacy Act (CCPA). This law came into force on January 1, 2020. This is primarily based on the European Union General Data Protection Regulation (EU-GDPR). The act appliesto all business entities working in California from California or remotely. The purpose of this act is to protect the personal data collected by the entities against the use which is not consented to by the users. Also, the law prohibits any type of discriminatory practices based on the data which is possessed by the business entities. The law also provides the users with rights similar to EU GDPR like disclosure, access, etc. Another right that has been possessed by the users to prevent their information from getting transferred to a third party and the users at any point in time can ask the business to remove the personal data of the user stored with them. This law is specifically designed to protect California residents from any form of violation of the privacy of personal information held by businesses. For similar reasons, "personal data" is defined as any data that allows the identity of a user or his family members to be traced.[27]

VI. COMPARATIVE ANALYSIS OF SPECIFIC CYBER CRIMES

Every developed country in the world has prepared cyber law to regulate cyberspace and cybercrime. There are certain cyber-crimes, which are common in every corner of the world, though the territorial aspect of cybercrime offenses has been recognized as transnational, similar or rather the same cybercrime treated differently in different two countries, this make sit difficult to buildup cooperation among the Nations at the international level. As the world is a global village, computer internet use is quite similar, especially for committing crimes. Though the manner and modes to misuse the computer are different, the object and main aim are similar. The similarity in the object is there because the offenses in the cyber world are rather offenses against property or privacy. Every legal system has recognized the right to privacy in their respective countries. As well as property right is also recognized as an inherited right of human beings in the world, and it is internationally recognized in every country. The

[26]International Law and Human Rights, Dr. S.K. Kapoor, Central Law Agency, Allahabad, India, p. 70 3rd Edition, 2018.
[27]Supra Note 3.

various cyber-crimes which are known by different names are nothing but similar acts against the right to privacy and property. The pits and pills of information stored in cyberspace come up as a new wealth targeted by cybercrime criminals. Cybercriminalshave a lust for data storage and use all illegal ways to either temper with it or to destroy it completely which givesa new dimension to the traditional crime of mischief. This new dimension of conventional crime is going to commit by using new technology.[28]These new techniques bring new clusters which is unheard of it. It is only a new dimension, but the base of the crime is the same. The cyber-world recognized two kinds of offenses, which are known as pure cybercrime. That is vandalizing digital information and security-relatedoffenses. These two offenses are nothing but against property and privacy. Vandalizing digital information means hacking or viruses, and worms. These acts destroy or damage intellectual property or important data. Security-related crime means violating individual privacy like cyber defamation. The cyber law of different countries deals differently with this act. Hacking, stalking, cyber defamation, or tampering with computer sources are common offenses, which are going to, committed in every corner of the world. All legal system has enacted different laws to prohibit these offenses. There are various offenses, which are common and prohibited in almost all the legal system. However, different Laws and policies are recognized in every country. Therefore, it makes a great impact on the execution of the cyber laws. For example, information vandalism is a common problem in the cyber world, and various countries' laws deal with the problem as follows.[29]

VII. CONCLUSION

In this chapter, we understood the binding and well-adjudicated international law on cyberspace, which does not effectively apply to states given the challenges taking place in public international law related to jurisdiction, arbitration, and legal instruments and jurisprudence.

*****

[28]Ibid.
[29]Supra Note pp. 786.