Navigating Ethico-Legal Complexities in the Digital Age: Addressing Human Rights, Intellectual Property, Data Protection, Privacy, and Cybersecurity Challenges

Author:

Prof. Jharna Jagtiani , Assistant Professor, IFIM Law School, Bangalore

Aishwarya Ganapathy Student, IFIM Law School, Bangalore

Email: jharnavjagtiani@gmail.com; aishwaryagsaravanan@gmail.com

INTRODUCTION:

The paper explores the ethical and legal challenges of the digital era, including human rights, privacy, intellectual property, data protection, and cybersecurity. It emphasizes the need for a balance between preserving individual rights and maximizing technological advancements, while also discussing the challenges of enforcing digital rules.

Human rights are changing on the internet; thus, they need to be protected just like they are offline. Many people believe that technology can help advance human rights like free expression. But the digital era has also introduced new risks to fundamental rights, such filtering material, limiting, and cutting off access to technology. This process encompasses other rights, including the right to free speech, and is jeopardized by continuous data collection techniques that don't reveal anything concerning. New technologies have transformed the legal system of today, giving rise to new rights and viewpoints on long-standing human rights. In light of digital advancements, this study highlights the significance of reinterpreting the principles of indivisibility and interdependence of human rights.

The digital age has significantly impacted society, introducing challenges in intellectual property, privacy, security, legislation, and governance. Maintaining security and privacy is a major challenge, as businesses and governments constantly gather and store personal information. Intellectual property protection is another challenge, as technology simplifies the process of producing and disseminating content protected by patents, trademarks, and copyrights. Governance and regulation are also challenging due to the rapid evolution of digital technology. To address these issues, stricter privacy rules, customer awareness, and increased transparency from businesses are needed. International agreements are also needed to safeguard intellectual property rights and enable copyright holders to defend their rights. New regulatory frameworks for the digital era must be established, with stakeholders like corporations and civil society groups involved in the process. We can build a more advantageous digital environment for everybody by tackling these issues and worries.

The digital age presents both advantages and moral and legal challenges, such as security, privacy, intellectual property rights, discrimination, control, autonomy, and misinformation. It also poses challenges in copyright, patents, and trademarks, and promotes bias in machine learning and artificial intelligence algorithms.

HUMAN RIGHTS IN THE DIGITAL AGE:

Technology can limit rights and exacerbate inequality, with governments and corporations imposing restrictions on internet speech and information access. Digital monitoring techniques target activists, racial minorities, and labor. AI and data-driven technologies influence workers and poor people's rights. Legislation and regulations are needed to encourage social media platforms to respect privacy and human rights. Technological innovations have serious consequences for the human rights framework.

Technology can limit rights and exacerbate inequality, with governments and corporations imposing restrictions on internet speech and information access. Digital monitoring techniques target activists, racial minorities, and labor. AI and data-driven technologies influence workers and poor people's rights. Legislation and regulations are needed to encourage social media platforms to respect privacy and human rights. Technological innovations have serious consequences for the human rights framework.

The 21st century's advancements in science and technology, including the Internet, social media, artificial intelligence, and climate change, present both hazards and opportunities for human rights, necessitating careful consideration of potential harm and innovative solutions.

Risks:

1) Observing and gathering large amounts of data: New technology allows businesses and governments to gather and store vast amounts of data on people's interactions and activities, leading to privacy issues and misuse possibilities. Governments can use surveillance data to monitor political dissidents and businesses can discriminate against individuals. The European Court of Human Rights ruled in ***S. and Marper v. the United Kingdom***[1] that the indefinite retention of fingerprints, cell samples, and DNA profiles violated applicants' right to privacy, stating there was a serious risk to their privacy.

The Ninth Circuit Court of Appeals ruled in ***Carpenter v. United States***[2] that the government's unauthorized collection of location data from cell phones violated the Fourth Amendment, as it

[1] ECHR 1581

[2] §§924(c), 1951(a)

provided sensitive personal information about an individual's habits and whereabouts, thereby invading their privacy.

2) Algorithmic bias and artificial intelligence (AI): AI systems are increasingly used in decision-making processes, such as hiring, lending, and criminal justice, but they can also be biased. AI recruiting systems may discriminate against certain groups, such as minorities or women. The US Supreme Court's ***Bostock v. Clayton County***[3] ruling prohibits discrimination based on sexual orientation and gender identity under Title VII of the Civil Rights Act of 1964. This could lead to discrimination in AI algorithms used in hiring decisions.

3) New reproductive technologies: New reproductive technologies (NRTs) have revolutionized child production, but they also raise concerns about prejudice and eugenics. NRTs can be used to select individuals based on certain qualities, potentially leading to a society where certain individuals are valued more. The US Supreme Court's decision in the ***Planned Parenthood v. Casey***[4] case protects women's right to privacy, which could impact NRTs' use to limit access to abortion. The European Court of Human Rights ruled in the Evans v. United Kingdom case that the UK government's prohibition on artificial insemination for single women violated Article 8 of the European Convention on Human Rights, resulting in discrimination against single women.

4) Cybercrime and cyberwarfare: New technology has made it easier for governments and criminals to launch cyberattacks, potentially causing false information, data theft, and infrastructure disruption. Ahmad Al Faqi Al Mahdi was found guilty of war crimes and crimes against humanity in the ***Prosecutor v. Al Mahdi***[5] case, affecting the prosecution of cyberattacks targeting cultural heritage sites. The US Court of Appeals for the Second Circuit has also ruled that trade secret theft qualifies as economic espionage, potentially impacting the prosecution of cyberattacks targeting trade secrets.

Potentialities:

1) Information and education accessibility: New technology has revolutionized knowledge and education, empowering individuals to share their experiences, interact with human rights advocates, and access information on their rights, thereby enhancing their empowerment.

2) Collaboration and communication: New technology enables easier interaction and collaboration, benefiting human rights movements and holding companies and governments accountable. Social media can be used to plan rallies, highlight human rights violations, and pressure policy changes.

3) Medical and healthcare advancements have been made possible by new technology: People may live longer, healthier lives as a result of this. For instance, new vaccinations have

3 140 S. Ct. 1731 (2020)

4 505 U.S. 833 (1992)

5 ICC-01/12-01/15

contributed to the eradication of illnesses like polio and smallpox. People with illnesses like cancer and HIV/AIDS are living longer because of new medicines.

4) Protection of the environment: Utilizing new technology can help safeguard the environment. Technologies based on renewable energy, for instance, can decrease greenhouse gas emissions and lessen the consequences of climate change. Our dependency on fossil fuels can be lessened by the use of energy-efficient devices.

In general, emerging technologies have the capacity to cause damage as well as good to international human rights. In order to employ new technologies to promote and defend human rights for everyone, it is critical to understand the risks and opportunities they present.

AI aims to increase workplace efficiency and save lives through individualized health, police, and warfare. In some professions, AI will enable further individualization, such as schooling based on each student's needs and intellectual talents. Martijn van Otterlo, assistant professor of artificial intelligence at Tilburg University, believes AI will change most lives for the better, especially in the short horizon of 2030 and beyond. The Cambridge Analytica case highlights privacy challenges in modern social networks, while Facebook provides improved communication and sharing capabilities.

The Artificial Intelligence (AI) industry is facing increasing concerns about discrimination and privacy, as well as the potential risks it poses to human rights, such as freedom of association and speech. Online threats to free speech and incitement of violence and hatred are also a concern. In some areas, harassment, trolling campaigns, and intimidation have tarnished offline safety. In 2017, the Rohingya people in Myanmar were subjected to hate speech and calls for violence due to algorithmically generated news feeds on Facebook. AI systems can impact freedom from discrimination, privacy, and other fundamental rights. In China, the government uses AI to filter communication related to anti-lockdown demonstrations. Prejudice and privacy violations also occur in the West. Excessive controls by authorities on speech and internet usage can endanger human rights. Countries restrict access to political expression and social media to combat extremism and hate speech. Internet shutdowns have become a standard tactic to quell lawful criticism, protests, and debate.

Data storage poses significant risks and consequences, including privacy, safety, free elections, freedom of expression, and the ability to discern truth from false information. The digital spectrum also threatens free and fair elections, freedom of expression, and the ability to discern truth. Programs for recruiting denigrate women, systems attribute higher likelihoods of reoffending to black suspects, and predictive policing overly policing underprivileged communities. Addressing these issues requires a human rights approach that recognizes individuals as unique individuals with rights, establishes legal frameworks, and pursues remedies for infringements or abuses.

Here are some instances of case law pertaining to the impact of technology on human rights:

Union of India v. K.S. Puttaswamy (2017)[6]: The Indian Supreme Court ruled in this historic decision that the Indian Constitution guarantees the right to privacy as a basic freedom. The Court recognized that technology has made it simpler for businesses and governments to gather and examine personal data, which is a severe danger to privacy. This realization informed part of the court's ruling.

(2015) Schrems v. Commissioner for Data Protection[7]: In this instance, the EU-US Safe Harbor Agreement—which permitted the transfer of personal data from the EU to the US—was declared void by the Court of Justice of the European Union. The Court concluded that, in view of the vast monitoring programs of the US government, the Safe Harbor Agreement did not offer EU individuals sufficient protection for their privacy.

PRIVACY CONCERNS:

Digital surveillance can collect vast amounts of data on individuals, allowing them to track their movements, interests, and personal lives. This can restrict freedom of expression and discriminate against marginalized groups. Governments and corporations can also abuse digital surveillance by spying on citizens, suppressing dissent, and collecting and selling personal data without consent. The UN Human Rights Office's recent report on privacy in the digital age highlights the effects of widespread digital monitoring, misuse of intrusive hacking tools, and the importance of strong encryption techniques in protecting human rights online.

Modern digital technologies, such as Pegasus software, are increasingly posing a threat to privacy. These tools allow intruders to access and eavesdrop on our phones, turning them into 24-hour surveillance devices. These spyware programs have been used illegally to silence opposing viewpoints, including human rights advocates, journalists, and opposition politicians, despite their purported use to combat terrorism and criminal activity. Therefore, international human rights laws and standards are crucial for controlling these technologies.

The Pegasus malware has been used by various governments to break into the phones of Palestinian journalists, activists, and journalists. The Indian government also used the malware in 2020 to access the phones of opposition lawmakers, human rights advocates, and journalists. Despite its importance in promoting privacy and human rights, encryption is under attack. States should avoid implementing measures that might erode encryption, such as requiring backdoors or client-side scanning. A 2022 study found that extensive digital surveillance in China has raised people's tendency to self-censor, leading to a society characterized by mistrust and terror. The Chinese government uses facial recognition technology to track and persecute Uyghur Muslims,

6 (2017) 10 SCC 1

7 (C-362/14) EU:C

while the US police use it to apprehend and charge protestors. The Indian government has also used digital monitoring to track and suppress Muslim and Dalit groups, political dissidents, and employers.

Governments and companies can misuse digital surveillance to crack down on opposition, collect and sell personal data without the consent of individuals, and suppress opposition. The Russian government uses digital surveillance to monitor its populace and suppress opposition, while tech businesses in the US have gathered and sold personal information without the consent of individuals involved.

In the ***Klass v. Germany***[8] case, the European Court of Human Rights declared in 2001 that the German government had infringed upon the right to privacy when it used surveillance software to track a political activist's emails and phone conversations.

In the ***Riley v. California***[9] decision from 2013, the US Supreme Court decided that police must have a warrant in order to search a person's cell phone prior to making an arrest. This decision was made in light of the fact that a significant quantity of personal data is stored on cell phones.

In the ***Pegasus Software S.p.A. v. Union of India***[10] case, the Indian Supreme Court decided in 2022 that the Indian government had to form an impartial expert committee to look into the claims of Pegasus usage.

The development of privacy laws and regulations faces challenges in balancing innovation, economic progress, and individual privacy. Key trends include a shift from sector-specific approaches to comprehensive ones, with early regulations targeting industries like finance and healthcare. This shift is driven by the increasing interconnectedness of companies and the growing usage of personal data across these sectors.

The emphasis on personal responsibility: The goal of more recent privacy regulations is to give people more control over their personal information. This covers the rights to refuse participation in specific data processing operations as well as the ability to view, amend, and remove personal data.

The acknowledgment of novel privacy rights: Apart from the customary right to privacy, authorities are starting to acknowledge novel privacy rights, such the right to data portability and the right to be forgotten. Using technology-based solutions An increasing number of people are using technological tools like anonymization and encryption to preserve their privacy. For instance, the GDPR mandates that companies put in place the proper organizational and technical safeguards to secure personal data.

8 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978)

9 573 U.S. 373 (2014)

10 2021 SCC OnLine SC 985

INTELLECTUAL PROPERTY RIGHTS:

Intellectual property, including innovations, creative works, designs, symbols, and names, has been significantly impacted by the digital age, with the internet and other technologies causing new challenges for consumers, governments, and owners. Copyright infringement is a major issue, as the proliferation of digital information has made it easier to steal and distribute copyrighted works without authorization, resulting in significant losses for producers and sellers.

The enforcement of intellectual property rights has been significantly impacted by communication technology, with advancements in storage and advertising models emerging. However, concerns about unapproved broadcasts, service theft, and illegal copying persist due to the emergence of cable and satellite television. To overcome these challenges, public support for intellectual property rights is crucial, as technology has made enforcement more challenging.

Storage technology has significantly impacted intellectual property rights, making it easier to duplicate and distribute protected works. This has expanded the scope of infringements and made it harder for copyright holders to regulate reproduction. The less specialized nature of storage technologies and their integration into computerized systems make controlling and monitoring copying more challenging. As a result, new obstacles to enforcing intellectual property rights have been created.

The advent of communication technologies like television and radio has significantly impacted copyright enforcement. Prior to these advancements, copyright owners could protect their works through physical transport or live performances. However, radio transmission spread performances across regions, making enforcement more challenging. Networks like NBC made it difficult to collect royalties at the door. Broadcasters and copyright holders created advertiser-supported models and agreements with collecting societies to track and pay royalties. Legal and legislative initiatives have complicated the relationship between cable broadcasters and copyright holders, and issues like theft of service and illegal signal interception have further complicated enforcement.

The development of communication satellites enabled the transmission of copyrighted content, requiring programmers and operators to uphold property rights. The widespread use of technology has made enforcing copyright harder, necessitating advertiser support, monitoring systems, and encryption technology.

Regarding copyright enforcement, cable and satellite television have brought up a number of problems. Theft of service, which is defined as connecting to a cable or satellite provider without authorization, is one of the biggest problems. Since royalty payments for copyright holders are usually contingent on the size of the paying audience, this illicit access robs them of their just reward.

Cable providers face challenges in copyright enforcement due to high processing costs and the difficulty in locating and negotiating royalty payments with television copyright holders. Satellite television has made copyright enforcement more challenging, as unauthorized users can access content without paying, compromising copyright holders' economic interests. Congress has tasked

program providers and satellite system operators to uphold property rights in satellite transmissions, urging encryption and market mechanisms for payment. However, intercepting satellite transmissions is not considered a violation if certain requirements are met. Issues such as theft of service, illegal access to copyrighted content, and the need for encryption and market mechanisms have been addressed by cable and satellite television.

The rise of digital communication and facsimile technologies has raised concerns about copyright enforcement. The ease of transferring digital information, including copyrighted content, has made it difficult for copyright holders to monitor and control unlawful use. The use of facsimile machines has also made it easier to spread illegal copies of protected material. Although sending documents via facsimile is more expensive, potential copyright issues may arise when costs decrease. Therefore, safeguarding intellectual property rights in the digital realm is crucial.

Technology has significantly impacted the enforcement of intellectual property rights. Advancements in storage technology, such as optical disks, have reduced the cost and ease of copyrighted content storage, increasing the risk of infringements. Communication technology advancements, such as satellite, cable, radio, and television broadcasting, have made it easier to monitor and enforce copyright, especially in cases of theft of service and unlawful dissemination. The rapid information flow has also made it harder for copyright holders to identify and demonstrate infringements. Additionally, technology has provided copyright holders with additional options to regulate their works' distribution, such as monitored electronic access control systems. However, a balance between control and public access must be carefully studied to prevent infringements and protect private rights.

Open-source software, which allows unrestricted modification and distribution of source code, poses a challenge for businesses in protecting their intellectual property. This openness to modification and distribution exposes the code to copying and exploitation. While it encourages cooperation and creativity, it also tests established software development processes, making intellectual property protection more challenging. Therefore, businesses must carefully consider the impact of open-source software on their rights.

Patent protection is an intellectual property right that safeguards innovations, but the digital age has introduced new challenges. One of the main issues is patent trolls, who obtain patents and sue other businesses for infringement, leading to pointless lawsuits and high legal costs. Governments and groups have implemented patent review programs and reform laws to expedite the patent application process and reduce litigation. Trademarks, on the other hand, protect corporate names, logos, and other distinguishing marks. However, trademark protection faces challenges in the internet environment, including domain name infringement, cybersquatters, and brand emulsion. Cybersquatters register domain names similar to well-known brands, while brand emulsion is made easier by social media and online marketplaces, causing confusion and damage to the original brand's reputation.

The digital era has made intellectual property enforcement difficult due to the ease of copying and distribution of digital material worldwide. Piracy, the unapproved use, duplication, or distribution of protected works, is a major obstacle, particularly in software, music, and film sectors. Jurisdiction is another challenge, as the global nature of the internet makes it difficult to enforce intellectual property rights across multiple jurisdictions. Regional variations in intellectual

property laws and regulations also make it difficult for content producers and owners to take legal action against infringers in different locations.

Digital rights management systems and advancements in machine learning and artificial intelligence can prevent digital material piracy and unlawful usage. Cooperation between legal and technology specialists is crucial for effectively handling intellectual property issues, with technology specialists creating solutions and legal professionals advising legislation.

The following are some particular instances of how IP rules have changed to reflect the digital age: (number these)

- Online service providers are shielded from copyright liability under the Digital Millennium Copyright Act (DMCA) in the US if they delete illegal content from their websites.
- Online platforms are required under the 2019 adoption of the European Union's Copyright Directive to take action to delete and stop the uploading of information that violates intellectual property rights.
- In 2012, the Indian Copyright Act was modified to incorporate clauses pertaining to digital rights management and internet piracy.

The Supreme Court has ruled in various cases regarding copyright infringement, stating that it is reasonable to use a VCR for personal viewing of protected content. However, in 2005, the court ruled that Grokster, Ltd. was not accountable for copyright infringement as it lacked direct control over its users' illegal actions. The Lanham Act and 15 U.S.C. § 1125(a) forbid using a trademark that might lead to consumer misunderstanding.

In 1997, ***American Internet v. Housing Galleries, Inc.*** ruled that internet service providers might be held liable for trademark infringement.

In ***Booking.com B.V. v. USPTO***[11], the name "booking.com" cannot be protected by trademark. Technology has made copyright enforcement more challenging, but maintaining control is essential.

DATA PROTECTION AND CYBERSECURITY:

Data is crucial for businesses, influencing personalized experiences and automated marketing. However, legislators are also concerned about data security and privacy. With the growing digitalization, people are becoming more aware of potential data vulnerabilities. High-profile data breaches and privacy scandals highlight the urgent need for strong data protection regulations. Authorities worldwide agree that safeguarding individuals' data rights is an important issue, and global efforts aim to balance economic development and innovation with defending privacy and control over personal data.

11 591 U.S. _ (2020)

The Information Technology Act of 20002 in India, despite being a crucial privacy regulation, has been criticized for its insufficient provisions for data privacy, limited scope, lack of explicit guidelines for consent and control, and inability to address issues with data localization, cross-border transfers, and advanced technologies like machine learning and artificial intelligence. The Act's enforcement is also hindered by lack of harsh penalties and inadequate notification procedures for data breaches.

The Digital Personal Data Protection Bill, 2022, is a comprehensive framework for India to safeguard personal data and promote responsible data processing. It covers data fiduciaries, processors, and other entities handling personal data. The bill manages the entire lifecycle of personal data, focusing on sensitive and cross-border data exchanges. The Digital India Act, 2023.4 enhances the Digital Personal Data Personal law, focusing on digital progress, cyber security, artificial intelligence, infrastructure, and competition.

The Digital Personal Data Protection Bill of 2022 is a law aimed at protecting personal data, ensuring accountability, and empowering individuals. It includes provisions for explicit consent, access to personal information, the right to be forgotten, data localization, and control over profiling practices. The bill aligns with global data protection norms like General Data Privacy Regulation, promoting data protection concepts like purpose restriction, data minimization, and accountability. This aligns with international norms, facilitating cross-border data transfers and boosting Indian business confidence.

The bill acknowledges the right to data portability but lacks precise mechanisms for seamless transfer. It lacks clarity in definitions, making it difficult to interpret and apply the law. The bill recognizes data principals' rights but lacks effective enforcement mechanisms, making it difficult for people to assert their rights and hold data fiduciaries accountable for violations. The lack of clear enforcement provisions may hinder compliance.

There is also not enough clarity in the regulations governing the transfer of personal data outside of India. The Central Government grants the Central Government the discretion to decide which countries or regions may receive data transfers, but it makes no mention of any transparent processes for doing so. This ambiguity may have an effect on businesses conducting business internationally by possibly causing inconsistent decisions and impeding cross-border data flows.

The Digital Personal Data Protection Bill, 2022, aims to enhance consent mechanisms by creating comprehensive policies for obtaining and managing consent, including explicit consent for sensitive data. Clear guidelines for consent forms should be made understandable, transparent, and accessible. Additionally, robust data security systems and privacy policies should be implemented to protect personal data and ensure compliance across sectors. Data breaches, which can occur in various scenarios, can result in serious repercussions such as monetary losses and reputational damage. Governments have enacted rules for data breach notification, such as the Health Insurance Portability and Accountability Act, GDPR, California Consumer Privacy Act, and Gramm-Leach-Bliley Act. Robust procedures for data security and privacy can reduce the likelihood of breaches and their effects.

Data Privacy Laws and GDPR

GDPR is a set of EU and EEA regulations governing data protection and privacy. It applies to all businesses, regardless of size or location, and can result in fines of up to €20 million or 4% of gross yearly revenue. In recent months, US states have enacted similar legislation, giving consumers control over their personal data. New consumer privacy regulations in Virginia, Colorado, and Utah will take effect in 2023. The EU has also enacted new regulations governing digital platforms, such as the Digital Markets Act to prevent unfair business practices and the Digital Services Act to create contact points with government agencies.

Other noteworthy global data privacy legislation that are worth mentioning include:

The United States federal legislation known as the **Children's Online Privacy Protection Act (COPPA)** mandates that parental consent be obtained prior to the collection of personal data from children less than 13 years old.

The Health Insurance Portability and Accountability Act (HIPAA) is a federal statute that safeguards the confidentiality of medical records gathered by different organizations.

Regulation on the General Data Protection (GDPR): This European legislation, which has previously been stated, establishes guidelines for the gathering and use of personal data throughout Europe. It also gives individuals the ability to seek the deletion of their personal data or to opt out of having their data collected.

Organizations have a fiduciary duty to protect sensitive information, based on corporate imperatives, ethical standards, and legal constraints. They can use security measures like access restrictions, encryption, and employee training on cybersecurity best practices. They should also update software, monitor unusual system behavior, and have a thorough incident response strategy. Data breaches can lead to negative effects, so companies must be proactive in reducing the likelihood of such incidents.

Cyberterrorism is a growing concern, but actual incidents are rare. Factors like psychology, politics, and the economy contribute to its dread. Cyberattacks can target infrastructure, but it's difficult to differentiate between them. Terrorists find cyberterrorism appealing due to cost, anonymity, and potential targets. The threat is often overstated, and as technology advances, it may grow. Emphasis should be on addressing this real danger without exaggeration.

Cyberterrorism is a significant concern, but it is often misrepresented and overstated. There are no actual cases reported, and the lines between cyberterrorism and cyberattacks are often crossed. Factors like psychology, politics, and the economy contribute to the fear of cyberterrorism. As technology advances, cyberterrorism may become a bigger threat, making it crucial to remain aware of potential threats.

Cyberterrorism is influenced by psychological, political, and economic factors. People often view unknown threats as more dangerous than well-known ones, leading to fear and distrust of computer technology. The fear of cyberterrorism can have significant psychological effects on fearful communities, similar to those caused by terrorist bombings. Post-2001, cyberterrorism became a political hot topic, with discussions on national security often involving political agendas. The risk of cyberterrorism has become a lucrative and contentious subject, leading to the development of an industry, government funding for infrastructure security, and law enforcement organizations committing resources to cyber investigations.

Cyberterrorism is a complex combination of psychological, political, and economic factors that contribute to the sense of serious danger. Terrorists are drawn to cyberterrorism due to its cost-effectiveness and ability to carry out attacks with just a laptop and internet connection, eliminating the need for physical weapons. They can use cables, wireless connections, and phone lines to distribute computer infections.

Cyberterrorism offers greater anonymity compared to conventional methods, as terrorists can use online aliases or sign in as "guest users." It allows for a wide range of targets, including public utilities, private planes, individuals, and governments, and can exploit vulnerabilities in critical infrastructures. The complexity of cyberterrorism makes it difficult for law enforcement and security organizations to identify and combat it. The potential for direct impact on a large population, as demonstrated by the I LOVE YOU virus, further highlights the appeal of cyberterrorism. Despite its affordability, anonymity, broad target base, and potential for extensive damage, it remains a significant threat to global security.

To combat the current cyberterrorism threat, a comprehensive strategy should be adopted. This includes strengthening security protocols, increasing cooperation and information sharing, creating thorough incident response plans, raising public awareness about cybersecurity, promoting international standards and collaboration, and investing in research and development.

Securing systems, firewalls, encryption, and frequent security upgrades are crucial for individuals, governments, and businesses. Increased cooperation and information sharing among governments, international organizations, and private sector businesses can help detect and counter cyber threats. Tested and well-defined incident response procedures can help identify, stop, and address cyber events. Public education on safe internet behaviors, such as strong passwords and frequent software updates, can help reduce cyberattacks. Promoting international standards and collaboration can set responsible online conduct and facilitate collaboration to find and apprehend cybercriminals. Continuous funding for research and development in technology like machine learning, artificial intelligence, and behavioral analytics can help identify and address threats.

The Seventh Circuit Court of Appeals ruled that businesses that neglect to protect customer data are subject to the Federal Trade Commission's enforcement of its unfair and deceptive trade practices power. Equifax Inc. agreed to pay $575 million to resolve a class action lawsuit alleging inadequate customer data security after a 2017 data breach. Yahoo! Inc. was held accountable for damages resulting from a 2013 data breach, while the European Court of Justice (CJEU) ruled that firms must obtain user consent before exploiting user data for targeted advertising. The EU-US Privacy Shield was deemed illegal in Schrems II, Case C-311/18. In 2015, the Ontario Superior Court of Justice held Ashley Madison accountable for damages resulting from a 2015 data breach.

The Full Federal Court of Australia required businesses to inform the Australian Information Commissioner of any data breaches causing significant harm. In ***Canada's Privacy Commissioner v. Equifax Canada Co., Equifax Canada Co.***[12] was found to have failed to secure customer data, violating Canadian privacy legislation.

CONCLUSION:

The digital age has brought about numerous ethical and legal issues, including cybersecurity, data protection, human rights, privacy, and intellectual property. These issues are complex and multidimensional, posing a significant threat to core human rights and values. Human rights concerns include citizen surveillance, repression of dissent, and false information dissemination. Privacy issues arise from increased data collection and usage by governments and businesses. Intellectual property rights are challenged by new technologies like blockchain and internet piracy. Data protection is increasingly important due to the frequency and cost of data breaches. Cybersecurity risks are also increasing due to hacking, cyber espionage, and cyberterrorism. These issues are interconnected and can lead to identity theft, damage to services, and disruption of infrastructure. To address these issues holistically, it is essential to encourage digital inclusion, safeguard moral principles and human rights, create robust data protection frameworks, strengthen cybersecurity defenses, and promote ethical innovation. By working together, we can make the digital world more fair, just, and safe for everyone.

References:

- https://articles.manupatra.com/
- https://www.usip.org/
- https://www.princeton.edu/
- https://www.globalipconvention.com/
- https://www.ohchr.org/
- phrg.padovauniversitypress.it
- https://www.lawfaremedia.org/
- https://www.cambridge.org/
- https://www.pewresearch.org/
- https://www.hrw.org/topic/technology-and-rights

12 #2019-001