Forum: Human Rights Council
Topic: Mitigating the impact of emerging technologies on human rights
Student Officer: Mariza Michalaki
Position: Deputy President

PERSONAL INTRODUCTION

Dear Delegates,

My name is Mariza Michalaki and I am a tenth grade student at HAEF Athens College. This year I have the utmost honour of serving as a Deputy President in the Human Rights Council of SCMUN, marking my 8th MUN conference and my second time serving as a student officer. I am delighted to share this experience with you!

First of all I would like to welcome you to the 3rd session of SCMUN and congratulate you for your decision to participate in the conference. Through participating in MUNs I have broadened my horizons, I have become more globally aware and have made long lasting friendships. I really hope that this conference will be an eye opening opportunity for you and that you will be able to enjoy it at its fullest.

This study guide will provide you with insightful information concerning the second topic of the agenda, mainly "Mitigating the impact of emerging technologies on human rights". Due to the rapid development of technology and Artificial Intelligence the past few years, many concerns have been raised regarding their negative impact on human rights. This years' conference theme is post war societies and it is highly connected to the issue at hand due to the fact that post war societies are still developing and are more susceptible to the impact of emerging technologies. In this study guide, those problems will be explained, analysed, and addressed through various aspects. Its purpose is to familiarise you with the issue, aid and guide you through the creation of your policy statements and resolutions. However I strongly recommend that you also conduct your own research in order to fully comprehend your nation's policy.

I am sincerely looking forward to meeting you all this February and if you have any questions regarding this study guide or your nation's policy do not hesitate to contact me at my email address! (mmichalaki@athenscollege.edu.gr)

Best Regards,

Mariza Michalaki

TOPIC INTRODUCTION

We live in the age of technology. In the past few years mankind has developed a lot of new technologies which have definitely helped in shaping an easier and more convenient reality for humanity in various aspects. Those new technologies include Artificial Intelligence (AI), Biometric Technologies, the Internet of Things (IoT), Augmented and Virtual reality, Surveillance Technologies, and Biotechnology. Emerging technologies have the potential to both positively and negatively impact human rights. While they can offer innovative solutions to various global challenges, they also bring about risks and challenges that can undermine human rights in several ways.

Those new technologies have raised the concerns of many organisations such as the United Nations Human Rights Council. The human rights that those technologies violate include the right to privacy, the right to nondiscrimination, the right to health privacy, the right to security, and the right to work. A 2020 report stated that automation is able to replace more than 85 million jobs by 2025[1]. Not to mention that as reported by another 2020 report, there were over 36 billion records exposed in data violations in the first half of 2020.[2]

It is of utmost importance to extenuate the negative impact of those technologies on human rights if we want to preserve them, and protect humanity against the severe consequences of their excessive development and usage. It is vital to strike a balance between technological advancement and the preservation of fundamental human values. Failure to do so can have a number of negative consequences, including violations of individual rights, discrimination, and threats to democracy and social cohesion.

DEFINITION OF KEY TERMS

Emerging Technologies

"Emerging technologies refer to innovative tools, systems, or advancements that hold the potential to dramatically alter the current landscape of industries, economies, and societies. These technologies often stem from groundbreaking research and can introduce new ways of addressing existing challenges, offering transformative solutions that were previously unattainable"[3]

---

[1] "Robots to Replace 50% of Work Tasks by 2025: WEF." *Best Practice*, 22 Oct. 2020, bestpractice.biz/robots-to-replace-50-of-work-tasks-by-2025-wef/#:~:text=The%20WEF%20expects%20that%2085%20million%20labour-intensive%20jobs. Accessed 24 Oct. 2023.

[2] "36 Billion Data Records Exposed (so Far) in 2020: Risk Based Security." *Spiceworks*, www.spiceworks.com/it-security/data-security/news/36-billion-data-records-exposed-so-far-in-2020-risk-based-security/.

[3] Williams, Conor. "What Is Emerging Technology?" *Tech Training HQ*, May 2023, www.techtraininghq.com/what-is-emerging-technology https://www.techtraininghq.com/what-is-emerging-technology/.

Artificial Intelligence (AI)

"Is the capacity of a computer, robot, or other programmed mechanical device to perform operations and tasks analogous to learning and decision making in humans, such as speech recognition or question answering"[4]

Human Rights

"Fundamental rights, especially those believed to belong to an individual and in whose exercise a government may not interfere, as the rights to speak, associate, work, etc."[5]

Biometric Technologies

"Biometric technology is defined as the measurement and analysis of unique human characteristics such as DNA, fingerprints, voice patterns, hand measurements, and eye retinas and irises."[6]

Internet of Things (IoT)

"The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software and network connectivity that allows them to collect and share data."[7]

Augmented Reality

"An enhanced image or environment as viewed on a screen or other display, produced by overlaying computer-generated images, sounds, or other data on a real-world environment"[8]

Surveillance Technologies

"The term 'surveillance technology' encompasses any digital device, software or system that gathers information on an individuals' activities or communications."[9]

---

[4] "Artificial Intelligence Definition and Meaning | Dictionary.com." *Dictionary.com*, 11 Feb. 2021, www.dictionary.com/browse/artificial-intelligence.

[5] "Human Rights Definition and Meaning | Dictionary.com." *Dictionary.com*, 5 Feb. 2021, www.dictionary.com/browse/human-rights.

[6] "What Is Biometric Technology." *BiometricCentral.com*, 2 Aug. 2020, www.biometriccentral.com/what-is-biometric-technology.

[7] *What Is the Internet of Things? | IBM*. www.ibm.com/topics/internet-of-things.

[8] "Augmented Reality Definition and Meaning | Dictionary.com." *Dictionary.com*, 22 Jan. 2021, www.dictionary.com/browse/augmented-reality.

[9] "Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/en-us/insights/decoder/s/surveillance-technology#:~:text=The%20term%20%E2%80%98surveillance%20technology%E2%80%99%20encompasses%2

Biotechnology

"The use of living organisms or other biological systems in the manufacture of drugs or other products or for environmental management, as in waste recycling: includes the use of bioreactors in manufacturing, microorganisms to degrade oil slicks or organic waste, genetically engineered bacteria to produce human hormones, and monoclonal antibodies to identify antigens"[10]

BACKGROUND INFORMATION

The Development of Emerging Technologies

The past few years many new and improved technologies have emerged and have highly raised the concerns of experts regarding their deep impact on the fundamental human rights of people. So In this section of the study guide those technologies that are being referred to will be analysed. One of them is Artificial Intelligence. Even though it is considered that Artificial Intelligence was recently developed, it is not the case. In 1950, Clause Shannon designed a robotic mouse that had the ability to find its own way out of a maze. Since then, technology has come a long way and Artificial Intelligence is able to produce photorealistic images, interpret and generate language but also conduct tasks that require human intelligence.[11] Artificial Intelligence is also used in many workplaces where tasks were once performed by humans, since it can increase productivity, reduce costs, process information in a rapid manner, and improve the quality of products. [12]

[10] "Biotechnology Definition and Meaning | Dictionary.com." *Dictionary.com*, 20 Jan. 2021, www.dictionary.com/browse/biotechnology.

[11] "How Has AI Developed Over the Years and What's Next?" *World Economic Forum*, 6 Oct. 2023, www.weforum.org/agenda/2022/12/how-ai-developed-whats-next-digital-transformation.

[12] "Is Artificial Intelligence Really Replacing Jobs? Here's the Truth." *World Economic Forum*, 28 June 2021, www.weforum.org/agenda/2018/09/is-artificial-intelligence-replacing-jobs-truth.

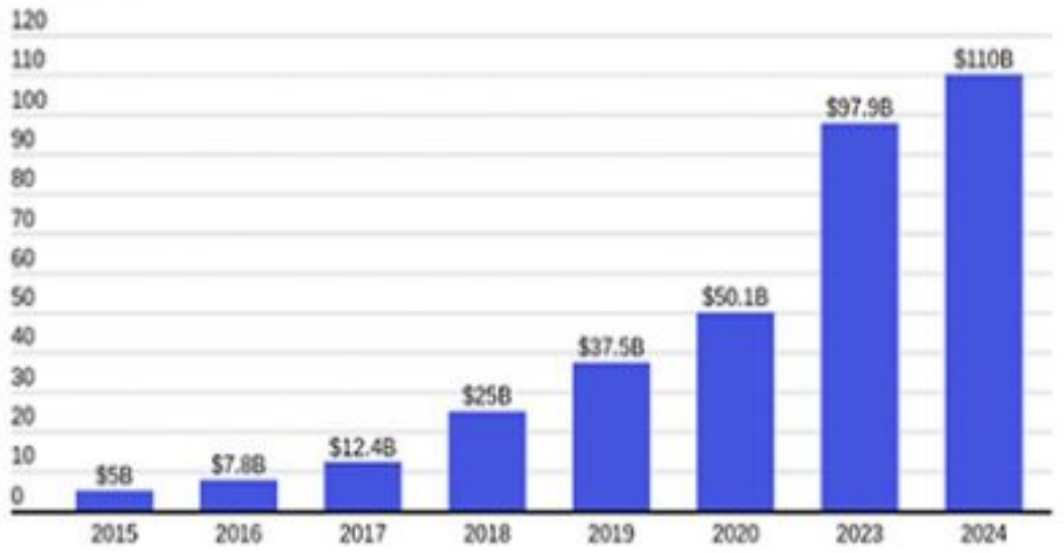

Figure 1: Global annual growth in the billions of US dollars invested in Artificial Intelligence

Another notable example of those emerging technologies are biometric technologies. The first form of biometric technology to ever exist is fingerprint recognition. Fingerprint recognition originated in 1858, when Sir William Herschel who utilised them in order to reduce fraud, of course not digitally.[13] Since then many technological advancements have been made and fingerprint recognition is now utilised for mobile phone unlocking, mobile payments, medical information, drivers licences and so on. [14] Biometric systems are mostly used for identification and authentication purposes in hotels, hospitals, airports, grocery stores, and government buildings. They include iris scanning, fingerprinting, palm printing and voice patterns which are mostly used in everyday life and for a variety of security measures. They are also utilised by people since it can aid significantly in making their life easier, cheaper and more secure. [15]

[13] Watson, Stephanie. "How Fingerprinting Works." *HowStuffWorks*, 24 Mar. 2008, science.howstuffworks.com/fingerprinting3.htm .

[14] Yu, Yirong, et al. *A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications*. Vol. 14, no. 6, 14 June 2023, pp. 1253–1253, https://doi.org/10.3390/mi14061253. Accessed 10 July 2023.

[15] "What Is Biometric Technology." *BiometricCentral.com*, www.biometriccentral.com/what-is-biometric-technology/#:~:text=Biometric%20technology%20is%20defined%20as%20the%20measurement%20and.

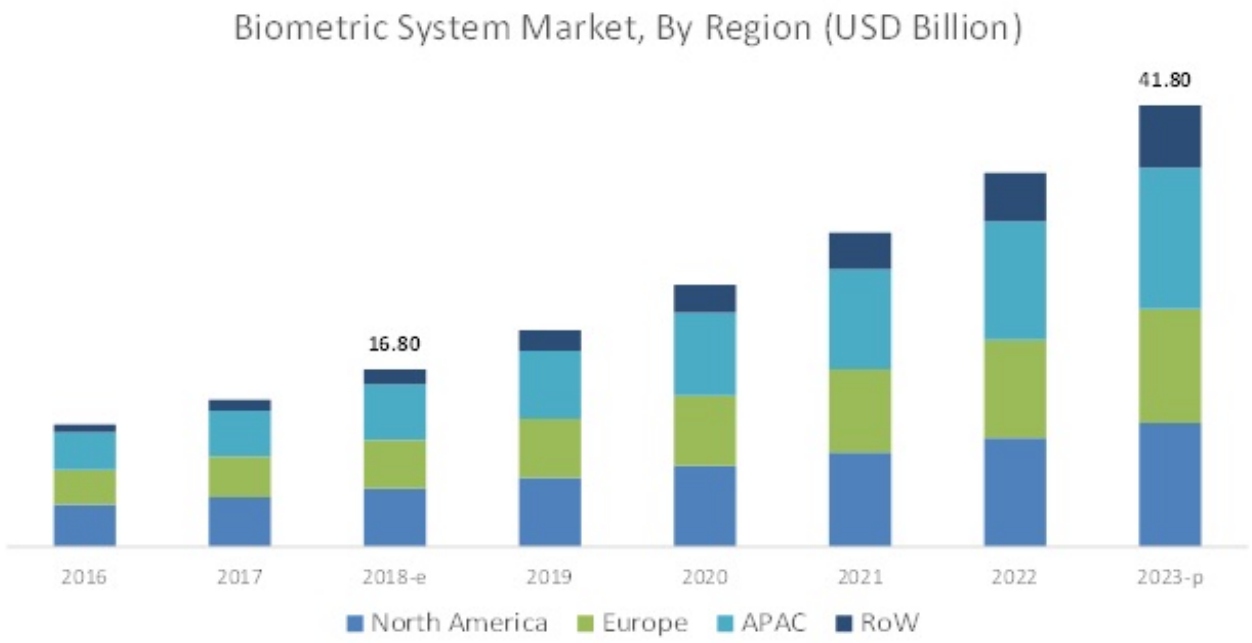

Figure 2: Biometric Technology market size and increase

The Internet of Things (IoT) is also a technology that has greatly emerged in the past years. It creates a massive network in which devices are interconnected and have the ability to exchange data and perform various automated tasks. Some of the abilities of the Internet of Things are controlling the process of manufacturing in factories, monitoring several environmental conditions that occur in crop fields, managing traffic patterns, and many more. They have made vast advancements in sectors such as transportation, manufacturing, health care and agriculture. As the number of inter-connected devices increases, so does the significance of the role that the IoT has in reshaping our world and completely changing how we work, live and interact with one another. It also can greatly aid companies in modernising several processes and boosting significantly their profits due to its ability for the provision of data, which we can examine in order to find trends, patterns and anomalies.[16]

Surveillance technologies are also a valid example of a technology that has significantly emerged in the past years. They are being utilised in order to monitor individuals' communications, physical and digital actions. Those technologies include, data-gathering apps on smartphones, and facial recognition software in smart security camera systems. In the present days, those tools that are being used in order to share and collect data have become a nearly undetectable form of surveillance. For example, smartphones are able to gather but also store personally identifiable information which includes the people that we talk to, the locations that we visit, our internet search history, our social media presence and a lot more. Usually this data is being collected and then analysed in order for companies to

[16] IBM. "IBM - United States." *Www.ibm.com*, 1 Oct. 2015, www.ibm.com/topics/internet-of-things.

better understand consumers in order to have a wider perspective on consumers behaviour and employees activities. [17]

Human Rights and their Significance

"The Universal Declaration of Human Rights is a milestone document in the history of human rights". It was established by the United Nations General Assembly on December 10 1948 by representatives from all nations. It is the first document that set the Universal Fundamental Human Rights and was translated to more than 500 languages.[18] The Articles that concern the violation of human rights by emerging technologies are Article 2, Article 3, Article 19, Article 12 and Article 23.

Article 2 refers to the right to non-discrimination which is a vital Human Right for several reasons. This right ensures that individuals are not subjected to any discrimination or prejudice based on their gender, ethnicity or race while also promoting respect for every person. Additionally it creates a feeling of belonging among all members of a community by advocating for social cohesion. Furthermore non-discrimination is crucial in order to achieve social progress. In the future it aims to rectify several systemic and historic inequalities while also nurturing a more equitable society. It also guarantees the diversity of the community that we all live in and that all people are treated in an equitable, fair and equal manner even though coming form completely different backgrounds. [19]

Article 3 examines the right to security which in this case includes cyber security. This right is truly significant since it ensures privacy protection and the non-misuse of someones or an organisation's data from theft and unauthorised access. It is also crucial since it protects the security of all nations. Most States are extremely reliant on defence infrastructure and secure communication systems which can now be hacked easily due to new technologies that have emerged and have made unauthorised access towards devices easier. The right to cybersecurity is of utmost importance in order to protect the privacy of information and its non-distribution, data and critical infrastructure as well as to preserve trust in digital systems and defend fundamental human rights. In the digital age that we live in, breaches of the right to cybersecurity have a broad ranging impact on individuals, nations and businesses.[20]

Article 19 introduces the Right to Freedom of expression which is crucial for a society to be able to operate smoothly. It enables people to fully express their opinion and beliefs without the fear of being damped down by the government or being subject to censorship. It also promotes friendly discussion among the government and people without the fear of being

[17] "Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/insights/decoder/s/surveillance-technology.

[18] United Nations. "Universal Declaration of Human Rights." *United Nations*, 10 Dec. 1948, www.un.org/en/about-us/universal-declaration-of-human-rights.

[19] Weihrauch, Alexander. "The Principle of Non-Discrimination." *Humanium*, 2 Mar. 2021, www.humanium.org/en/the-principle-of-non-discrimination/.

[20] "Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/insights/decoder/s/surveillance-technology.

deprived of that right. The right to freedom of expression is fundamental for social and economic growth but most importantly for the smooth operation of a democratic society. Especially in post war societies because due to their under development and the fact that they might not have a stable government it is crucial for individuals to possess that right in order for a democratic society to progress and develop in a collective manner. [21]

Article 12 addresses the Right to Privacy, in this case the right to cyber privacy, which is fundamental in a society. Through information technology, the right to privacy plans of advancing individuals' ability to manage internet usage, private data and communications. Without the right to cyber security individuals sense that they are being watched which leads to their self-censorship but also to them feeling deprived of their right to freedom of expression. Cyber security is extremely significant in order to protect critical and confidential information. This furtherly includes, but is not limited to, private conversations, business data, healthcare records, and intellectual property. When privacy protection is non-existent, data like the ones mentioned above can be easily and (un)lawfully accessed and then misused.[22]

Article 23 refers to the Right to Work which is of utmost importance to society. Through this right, economic stability is ensured for individuals but also their possession of a sufficient wage that is able to support them and their family. Also, by offering people the right to work, they are able to make a living and not be reliant on the government for funds."The right to work is a foundation for the realisation of other human rights and for life with dignity. It includes the opportunity to earn a livelihood by work freely chosen or accepted." [23]

Challenges created by Emerging Technologies

Even though emerging technologies possess great capabilities and are able to provide significant aid and solutions to various crucial world issues, they also pose major challenges to society as a whole.

First and foremost emerging technologies have raised several security and privacy concerns. The past years due to the rapid development of many new technologies, many intrusions into government but also private owned sectors have exposed private but also business information. Every day more and more systems are being hacked and this resulting to a

[21] "Freedom of Expression: A Fundamental Human Right Underpinning All Civil Liberties." *UNESCO*, 14 Apr. 2015, webarchive.unesco.org/web/20170204064206/en.unesco.org/70years/freedom_of_expression.
[22] Soken-Huberty, Emmaline. "10 Reasons Why Privacy Rights Are Important." *Human Rights Careers*, 2 May 2020, www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/.
[23] "The Right to Work and Workers' Rights." *ESCR-Net*, www.escr-net.org/rights/work#:~:text=The%20right%20to%20work%20is%20a%20foundation%20for. Accessed 13 Oct. 2023.

sufficient amount of private information being available on the web. [24] Many sectors such as government, health care, finance and transportation had to vitally increase their budget due to prevent and minimise the rise of cyber attacks.

Governmental entities are usually a prime target of cyber attacks due to their possession of valuable data and information, but also due to their provision of essential services. Research has shown that the government is the second most cyber-attacked sector with an average of 1564 attack cases every week, marking a 20 percent increase from the year 2021.[25] One of the biggest government cyber attacks took place in 2012 in the United States office of Personnel Management where hackers were able to steal around 22 million records that included biometric data, such as fingerprints, addresses and Social Security Numbers. [26] Those government cyber attacks can lead to damaged reputation, increased privacy and security risks of individuals, distribution of highly confidential information, increase of operational costs and the damage of the reputation of certain governmental entities. [27]

The healthcare sector is another highly affected one by cyber attacks. Research has shown that it is the third most affected sector by cyber attacks due to the high worth of patient information for cyber attackers, the easy accessibility of medical devices for attackers, the fact that most medical devices are outdated and the non education of healthcare staff on the protection of private data.[28] Those breaches in healthcare can lead to compromising patients' privacy and safety, medical identity theft, the disruption of the healthcare sector, financial problems and trust erosion in the healthcare sector. Over 100 million records have been stolen, of every kind, which include patient medical records, private details of medical donors, security numbers and financial data.[29] One of the biggest and most significant data breaches that occurred in the medical sector was in 2015 in the company Anthem Inc. Hackers were able to access its corporate database and steal more than 79 million medical records which included patient and employee data such as names, addresses, Social Security numbers, birth dates, medical IDs, insurance membership numbers, income data, and employment information. This affected 78.8 millions of patients and employees and

---

[24] Ross, Ron. "Why Security and Privacy Matter in a Digital World." *NIST*, 28 Sept. 2017, www.nist.gov/blogs/taking-measure/why-security-and-privacy-matter-digital-world#:~:text=Given%20this%20backdrop%2C%20it%20is%20often%20easy%20to. Accessed 26 Oct. 2023.

[25] etal. "Check Point Research: Third Quarter of 2022 Reveals Increase in Cyberattacks and Unexpected Developments in Global Trends." *Check Point Software*, 26 Oct. 2022, blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

[26] "The 7 Biggest Government Cyberattacks since 2011 | Swivel Secure." *Swivel*, 2011, swivelsecure.com/solutions/government/top-cyber-attacks/.

[27] II, Clint Crigger. "Impact of Cyber Attacks on Organizations." *ILLÜM ADVISORS*, 25 Oct. 2021, www.illumadvisors.com/insights/cybersecurity-insights/this-blog-will-highlight-some-of-the-ways-cyber-attacks-affect-organizations-and-how-we-can-help/.

[28] Swivelsecure. "9 Reasons Healthcare Is the Biggest Target for Cyberattacks." *Swivel*, 2018, swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

[29] Duguin, Stephane. "If Healthcare Doesn't Strengthen Its Cybersecurity, It Could Soon Be in Critical Condition." *World Economic Forum*, 8 Nov. 2021, www.weforum.org/agenda/2021/11/healthcare-cybersecurity/.

required 115 millions of dollars compensation for the resolvement of the litigation. This is considered the largest healthcare cyber attack in history. [30]

Additionally, a lot of privacy and security concerns have been raised in the finance sector. Cyber attacks are a usual occurrence in the financial sector due to the motivation to make money which can be granted on the account of insurers, banks and financial records which can be accessed with hacking. The access to personal and sensitive information which is existent in the financial sector can significantly attract the attention of hackers but also the existence of extremely profitable cryptocurrencies and ransomware are also a subject which motivates those attacks. [31] One of the biggest data breaches in the finance sector occurred in May 2019 in the company First American Corporation where more than 885 million financial and personal records linked to real estate transactions were exposed through a common website design error where the names, email addresses and phone numbers of closing agents and buyers of this company became available. And the possession of this information resulted in identity theft, malware injections and ransomware attacks. [32]

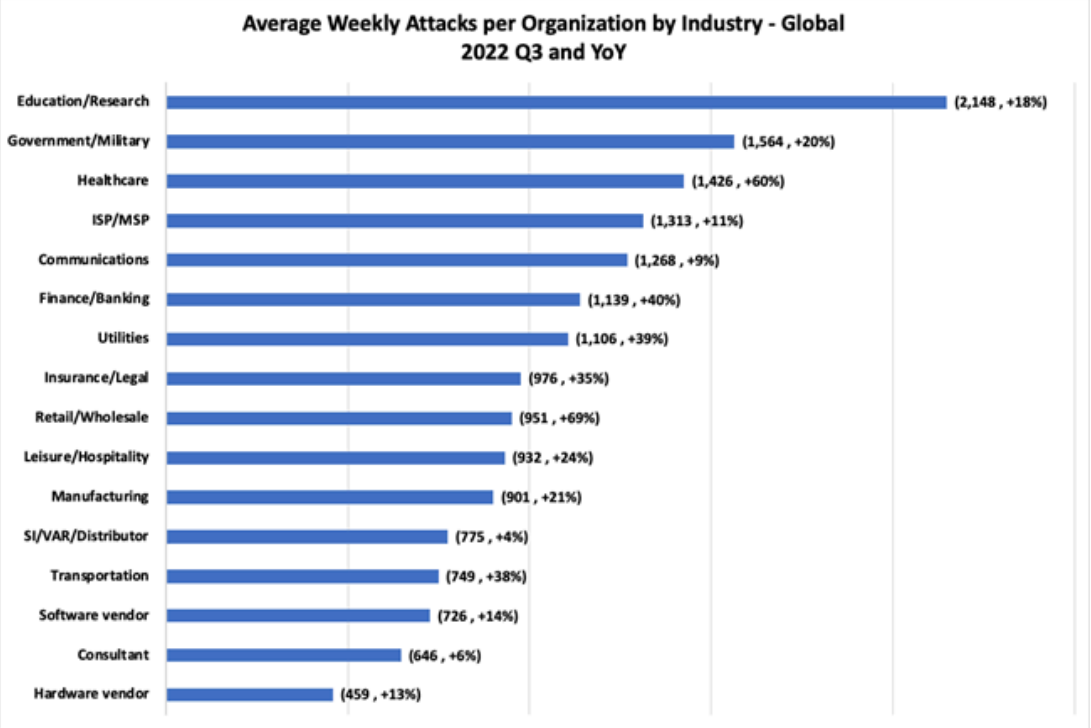

Image 3: Sectors most affected by cyber attacks in 2022

[30] Wolf, Arctic. "Biggest Healthcare Industry Cyberattacks." *Arctic Wolf*, 16 June 2021, arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/.

[31] "Why Is the Finance Sector a Target for Cyber Attacks? | UpGuard." *Www.upguard.com*, www.upguard.com/blog/finance-sector-cyber-attacks#:~:text=Why%20Do%20Cybercriminals%20Target%20the%20Financial%20Sector%3F%201. Accessed 26 Oct. 2023.

[32] Kost, Edward. "The 8 Biggest Data Breaches in Financial Services (2021 Edition) | UpGuard." *Www.upguard.com*, 1 Dec. 2022, www.upguard.com/blog/biggest-data-breaches-financial-services.

Intersection of emerging technologies and Human Rights

Article 2, of the Universal Declaration on Human Rights, refers to the right to non-discrimination which is being violated due to the new technologies that have emerged, but more specifically as a result of the development of Artificial Intelligence. One reason for this occurrence is the existence of algorithmic bias. Artificial Intelligence inherits the data and ideologies that it is trained on by humans. So if its training includes discriminatory patterns, they will be adopted by Artificial Intelligence which leads to discrimination in areas such as criminal justice lending and hiring. Furthermore, surveillance technologies which include facial recognition, surveillance cameras and data mining can lead to discrimination due to the surveillance of specific groups which results in various groups based on characteristics such as skin colour, ethnicity and religion. The development of those technologies raises again the question of access inequalities. Those technologies that have emerged the past years are not available to certain groups, thus creating again a segregation among certain communities.[33]

Article 3 refers to the right to security, in this case the right to cyber security, which is subjected to one of the most significant breaches by emerging technologies. Cyber security is of utmost importance in the days that we live in and the technologies which have emerged have made its maintenance significantly harder. Due to the evolution of technology, it has been made significantly easier for hackers to conduct data breaches, identity thefts and threaten the cyber security of individuals. Furthermore the recent development of autonomous weapons such as Artificial Intelligence, have created a sense of insecurity, on a personal, national but also on a global level. Furthermore, due to many advancements in biotechnologies that include gene editing and synthetic biology have highly raised concerns since their misuse can lead to creating genetically modified organisms or dangerous pathogens which can threaten global security significantly. Additionally, those emerging technologies can potentially really harm the environment as a result of the high amount of carbon emissions that they produce. And environmental degradation negatively impacts global security due to the national disasters that it can cause.[34]

Article 12 mentions the right to privacy, and in this case the right to cyber privacy, which is being violated through emerging technologies. Emerging technologies have in their possession a large amount of sensitive data that has been collected without the knowledge of individuals, which highly intrudes their right to privacy. That sensitive information includes, but is not limited to, location data which is tracked through their Wi-Fi and GPS, online activities so the websites that they visit and the products they browse, biometric data such as peoples digital fingerprints and digital facial recognition, communication content

[33] "Does Technology Increase the Problem of Racism and Discrimination?" *SearchEnterpriseAI*, www.techtarget.com/searchenterpriseai/opinion/Does-technology-increase-the-problem-of-racism-and-discrimination.

[34] Griffith, Melissa K. "Cyber Security and Emerging Technologies." *Survival*, vol. 64, no. 5, 3 Sept. 2022, pp. 174–180, https://doi.org/10.1080/00396338.2022.2126189.

which includes all of the phone calls, text messages and emails that people receive and send, financial data such as account balances, credit card details and transaction histories through online banking apps, DNA and Genetic information due to online testing services and voice recordings that can be collected through voice activated devices. The collection and distribution of such data can pose serious privacy risks, when utilised for "identification, tracking, profiling, facial recognition, classifying and behavioural prediction or the scoring of individuals" according to the United Nations General Assembly.[35]

Article 19 names the right to freedom of expression which in another one of many, that is being violated on the account of the rise of emerging technologies. Firstly a lot of governments, mostly in Less Economically Developed Countries (LEDCs) and states with strong religious affiliations, utilise those technologies in order to control and censor online content that they do not want citizens to get informed about, thus limiting their chances to form an opinion based on important issues so this depriving them of their right to express their opinion freely. Furthermore, the creation of echo chambers, that are environments in which individuals encounter only their beliefs, their opportunities to broaden their horizons are minimised and they are not able to express a different opinion due to the lack of information. Additionally due to the rapid evolution of Artificial Intelligence a lot of convincing fake content can be created and also realistic sounding text, which can be utilised for spreading false information and manipulating the opinion of the public which leads to the deprivation of the right to freedom of expression. [36]

Finally, Article 23 introduces the right to work which is also breached by emerging technologies. Due to the rise of Artificial Intelligence and the Augmented Workforce the issue of job displacement and the replacement of human tasks and jobs by machines has arised. Furthermore, as a result of the vast skills that Artificial Intelligence possesses and its ability to conduct complex tasks in an extremely rapid manner, a gap has been developed among the skills that individuals possess and the requirements of certain employment positions, leading to many challenges for individuals to find employment.[37]

---

[35] "To Protect Privacy in the Digital Age, World Governments Can and Must Do More | Association for Progressive Communications." *Www.apc.org*, www.apc.org/en/pubs/protect-privacy-digital-age-world-governments-can-and-must-do-more#:~:text=The%20resolution%20correctly%20notes%20that%20new%20technologies%20process. Accessed 27 Oct. 2023.

[36] Silva, Alberto Cerda. "Protecting Free Speech in the Digital Age: Q&a with UN Special Rapporteur for Freedom of Expression." *Ford Foundation*, 11 Oct. 2016, www.fordfoundation.org/news-and-stories/stories/protecting-free-speech-in-the-digital-age-qa-with-un-special-rapporteur-for-freedom-of-expression/.

[37] Burgess, John, and Julia Connell. "New Technology and Work: Exploring the Challenges." *The Economic and Labour Relations Review*, vol. 31, no. 3, 8 Aug. 2020, pp. 310–323, journals.sagepub.com/doi/10.1177/1035304620944296, https://doi.org/10.1177/1035304620944296.

TIMELINE OF EVENTS

Date of the Event	Event
1858	Fingerprint recognition was firstly introduced by Sir William Herschel marking the commencement of the creation of surveillance technologies
December 10 1948	The Universal Declaration of Human Rights was established in Paris and signed by all States around the world
1950	The first type of Artificial Intelligence was discovered by Clause Shannon
May 28 1961	Amnesty International, an organisation which aims in protecting the fundamental human rights, was established
1971	The World Economic Forum was established which is an organisation which created surveys, researches and reports based on significant world issues.
1974	The USA Privacy Act was implemented which is one of the first legislations ever designed in order to protect the right to privacy.
2012	Cyber attack in the United States office of Personnel Management marking one of the biggest cyber attacks in the government sector.
2013	The National Cyber Security Policy was implemented by India which is a framework aiming to safeguard the right to security
2015	The biggest Cyber Attack ever recorded in the healthcare industry occured in the company Anthem Inc. where tens of millions of medical records got stolen
1 June 2017	China implemented the CyberSecurity Law which provides authorities with the power to control the information distributed online in order to maintain national security.
2018	The California Consumer Privacy Act (CCPA) was implemented which aims in protecting individuals from privacy breaches in the corporate sector
May 2018	The General Data Protection Regulation (GDPR) was

	implemented by the European Union which is one of the strongest data protection regulations whose goal is to protect the right to privacy
May 2019	A Cyber Attack occurred in the company First American Corporation which is considered one of the largest cyber attacks in the Financial sector
11 July 2019	The A/HRC/RES/41/11 was adopted by the United Nations Human Rights Council whose goal is to address the issue of human rights violation in the digital age
1 June 2020	The European Digital Media Observatory began operating whose responsibility is to tackle online propaganda and misinformation in the European Union
16 December 2020	The A/RES/75/176 was adopted by the United Nations General Assembly whose goal is to maintain the right to privacy in the digital age
6 April 2022	Adoption of the CM/Rec(2022)13 by the Council of Ministers which aims in safeguarding the right to freedom of expression in the digital age
2023	The California Privacy Rights Act, which is a framework by the USA and aims in protection the privacy of individuals, was further improved and implemented
August 9 2023	India implemented the Personal Data Protection Bill, a regulation which aims in protecting the fundamental human right to privacy of individuals

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

China

China has taken a completely different approach from western nations, regarding the solution of the issues which has raised the concerns of various western nations but has also led to a lot of criticism by them. They prioritise the maintenance of political and social stability by censoring information flow and controlling the content that is being distributed on the internet. China possesses one of the most complicated censorship systems which is called the Great Firewall. This system filters the information that users research and denies them access to websites that it believes are harmful. It censors political criticism towards the

Chinese government and the access to websites that provide such political information.[38] Furthermore, China has installed heavy surveillance technologies that are being utilised in order to maintain social security but can also violate privacy rights and civil liberties. Those technologies include facial recognition, Artificial Intelligence driven monitoring systems and CCTV cameras. The Chinese government has also implemented digital ID systems which links citizens' online activities with their real world identities. This enables the government to track and monitor the online activities of individuals easily. China has additionally implemented the Cyber Security Law, which was established in June 1 2017, and gives authorities the power to moot and control online activities in order preserve national security.[39] China's approach has raised the concerns of multiple experts and organisations due to certain violations of the Human Rights to privacy and freedom of expression.

India

Even though India is a Newly Industrialised Country (NIC), and has only recently gathered efforts towards its economic development, it has made efforts of utmost importance in order to aid in limiting the impact of emerging technologies on human rights. In spite of their recognition of the benefits of technology and everything that it is able to offer to humanity they acknowledge the measures that have to be implemented in order to resolve this significant issue. India has introduced several data privacy protection laws, with the most vital one being the Personal Data Protection Bill. It was put into operation on August 9 2023. This regulation establishes guidelines for the exploitation of personal data by organisations and aids individuals gain a greater control of their personal data. It highlights the significance of consent and data localization.[40] In addition India has been working on enhancing and improving its cybersecurity framework in order to preserve the security of the citizens in the digital world. Namely, The National Cyber Security Policy, which was implemented in 2013 and aims in addressing threats and providing critical infrastructure.[41] Furthermore the government has established several programs which promote the digital literacy of populations mainly living in rural areas. It is crucial for individuals to be aware of the dangers that they are being exposed to during their usage of emerging technologies.

---

[38] Gisonna, Nicholas. "Great Firewall". Encyclopedia Britannica, 21 Sep. 2023, https://www.britannica.com/topic/Great-Firewall. Accessed 27 October 2023.

[39] Creemers, Rogier, et al. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *DigiChina*, 29 June 2018, digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[40] "Digital Personal Data Protection Bill 2023 Passed in Rajya Sabha: Key Points." *The Times of India*, 11 Aug. 2023, timesofindia.indiatimes.com/gadgets-news/digital-personal-data-protection-bill-2023-passed-in-rajya-sabha-key-points/articleshow/102579315.cms.

[41] "National Cyber Security Policy- Objectives, Features." *Testbook*, testbook.com/ias-preparation/national-cyber-security-policy. Accessed 27 Oct. 2023.

United States of America (USA)

The United States of America have conducted several significant actions in order to aid in mitigating the negative impact of emerging technologies on human rights. To begin with, The First Amendment of the United States Constitution[42], advocates for the Right to Freedom of Expression which is violated by emerging technologies and the US government constantly advocates for the protection of that right. Furthermore the USA have developed several regulations and policies in order to protect the right to privacy of the citizens. Those efforts began in 1974 when the Privacy Act was implemented which explained how federal agencies can utilise the data that they have collected from individuals. In 2018, the California Consumer Privacy Act (CCPA) was implemented which is considered one of the strictest data privacy laws. This act outlines specifically the rights that consumers have regarding the collection of their personal data by companies, but also it gives them the right to erase certain information collected by companies. It was updated by a second act, namely the California Privacy Rights Act, which further improved the rights of consumers and was set into place in 2023.[43] Furthermore the USA have set strong export control systems such as, the Arms Export Control Act (AECA), the International Emergency Economic Powers Act (IEEPA) and the Export Controls Reform Act (ECRA) which is able to restrict the export of defence articles, nuclear materials and technology, so generally items that would aid the amplification of nuclear, biological and chemical weapons. This aids in restricting the export of certain technologies whose usage can severely violate the Human Rights of Individuals.[44]

Amnesty International

Amnesty International is a non governmental organisation that was founded in London on May 28 1961 whose purpose is to hold governments accountable for their violations of the Universal Declaration of Human RIghts. Due to their purpose they have shown an interest in the issue of mitigating the impact of emerging technologies on Human Rights. They have conducted extremely analytical research reports on the impact of those technologies on Human Rights, which have been published on the internet, they have created multiple campaigns that aimed in advocating for the significance of Human Rights in the digital age, they have extensively cooperated with governments in order to aid them implement legislation that will protect the fundamental Human Rights, and have raised the awareness of the public about this significant modern world issue. Furthermore they have conducted substantial monitoring and reporting of Human Rights abuses which are traced back to emerging technologies and they are able to hold governments accountable regarding those violations. They have made significant efforts in order to preserve and protect the

[42] Congress.gov. "U.S. Constitution - First Amendment ." *Constitution.congress.gov*, Library of Congress, constitution.congress.gov/constitution/amendment-1/.

[43] Murray, Conor. "U.S. Data Privacy Protection Laws: A Comprehensive Guide." *Forbes*, 2023, www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/.

[44] The U.S. Export Control System and the Export Control Reform Act of 2018 (congress.gov)

fundamental human right of people despite the hardships due to us living in the age of technology.[45]

European Union

The European Union has also been a contributor in mitigating the negative impact of Emerging Technologies on Human Rights. First of all they have implemented a lot of regulations towards data privacy, the most significant one being the General Data Protection Regulation. It was implemented in May 2018 and aims to protect the private data of individuals. The GDPR aids individuals to have a better control of their data that can be distributed and it also requires companies to obtain consent clearly for the collection of data from consumers and it also holds companies accountable for the misuse of consumers' data. The GDPR will be further analysed in another section of the guide.[46] Furthermore the EU has created the European Digital Media Observatory, which is responsible for monitoring and tackling online misinformation. It began operating on 1 June 2020 and it is responsible for fact checking organisations, building a public portal for information, coordinating research activities, establishing frameworks that ensure secure access to platform data and supporting public authorities.[47] Additionally the European Union is an active participant in international discussions and negotiations that are being held globally in order to limit the violations of human rights in the digital age. It is a firm supporter of Human Rights and more specifically advocates for the protection of privacy in the digital world. Finally the EU provides generous funding towards projects that aim in eliminating the impact of Emerging Technologies on Human Rights.

World Economic Forum (WEF)

The World Economic Forum is a non-profitable organisation which was established in 1971. It has been highly involved in certain initiatives about the responsible usage of emerging technologies and the non violation of Human Rights in the process. Even though it does not have the ability to implement regulations, it plays a crucial role in raising awareness and creating international discussions regarding the impact of emerging technologies on human rights. It is able to advance partnerships among governments and bring them together in order for them to be able to tackle the issue collectively. It also has produced research reports that show the impact that those technologies hold in human rights which provide possible solutions in order to combat this complicated issue. Additionally it supports initiatives undertaken by governments which are able to provide feasible solutions for the

[45] "Digitally Divided: Technology, Inequality and Human Rights." *Amnesty International*, www.amnesty.org/en/documents/pol40/7108/2023/en/. Accessed 27 Oct. 2023.

[46] GDPR. "General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, Intersoft Consulting, 2018, gdpr-info.eu/.

[47] "European Digital Media Observatory (EDMO) | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, 20 Oct. 2023, digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory#:~:text=The%20European%20Digital%20Media%20Observatory%20%28EDMO%29%20is%20a. Accessed 27 Oct. 2023.

issue. The World Economic Forum serves as an awareness building but also as an aid in the very common intersection among Human Rights and emerging technologies. It has made a lot of significant efforts in order to aid nations tackle the issue but also to bring nations together to discuss and implement policies together. [48]

RELEVANT UN TREATIES CONVENTIONS AND RESOLUTIONS

New and Emerging Digital Technologies and Human Rights (A/HRC/RES/41/11)

This resolution was adopted by the United Nations Human Rights Council on 11 July 2019, and it is regarding emerging digital technologies and human rights. It highlights the importance of the new digital emerging technologies and how they promote Human Rights, but also recognises that there is a need for an open-minded approach towards the potential impacts, opportunities and challenges that have arised with the development of those technologies while encouraging the cooperation of government and other stakeholders in order for the collective tacklement of the issue. Furthermore it requests the Advisory Committee to compose a report based on that issue but also to discuss it in the 44th session of the panel but this time recognizing the additional issue that disabled people face due to their inaccessibility. It also emphasises that aid from member States and various organisations is of utmost importance in order to address this highly discussed issue in an appropriate manner. Finally it considers the Office of the High Commissioner responsible for the organisation of the panel and the participation of multiple stakeholders. [49]

The Right to Privacy in the Digital Age (A/RES/75/176)

This resolution was adopted by the United Nations General Assembly on 16 December 2020 and it is regarding the right to privacy in the digital age which is significantly violated by emerging technologies. It reaffirms the right to privacy exactly as it was established in the Universal Declaration of Human Rights, while recognising the importance to preserve the right to privacy in the real but also in the digital world. Furthermore it highly encourages member states to create a secure digital environment that respects human rights but also to review and improve their already existing legislations regarding digital privacy. It also supports the establishment of oversight mechanisms that ensure transparency in state surveillance and encourages businesses to have an open communication with customers regarding data collection but also processing. Additionally, it supports the implementation of various technologies that ensure the protection and encryption of data while also encouraging member states and other stakeholders to engage in peaceful discussions regarding the right to privacy. [50]

---

[48] Hickin, Ruth. "How Is Technology Affecting Our Human Rights?" *World Economic Forum*, 11 Dec. 2017, www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/.

[49] "ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/G19/218/53/PDF/G1921853.pdf?OpenElement.

[50] "ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement.

Universal Declaration of Human Rights

"The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights." It was established by the United Nations General Assembly on 10 December 1948 in Paris and it clearly presented, for the first time, the fundamental Human Rights of people of which they cannot be deprived of. The rights that this issue is referring to are the right to non-discrimination, the right to security, the right to privacy, the right to freedom of expression and the right to work. Namely articles of the Declaration 2,3,12, 19,23.[51]

Recommendation on the Impacts of Digital Technologies on Human Rights (CM/Rec(2022)13)

This recommendation was adopted by the Committee of Ministers on 6 April 2022 at the 1431st meeting of the Ministers' Deputies and it is regarding the impacts of digital technologies towards the right to freedom of expression. It was issued in order to provide guidance to member states regarding that crucial issue. Through its clauses it addresses the challenges that humanity is exposed to in the digital age that we live in, but also all the benefits that we can gain from it. But also it highlights the significance of promoting but also protecting the Human Right to Freedom of Expression in these circumstances. It is composed of detailed guidelines for member states to implement in order to safeguard this significant right while also addressing crucial issues such as inline censorship, hate speech but also the fine line among privacy and the right to freedom of expression. Finally it persuades member states to implement policies in order to create a healthy digital environment in which all opinions are respected and can be expressed democratically. [52]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

General Data Protection Regulation (GDPR)

The General Data Protection Regulation is a data protection and privacy regulation that was established on May 25 2018 by the European Union. It replaced the Data Protection Directive 95/46/EC and signified an important update in EU legislations regarding privacy. This regulation has been applied to all European Union member states and it only affects nations and organisations outside the EU only if they are associated with it in any way. It has expanded the definition of personal data by also including that personal data are information that can directly or indirectly impact an individual while also requiring organisations to obtain clear consent from users before collecting and processing their personal data while also informing individuals about how their data is going to be utilised. It

[51] ---. "Universal Declaration of Human Rights." *United Nations*, 10 Dec. 1948, www.un.org/en/about-us/universal-declaration-of-human-rights.

[52] *Coe.int*, 2023, search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680a61729. Accessed 27 Oct. 2023.

also gives individuals the ability to erase their data at any given time as well as the ability to object to the usage of their data. It furtherly requires certain organisations to appoint a Data Protection Officer which will be responsible for ensuring the compliance of GDPR and for organisations to inform authorities about data breaches within 72 hours of being aware of them if it is possible that the breach can deprive individuals of their right to privacy. It also asks companies to have records of their data exploitations and encourages them to add data protection to their products and not just include it after. Finally the GDPR has established fines for organisations who do not follow the regulations, which go up to 4 percent of their revenue or even 20 million euros.[53]

The Paris Call for Trust and Security in Cyberspace

The Paris call for Trust and Security in Cyberspace was established by French Authorities in November 2018 and is a non binding agreement which calls for states, civil society organisations and the private sector to collaborate in order to shape a secure cyberspace, address the misinformation of citizens but also the new cyber threats that endanger individuals. Since it recognises that cyber security is an issue that needs to be tackled collectively it encourages nationals and interns stakeholders to collaborate peacefully in order to resolve the issue while also requiring their commitment to principles which are based on international law in order to ameliorate the current situation with cyber security and safety. Furthermore it aspires to prevent cyber attacks and cybercrimes while also protecting the safety of civilians. It also aims in protecting the intellectual property rights in cyberspace which are vital for economic development and innovation while highlighting the importance of the protection of digital supply chains. Generally this agreement promotes the respect of Human Rights in cyberspace and emphasises the importance of their breaches. Numerous organisations, nations and corporations have signed it, this marking their commitment to address the problems of cybersecurity in a collaborative manner.[54]

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was adp[retd by the council of Europe on November 23, 2001 and is an international treaty which aims in tackling and dressing the issue of cybercrime. It has been signed by many nations world wide, including the European Union member states but also non member of the European Union due to its global significance. It investigates a wide range of cybercrimes that include the intrusions of computer systems, data and content and also requires member states to hold criminally accountable people and organisations who conduct various cybercrimes. It also enables member states to exercise jurisdiction over cyber crimes that affect their national security or

[53] ---. "General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, Intersoft Consulting, 2018, gdpr-info.eu/.

[54] "Paris Call for Trust and Security in Cyberspace Working Group 5 Building a Cyberstability Index Final Report." *CyberPeace Institute*, 9 Nov. 2021, cyberpeaceinstitute.org/publications/paris-working-group-report/. Accessed 27 Oct. 2023.

are able to negatively impact international security. It also includes procedural manners regarding the preservation of data. It requires member states to collaborate with each other by the provision of mutual legal assistance but also encourages cooperation in the private sector, so among privately owned corporations. It highlights the importance of the protection of sensitive data and private information and also the need for capacity building in order to combat the issue. Even though it offers a plausible legal framework in order to tackle the issue, it has raised concerts and faced criticism due to its provisions on data retention and surveillance. [55]

United Nations Guiding Principles on Artificial Intelligence (AI)

The United Nations Guiding Principles on Artificial Intelligence (AI) was established in the second regular session of 2022 and more specifically on October 27-28 of 2022 by the chief executives board for Coordination. It acknowledges everything that Artificial Intelligence can offer to humanity and all of its benefits but also mentions the huge impact that it can have on human rights. Then it offers certain principles regarding the ethical usage of Artificial Intelligence in various aspects. It mentions security and safety and how such threats must be identified early on and then tackled through robust and strong legal frameworks. Furthermore it urges stakeholders to always ensure the fair and equal distribution of all the benefits but also all the downsides of Artificial Intelligence, thus ensuring the fundamental human right to non discrimination in compliance with international law. It also establishes ethical guidelines regarding data protection and privacy through the usage of Artificial Intelligence which successfully addresses the right to privacy of individuals.[56]

POSSIBLE SOLUTIONS

Harmonisation of GDPR Provisions Across the Globe

Even though the General Data Protection Regulation is an extremely successful policy and has been applied eminently in the European Union, it only aims in protecting and regulating the data collection and distribution of European citizens. So GDPR being the strictest and one of the most respectful regulations towards the consumer it would be adequate for nations that are outside the European Union to utilise all the European Provisions stated in the GDPR regulations and create their own frameworks and policies in which they will be implementing those provisions. The European Provisions have offered safety and security towards the citizens regarding their personal data and have made them feel in control of their distribution and processing while also holding companies accountable for the misuse of such data. It would be extremely beneficial for nations that do not belong in the European

[55] CCG NLU Delhi. "Budapest Convention on Cybercrime – an Overview." *Legallyindia.com*, 3 Mar. 2016, www.legallyindia.com/views/entry/budapest-convention-on-cybercrime-an-overview.

[56] Chief Executives Board for Coordination Summary of Deliberations Addendum Principles for the Ethical Use of Artificial Intelligence in the United Nations System. 2022.

Union to apply such provision in order to protect the fundamental human rights of their citizens.

Establishing a Global Framework for the Ethical Use of Emerging Technologies

At this point the negative impact of emerging technologies and the violations towards fundamental human rights have been recognised worldwide. So a solution that could address the issue at hand, in a figurative and balanced manner is the creation of a framework that includes policies and regulations regarding the protection of Human Rights in the digital world. This framework could be under the aegis of the United Nations, but composed by member states in a General Assembly session. It is crucial to have a sich framework since it standardises ethical guidelines regarding the usage of emerging technologies and ensures the consistency among the regulations that all organisations follow. It also offers a multistakeholder approach towards the issue, which ensures the collective combat of the issue but also offers different perspectives which could be considered more inclusive. Finally, such frameworks always promote and encourage friendly cooperation among nations which is of utmost importance in order to tackle such significant issues.

Monitoring and Reporting on the Artificial Intelligence Augmented Workforces

In the digital age that we live in, the existence of AI Augmented Workforces has risen significantly. Those workforces include both humans and AI which work together, while tasks that used to be conducted by humans are now replaced by AI and are being carried out in an automated manner. So in order to preserve the fundamental human right to work and to take action when the job replacements in the AI Augmented workforce get out of control, monitoring and reporting would be adequate solutions in order to refrain from complete automation. Through the establishment of a monitoring mechanism which will collect data on the job replacements that occur in the such workforces, and report it to organisations such as Amnesty International of the World Economic Forum governments would have a fuller image and would then be enabled to take appropriate actions in order to combat the issue. Finally if those reports are accessible to the general public under the aegis of such organisations public awareness would be raised and transparency among companies and the public would be ensured.

Promoting Digital Literacy in All Parts of the Globe

Due to the rapid advancements of technology in the past years it has been extremely hard for people, especially in Less Economically Developed Countries, to keep up with all the technologies that have emerged and how they can deprive them of their fundamental human rights. So it would be a suitable idea to encourage digital literacy through all parts of the globe in order for people to be informed about how technology can violate their rights and how, by using it responsibly, can they avoid the negative impacts of technology. This

information could be distributed through educational videos created by organisations, online talks of experts that could be observed by everyone, and social media posts of prestigious establishments. The knowledge that people will gain from such information distribution can help them shield themselves and be aware of how to use technology in a responsible manner while also empowering them to advocate for their digital safety and to peacefully express their opinions.

BIBLIOGRAPHY

"Robots to Replace 50% of Work Tasks by 2025: WEF." *Best Practice*, 22 Oct. 2020, bestpractice.biz/robots-to-replace-50-of-work-tasks-by-2025-wef/#:~:text=The%20WEF%20expects%20that%2085%20million%20labour-intensive%20jobs.

"36 Billion Data Records Exposed (so Far) in 2020: Risk Based Security." *Spiceworks*, www.spiceworks.com/it-security/data-security/news/36-billion-data-records-exposed-so-far-in-2020-risk-based-security/.

Artificial Intelligence Definition and Meaning | Dictionary.com." *Dictionary.com*, 11 Feb. 2021, www.dictionary.com/browse/artificial-intelligence.

"Human Rights Definition and Meaning | Dictionary.com." *Dictionary.com*, 5 Feb. 2021, www.dictionary.com/browse/human-rights.

"What Is Biometric Technology." *BiometricCentral.com*, 2 Aug. 2020, www.biometriccentral.com/what-is-biometric-technology.

What Is the Internet of Things? | IBM. www.ibm.com/topics/internet-of-things.

"Augmented Reality Definition and Meaning | Dictionary.com." *Dictionary.com*, 22 Jan. 2021, www.dictionary.com/browse/augmented-reality.

"Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/en-us/insights/decoder/s/surveillance-technology#:~:text=The%20term%20%E2%80%98surveillance%20technology%E2%80%99%20encompasses%2

"Biotechnology Definition and Meaning | Dictionary.com." *Dictionary.com*, 20 Jan. 2021, www.dictionary.com/browse/biotechnology.

"How Has AI Developed Over the Years and What's Next?" *World Economic Forum*, 6 Oct. 2023, www.weforum.org/agenda/2022/12/how-ai-developed-whats-next-digital-transformation.

Is Artificial Intelligence Really Replacing Jobs? Here's the Truth." *World Economic Forum*, 28 June 2021, www.weforum.org/agenda/2018/09/is-artificial-intelligence-replacing-jobs-truth.

Watson, Stephanie. "How Fingerprinting Works." *HowStuffWorks*, 24 Mar. 2008, science.howstuffworks.com/fingerprinting3.htm .

Yu, Yirong, et al. *A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications*. Vol. 14, no. 6, 14 June 2023, pp. 1253–1253, https://doi.org/10.3390/mi14061253. Accessed 10 July 2023.

"What Is Biometric Technology." *BiometricCentral.com*, www.biometriccentral.com/what-is-biometric-technology/#:~:text=Biometric%20technology%20is%20defined%20as%20the%20measurement%20and.

IBM. "IBM - United States." *Www.ibm.com*, 1 Oct. 2015, www.ibm.com/topics/internet-of-things.

"Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/insights/decoder/s/surveillance-technology.

United Nations. "Universal Declaration of Human Rights." *United Nations*, 10 Dec. 1948, www.un.org/en/about-us/universal-declaration-of-human-rights.

---. *Universal Declaration of Human Rights*. 10 Dec. 1948.

Weihrauch, Alexander. "The Principle of Non-Discrimination." *Humanium*, 2 Mar. 2021, www.humanium.org/en/the-principle-of-non-discrimination/.

"Decoder: Surveillance Technology." *Thoughtworks*, www.thoughtworks.com/insights/decoder/s/surveillance-technology.

"Freedom of Expression: A Fundamental Human Right Underpinning All Civil Liberties." *UNESCO*, 14 Apr. 2015, webarchive.unesco.org/web/20170204064206/en.unesco.org/70years/freedom_of_expression.

Soken-Huberty, Emmaline. "10 Reasons Why Privacy Rights Are Important." *Human Rights Careers*, 2 May 2020, www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/.

"The Right to Work and Workers' Rights." *ESCR-Net*, www.escr-net.org/rights/work#:~:text=The%20right%20to%20work%20is%20a%20foundation%20for. Accessed 13 Oct. 2023.

Ross, Ron. "Why Security and Privacy Matter in a Digital World." *NIST*, 28 Sept. 2017, www.nist.gov/blogs/taking-measure/why-security-and-privacy-matter-digital-world#:~:text=Given%20this%20backdrop%2C%20it%20is%20often%20easy%20to. Accessed 26 Oct. 2023.

etal. "Check Point Research: Third Quarter of 2022 Reveals Increase in Cyberattacks and Unexpected Developments in Global Trends." *Check Point Software*, 26 Oct. 2022, blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

"The 7 Biggest Government Cyberattacks since 2011 | Swivel Secure." *Swivel*, 2011, swivelsecure.com/solutions/government/top-cyber-attacks/.

II, Clint Crigger. "Impact of Cyber Attacks on Organizations." *ILLÜM ADVISORS*, 25 Oct. 2021, www.illumadvisors.com/insights/cybersecurity-insights/this-blog-will-highlight-some-of-the-ways-cyber-attacks-affect-organizations-and-how-we-can-help/.

Swivelsecure. "9 Reasons Healthcare Is the Biggest Target for Cyberattacks." *Swivel*, 2018, swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

Duguin, Stephane. "If Healthcare Doesn't Strengthen Its Cybersecurity, It Could Soon Be in Critical Condition." *World Economic Forum*, 8 Nov. 2021, www.weforum.org/agenda/2021/11/healthcare-cybersecurity/.

Wolf, Arctic. "Biggest Healthcare Industry Cyberattacks." *Arctic Wolf*, 16 June 2021, arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/.

"Why Is the Finance Sector a Target for Cyber Attacks? | UpGuard." *Www.upguard.com*, www.upguard.com/blog/finance-sector-cyber-attacks#:~:text=Why%20Do%20Cybercriminals%20Target%20the%20Financial%20Sector%3F%201. Accessed 26 Oct. 2023.

Kost, Edward. "The 8 Biggest Data Breaches in Financial Services (2021 Edition) | UpGuard." *Www.upguard.com*, 1 Dec. 2022, www.upguard.com/blog/biggest-data-breaches-financial-services.

"Does Technology Increase the Problem of Racism and Discrimination?" *SearchEnterpriseAI*, www.techtarget.com/searchenterpriseai/opinion/Does-technology-increase-the-problem-of-racism-and-discrimination.

Griffith, Melissa K. "Cyber Security and Emerging Technologies." *Survival*, vol. 64, no. 5, 3 Sept. 2022, pp. 174–180, https://doi.org/10.1080/00396338.2022.2126189.

"To Protect Privacy in the Digital Age, World Governments Can and Must Do More | Association for Progressive Communications." *Www.apc.org*, www.apc.org/en/pubs/protect-privacy-digital-age-world-governments-can-and-must

-do-more#:~:text=The%20resolution%20correctly%20notes%20that%20new%20technologies%20process. Accessed 27 Oct. 2023.

Silva, Alberto Cerda. "Protecting Free Speech in the Digital Age: Q&a with UN Special Rapporteur for Freedom of Expression." *Ford Foundation*, 11 Oct. 2016, www.fordfoundation.org/news-and-stories/stories/protecting-free-speech-in-the-digital-age-qa-with-un-special-rapporteur-for-freedom-of-expression/.

Burgess, John, and Julia Connell. "New Technology and Work: Exploring the Challenges." *The Economic and Labour Relations Review*, vol. 31, no. 3, 8 Aug. 2020, pp. 310–323, journals.sagepub.com/doi/10.1177/1035304620944296, https://doi.org/10.1177/1035304620944296.

Congress.gov. "U.S. Constitution - First Amendment ." *Constitution.congress.gov*, Library of Congress, constitution.congress.gov/constitution/amendment-1/..

Murray, Conor. "U.S. Data Privacy Protection Laws: A Comprehensive Guide." *Forbes*, 2023, www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/.

GDPR. "General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, Intersoft Consulting, 2018, gdpr-info.eu/.

"European Digital Media Observatory (EDMO) | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, 20 Oct. 2023, digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory#:~:text=The%20European%20Digital%20Media%20Observatory%20%28EDMO%29%20is%20a. Accessed 27 Oct. 2023.

Gisonna, Nicholas. "Great Firewall". Encyclopedia Britannica, 21 Sep. 2023, https://www.britannica.com/topic/Great-Firewall. Accessed 27 October 2023.

Creemers, Rogier, et al. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *DigiChina*, 29 June 2018, digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

Hickin, Ruth. "How Is Technology Affecting Our Human Rights?" *World Economic Forum*, 11 Dec. 2017, www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/.

Hickin, Ruth. "How Is Technology Affecting Our Human Rights?" *World Economic Forum*, 11 Dec. 2017,

www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/.

"Digital Personal Data Protection Bill 2023 Passed in Rajya Sabha: Key Points." *The Times of India*, 11 Aug. 2023, timesofindia.indiatimes.com/gadgets-news/digital-personal-data-protection-bill-2023-passed-in-rajya-sabha-key-points/articleshow/102579315.cms.

"National Cyber Security Policy- Objectives, Features." *Testbook*, testbook.com/ias-preparation/national-cyber-security-policy. Accessed 27 Oct. 2023.

"ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/G19/218/53/PDF/G1921853.pdf?OpenElement.

"ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement.

Coe.int, 2023, search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680a61729. Accessed 27 Oct. 2023.

"Paris Call for Trust and Security in Cyberspace Working Group 5 Building a Cyberstability Index Final Report." *CyberPeace Institute*, 9 Nov. 2021, cyberpeaceinstitute.org/publications/paris-working-group-report/. Accessed 27 Oct. 2023.

CCG NLU Delhi. "Budapest Convention on Cybercrime – an Overview." *Legallyindia.com*, 3 Mar. 2016, www.legallyindia.com/views/entry/budapest-convention-on-cybercrime-an-overview.

Chief Executives Board for Coordination Summary of Deliberations Addendum Principles for the Ethical Use of Artificial Intelligence in the United Nations System. 2022.