TABLE OF CONTENTS

1. Welcome Letters

To those who dare to imagine and build the future,

ULTEK has long been the destination of choice for participants who are passionate about technology, eager to develop their skills, and ready to share their innovative ideas. After a five-year hiatus, we return stronger and more comprehensive than ever before — and it is my honor to welcome you to ULTEK, the 4th International Congress on Technology and Society. Over three days, you will engage with distinguished scholars, share forward-thinking ideas, and contribute to knowledge that bridges technology and society. ULTEK provides not just a platform for sharing, but a space for action — where ideas become solutions and collaborations create lasting impact. Welcome to ULTEK'25 — where the future begins.

Nilgün Nihal Çalık,
Chairperson of the Board

Dear Congresspeople,

It is a great honor to respectfully welcome each and every one of you to the committee of Digital Realities, in which we will be discussing the technical and ethical concerns around the world about evolving technologies in people's lives.

In the modern world, technology plays a significant role in molding the future. Therefore, in order to comprehend, learn, and advance the topic, we wanted to go into further detail about this important aspect in the Digital Realities Committee. Our goal is to explore the various ways in which technology impacts society, businesses, and individuals. By discussing these implications, we hope to gain a deeper understanding of how we can harness technology for positive change and progress.

I encourage everyone to actively participate in the discussions and share their insights and experiences related to technology. Your active participation will not only enrich our understanding but also contribute to the collective knowledge of the committee. I hope that our discussions will inspire innovative solutions and collaborations that will shape a brighter future for all.

I wish you all a pleasant and memorable conference.

Under Secretary General
Zeynep KAYMAZ

2. Terminology

2.1. Digital ecosystem

Digital ecosystem is a complex network of interconnected organizations, individuals, and technologies that interact and create value. It includes platforms, data, processes, and applications that enable seamless collaboration and innovation. In a digital ecosystem, each component plays a crucial role in driving growth and efficiency. By leveraging these interconnected resources, businesses can adapt to changing market demands and stay competitive in the digital age. Ultimately, a well-functioning digital ecosystem can lead to increased customer satisfaction. This interconnected network allows for rapid development and deployment of new products and services, giving businesses a competitive edge in the ever-evolving market landscape.

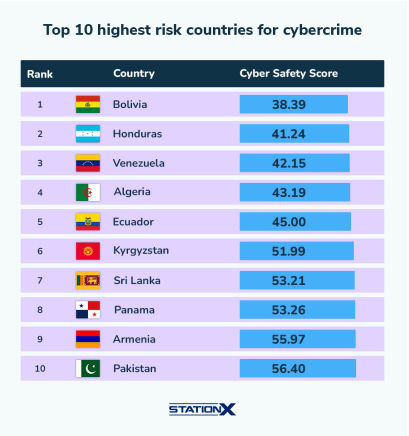
2.2. Digital Footprint

A digital footprint is the unique trail of data that a person or business creates while using the internet. Such as browsing history, social media activity, online purchases, and interactions with digital devices. Nearly every online activity leaves a trace. Some traces are obvious, like a public social media post. Others are subtler, like the cookies that websites use to track visitors. Every trace a person or company leaves behind, taken together, forms their digital footprint.

While internet users and organizations both have digital footprints, they differ in meaningful ways. A person's footprint consists of the personal data they directly and indirectly share. It includes online account activity, browsing history, and the details that data brokers collect in the background. An organization's footprint is more complex. It consists of the company's entire online presence, including all its public and private internet-facing assets, content, and activity. Official websites, internet-connected devices, and confidential databases are all part of a company's footprint.

2.3. Digital law

Digital law refers to the legal rights and restrictions that govern the use of technology and digital environments. It includes laws related to internet use, data privacy, cybersecurity, intellectual property, online behavior, and digital communication. Digital law protects users and organizations from cybercrimes like hacking, identity theft, and illegal file sharing. It also ensures ethical behavior in digital spaces and holds individuals accountable for their actions online.



These laws are often created, regulated, and enforced by the governments and international organizations. Despite the existence of various universal regulations, national laws pertaining to digital technology often vary. There are several consequences from this situation; some nations have strict laws, while others have relaxed laws and increased internet freedom. When all of these components are combined, they form the cyber threat of the world.

2.3.1. Cybercrime

Cybercrime encompasses a wide number of acts, crimes or illicit conduct perpetrated by both individuals or groups against computers, computer-related devices, or information technology networks, as well as traditional crimes that are facilitated or maintained by the use of the internet or information technology.

These activities include phishing, cyberstalking, online harassment, cyberbullying, identity theft, non-consensual image sharing, online scams, hacking, ransomware attacks, Distributed Denial-of-Service (DDoS), malware injection, data breaches, online piracy, cyberterrorism, espionage, hacking government databases, defacing official websites, political misinformation or manipulation, credit card fraud, banking malware, cryptocurrency fraud,

online money laundering, investment fraud, spreading child exploitation materials, hosting or spreading hate speech or extremist content, and selling illegal goods or services online. Each crime listed is another critical problem to be addressed and solved.

Understanding the factors that contribute to varying cybercrime rates can help inform the development and enforcement of digital laws to combat these threats effectively. Cybercrime is promoted by several key factors. The widespread availability of technology makes it easier for criminals to find and exploit targets. Weak cybersecurity, such as poor passwords or outdated software, creates vulnerabilities that are easy to attack. Online anonymity allows criminals to hide their identities and operate without being easily traced. In some countries, the lack of strong cyber laws or enforcement makes it difficult to catch and punish offenders. Financial gain is a major motivation, as hackers can steal money, data, or sell information illegally. The low risk of being caught further encourages cybercriminals to continue their activities.

Cybercriminals often use phishing emails or malware to gain access to sensitive information, making it crucial for individuals and organizations to stay vigilant and regularly update their security measures. Additionally, the rise of cryptocurrencies has provided a new way for criminals to launder money and avoid detection by law enforcement agencies.

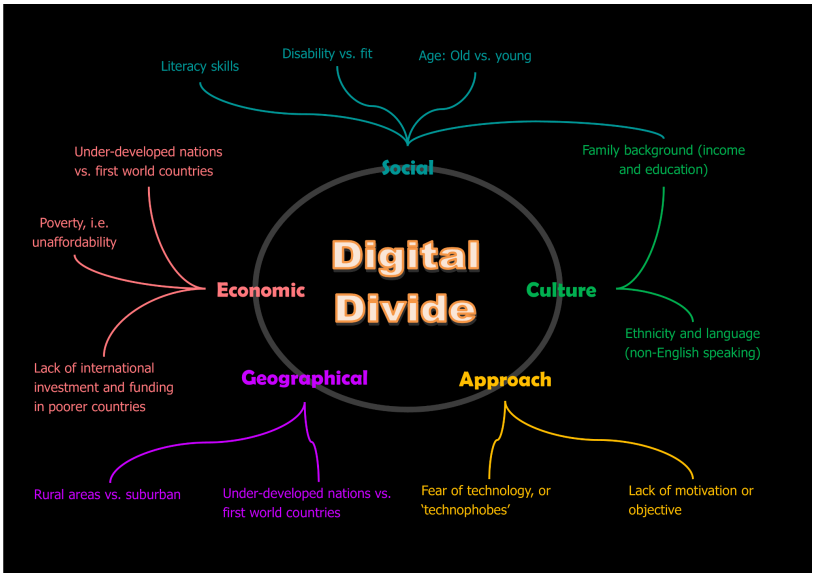
2.3.2. GDPR (General Data Protection Regulation)

The GDPR (General Data Protection Regulation) is a law adopted in 2016 in the European Union that protects people's personal data and privacy. The GDPR is considered to be the toughest privacy and security law in the world. Although it was drafted and passed by the European Union (EU), it places responsibilities on organizations everywhere.

GDPR protects people’s data by requiring companies to ask for clear consent before collecting personal data, permit users to view, edit, or remove it, inform people if their data has been compromised or disclosed, only gather what is required, and only use information for those goals. The GDPR holds businesses legally responsible and grants individuals rights over their data.

2.4. Digital Divide

The digital divide refers to the disparity between individuals, communities, or countries in terms of access to, use of, or knowledge about information and communication technologies. This gap often results from differences in socioeconomic status, geographic location, education, and infrastructure availability. The digital divide affects opportunities for education, employment, social participation, and access to information, creating inequalities in the digital age.



2.5. Extended Reality

Extended Reality (XR) is a broad term used to describe technologies that merge the physical and digital worlds, including Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR). These technologies create immersive experiences that either replace the real world with simulated environments, enhance it with digital elements, or blend both in real time. XR relies on devices such as VR headsets, AR glasses, and advanced sensors to provide interactive and engaging environments for users. By offering a spectrum of immersion, XR opens new ways for people to experience information, entertainment, and communication.

The applications of XR span across multiple sectors, making it a versatile tool in both professional and personal contexts. In education, it enables interactive learning by allowing students to explore complex concepts in simulated environments. In healthcare, it supports training for medical professionals and assists in patient rehabilitation. In business and industry, XR can be used for virtual meetings, design visualization, and product development.

Despite its promise, XR also presents challenges that must be addressed for its wider adoption. High equipment costs, limited accessibility, and the need for strong digital infrastructure are some of the barriers to benefit fully from these technologies. Additionally,

issues related to privacy, data security, and user well-being must be considered when developing and using XR systems.

2.6. Metaverse

The metaverse is a persistent and immersive virtual world where users can communicate, collaborate, and socialize in real time while being represented by digital avatars. With the help of technologies like virtual reality, augmented reality, and blockchain, it combines the real and virtual worlds for a range of uses in entertainment, education, and business.

Similar to other technologies, Metaverse has both positive and negative aspects. Metaverse offers its users an advanced technology, while providing opportunities to explore diverse virtual environments and engage in a wide range of interactive activities. It enables social interaction, education, entertainment, and commerce to take place in digitally simulated spaces. Additionally, the Metaverse establishes an unrestricted and neutral environment where users can have avatars that look like anyone, be anywhere, and be with anyone they choose.

Although extended reality and Metaverse provide various advantages, there are several threads they contain. As online games are already known to be addictive, the growing popularity of the metaverse is likely to further increase the prevalence of digital addiction, potentially intensifying its psychological and social impacts on users. Furthermore, Metaverse requires excessive personal data compared to other technologies. Consequently, some users may have concerns about privacy and security when using Metaverse platforms. It is important for companies to prioritize protecting user data and ensuring transparency in how it is collected and used.

Notably, the metaverse involves significant costs, making it a high-priced technology that may limit accessibility for many users. These financial barriers could hinder widespread adoption and contribute to the digital divide.

2.7. Cryptocurrency

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When transferring cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

2.8. Digital Literacy

The ability to access, assess, produce, and share information using digital technology in an efficient and responsible manner is known as digital literacy. It requires a variety of abilities, such as the ability to utilize gadgets, software, and online platforms with competence and the ability to use critical thinking to evaluate the reliability and applicability of digital content. Understanding online safety, privacy, and ethical issues when participating in digital environments is another aspect of digital literacy. It is a necessary skill for civic engagement, work, and education in the modern world since it helps people to adjust to new technological developments and traverse a society that is becoming progressively digital.

3. Technical Challenges of Digitalisation

Technology is a significant development that continues to shape and enhance modern life. However, its full integration remains limited by ongoing technical challenges, requiring continuous development and adaptation to ensure its effective and sustainable integration into the diverse activities and structures of contemporary society.

3.1. Accessibility

Most of the time technology is not equally accessible for everyone. Individuals from marginalized communities, such as low-income households, people with disabilities, and rural populations, often face barriers to accessing technology due to factors such as cost, lack of infrastructure, and digital literacy. Additionally, some nations struggle with a lack of technology, while others have developed resources, infrastructure, and system integration.

This digital divide can further exacerbate existing inequalities and limit opportunities for those who are already disadvantaged.

Numerous issues arise due to varying degrees of accessibility. Without access to technology, individuals may struggle to find employment, access educational resources, or participate in important communication channels. In other words, digital accessibility has an impact on many aspects of human life.

3.2. Disparities Between Nations

Technology is developing day by day, but this development does not always have the same speed everywhere. While some countries are developing technologies and devices rapidly, some countries are dealing with various technical and social challenges. As it was stated before, this situation causes some people to have less access to technology than others.

In underdeveloped countries, access to technology is limited due to factors such as lack of infrastructure, resources, and education. This digital divide further widens the gap between developed and underdeveloped nations, hindering progress and opportunities for those who are already marginalized.

Besides the lack of accessibility to technology, there are other disparities between nations. Such as, educational and digital literacy gap, economic gap, language and culture barriers, regulatory issues. These issues collectively widen the gap between individuals and businesses from different countries. Economic gaps widen the digital literacy gap, which in turn exacerbates regulatory issues and regulatory issues impede accessibility.

3.3. Technical Challenges of Cryptocurrency

Though cryptocurrency offers a range of benefits, it brings along a set of adversities and complexities which can't be ignored. Unofficial fiat currency does not have government support or a bullion backing, in contrast to official fiat currency. Even while cryptocurrencies have certain unique features or

material advantages that they advertise, their market potential is dependent on a number of interrelated elements. Among these are developments in technology, behavioral economics, and the size of financial investments. The volatility and extreme shocks make cryptocurrency's inherent worth insignificant. These private digital currencies lack intrinsic value due to their lack of legal tender status, aside from the utility that their underlying technology provides.

Every system has a set of inherent vulnerabilities. The exploitation of these vulnerabilities can enable the hackers to generate enormous amounts of virtual currency, leading to further macroeconomic consequences. Once compromised, these malicious users can create fake virtual currency by a small weak of wallet addresses. This can not only damage the reputation of the affected organization but also result in financial losses for investors and customers.

Furthermore, cryptocurrencies have opened further avenues of money laundering and other illicit activities. Owing to their inherently decentralized nature, authorities struggle a lot to adjudicate. Compromised personal accessories of the participants due to penetration of malware facilitate offenders exploiting the vulnerabilities of a consumer not so technologically savvy. Hence, these crypto transactions can be misused by criminal organizations for their illegal purposes, harmful to any nation.

Inadequate literacy about the risks associated with cryptocurrency transactions also contributes to the challenges faced by authorities in regulating these activities. Limited awareness related to cryptocurrencies and blockchain technology plays a key role in imposing resignation on cryptocurrency settlement. Researchers have time and again observed that digital assets, especially crypto and bitcoin, are vulnerable to various exploitations. This is a major impact on the limited success and thriving nature of start-ups and fintech organizations emerging in this domain.

4. Ethical Challenges of Digitalisation

A large portion of the many issues that still confront technology are ethical challenges. These challenges include concerns about data privacy, online security, misinformation, misrepresentation, artificial intelligence ethics, and the impact of technology on society.

4.1. Safety, Security, and Privacy

The digital communication revolution has established itself as a cornerstone of personal sovereignty. As the collecting and storage of personal and sensitive information expands, consumers' ability to regulate how their data is used online becomes increasingly important. Furthermore, data protection is an essentially complicated and diverse issue that affects a wide range of sectors and necessitates insights from different fields. It concerns healthcare, employment, marketing, trading and more.

The healthcare sector is one of the most significant collectors of personal data from clients. Data security in healthcare involves the collection and storage of patient information to protect the confidentiality of sensitive data, which can include medical histories, diagnostic information, and treatment plans. As healthcare organizations increasingly use digital technologies, the number of data breaches in the sector is rising.

In the business landscape, collecting and processing employee data is essential to a company’s operations. Employee personal data primarily consists of personally identifiable information, which includes financial records, medical history, criminal background, and demographic data. This information is crucial for managing payroll, benefits, human resources, and complying with employment laws. Under the GDPR, companies are allowed to process such data only if they have a lawful basis and comply with strict data protection principles, ensuring privacy and upholding high standards.

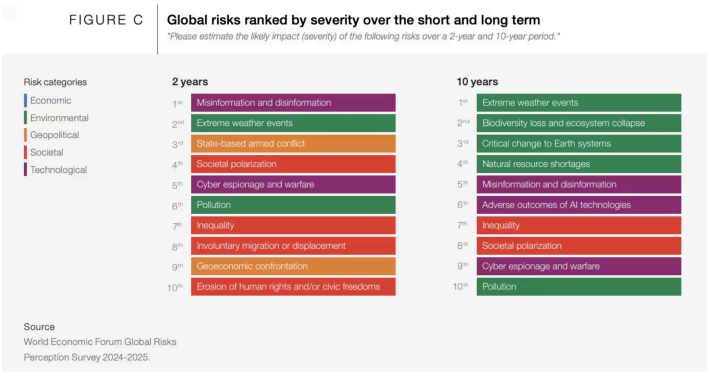
Ensuring data protection is inseparable from the broader concepts of security and safety. Security refers to the technical and organizational measures that prevent unauthorized access, data breaches, and cyberattacks, while safety emphasizes the protection of individuals from potential harm that may arise from the misuse of their personal information. A breach of medical records can endanger patient safety by leading to identity theft, discrimination, or even incorrect treatment. Likewise, compromising employee data can threaten not only financial security but also personal well-being, potentially resulting in harassment or reputational damage. Examples can be varied.

4.2. Misinformation and Disinformation

In an era of rapidly evolving digital technologies, information integrity has become a growing concern. Current threats include misinformation, defined as inaccurate information shared

without the intent to cause harm, and disinformation, inaccurate information deliberately disseminated with the purpose of deceiving audiences and doing harm

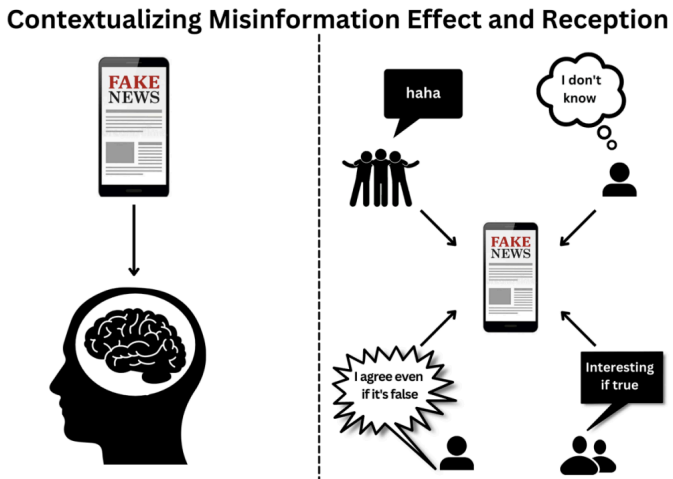
According to the World Economic Forum's Global Risks Report 2025, survey respondents identified misinformation and disinformation as leading global risks. Moreover, misinformation and disinformation can interact with and be exacerbated by other technological and societal factors, such as the rise of AI-generated content.



Global risks ranked by severity over the short and long term. Image: World Economic Forum

Generative AI is revolutionizing content creation, offering new opportunities for creativity and innovation. However, its misuse has rapidly escalated the creation and spread of harmful content. The rise of deepfakes, manipulated media and explicit synthetic content is blurring the lines of reality, amplifying disinformation and undermining trust in online ecosystems.

Furthermore, one of the most common explanations of the causes of misinformation in its various forms relates to the advances in technologies that produce and distribute information. The information ecosystem is assumed to be driving the problem of misinformation, because it is the critical means by which people now all source information, and it has itself been contaminated by misinformation. There is nothing like the digital landscape for quick and wide dissemination of misinformation, and it is considered to have transformed consumers into producers of information, and misinformation. It is important to emphasize that the sheer volume of information that is now available encourages sharing behavior through online networks and leads to biased information-selection processes with potentially adverse consequences.



Also seen as facilitating the proliferation of misinformation are technological tools such as recommender systems, web platforms, and social media. Also, social media

environments allow swarms of bots to disseminate or obscure information. The manipulation of these tools and platforms can have far-reaching effects on society.

The digitization of media also enables producers of misinformation to access sophisticated and extremely convincing tools of digital forgery, such as deepfakes, the digital alteration of an image or video that convincingly replaces the voice, the face, and the body of one individual for another. Even accurate news of actual events can be distorted as successive users are adding their own contexts and interpretations. Opaque algorithmic curation that takes humans out of the loop aims to maximize consumption and interactions, causing viral appeal to take precedence over truthfulness. However, technology also offers ways to tackle misinformation. The comments on social media are as effective as algorithms in correcting misperceptions, as well as contributing to the development of tools to track misinformation.

4.3. Ethical Concerns About Artificial Intelligence (AI)

Artificial Intelligence (AI) is reshaping the world in profound ways; some of its impacts are certainly beneficial, but widespread and lasting harms can result from the technology as well. As AI becomes integrated into various aspects of human life, the complex ethical concerns that arise from the design, deployment, and use of the technology serve as a reminder.

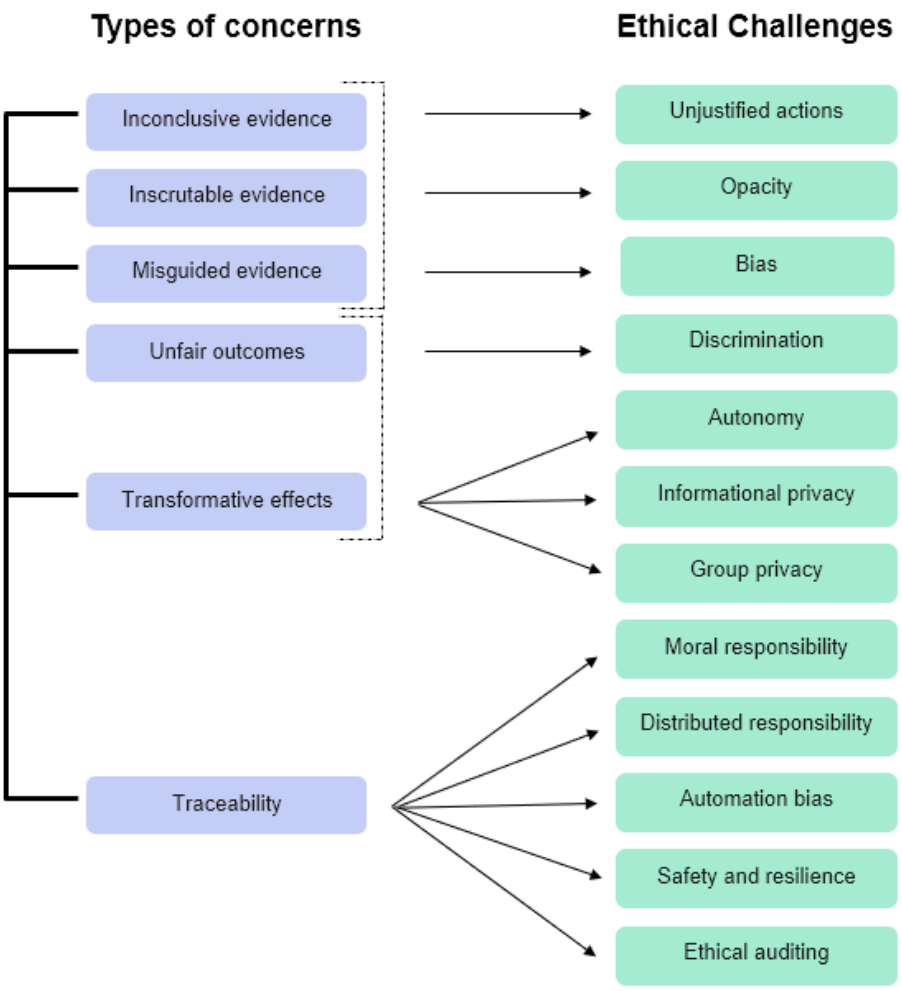
AI systems often require access to large amounts of data, including sensitive personal information. The ethical challenge lies in collecting, using, and protecting this data to prevent privacy violations. The potential for abuse and exploitation of personal data is the primary issue with artificial intelligence and its data access. This brings up issues with discrimination, surveillance, and the degradation of people's right to privacy. People's willingness to share personal information and their level of trust in AI systems are directly impacted by data security.

Due to their difficulty in being comprehended or interpreted, many AI algorithms are frequently referred to as "black boxes." For users to trust AI and for AI to be used ethically, openness and accountability in decision-making are essential. But this transparency is often lacking in the development and implementation of AI systems, leading to concerns about bias and unfair treatment. As AI continues to advance, it is crucial for regulations and ethical guidelines to be put in place to ensure the protection of individuals' privacy and rights.

Another pressing ethical concern is the impact of AI on employment and economic stability. As automation and intelligent systems replace human labor in sectors such as manufacturing, transportation, healthcare, and customer service, the displacement of workers poses significant social and economic challenges. While AI can increase efficiency and reduce costs, it also risks widening income inequality and exacerbating social divides if strategies for workforce reskilling and job transition are not implemented. This raises an important ethical responsibility for governments, corporations, and policymakers to ensure that technological progress does not come at the expense of human well-being and societal cohesion.

In addition to economic disruption, the rapid integration of AI into decision-making processes raises serious concerns about accountability and responsibility. When an AI system makes an error such as a misdiagnosis in healthcare, an unfair rejection in job recruitment, or an accident involving an autonomous vehicle, it is often unclear who should be held responsible: the developer, the organization deploying the system, or the algorithm itself. This ambiguity creates a gap in legal and ethical frameworks, making it difficult to ensure justice for those harmed by AI-driven decisions.

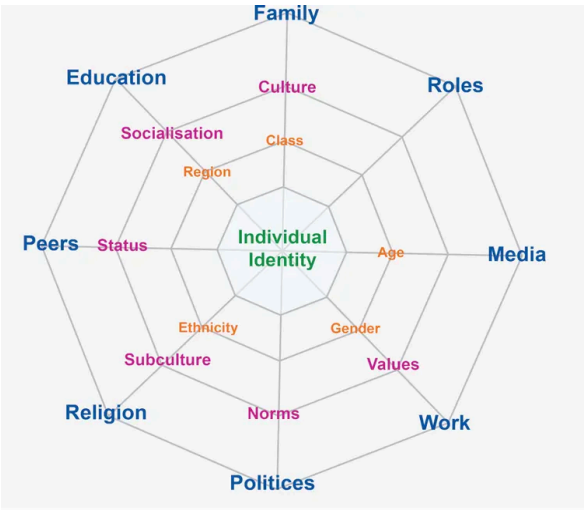
AI also highlights issues of global inequality. Advanced AI systems are primarily developed and controlled by a small number of powerful corporations and technologically advanced nations. This concentration of resources and expertise risks widening the digital divide, as countries with limited infrastructure and investment fall further behind. As a result, the benefits of AI may be disproportionately distributed, reinforcing existing global disparities in wealth, education, and opportunity.



4.4. Media Representation and Racism

The media has the ability to both promote and undermine various viewpoints, conventions, and beliefs. It has the ability to greatly impact people all throughout the digital globe. Globally, people have a tendency to follow social media norms, which makes media representation increasingly important.

Positive, multi-dimensional representations can challenge and subvert dominant stereotypes, promoting understanding, empathy, and disrupting conventional expectations and biases. Good media representation has the power to motivate people and help them to realize that they are not alone. It shapes the way people



think about identity, stereotypes, norms, and discriminatory behaviors. On the other hand, the media can perpetuate stereotypes and maintain social hierarchies through underrepresentation or misrepresentation of marginalized groups, reinforcing their subordinate status, thus hindering progress towards equality and social justice.

Racism is a belief system or set of discriminatory practices that unjustly considers one race or ethnic group to be superior or inferior to others, leading to prejudice, discrimination, or hostility based on race. The relationship between racism and the media is demonstrated by the effects of media depictions. The media has more ability than anything to eradicate racism. There are efforts being made to increase diversity and representation in media, which can help combat harmful stereotypes and biases.

5. Questions To Be Answered

How do digital ecosystems and footprints affect individuals and companies?

Why do the rates of cybercrime vary among nations? What role does digital law play here?

What changes will extended reality and Metaverse bring to people's lives?

What steps can be taken to increase Metaverse accessibility?

How to make technology more accessible?

How can AI and its data use be controlled?

What can be done to increase technological accessibility?

What is the digital divide and how to solve the problem?

How can data security and privacy be increased?

What is misinformation and disinformation? How to prevent them?
What is the importance of media representation? What steps can be taken to increase it?

6. Conclusion

In the modern world, digital realities are inevitable and essential factors of human lives. In order to evolve them successfully in human lives, their advantages and disadvantages must be determined and addressed carefully.

Artificial intelligence, cryptocurrency, the digital divide, extended reality, the metaverse, data privacy, misinformation, media representation, cybercrime, and the other issues are all important cornerstones to shape the best possible future.

To summarize, It is crucial to understand how digital realities can improve efficiency, connectivity, and accessibility while also considering potential risks such as privacy breaches and addiction. By striking a balance between embracing innovation and safeguarding against negative consequences, individuals and society can fully harness the power of digital technologies.

7. Bibliography

https://www.ibm.com/think/topics/digital-footprint

https://ocindex.net/rankings/cyber-dependent_crimes

https://www.stationx.net/cybercrime-statistics/

https://direct.mit.edu/books/monograph/3275/Digital-CitizenshipThe-Internet-Society-and

https://dijitalvatandaslik.org/dijital-hukuk/

https://www.mdpi.com/2673-6756/2/2/28

https://docs.neu.edu.tr/library/6812699178.pdf

https://gdpr.eu/what-is-gdpr/

Ribble, M. (2011). Digital Citizenship in Schools: Nine Elements All Students Should Know

https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA(2015)565890_EN.pdf

https://charmainepu.wordpress.com/2014/09/26/week-4-participation-and-the-digital-divide-who-misses-out/

Analysys Mason (2013, July 8). Bridging the digital divide: connecting the unconnected.

https://www.temjournal.com/content/131/TEMJournalFebruary2024_771_782.pdf

https://dap.berkeley.edu/web-a11y-basics/what-digital-accessibility

https://library.fiveable.me/understanding-media/unit-19/theories-representation-media/study-guide/9nsX9EUK5nmNMKD1

Wilder, SeMarial, "Racism in Media: How Media Shapes Our View of People of Color in Society" (2020). Community Engagement Student Work. 46.

https://www.cbclaw.com.tr/en/data-privacy-in-a-digital-world-a-multi-disciplinary-cross-industry-examination

Kohel, M., & Strine, A. (2024, January 31). Where Trade Secrets and Data Privacy Strategies Overlap. Retrieved from IPWatchdog: https://ipwatchdog.com/2024/01/31/trade-secrets-data-privacy-strategies-overlap/id=172502/

Kayaalp, M. (2017, September 11). Patient Privacy in the Era of Big Data. Retrieved from Dergipark: https://dergipark.org.tr/en/download/article-file/607947

Altay S., Berriche M., Acerbi A. (2021). Misinformation on misinformation: Conceptual and methodological challenges. Retrieved from: https://psyarxiv.com/edqc8

What are the Legal risks to Cryptocurrency investors? By Nathan Reiff (October 2021) Retrieved from: https://www.investopedia.com/tech/what-are-legal-risks-cryptocurrency-investors/

https://annenberg.usc.edu/research/center-public-relations/usc-annenberg-relevance-report/ethical-dilemmas-ai