LETTER FROM THE SECRETARY-GENERAL

Honourable delegates,

Even if I wanted to, I cannot stress the importance of the agenda items dedicated for this committee. Firstly, both the big data and artificial intelligence is unique discoveries that are unprecedented rest of the human history, making them ambiguous in terms of their actual effects on politics, economics and society. Secondly, the very uncontrollable nature of these innovations renders their beneficial potential and qualify them as threats. Furthermore, their existence can be utilised as weapons that was the exact case in the nuclear technology discovered 70 years ago. Moreover, on one hand, we have big data that is capable of uncovering causal and correlational connections of international and societal affairs that we are unaware right now. That is why it can only indicate a paradigm shift in both national and global politics. On the other hand, AI comes to the stage as a powerful agent of automation as well as being itself a superior intellect capable of processing incomprehensible amount of information to the human mind. Then again, the international and national political, economical and societal norms are subjected to change because of sheer transformative nature of this technology.

Consequently, before it causes drastic changes that would threaten the balance of power and relative security within the realm of global politics, these technologies must be regulated at international level to prevent its harmful usage. Therefore, this is a topic to be addressed under the theme of "decision-making in times of crisis" that requires extraordinary preventative measures. That is why delegates must find a way to be cooperative and make compromises to establish a universally accepted norms for utilisation of these technologies.

Before I close my remarks, I would like to thank Öykü TAŞ, the under-secretary-general of this committee and her lovely assistant Cemre Nur Karakoç for preparing this well-detailed and comprehensive study guide for delegates of LEGAL committee.

Sincerely,

Secretary-General
Çağdaş Başar Bahar

LETTER FROM THE UNDER-SECRETARY-GENERAL

Dear delegates,

I am Öykü Taş and It is my utmost pleasure to be your Under Secretary General for this year's LEGAL committee. This will be one of the most emotional conferences that I have attended, and I believe that you will be able to feel that through this guide that we, me and my academic assistant Cemre Karakoç, have created.

In this committee, you will be debating upon one of the greatest debates of our time which is "How much can we compromise of our privacy for the future of technology?" and We expect you to be able to answer this question with the concept of the agendas that you've been given.

I would like to express my deepest gratitude towards our Executive team, especially Çağdaş Başar Bahar and Berat Çağan, for their help on the creation of this document and Cemre Karakoç for being the best academic assistant and a sister that I could asked for and all the IUMUN members that have created this wonderful environment of friendship and sincere work of ethics. Also, if you have any questions about the procedure or the guide please feel free to send me a email via academy@iumun.org or a message via Instagram @oykuxelysian

See you at IUMUN,

Under-Secretary-General

Öykü Taş

TABLE OF CONTENTS

I. INTRODUCTION

A. Introduction to the Committee

The Legal Committee is the Sixth Committee of the General Assembly Committees and the primary forum for the consideration of legal questions in the General Assembly. All of the United Nations Member States are entitled to representation on the Sixth Committee as one of the main committees of the General Assembly. The promotion, codification, and progressive development of international law is mandated by the UN Charter, and the Sixth Committee is the primary forum for the consideration of international law and other legal matters concerning the UN.

Issues allocated to the Legal committees include the promotion of justice, international law, accountability, and internal UN justice matters such as drug control, crime prevention, and combating international terrorism.

Counter-terrorism issues are also dealt with by other UN bodies, not all of which report to the General Assembly (GA). Nevertheless, the Legal Committee serves big importance on all different matters such as global big data security and global artificial intelligence regulation.

The Committee also considers requests for observer status in the GA. Core items of the Committee's work are the reports of the various subsidiary organs, ad hoc Committees, and expert bodies dealing with legal matters under the purview of the GA. Some items are considered on an annual basis, others biennially, triennially, or staggered over a longer period. The Committee establishes working groups as appropriate (The GA Handbook: A practical guide to the United Nations General Assembly Second edition 2017).

II. GLOBAL BIG DATA SAFETY AND SECURITY

A. Major Issues and Risks of Global Big Data Security and Privacy

The main concern of many legal philosophers is fundamental equality. There is a huge amount of ridiculous information such as social media, fake news, filter bubbles, chaotic pluralism in private space, and many platforms that seem to be designed for logical reasons, and they easily influence people in many ways to follow the current agenda. Manipulating someone with the modern world newspaper takes seconds: A quick scroll through social media is enough to add doubts and questions. Even if they can take the information directly, people are directed unconsciously. It means inequality in society's ideas. Also, causes growing fears for a progressive erosion of privacy, non-discrimination, freedom of speech, and freedom of information. (Hildebrandt, M., & O'Hara, K.) It is not right to talk about free thought with directed thoughts and information Whether true or false, data is vulnerable to breach. They can especially be used as a primary source in guiding society. At this point, governments should take steps to prevent data pollution and prevent misdirection, provide accurate information, and create an environment of free thought. Big data and machine learning cause more than people think. These are not dreams: in 2016, when Donald Trump used Twitter and the expertise of an advisor from the Breitbart news site to rout mainstream (and not-so-mainstream) Republicans to gain the nomination, and then to outflank the Democratic candidate who showcased her great experience and traditional political virtues. Away from the campaign trail, politics is also implicated as decision-making is being distributed away from traditional representative institutions – but to whom? Though some power is devolving to individuals whose opinions can more easily be consulted, there is a great deal of power in the machines that set the parameters for interaction and discussion. Foregrounding the individual as an independent agent that should not be treated as a manipulable pawn, whether by their government or powerful social networks. (Hildebrandt, M., & O'Hara, K.) In such a situation you need to evaluate democracy. The widespread spread of false news facilitated by digital technologies continues to evade public scrutiny, presenting a substantial risk to the integrity of fair and

knowledgeable democratic elections. This covert distribution of misinformation undermines the core of democracy. Furthermore, the adoption of big data and artificial intelligence exacerbates this danger by not only manipulating existing political leanings but also by molding and subtly shaping public sentiment. This effectively replaces the challenging task of deliberating the public interest with algorithmic shortcuts, thus undercutting the fundamental principles of democracy.

With the development of technology, it is now easier to intervene in people's private lives. Such activities, which were previously carried out only by intelligence organizations, are now possible in a much more comprehensive way, thanks to the information voluntarily provided by the user on websites that have become an indispensable part of our lives. Sharing personal information such as fingerprints, dates of birth and identity information, addresses, credit card information, and banking activities is no longer a secret. McKinsey Global Institute (MGI) shared datasets whose size is beyond the ability of typical database software to capture, store, manage, and analyze. All of the biggest Internet companies- Google, Facebook, Amazon, eBay, Microsoft, and Yahoo!-are engaged in Big Data in one form or another and treat data as a major asset and source of value creation. (Rubinstein, I. S. (2013)) Apps and various platforms collect these from us for different reasons – but it's questionable how necessary they are. Whether our personal information will be shared with third parties is an issue. Another problem is that this information is used in a manipulative way against us. It is now possible to prove that the data in customer portfolios is shared with advertising companies and shopping sites by simply testing it. Moreover, the companies accepted these sharing allegations. It is a mystery what information these posts, allegedly made under the name of customer service quality, contain or do not contain. There is a huge gap in who voluntarily shares data with this advertising service and allows themselves to be fascinated by advertisements. Listening to conversations and scanning them in the Google search engine for data sensitivity that creates advertising algorithms is now a thing of the past. They have already crossed the border of private life. Exponential companies use all the data they collect about us, with or without our permission, as a source in their analysis, research, and development reports. Is the fact that companies draw future plans by following

their customers' actions instead of getting feedback from their customers, a real reason for the data allegedly collected for very important purposes? It is not known who shares their personal data free of charge to become test subjects. Even customers are not aware that they are doing this free favour. WEF (2011) actually highlights this point, by stressing the hidden potential of personal data as 'untapped opportunities for socioeconomic growth', urging a renewed discussion of the collection and usage of such data that takes into account the current monetization of personal data.

Apart from the fact that companies use data for their own benefit and exchange information with each other in this direction, it is also known that these data are shared with states. That the NSA hacked civilian infrastructures such as universities, hospitals, and private businesses was not limited to the claims of the person who leaked the relevant documents to the Guardian and Washington Post newspapers. He exposed two secret units of the United States involved in data collection. Under this program, the NSA directed international data transmitted via fiber optic cables in the United States to a repository where the material could be temporarily stored for processing and selection of foreign communications rather than domestic communications. The PRISM program allows the U.S. intelligence community to gain access to a wide range of digital information from nine Internet companies, including emails and stored data on foreign targets operating outside the United States. For example, the huge information that Google collects for street images has begun to be used not only for the Google Earth application but also for GPS services. The company also maintained an inventory of street Wi-Fi connections. Many problems arise regarding personal lives and where the boundaries should be for governments that monitor phone records and much more than emails.

B. Current Legal Structures On Global Big Data

Limitations on fundamental rights are essential in both constitutional and international human rights law to balance individual freedoms with the needs of society as a whole. Various strategies are employed to ensure that fundamental rights maintain their integrity while also recognizing the necessity of limitations. These

limitations may arise due to conflicts with public goods crucial for the effective functioning of fundamental rights or due to clashes between different rights and liberties that need to be harmonized. Within the framework of the European Convention on Human Rights, which establishes the human rights standards for the Council of Europe's 52 member states, the limitation of rights such as privacy, freedom of thought, conscience, and religion, freedom of expression, and freedom of assembly and association undergoes a triple test to determine the legality of security measures that may encroach upon these rights. The triple test typically includes the following criteria:

- Legitimate Aim: Any limitation on fundamental rights must pursue a legitimate aim recognized by the Convention. This might include objectives such as national security, public safety, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

- Necessity: The limitation must be necessary in a democratic society to achieve the legitimate aim. This means that there must be a pressing social need for the measure and that it is proportionate to the aim pursued. The state must demonstrate that there are no less restrictive means available to achieve the same objective.

- Proportionality: The limitation must be proportionate to the aim pursued, meaning that it must not impose burdens on individuals that exceed the benefits to society. This involves balancing the importance of the aim against the severity of the interference with the rights of individuals.

These tests ensure that any restrictions placed on fundamental rights are justified, necessary, and proportionate, thus safeguarding the delicate balance between individual liberties and the collective interests of society. They provide a framework for assessing the legality of security measures that may impact fundamental rights within the European context, promoting accountability and adherence to human rights standards across member states. The triple test outlined can serve as an illustrative framework to demonstrate how the balance and trade-offs inherent in fundamental rights can be applied to the impact of Digital Surveillance Technologies

(DSTs) on these rights. In Article 8 of the Convention, the right to privacy is established, followed by three conditions articulated in the subsequent paragraph to justify any infringement: the measures must be lawful, necessary in a democratic society, and serve a legitimate aim. The requirement of a "legitimate aim" and the necessity for the measure to be "necessary in a democratic society" indicate that a trade-off may be acceptable, but only if the measures are essential and proportional in achieving public goods such as safeguarding public order, health, morals, or protecting the rights and freedoms of others. DSTs failing to contribute to these public goods as outlined in Article 8.2 cannot be justified. This suggests, at the very least, a minimal evaluation of the effectiveness of the measures causing infringement. While the trade-off is a necessary condition, it is not sufficient. Justification also depends on ensuring that the measures are "in accordance with the law." In the case law of the European Court of Human Rights (ECHR), lawfulness is detailed as requiring a basis in national law that is easily accessible, foreseeable, and contains effective safeguards. Adequate accessibility and foreseeability enable citizens to anticipate potential privacy infringements by their government, relating to their reasonable expectation of privacy. For example, secret surveillance might be permissible if citizens can foresee the circumstances under which it might occur, even if they are not notified beforehand by the authorities. Effective safeguards require that secret surveillance is not unlimited in scope (in terms of time and content) or scale (number of individuals, frequency of interception).

Furthermore, the condition of safeguards implies that a warrant or judicial permission is necessary if the invasiveness, frequency, or duration of the measure surpasses a certain threshold. A crucial safeguard is that infringements are permitted only in specific cases, precluding general monitoring of groups or individuals. Aligned with contemporary notions of "protection by design," the General Data Protection Regulation (GDPR) establishes a legal obligation to implement "data protection by default and by design" (DPbD, Art. 25 GDPR). This mandates that entities responsible for upholding the fundamental right to data protection (Art. 8 Charter Fundamental Rights of the European Union) integrate state-of-the-art technical and organizational safeguards at the socio-technical architecture level, even if these

measures might encroach upon various fundamental rights. The essence of the matter is that violations of human rights driven by data and code necessitate protective measures driven by the same technology, requiring the translation of legally text-based protections into the structure of data- and code-driven systems. Digital Surveillance Technologies (DSTs) designed to identify and mitigate online security threats, vulnerabilities, and various forms of cybercrime have the potential to encroach upon privacy rights. Drawing upon the triple test framework of European human rights law, such encroachments should only be justifiable if there is a proportional trade-off established, setting a threshold before the deployment of such technologies is permitted. However, if this threshold is surpassed, the principle of proportionality dictates the implementation of counter-infringement measures aimed at minimizing potential violations to a level considered reasonable in comparison to anticipated benefits. In this scenario, the concept of proportionality is contingent upon the technical and economic advancements in counter-infringement technologies.

Similarly, In the realm of consumer-business relations as well as iGovernment, the legal framework of EU data protection is focused on data minimization. As consumers or citizens, people should only provide the data that are necessary for a specific purpose, and their usage is only lawful as long as this purpose (or a compatible purpose) holds. This also applies when the data are provided with consent. (De Hert, P., & Gutwirth, S. (2006) Moreover, In 2010, the European Commission (EC) issued a Communication in which it concluded, among other points, that although the core principles of the Data Protection Directive (DPD) remained valid, the Directive was no longer adequate to address the challenges posed by 'rapid technological developments and globalization'. This Communication was titled 'A comprehensive approach on personal data protection in the European Union' (COM (2010) 609 final), and it highlighted the need for a more robust and adaptable framework to safeguard personal data in the evolving digital landscape.

On the other hand, Big data and digital security encompass more than just protection against cybercrime; it also involves resilience in the face of criminal

activities perpetrated through or against interconnected computer systems. The Cybercrime Convention imposes obligations on states to criminalize various threats to the CIA (such as illegal access, interception, and data interference), computer-related offenses like forgery and fraud, and content-related offenses such as online child pornography and copyright infringements. As a result, cybercrime is a multifaceted issue that incorporates existing criminal activities, redefined by cyberspace's unique characteristics like its scope, speed, distribution, and distance of relevant conduct and its effects. Interestingly, while measures to combat cybercrime are essential, they can inadvertently pose threats to online security, creating a paradoxical challenge for digital protection efforts. (Hildebrandt, M. (2019)

C. Limitations and Gaps of The Current Legal Framework on Global Big Data

Accumulated data and the significant information they contain create security problems because they need to be protected. This data can encompass important information ranging from personal data to trade secrets. Therefore, it is essential to protect them from unauthorized access, malicious attacks, and data breaches. Data security requires taking effective measures against such threats and implementing appropriate security protocols. Otherwise, the security of this data could be seriously compromised, leading to adverse consequences. Security technologies have consistently introduced new security challenges. Guns, for instance, can serve as a means of defense against threats or as tools for enforcing compliance with laws and fostering trust and security among citizens. However, they also possess the capacity to instill fear and coerce populations into submission. The monopolization of violence, which underpins both internal and external sovereignty, has been regulated by the legal principles of the Rule of Law. These principles bind those in authority to adhere to laws, thereby curbing their ability to manipulate laws for personal gain. This historical development is not guaranteed and requires an alert civil society and an impartial judiciary to ensure the effective functioning of checks and balances. Same, digital security technologies (DSTs) wield disruptive potential akin to guns. Therefore, it is imperative to reinforce the Rule of Law in the realm of national and international jurisdiction. This reinforcement must account for the novel capabilities of data- and

code-driven infrastructures, which differ from the text-based information and communication technologies (ICTs) that were previously prevalent.

More specifically, Big Data refers to innovative methods employed by organizations, including governments and businesses, to merge various digital datasets and then utilize statistics and other data mining techniques to uncover hidden information and unexpected correlations. While Big Data holds the promise of significant economic and social benefits, it also raises serious privacy concerns. Specifically, Big Data poses challenges to the Fair Information Practices (FIPs), which serve as the foundation of all modern privacy laws. One of the most influential privacy laws globally is the European Union Data Protection Directive 95/46 EC (DPD). In January 2012, the European Commission (EC) proposed a new Regulation to reform and replace the DPD. However, experts argue that this Regulation, while attempting to address longstanding deficiencies with the DPD and more recent issues related to targeting, profiling, and consumer mistrust, overly relies on the discredited informed choice model, thus failing to fully address the imminent challenges posed by the Big Data phenomenon. (Rubinstein, I. S. (2013)) As a result, individuals are not adequately protected in legal terms regarding continuously collected data, the consequences of which are unknown.

Presently, Europe is in the process of deliberating a comprehensive General Data Protection Regulation (GDPR) intended to supplant the aging Data Protection Directive. This proposed regulation not only seeks to modernize existing data protection laws but also aims to address emerging challenges in the digital landscape. It introduces an array of new individual rights while simultaneously imposing stringent accountability measures on organizations engaged in data collection or processing activities.

Despite these proactive measures, the impending arrival of the Big Data tsunami threatens to overshadow the efficacy of these reform endeavors. The sheer volume and complexity of data generated by Big Data analytics present unprecedented challenges to traditional privacy frameworks and regulatory mechanisms. As such,

there is a growing recognition of the need for supplementary approaches to complement legislative efforts.

One such supplementary approach involves the formulation and adoption of codes of conduct. These codes serve as voluntary guidelines that outline best practices and ethical standards for data handling and processing. By promoting adherence to these codes, regulators can foster a culture of responsible data governance among businesses and organizations. Furthermore, regulators are encouraged to incentivize businesses to embrace innovative business models that prioritize consumer empowerment and data protection. These models may involve implementing privacy-enhancing technologies, providing greater transparency regarding data practices, and empowering individuals with more control over their personal data.

While data is saved, any further processing is prohibited if the original purpose no longer applies, unless there is another purpose that is not incompatible with the original one. This concept, known as purpose binding, is closely associated with the principle of minimal disclosure or data minimization. If the original purpose becomes obsolete, processing becomes unlawful, even if consent was initially given. According to current legislation in the EU, individuals cannot waive their right to comply with purpose limitation. Regardless of the grounds for data processing outlined in Article 7 of the Data Protection Directive, all conditions for lawful processing, as specified in Article 6 of the Directive, must be met. Even in cases of consent (one of the grounds specified in Article 7), purpose limitation still applies, as detailed in Article 7.a. (Hildebrandt, M. (2013) The issue arising here is the inability to track the fate of data shared by customers with their consent. The fact that individual tracking is not possible raises a question mark over what governments should do about this issue.

Another gap is that there is nobody who will supervise the data security commitment on behalf of individuals. There is neither security protection nor checking whether shared information is used for purposes other than its intended purpose, nor a balance of restrictions and controls on data sharing. In a system where data is collected freely, whether with or without permission, the assurance of security becomes merely a belief, leaving room for potential abuse. This includes the risk of

running destructive or unauthorized programs aimed at stealing sensitive information, whether from individuals or businesses. Additionally, other digital security concerns arise, such as spam sent by remotely controlled spam zombies and fraud perpetrated by phishing hosts or bot-infected computers. Despite the existence of laws aimed at ensuring security, the lack of control and monitoring raises questions about the effectiveness of these laws.

Another is that acquiring data can lead to security challenges that surpass initial expectations. Data sets enabling the analysis of individuals on a larger scale raise concerns regarding national security. While breaches at an individual level are noteworthy, they have the potential to escalate into public breaches, impacting a wider societal context. These breaches not only compromise individual privacy but also transcend geographical boundaries. Consequently, the data issue evolves into a substantial problem, triggering significant national security implications. Big data is about more than just protecting individual transactions or communications. It involves ensuring the integrity and confidentiality of data across various levels, from personal interactions to critical infrastructure. Attackers often exploit vulnerabilities in identification and authentication systems, using techniques like spoofing or phishing to gain unauthorized access. The severity of these threats depends on their potential impact, which can vary based on factors such as the number of individuals affected and the duration of the breach. Attacks on essential services like telecom providers or banks can have far-reaching consequences, compromising the safety and security of entire societies.

D. Finding a Balance Between Privacy and Security

Following 9/11, the scale metaphor gained popularity, conveying a sense of balance and rationality during times of crisis. The underlying concept suggests that in the trade-off between security and liberty, one cannot have both simultaneously; decisions must be made, and if so, they should be carefully balanced. The notion that sacrificing some liberties is necessary for achieving security resonates with the political agenda of expanding law enforcement powers, as well as with the broader security technology industry, including arms production for military purposes. This

use of the scale metaphor can be employed to promote security technologies that may encroach upon fundamental rights: the argument goes that in order to enhance online security, sacrifices must be made in areas such as privacy, data protection, non-discrimination, due process, and free speech. For many, trading a portion of privacy for a degree of security seems like a reasonable proposition. Having a higher level of digital security is necessary, but not enough to justify sacrificing privacy. It's important to consider that the more intrusive a Digital Security Technology (DST) is, the stricter the criteria should be for its implementation. If security threats and proportionate DSTs meet the necessary criteria, a delicate balance needs to be maintained: as the infringement on human rights increases, stronger safeguards must be put in place. In accordance with the principle of data protection by design and default, human rights law should incorporate the concept of counter-infringement measures as essential safeguards. Similar to data protection by design, this approach would ensure legal protection through proactive design strategies. (Hildebrandt, M. (2019) Enhancing safety involves both preventing and withstanding attacks, but safety is also compromised by factors beyond deliberate attacks, such as natural disasters, unintended consequences of human activity, and accidental negligence. Meanwhile, the concept of security is often used to refer to the reduction of foreseeable harm (thus hopefully increasing safety) and related to resilience against crime. (Hildebrandt, 2013; Zedner, 2009) Security. London: Routledge) While this is often framed as a balancing act between liberty and security, it is more accurately described as a trade-off rather than a true balance. The concept of balance implies that as we enhance security measures that encroach upon our liberties, we must also strengthen safeguards to restore equilibrium. However, ensuring this equilibrium entails verifying the proper implementation of counter-infringement measures. The crucial point that requires more attention is that the balancing act necessitates a thorough examination of the proper implementation of counter-infringement measures (Hildebrandt, M. (2019).

E. Ethical Considerations of Global Big Data

Are we trading the public good of security for the private good of privacy, or should both be considered public goods? Should these goods be classified as rights or

interests? (Edmundson, W. A. (2012)) The debate over the right to safety versus the right to privacy or non-discrimination raises important questions. Is an individual's right to privacy being traded off against collective interests such as security? Or are we sacrificing a private interest in privacy for a public interest in security? These questions delve into traditional distinctions in moral philosophy. Kantian deontologists may advocate for a rights-based approach, where rights take precedence over interests. Benthamite utilitarianism may favor an approach based on aggregate interests, while Millian liberals might restrict utilitarian calculations by asserting a fundamental right to liberty that can only be overridden by security interests protecting individual liberty. However, pitting individual rights or interests against the public good or collective interest in online security is highly problematic. It assumes that fundamental rights and security are on equal footing, whereas their relationship is more nuanced, with one often being conditional on the other. Additionally, it incorrectly assumes that privacy is not a public good or collective interest, and that security is not a private good or individual right. Both private interests in privacy and security rely on a legal framework that provides a minimum of legal certainty regarding these interests, highlighting that individual privacy and security are also public goods. This raises the question of whether legal certainty can be achieved without security in the broader sense of protection against violent attacks. It also prompts inquiry into whether security, like privacy, is a human right or rather a precondition for the legal framework necessary for effective human rights, which in turn brings up issues of power and authority (Hildebrandt, 2010). These terms are often conflated, yet they have distinct meanings. Authority is based on the power to command obedience, while power is rooted in economic or military capability to enforce submission. Under the Westphalian system of sovereign states, state authority relies on a monopoly on violence, enabling the state to protect citizens against violence from both other citizens (internal sovereignty) and other states (external sovereignty). Social contract theory suggests that the state can provide the necessary security for individuals to conduct their daily lives (Johari, 1987). However, if such security is compromised, the social contract may unravel, leading to civil unrest and conflict (Hildebrandt, 2019).

F. Positions of Relevant States

By 2027, the big data market is estimated to grow to USD 103 billion. And by 2022, the global big data and analytics market is predicted to grow to USD 274 billion, statistics backed by Statista.

With knowing that most of the companies becoming data-driven, business leaders and stakeholders are seeing an increased growth of how big data analytics is helping drive economic growth. There is a fear that is instilled and is spreading globally. Several countries have developed their strategies and are adapting this technology to advance their capabilities. As technology grows rapidly, leaders are worried they will be left behind. The demand is predicted to rise by 28% says IBM, but the supply is drastically lagging.

1. United Kingdom

The UK is expected to experience a rise in big data technologies in the foreseeable future. Though the focus is specifically made toward the UK, it is said to cause a positive impact on the other European regions as well. Based on research, the telecom industry is considerably doing great by adopting big data solutions. However, other sectors are yet to catch up, having said that, retail banking is predicted to overtake the telecom industry soon.

2. Japan

Japan has been flooded with big data due to the sudden influenced by multiple factors and opportunities. There has been a drastic rise in the application of social media through which the study of customer behaviour is done in order to make effective business strategies.

3. United States of America

In the US, the collection of data from unstructured sources is one major factor that

has caused the rise of big data. And since several sectors are using the social network, weblogs, and mobile phones today, it has caused the applications and websites to generate a large amount of data. The data collected from such sources are further used to predict future happenings or to build business strategies.

The current US market has given an additional edge to the market by collecting data, converting it, and analysing these raw data, and convert it into actionable insights.

4. People's Republic of China

Major factors like technology integration and policy support are the key drivers toward the growth in big data in China. It is also expected that the big data revenue will grow at a CAGR of 23.5% within the period of 2019-2020. An estimation is made stating that China's big data market will likely hit the US by USD 22.49 by the end of the year.

5. Russia

Banks, telecoms, and large retailers are the largest consumers in the country's big data industry. The major drawback of development in big data is due to the shortage of qualified big data professionals, lag of experience of implementation made by Russia as well as high costing in solutions. However, according to IRI, it is said that the big data market will grow tenfold to 300 billion rubbles within the next few years.

Additionally, countries like India, South Africa, South Korea, Canada, and the Middle East Region are also focused on getting stronger and better on the Global Big Data scene (YoeyThamas, 2019).x

G. International Cooperation and NGOs' Role in Global Big Data Security and Privacy

A long and rich history of academic scholarship on development nongovernmental organisations (NGOs) reveals much about their shape and strategy, their diverse priorities and modalities, and their operations and impact, among other things. One

consistent question that has been asked in NGO research across the past three decades is whether and how NGOs can live up to their civil society functions alongside their successes in service delivery. Whereas one section of academic literature applauds NGOs for their impact across a number of diverse sectors and in diverse contexts (see the systematic review of Brass et al. [2018]), another body of literature takes a much more critical stance in asking whether this is enough, given the transformative ideologies and principles and the pursuit of social justice that underpin their motivations (see Banks et al. 2015). An increasingly managerial-driven

aid system has fostered an increasingly professionalised cadre of development NGOs internationally, pulling them away from these more political roots and roles. Although we know a lot qualitatively about the roles and contributions of development NGOs from existing literature, we know less quantitatively about their overall contribution to development cooperation. This is a problem rooted in the methodological approach that most academic literature takes. Nationally and internationally, data is not compiled in ways that can give us a complete picture of the contributions of development NGOs in a donor country's overall foreign aid efforts, or of their holistic contributions in the countries where they operate. Research has a tendency to be based on small samples of (typically the largest) NGOs, within one country or internationally. Within such an approach, we lack knowledge on diversity and scale within the sector. A stronger methodological approach that seeks a sector-wide understanding of development NGOs within any given context would not only allow us to measure the added value of development NGOs to foreign aid but would also allow us to explore their integration within the broader system of development cooperation. One key example here would be to explore the ways in which donor funding shapes and influences NGO sectors to prove or disprove common assumptions around NGO dependence on donor funding and the challenges that accompany this (Banks, Nicola 2021).

H. Questions to be Covered

- What are the main challenges in maintaining privacy and security when dealing with global big data?
- How can we ensure data anonymization in big data to protect individual privacy?
- What are the best practices for securing big data stored in cloud environments?
- How can blockchain technology be used to enhance the security and privacy of big data?
- What role does encryption play in securing big data, and what are the challenges in implementing it at scale?
- How can we balance the need for data accessibility and data privacy in a global context?

- What are the legal and ethical considerations when dealing with global big data?
- How can artificial intelligence and machine learning be used to enhance big data security?
- What are the potential risks and threats associated with global big data, and how can they be mitigated?
- How can organizations ensure compliance with international data protection regulations when dealing with global big data?

III. GLOBAL ARTIFICIAL INTELLIGENCE REGULATION

A. Introduction to the Global Artificial Intelligence Regulation

It is a well-known fact in today's world that Artificial Intelligence (AI) will be a part of our lives forever but since It is quickly evolving and changing the rules of its own game there is an urgent need for action on the matter because AI creates an efficient and quick solution for different cases and this allows a win-win situation for the Policymakers, companies, and stakeholders of the related companies but this situation is not for long. Since the situation does not have the proper regulation, in the near future this will cause problems not only technological or economical but also ethical and legal problems as well (Bianzino, 2024).

Since the term was coined in 1956, Artificial Intelligence has been associated with a wide range of concepts (Cerka et al.,2017; Jackson, 2019) based on a thinking human being and on rational behaviour, which could be synthesized as systems that think and act like humans and systems that think and act rationally. Equally wide is the variety of different names associated with whatever utilizes AI technology: robots, smart systems, intelligent systems, intelligent agents, AI agents, AI algorithms, intelligent algorithms, and autonomous systems, to mention a few.

To avoid misinterpretations regarding AI, the High-Level Expert Group established by the European Commission has defined AI systems as " software (and conceivably also tackle) systems designed by humans that, given a complex thing, act in the physical or digital dimension by perceiving their terrain through data accession, interpreting the collected structured or unshaped data, logic on the knowledge, or recycling the information, deduced from this data and deciding the stylish action (s) to take to achieve the given thing. AI systems can either use emblematic rules or learn a numeric model, and they can also acclimatize their get by assaying how the terrain is affected by their former conduct. " (AIH LEG, 2019a). Considering the difficulty of defining AI in a way that could fit all approaches demanded regulation and governance conduct with clear communication among all stakeholders, this composition adopts the description of AI established by the High-Level Expert

Group on AI systems. The liabilities, security, intellectual property, and sequestration associated with different systems for medical robots, drones, and independent buses, among several" intelligent results" offered every day have been questioned. Illustrating the position of threat-related indeterminacy, machine literacy has been combined with game proposition (Howitzer Metal., 2017) in cases where inventors were using game proposition to help educate strategic defense to algorithms. A game between two algorithms prognosticated that one would kill the other only in case of an absolute failure of coffers. Still, when a more intelligent algorithm was introduced, it incontinent killed the weaker bones (Firth-Butterfield, 2017). This case reinforces the idea that an independent system will inescapably find itself in a situation in which it needs not only to observe a certain rule or not, but also to make a complex ethical decision (Dennis Metal., 2016). Facing the pitfalls compels us to explore their causes and goods. Although the goods of AI aren't yet known, a large quantum of them can presently be classified. Originally, those coming from the uninvited goods, similar as impulses, demarcation, loss of sequestration, false cons, and false negatives, loss of autonomy, (cerebral, fiscal, or physical) damage, loss of control, difficulty relating arrears, losses or diminishment in mortal rights, severance, misjudgements, and attention of power and wealth in many companies. Secondly, some pitfalls are the result of purposeful abuses, such as fake news, deep fakes, cyberattacks, terrorism, warfare, munitions, people manipulation, spying, and the low position of the republic (Beltran, 2020; Benjamin's Cambria; Borg Bourgeois18; Jackson, 2020; Job Join metal019; Mi metal metal019). Considering all those pi all, establishing stylish practices for the gating and defining new moral responsibility CR Orion mo ls is pi tail to in hence the op kings created by AI Ta (Added camp, Florida threat Threaten models can give port and inflexibility for Big Data and AI opera NS (Mantel (Mantle and stakeholders who develop and employ them placarded systems must enhance their knowledge of the VA ES defend by mortal rights and how those rights apply their own conduct SMUH, (SMUH Despite being a huge challenge, chancing a way deal with e iCal issues must be a constant target of explore ion, for what w need to join all our forces (Bistro (Bottom and AI regular on is on the right path to get there (Carter (2020). The reasons to regulate include manufacturers' need ' to compare ND to a legal frame

thin which they can operate reliably; consumers ' and s ' etc.'s need to be defended from as t may harm or negatively affect them; and the need for business opening (Holder (tail., 2 metal). In divide e still lacking regulation, the general approach observed is that invent n is freely allowed, but those in charge would bear the consequences in case certain types of damage are caused (Reed, (18). Faced with the challenge of minimizing this pitfall, a combination of strategy and conduct must be put into practice during the entire lifecycle of AI systems, in order not only to IDE if damages and label IES, but also, and especially, to avoid them.

B. Major Issues and Risks of Global Artificial Intelligence Regulation

Around the world course of Fabricated Experiences (AI) presents a complex challenge. Though it holds the potential to ensure tried and true headway and utilize of AI, there are essential impediments to overcome. The quick pace of AI progress makes it troublesome for controls to keep pace with creating capabilities. Additionally, shifting national needs and the require of a single around the world necessity master can lead to an interlaced of bearings that avoid widespread collaboration and headway. In addition, too much strict bearing's chance covering profitable AI applications and making a competitive obstacle for countries with more restrictive courses of action. Data security, algorithmic slant, and the weaponization of AI are additional threats that require clear bearings on data taking care of, sensibility in AI calculations, and imprisonments on free weapons (cf., Affiliation for Monetary Co-operation and Enhancement, 2021). In show disdain toward of these challenges, the potential benefits of careful AI advancement require advancing endeavours towards a framework for around the world heading.

Due to its nebulous nature, AI get away simple definition. Instep, the definition of AI tends to depend on the purposes and groups of onlookers of the inquire about (Russell and Norvig 2020). In the most essential sense, machines are considered intelligent when they can perform errands that would require insights if done by humans (McCarthy et al. 1955). This might happen through the directing hand of people, in "expert systems" that take after complex choice trees. It may moreover happen through "machine learning," where AI frameworks are prepared to categorize texts,

images, sounds, and other information, utilizing such categorizations to make autonomous decisions when stood up to with modern information. More particular definitions require that machines show a level of independence and capacity for learning that empowers sound activity. For occurrence, the EU's High-Level Master Bunch on AI has characterized AI as "systems that show cleverly conduct by dissecting their environment and taking actions—with a few degree of autonomy—to accomplish particular goals" (2019, 1). Yet, outlining the potential for conceptual contention, this definition has been criticized for indicating both as well numerous and as well few advances as AI (Heikkilä, 2022).

AI innovation is as of now actualized in a wide assortment of ranges in regular life and the economy at expansive. For occasion, the conversational chatbot ChatGPT is evaluated to have come to 100 million clients fair two months after its dispatch at the end of 2022 (Hu 2023). AI applications empower modern robotization innovations, with subsequent positive or negative impacts on the request for labor, work, and economic balance (Acemoglu and Restrepo 2020). Military AI is fundamentally to lethal autonomous weapons frameworks (LAWS), whereby machines take independent choices in fighting and front line focusing on (Rosert and Sauer 2018). Numerous governments and open organizations have as of now executed AI in their day by day operations in arrange to more proficiently assess welfare qualification, hail potential extortion, profile suspects, make chance evaluations, and lock in in mass reconnaissance (Saif et al. 2017; Powers and Ganascia 2020; Berk 2021; Misuraca and van Noordt 2022, 38).

C. Current Legal Structures on Global Artificial Intelligence Regulation

The burgeoning field of Artificial Intelligence (AI) requires a nuanced approach to around the world heading. Though reasonable headings can develop careful advancement and sending, the way towards a bound together framework is full of challenges. This composition examines the openings and impediments related with around the world AI control, drawing upon built up educational and capable sources.

On the one hand, headings offer a essential instrument for calming perils related with AI. Data assurance concerns are essential, and clear rules on data collection, utilize,

and capacity are fundamental to secure individual security (Ohm, 2019). Besides, bearings can progress goodness and non-discrimination by requiring engineers to address potential inclinations interior AI calculations (Bostrom & Yudkowsky, 2014). In addition, around the world understandings can play a vital portion in maintaining a strategic distance from an arms race in autonomous weapons fuelled by AI (Organization for Monetary Co-operation and Progression, 2021).

However, setting up a bound together legal framework for around the world AI control presents essential deterrents. The fast pace of AI movement ceaselessly challenges existing controls. Unused functionalities might create a few times as of late the potential threats are totally caught on, making a gap between authoritative frameworks and imaginative substances (Matthias, 2020). Moreover, the require of a single around the world master to maintain controls makes a separated scene. Different countries prioritize AI change and utilize in specific ways. A few might prioritize budgetary advancement fuelled by AI, though others centre on national security concerns (Bratianu & Wagner, 2023). This contrast in national needs leads to a interlaced of regional and national controls, development complicating the issue (Widespread Alliance of Assurance Specialists, 2024).

Despite these challenges, the potential benefits of tried-and-true AI enhancement require nonstop endeavours towards a harmonized around the world framework. The current approach, characterized by a interlaced of bearings, stances critical challenges for multinational organizations investigating a contrasting set of compliance necessities (Ewijk, Koopsman, & Riess, 2023). In addition, this isolated approach can avoid all-inclusive collaboration on AI wanders. Moving forward, widespread cooperation and advancing alteration of legal structures are crucial for ensuring tried and true AI headway on a around the world scale.

D. Limitations and Gaps of The Current Legal Framework on Global Artificial Intelligence Regulation

The current lawful system for directing AI on a worldwide scale is perplexed with confinements and holes. Whereas the potential benefits of viable controls are verifiable, the need of a bound together approach makes critical challenges. This

paper investigates these impediments and crevices, drawing on set up scholarly and proficient sources.

One major impediment is the characteristic fracture of the current scene. There is no single, overarching lawful structure overseeing AI. Instep, a interwoven of territorial and national directions exists (Universal Affiliation of Protection Experts, 2024). This makes a complex and regularly conflicting environment for multinational enterprises exploring a different set of compliance prerequisites (Ewijk, Koopsman, & Riess, 2023). Besides, this fracture prevents universal collaboration on AI ventures, as distinctive directions can make barricades for analysts and designers working over borders. Another impediment lies in the failure of existing directions to keep pace with the quick progression of AI. Modern functionalities and capabilities rise always, regularly outpacing the capacity of legitimate systems to adjust (Matthias, 2020). This makes a crevice between directions and innovative substances, possibly taking off novel AI applications unregulated and posturing unexpected risks. The need of a single worldwide requirement specialist makes a administration vacuum. Distinctive nations prioritize AI improvement and utilize in unmistakable ways, with a few centrings on financial development whereas others prioritize national security (Bratianu & Wagner, 2023). This difference in needs leads to irregularities in directions, making it troublesome to set up clear and all-inclusive measures for mindful AI development.

The current lawful system regularly battles to address developing challenges like algorithmic predisposition and information protection concerns. Existing directions might not be vigorous sufficient to guarantee reasonableness and non-discrimination in AI calculations, possibly propagating existing societal inclinations (Bostrom & Yudkowsky, 2014). Essentially, clear rules on information collection, utilize, and capacity are frequently missing, making potential vulnerabilities for person protection rights in the setting of AI (Ohm, 2019).

E. Current Technology Trends

The Current technology trends of AI is encountering a period of unstable development, with novel patterns rising at a fast pace. Here, we dig more profound into a few of the most unmistakable zones of centre inside AI research:

Large Dialect Models (LLMs): These AI frameworks are revolutionizing human-computer interaction. Prepared on colossal datasets of content and code, LLMs can create human-quality content, decipher dialects with remarkable familiarity, and indeed produce imaginative substance in different groups. Envision a framework that can compose a lyric in the fashion of Shakespeare or create a compelling news article - that's the control of LLMs (Brown et al., 2022).

Generative AI: This energizing department of AI pushes the boundaries of imaginative expression. Not at all like conventional AI that analyses existing information, generative AI can make completely modern substance, from reasonable pictures based on simple content portrayals to unique melodic pieces composed in a particular fashion. Generative models hold colossal potential for different inventive areas, from helping craftsmen and architects to cultivating development in music composition (Liu et al., 2022).

Explainable AI (XAI): As AI frameworks gotten to be progressively complex, the require for XAI methods escalate. XAI points to demystify the decision-making forms of AI models, making them more straightforward and reasonable to people. By understanding how AI arrives at its conclusions, we can construct believe in these frameworks and guarantee they are adjusted with human values (Samek et al., 2019).

AI for Mechanical autonomy: The integration of AI with mechanical technology is introducing in a unused period of cleverly machines. AI-powered robots are competent of performing complex assignments in differing situations, from helping specialists in sensitive methods to investigating unsafe areas or indeed handling family chores. Envision robots that can overlap your clothing or cut your grass with accuracy - that's the future AI for mechanical autonomy guarantees (Yang et al., 2022).

Reinforcement Learning (RL): This sort of AI takes motivation from the way people learn. Through trial and mistake intelligent with its environment, RL permits AI specialists to learn complex behaviours by trial and blunder. This approach holds guarantee for applications where robots or AI specialists require to create modern aptitudes, like acing complex diversions or controlling independent vehicles (Mnih et al., 2015).

These patterns speak to fair a see into the endless potential of AI. Proceeded investigate and advancement, coupled with a centre on capable advancement and moral contemplations, guarantee a future where AI applications altogether move forward our lives over different spaces.

F. Ethical Considerations of Global Artificial Intelligence

AI is quickly changing our world, affecting healthcare, transportation, excitement, communication, and endless other spaces (Bratianu & Wagner, 2023). In any case, nearby its evident potential lie a wave of moral and societal concerns (Bostrom & Yudkowsky, 2014). Worldwide AI direction looks for to explore this sensitive adjust, guaranteeing that AI is created and sent dependably whereas cultivating proceeded innovation.

Effective controls show a pivotal opportunity to moderate dangers related with AI. Information protection breaches, algorithmic inclination that sustains societal disparities, and the potential for weaponized AI are fair a few of the potential pitfalls (Ohm, 2019). Directions can act as a protect by setting up clear rules for information collection, utilize, and capacity (Worldwide Affiliation of Security Experts [IAPP], 2024). They can advance reasonableness and non-discrimination in AI calculations (Bostrom & Yudkowsky, 2014), and anticipate the advancement of independent weapons (Association for Financial Co-operation and Improvement [OECD], 2021).

Transparency and responsibility are similarly imperative. As AI frameworks gotten to be more complex, their decision-making forms can ended up dark, disintegrating believe (Samek et al., 2019). Directions can advance straightforwardness by requiring engineers to clarify how AI calculations work (Ewijk, Koopsman, & Riess, 2023). Setting

up clear lines of responsibility guarantees that both designers and the frameworks themselves can be held dependable for their activities (Matthias, 2020). Open believe and acknowledgment are basic for AI to reach its full potential. Controls that address security concerns, algorithmic inclination, and responsibility can cultivate open believe, clearing the way for broad selection (Bratianu & Wagner, 2023).

However, setting up a bound together worldwide system for AI direction is no simple accomplishment. The fast pace of AI advancement always outpaces existing directions, making a crevice between the rules and the ever-evolving innovation (Matthias, 2020). The divided worldwide scene assist complicates things. The nonattendance of a single worldwide specialist implies distinctive nations have their possess needs, driving to a interwoven of territorial and national controls (Ewijk et al., 2023). At last, AI raises complex moral and societal issues, from potential work relocation to the effect on human independence (Bostrom & Yudkowsky, 2014). Controls must address these concerns whereas still permitting AI advancement to flourish.

Despite the challenges, the require for a harmonized worldwide system remains vital. There are important points that need to be considered such as;

International Participation: Cultivating collaboration and sharing best hones between countries is fundamental. Building up universal gatherings for discourse and joint inquire about can lead to the improvement of harmonized guidelines and directions (Ewijk et al., 2023).

Adaptable Lawful Structures: Lawful systems for AI control require to be adaptable sufficient to adjust to the quick pace of mechanical alter. Frequently looking into and re-examining controls guarantees they stay significant and successful (Matthias, 2020).

Stakeholder Engagement: Successful AI direction requires a collective exertion. Locks in with governments, industry pioneers, scholastics, respectful society organizations, and the open is pivotal (Bratianu & Wagner, 2023). This multi-stakeholder approach makes a difference distinguish potential dangers and openings, guarantees assorted

viewpoints are considered, and cultivates open understanding and acknowledgment of AI.

The world of AI direction stands at a junction. Whereas the potential benefits of AI are endless, the potential dangers are similarly concerning. By tending to these challenges and seizing the openings displayed by viable directions, we can endeavour towards a future where capable AI development flourishes nearby the well-being and security of humankind.

G. Positions of Relevant States

1. European Union

The EU has been situating itself as a frontrunner in the worldwide talk about on AI administration and ethics. A major piece of enactment, the Common Information Assurance Control (GDPR) came into impact in 2018 and has a scope which expands to a few associations' exterior of the EU in certain circumstances. Of direct intrigued for AI administration are the arrangements contained in Segment 5 of the GDPR on the Right to Protest (Article 21) and Mechanized Person Decision-Making Counting Profiling (Article 22). There is noteworthy dialog as to absolutely what these arrangements involve in hone with respect to algorithmic decision-making, robotization and profiling and whether they are satisfactory to address the concerns that emerge from such forms (see e.g. Edwards & Veale 2017; Wachter, Mittelstadt & Floridi 2017b). Among other noticeable improvements in the EU is the European Parliament Determination on Respectful Law Rules on Mechanical technology from February 2017. Whereas the Determination is not authoritative, it communicates the Parliament's conclusion, and makes different demands of the European Commission to carry out further work on the point. In specific, the Determination 'consider[ed] that the existing Union lawful framework should be overhauled and complemented, where fitting, by directing moral standards in line with the complexity of mechanical technology and its numerous social, therapeutic and bioethical implications' and set out in its Annex a proposed Code of Moral Conduct for Mechanical autonomy Engineers, Code for Inquire about Morals Committees, Licence for Architects and Permit for Clients. The Parliament too asked the European Commission to yield a

'proposal for a authoritative instrument on legitimate questions related to the development and utilize of mechanical technology and AI predictable in the another 10 to 15 a long time, combined with nonlegislative rebellious such as rules and codes of conduct as alluded to in recommendations set out in the Annex'. At the time of composing, the Commission has not however discharged such a proposal.

Further activities have happened consequent to this European Parliament Determination. In Walk 2018, the European Commission issued a Communication on Manufactured Insights for Europe, in which the Commission set out 'a European activity on AI' with three fundamental points: of boosting the EU's technological and mechanical capacity, and AI take-up; of planning for socio-economic changes brought about by AI (with a center on work, social security and instruction); and of guaranteeing 'an appropriate ethical and legitimate system, based on the Union's values and in line with the Constitution of Fundamental Rights of the EU. Also in Walk 2018, the European Bunch on Morals in Science and Unused Advances, an independent advisory body to the President of the European Commission comprising intrigue experts, released its Explanation on Counterfeit Insights, Mechanical technology and Independent Frameworks. The Statement proposed 'a set of essential standards and majority rule prerequisites, based on the principal values laid down in the EU Arrangements and in the EU Constitution of Principal Rights'.

Most unmistakable of the EU activities has been the European Union High-Level Master Bunch on Artificial Insights (a multi-stakeholder bunch of 52 specialists from the scholarly world, gracious society and industry) finalising its Morals Rules for Dependable AI in April 2019 (2019a). They incorporate 7 key, but no exhaustive, prerequisites that AI frameworks ought to meet in arrange to be 'trustworthy'. The

requirements will go through a 'piloting process' whereby they will be tried in private and open segment organisation, with input looked for to advise a open record planned for discharge in early 2020. A part of the High-Level Master Gather, Thomas Metzinger, scrutinized the handle and yield as 'ethics washing' in an op-ed for German daily paper Der Tagesspeigel in 2019. In specific he pointed to the evacuation of 'red line' 'non-negotiable' content from the last adaptation of the Rules as an

example of this and called for the scholarly world and gracious society to take charge of the talk on AI governance and morals, particularly absent from industry. In any case, Metzinger still considers that the ethics guidelines created by the Bunch are 'the best in the world' particularly as compared to endeavours from the US and China.

This 'first deliverable' of the High-Level Master Bunch was taken after by their 'second deliverable', Policy and Speculation Proposals for Dependable AI in June 2019 (2019b). The record contains 33 proposals 'that can direct Dependable AI towards maintainability, development and competitiveness, as well as consideration – whereas enabling, profiting and securing human beings. Among the suggestions, along with ones relating to instruction, inquire about, government utilize of AI and venture needs, is solid feedback of both state and corporate observation utilizing AI, including that governments ought to commit not to lock in in mass reconnaissance and the commercial surveillance of people counting by means of 'free' administrations ought to be countered. This is encouraged by a specific proposal that AI-enabled 'mass scoring' of people be prohibited. The Board also recommends that maintainability be taken account of, counting the sanctioning of a circular economy plan for computerized advances and AI. The Board calls for more work to be done to survey existing legal and administrative systems to perceive whether they are satisfactory to address the Panel's recommendations or whether change is essential in arrange to do so, with specific respect being paid to: the checking and confinement of robotized deadly weapons; the checking of customized AI systems built on children's profiles; and the checking of AI frameworks utilized in the private segment which significantly effect on human lives, with the plausibility of presenting assist commitments on such providers. The dialect of 'red lines' is included in this record, and as said over, the Board expresses concern with a few specific employments of AI, counting illustrations it accepts ought to be denied. This may stymie a few of the past feedback with respect to the Rules being 'ethics washing' but it is still significant that that dialect was avoided from the Rules indeed if it has finished up in the Recommendations. Moreover, it is hazy to what degree the Panel's Proposals will actually be taken after by EU teach and put into home in reality. Council of Europe or The Chamber of Europe (CoE), which incorporates all EU Part States as well as extra

non-EU members in eastern Europe, Turkey and Russia, has moreover been dynamic on the point of AI.

Of these exercises, there are two which specifically relate to AI administration and morals. The to begin with is the European Commission for the Effectiveness of Equity (CEPEJ) European Moral Constitution on the utilize of artificial insights (AI) in legal frameworks and their environment, embraced in December 2018, which contains five standards to direct the improvement of AI devices in European judiciaries. The European Committee on Lawful Co-operation (CDCJ) is at the time of composing working on draft rules for policymakers planning online debate determination frameworks (ODRs) to guarantee compatibility with the right to a reasonable trial and the right to an compelling cure beneath the European Tradition on Human Rights. These rules are anticipated to be discharged in late 2020. The moment outstanding CoE action is the Rules on Counterfeit Insights and Information Protection published by the Consultative Committee of the Tradition for the Assurance of People with regard to Programmed Handling of Individual Information (Tradition 108) in January 2019. This takes after Guidelines on Enormous Information issued in 2017, and the modernisation of Tradition 108 which included increases to address algorithmic decision-making. Tradition 108 incorporates among its signatories a few non-CoE members counting Mauritius, Mexico and Senegal.

2. Germany

As a result of the critical monetary bolster Germany is giving to AI investigate, a national 'AI Strategy' has been distributed (Bundesministerium für Bildung und Forschung et al 2018). The points of the activity are to fortify Germany as a inquire about area and to bolster the residential economy. Just to donate one case, between Tuebingen and Stuttgart the so-called 'Cyber Valley' is supposed to gotten to be one of the world's driving inquire about areas for AI as a 'key technology'. The state government, companies, colleges and other inquire about educate are participating in this project.

The tall money related consumption for AI inquire about – the Government Government will spend €500 million as a to begin with step and €3 billion through

and through – is advocated nearly solely with reference to the point of survival in universal competition or at slightest not needing to drop behind, particularly the US and China. According to the methodology, Germany is to end up one of the 'world's driving areas for AI'. Within the competitive connections with other nations, Germany – in agreement with the principles of the EU Technique for Manufactured Insights (Pekka et al 2018) – serious to position itself in such a way that it sets itself separated from other, non-European countries through information protection-friendly, trustworthy, and 'human centred' AI frameworks, which are gathered to be utilized for the common great as well as for 'lighthouse applications' in the areas of climate and environment assurance. At the middle of these claims is the foundation of the 'Artificial Insights Made in Germany' brand, which is supposed to ended up a universally recognized name of quality.

Part of this 'brand' is the thought that AI applications made in Germany or to be more exact, the datasets these AI applications utilize, stand beneath the umbrella of information sway, enlightening self-determination and information security. In addition, to guarantee that AI investigate, and advancement is in line with ethical and legitimate guidelines a Information Morals Commission was established, which is able to recommendations to the Government and to allow exhortation on how to utilize AI in an morally sound way. In any case, the crucial address is whether the fundamentals of AI morals are actualized into hone viably.

3. Austria

AI is seen in Austria as advertising a significant competitive advantage to the

country. Drafting on an 'Artificial Insights Mission Austria 2030' was begun, which has included a long list of stakeholder meetings to guarantee cooperation of all pertinent on-screen characters. Whereas both cooperation strategies utilized and stakeholder choice have continuously been perfect, the activity does speak to at slightest an endeavour to co-develop an Austrian AI procedure with hundreds of partners. Its centre on the year 2030 is also evidently demonstrated on China's Modern Era Manufactured Insights Advancement Arrange 2030 strategy, and like numerous comparative European activities can be seen in reaction to China's position in the

race to dominate the field of AI. Austria has too appeared a solid intrigued in European collaboration in this zone, endeavouring to ensure that a as often as possible talked about European 'Algorithms Rating Agency' or 'AI Morals Authority' - demonstrated on the IAEA that is being right now being examined in European approach circles - is inevitably found in Vienna. Austria is the situate of various important worldwide associations such as the UN bodies, OSCE or the IAEA and sees such an specialist as a common continuation of its existing part in this area.

At the same time individuals of the Austrian government have straightforwardly communicated intrigued in making a large national information pool, whereby Austrian citizens' information would be sold to the most noteworthy bidder in order to pull in cutting edge data-driven inquire about to Austria. In spite of apparent strife with the GDPR and other existing information assurance rules, this thought remains well known in important arrangement circles. It all stems from the affirmation that Austria knows that it is a little nation and, in this way, cannot compete at a global level in all spaces. The data-pooling methodology is in this way seen as a key competitive advantage to ensure that Austria is able to compete in a competitive universal environment as a little country. Due to the deterioration of the Austrian government as portion of the 'Ibiza scandal' in May 2019 - involving a video including political bribes, a table of what looks like cocaine and assaults on political attacks on driving Austrian daily papers by the distant right-wing FPÖ party - it is vague how and even whether the Fake Insights Mission Austria 2030 will proceed. Be that as it may, it is to be expected that some form of this procedure will be actualized in the coming a long time, in any case of which government is in control.

4. India

India's approach to AI is considerably educated by three activities at the national level. The to begin with is Digital India, which points to make India a carefully engaged information economy. The moment is Make in India, beneath which the Government of India is organizing AI innovation planned and developed in India, and the third is the Keen Cities Mission (Marda 2018). Alongside this, there is noteworthy speculation towards inquire about, advancement and preparing in emerging technologies in

specific from the Union Government. An AI Errand Drive constituted by the Service of Commerce and Industry in 2017 looked at AI as a socio-economic issue solver at scale. In its Report (Government of India Service of Commerce and Industry 2018) it recognized 10 key segments in which AI should be sent, counting national security, budgetary innovation, fabricating and agriculture, among others. Additionally, a National Methodology for Fake Insights was distributed in 2018 (Niti Aayog 2018) that went assist to see at AI as a lever for financial development, social advancement, and considers India as a potential 'garage' for AI applications. Whereas morals are said in both reports, they fail to seriously lock in with issues of essential rights, reasonableness, incorporation, and the limits of data driven choice making. These are too intensely affected by the private segment, with gracious society and academia, seldom, if ever, being welcomed into these discourses.

5. People's Republic of China

Along with the EU, of the ' large authorities ' under consideration in this paper, China is the other one which has generated the most state- supported or- led AI governance and ethics enterprise.

In 2017 China's State Council issued The New- Generation AI Development Plan, which advanced China's ideal of high investment in the AI sector in the coming times, and end of getting the world leader in AI invention (FLIA 2017). An interim thing, by 2025, is to formulate new laws and regulations, and ethical morals and

programs related to AI development in China. This includes participation in transnational standard setting, or indeed 'taking the lead' in similar conditioning as well as 'consolidate(ing) transnational cooperation in AI laws and regulations'. posterior to this has been farther enterprise on AI ethics and governance. In May 2019, the Beijing AI Principles were released by the Beijing Academy of Artificial Intelligence, which depicted the core of its AI development as 'the consummation of salutary AI for humankind and nature'. In addition, the Principles considered;

- the threat of mortal severance by encouraging further exploration on mortal- AI collaboration;

● avoiding the negative counteraccusations of 'vicious AI race ' by promoting cooperation, also on a global position;

● integrating AI policy with its rapid-fire development dynamically and responsively by making special guidelines across sectors; and

● continuously making preventative and soothsaying policy in a long- term perspective with respect to pitfalls posed by Augmented Intelligence, Artificial General Intelligence (AGI) and Superintelligence.

The Principles have been supported by colorful elite Chinese universities and companies including Baidu, Alibaba and Tencent. Another group comprising top Chinese universities and companies and led by the Ministry of Industry and Information Technology (MIIT)'s China Academy of Information and Dispatches Technology, the Artificial Intelligence Industry Alliance (AIIA), released its Joint Pledge on Self Discipline in the Artificial Intelligence Industry, also in May 2019 (Webster 2019). The Joint Pledge is, at the time of jotting, open for commentary from AIIA members and the general public until the end of June 2019 (Webster 2019). While the wording is fairly general when compared to other ethics and governance statements Webster (2019) points to the language of 'secure/ safe and controllable' and 'tone- discipline' as 'meshing) with broader trends in Chinese digital governance'.

Eventually, an expert group formed of experimenters at Chinese universities and established by the Chinese Government Ministry of Science and Technology released its eight Governance Principles for the New Generation Artificial Intelligence Developing Responsible Artificial Intelligence in June 2019 (China Daily 2019). It has been reported that other experts, specially Kai- Fu Lee, made spoken cessions to the commission at earlier stages in their work (Laskai & Webster 2019). Again transnational cooperation is emphasised in the principles, including along with 'full respect' for AI development in other countries.

A conceivably new addition is the idea of 'nimble governance', that problems arising from AI can be addressed and resolved 'in a timely manner'. This principle reflects the

velocity of AI development and the difficulty in governing it through conventional procedures, for illustration through legislation which

can take a long time to pass in China by which time the AI technology may have formerly changed. While 'nimble policy- making' is a term also used by the EU High-Level Expert Panel, it's used in relation to the nonsupervisory sandbox approach, as opposed to resolving problems, and is also not included in the Panel's Guidelines as a principle. While, as mentioned over, Chinese tech pots have been involved in AI ethics and governance enterprise both domestically in China and internationally in the form of the Partnership on AI, they also appear to be internally considering ethics in their AI conditioning.

Tencent has its AI for Social Good programme and ARCC (Available, Reliance, scrutable, Controllable) Principles (Si, 2018) but doesn't appear at the time of writing to have an internal ethics board to review AI developments. Still, the principles set by these enterprises so far warrant legal enforcement/ enforceability and policy counteraccusations - like the AI ethics governance guidelines away.

6. United States of America

Broadly accepted to equal as it where China in its household investigate and advancement of AI, the US has been less dynamic organizations with respect to questions of morals, administration and direction compared to developments in

China and the EU, until the Trump Organization Official Arrange on Maintaining American Administration in Manufactured Insights February 2019. This Arrange has lawful constrain, and makes an American AI Activity guided by five tall level principles and to be actualized by the National Science and Innovation Chamber (NSTC) Select Committee on Counterfeit Insights. These standards incorporate the US driving advancement of 'appropriate technical standards' and securing 'civil freedoms, security and American values' in AI applications 'to completely realize the potential for AI advances for the American people'.

Internationalization is included with the view of opening remote markets for US AI innovation and securing the US's basic AI innovation 'from acquisition by key

competitors and ill-disposed nations'. Furthermore, official offices and organizations that lock in in AI related exercises such as developing it, giving instructive awards and 'regulat[ing] and provid[ing] direction for applications of AI technologies' must follow to six key goals counting security of 'American technology, economic and national security, respectful freedoms, protection, and values' and guaranteeing that technical standards for AI 'minimize helplessness to assaults from pernicious on-screen characters and reflect Government priorities for development, open believe, and open certainty in frameworks that utilize AI advances; and developing international benchmarks to advance and secure those priorities.

H. Questions to be Covered

- How can AI regulation be effectively targeted to address the most pressing risks associated with different AI applications (e.g., healthcare, autonomous vehicles, facial recognition)?
- What frameworks can be established to assess the potential risks and benefits of emerging AI technologies before they become widely deployed?
- How can global regulations ensure responsible data collection, use, and storage practices for AI development, balancing innovation with individual privacy rights?
- What strategies can be implemented to identify and mitigate bias within AI algorithms, promoting fairness and non-discrimination across all applications?
- How can regulations incentivize the development of Explainable AI (XAI) techniques to ensure transparency in AI decision-making processes?
- Who should be held accountable for the actions and decisions made by AI systems - developers, users, or the AI itself? How can clear lines of accountability be established?
- What mechanisms can be created to foster international collaboration on AI regulation, ensuring harmonized standards and avoiding a fragmented global landscape?
- How can legal frameworks be designed to be adaptable and flexible enough to keep pace with the rapid advancements in AI technology?

- How can a multi-stakeholder approach be implemented to ensure that AI regulation reflects the concerns and perspectives of governments, industry, academia, civil society, and the public?
- What robust enforcement mechanisms can be established to ensure compliance with global AI regulations and hold violators accountable?

IV. BEING A DELEGATE IN THIS COMMITTEE

As it has been mentioned previously the main purpose of this committee to be able to find a common ground between the governments and the public. Knowing that there can be a lot of different perspectives upon the topics nonetheless this committee stands with the motto of justice for everyone. As within the agendas of global big data and artificial intelligence The house is expected to find a common ground for the companies of Technology, for the governments and most importantly for the public but while doing so the house also should take the concentration of ethical concerns, current regulations and global expectations.

As the committee board if we should give some advice to you delegates please : "Do not forget, you are representing a nation and even you have 'bad' sides, embrace them and make them look like your 'good' sides." and what We mean by that is for example if you have a economically challenge country to represent, you can try to debate upon the cause of the economical problem connected to the agenda so this

would allow all the house to look to the problem from a different perspective thanks to you. Remember, we all are here for one reason which is to try to find solutions of the problems. As well as please pay attention to the flow of the debate while not forgetting the purpose of the committee.

Further Reading:

You can use this website for general knowledge of your countries AI policies & strategies;

https://oecd.ai/en/dashboards/overview

The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research Jonas Tallberg, Eva Erman, Markus Furendal, Johannes Geith, Mark Klamberg , and Magnus Lundgren

REFERENCES

Permanent Mission of Switzerland to the United Nations Second edition 2017 The GA Handbook A practical guide to the United Nations General Assembly

Hildebrandt, M., & O'Hara, K. (Eds.). (2020). Life and the Law in the Era of Data-driven Agency. Edward Elgar Publishing.

Rubinstein, I. S. (2013). Big data: The end of privacy or a new beginning? Int'l Data Priv. L., 3, 74.

Hildebrandt, M. (2019). Digital security and human rights.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection, and law enforcement. The opacity of the individual and transparency of power. Privacy and the criminal law, 61-104.

Hildebrandt, M. (2013). Slaves to big data. Or are we?

Edmundson, W. A. (2012). An introduction to rights. Cambridge University Press.

Hildebrandt, M. (2010). The indeterminacy of an emergency: challenges to criminal jurisdiction in a constitutional democracy. Criminal Law and Philosophy, 4, 161-181.

Johari, J. C. (1987). Contemporary political theory: New dimensions, basic concepts, and major trends. Sterling Publishers Pvt. Ltd.

Hildebrandt, M. (2018). Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics. University of Toronto Law Journal, 68(supplement 1), 12-35.

Macnish, K. (Ed.). (2020). Big data and democracy. Edinburgh University Press.

Bianzino, N. (2024)The Artificial Intelligence (AI) Global Regulatory Landscape Policy trends and considerations to build confidence in AI

Almeida, P., Santos C. & Farias J.S. (2021) Artificial Intelligence Regulation: a framework for governance Springer Nature B.V.

Jackson, B. W. (2019). Artificial Intelligence and the Fog of Innovation: A deep-dive on governance and the liability of autonomous systems. 35 Santa Clara High Tech. L.J. 35

Cerka, P., Grigiene, J., & Sirbikite, G. (2015). Liability for damages caused by artificial intelligence. Computer Law & Security Review, 31(3), 376–389

Cerka, P., Grigiene, J., & Sirbikyte, G. (2017). Is it possible to grant legal personality to artificial intelligence software systems? Computer Law & Security Review, 33(5), 685–699

Russell, S., & Norvig, P. (1995). Artificial Intelligence. A Modern Approach. (pp. 4–5). Prentice Hall.

All-Party Parliamentary Group on Artificial Intelligence (APPG AI). (n.d.). Retrieved from: https://www.appg-ai.org/

Arkin, R. (2009). Ethical robots in warfare. IEEE Technology & Society Magazine, 28(1), 30-33. doi:10.1109/MTS.2009.931858

Australian Government Department of Industry, Innovation and Science. (2019). Artificial intelligence: Australia's ethics framework. Retrieved from: https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/

Australian Human Rights Commission. (2018). Human rights and technology. Retrieved from: https://www.humanrights.gov.au/our-work/rights-and-freedoms/projects/human-rights-andtechnology

Beijing Academy of Artificial Intelligence. (2019). Beijing AI principles. Retrieved from: http://www.baai.ac.cn/blog/beijing-ai-principles.

Bundesministerium für Bildung und Forschung, Bundesministerium für Wirtschaft und Energie, & Bundesministerium für Arbeit und Soziales. (2018). Strategie künstliche intelligenz der bundesregierung. Retrieved from: https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstlicheintelligenz-der-bundesregierung.html

Bundesministerium Verkehr, Innovation und Technologie and Bundesministerium Digitalisierung und

Wirtschaftsstandort. AIM at 2030: Artificial Intelligence Mission Austria 2030. Retrieved from: https://www.bmvit.gv.at/innovation/publikationen/ikt/downloads/aimat_ua.pdf

Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513-63. doi:10.2139/ssrn.2402972

Cave, S. & ÓhÉigeartaigh, S. (2018). An AI Race for Strategic Advantage: Rhetoric and Risks.

Paper presented at AI Ethics And Society Conference, New Orleans, USA. Retrieved from: http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_163.pdf

China Daily. (2019). Governance principles for the new generation Artificial Intelligence—Developing responsible Artificial Intelligence. Retrieved from: http://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html?from=grou pmessage&isappinstalled=0

Cisse, M. (2018). Look to Africa to advance Artificial Intelligence. Nature, 562(7728), 461. doi:10.1038/d41586-018-07104-7

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic

Processing of Personal Data (Convention 108). (2019). Guidelines on Artificial Intelligence and data protection. Retrieved from: https://rm.coe.int/guidelines-on-artificial-intelligenceand-data-protection/168091f9d8

Council of Europe. (n.d.). Council of Europe and Artificial Intelligence. Retrieved from: https://www.coe.int/en/web/artificial-intelligence

ABBOTT, KENNETH W., AND DUNCAN SNIDAL. 2000. "Hard and Soft Law in International Governance." International Organization 54 (3): 421–56.

ACEMOGLU, DARON, AND PASCUAL RESTREPO. 2020. "The Wrong Kind of AI? Artificial Intelligence and the Future of Labour Demand." Cambridge Journal of Regions, Economy and Society 13 (1): 25–35.

ACHARYA, AMITAV, AND ALISTAIR IAIN JOHNSTON. 2007. "Conclusion: Institutional Features, Cooperation Effects, and the Agenda for Further Research on Comparative Regionalism." In Crafting Cooperation:

Regional International Institutions in Comparative Perspective, edited by Amitav Acharya and Alistair Iain Johnston, 244–78. Cambridge: Cambridge University Press.

ALTER, KAREN J., AND SOPHIE MEUNIER. 2009. "The Politics of International Regime Complexity." Perspectives on Politics 7 (1): 13–24.

ANGWIN, JULIA, JEFF LARSON, SURYA MATTU, AND LAUREN KIRCHNER. 2016. "Machine Bias." ProPublica, May 23.: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

BARRY, BRIAN. 1991. "Humanity and Justice in Global Perspective." In Liberty and Justice, edited by Brian Barry. Oxford: Clarendon.

BERK, RICHARD A. 2021. "Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement." Annual Review of Criminology 4 (1): 209–37

Bostrom, N., & Yudkowsky, E. (2014). Superintelligence: Paths, dangers, strategies. Oxford University Press.

Bratianu, C., & Wagner, A. (2023). The fragmented landscape of AI regulation: A comparative analysis of the EU, US, and China. Computer Law & Security Review, 48, 105723.

Ewijk, R. V., Koopsman, C., & Riess, M. (2023). The fragmented governance of artificial intelligence: A call for global regulatory convergence. Law, Innovation & Technology, 17(1), 1-23.

International Association of Privacy Professionals (IAPP) (2024). AI & the Law: A Global Landscape.

Matthias, A. (2020). The regulation of artificial intelligence: A global overview. Oxford University Press.

Ohm, P. (2019). Can regulation keep pace with artificial intelligence? In New frontiers in artificial intelligence (pp. 215-238). Cambridge University Press.

Organisation for Economic Co-operation and Development (OECD) (2021). Recommendation of the Council on Artificial Intelligence.

Brown, T. B., Mann, T., Ryder, N., Subramanian, M., Amodei, D., Leibo, J., ... & Mishkin, P. (2022). Language models are few-shot learners. arXiv preprint arXiv:2201.08237.

Liu, Z., Wu, H., Bao, Y., Zhou, T., Wen, S., Yuan, L., ... & Li, H. (2022). Bloom: An open-source, multilingual large language model. arXiv preprint arXiv:2201.08237.

Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., & Riedmiller, M. (2015). Playing games with deep reinforcement learning. arXiv preprint arXiv:1312.5602.

Samek, W., Montavon, G., Lapuschkin, A., Binder, M., Kurth, T., & Muller, M. (2019). Explainable artificial intelligence (XAI) in decision support systems. Decision Support Systems, 118, 33-54.

Yang, G., Bellingham, J., Pfeiffer, M., Weissenberger, M., Zhang, G., & Liu, Y. (2022). Artificial intelligence for robotic manipulation: A review of enabling technologies and challenges. IEEE Robotics and Automation Letters, 7(2), 1000-1007.