CSTD

MUNMX RO 2023, Campus Morelia

The chair composed by Ximena Lozano, Valeria López, and Mariana Enriquez, wishes to welcome all of the delegates who are part of the committee CSTD. During this model, we will discuss topics related to the advancement of technology that are of relevance and importance in an international forum. The chair hopes the delegates can have a great experience through the acquisition of knowledge through the discussion of different international perspectives.

Ximena Lozano Guardado
President

Valeria López Rodriguez
Moderator

Mariana Enriquez Reyes
Conference Officer

The Commission on Science and Technology for Development (CSTD) is a subsidiary body of the Economic and Social Council (ECOSOC). This forum looks forward to discussing critical issues about technology and science in order to acknowledge their effects on present and future generations. The origins of this Commission were held in Vienna in 1979 with the UN Conference of Science and Technology for Development. In 1992, the CSTD was transformed into a functional commission of the Economic and Social Council (ECOSOC). The commission is composed of 43 active members.

The main objective of the CSTD is to provide solutions to the Economic and Social Council and the General Assembly. This is accomplished through the analysis and appropriate policy recommendations.

Topic A: Regulation of use and purposes of Artificial intelligence

Abstract

Artificial Intelligence is defined as a system that resembles human capacities because of its facility to process data automatically and learn new information in the same way as a human brain.

The development of Artificial intelligence during the last few years has engendered a highly impactful change in society. AI is now capable of helping individuals find solutions to the world's most urgent problems by taking into account statistics and analyzing significant amounts of data in a brief period of time, something that a human being could not achieve. In addition, AI has become a significantly useful tool in different fields, such as healthcare, cybersecurity, commerce, education, human resources, automobiles, and social media, among others.

However, as this type of technology started to evolve, ethical concerns about its use also arose. Even though AI makes life easier for humans, 300 million people have lost their jobs around the world due to this technology being capable of doing their work in a faster, more efficient, and less expensive way. Besides, other fields, such as the educational field, have been affected because of this technology. Students are now heavily reliant on AI to do all their work, promoting negligent behavior within their careers.

As the presence of artificial intelligence grows bigger each day, delegations must look for regulations that balance the use of this technology. Taking into account that the solution must not forbid its use and must instead encourage partnership between artificial intelligence and humans, thus making progress towards achieving the Sustainable Development Goals and the Secretary General's Common Agenda.

Statistics and General data
• According to Forbes, the AI market size is projected to expand 37.3% at an annual rate from 2023 to 2030. • AI is projected to reach $1,811.8 billion by 2030. • AI is expected to contribute $15.7 trillion to the global economy by 2030 • AI will replace nearly 85 million jobs worldwide by 2025. • The system works by analyzing large data of correlation patterns and using the patterns to make and form predictions about the future states of something that is being analyzed. • In 2022 the increase of the use has escalated globally, China has the highest rate of developing AI with a 58% adoption rate, followed by India with 57%. When talking about the exploration of new technologies Canada and the USA take the lead. • Europe spent more than 1.4 billion dollars in late 2022 on Artificial Intelligence.

Solutions

There are many solutions to accomplish the regulations and manage the control of the expansion and uses that are given to Artificial Intelligence. Since the last couple of years, Artificial Intelligence has been increasing to the point where it is hard to recognize the difference between things done with AI or not. Due to the concerns of this, the European Union Parliament created new regulations (AI Act) concerning technology's quick advance and how it is trespassing safety systems. This new regulation will make sure all AI systems are safe, transparent, traceable, non-discriminatory, and environment-friendly.

The new rules will categorize AI systems into different statuses like: unacceptable risk, where the system is completely banned, and could be like applications that compromise subliminal techniques, exploitation systems, or even social scoring systems are strictly prohibited. Also, biometric identifications are prohibited under any circumstance. High risk will be divided into two categories: limited risk where if a person is talking with a chatbot needs to be informed. And minimal risk where examples could be: spam filters, AI-enabled videogames, and inventory management systems. And last,

generative AI. The European Parliament has yet to completely approve these new rules, the last meeting about this was on the 14 of June 2023. But is expected to reach an agreement by the end of this year. The Parliament will try to dialogue with the European Commission to accomplish a provisional agreement until the new legislation is approved. An agreement that is acceptable for both. The Commission acts as a mediator. This provisional agreement must be adopted by each institution's legal procedures and laws.

However, besides Europe, there are many countries that are taking action to regulate artificial intelligence. For example, in Asia, China started the “Next Generation Artificial Intelligence Development Plan” in 2017, which are laws regulating these systems. Japan is a country that encourages AI development, it has its own regulations. In America, the United States created the “BluePrint for an AI Bill of Rights” where all legislations control the uses of AI like algorithmic discrimination protections, data privacy, notice and explanation, etc. The United States rules are the most strict, so it is believed that are the ones that will have a bigger impact globally. As an example, the country of Canada, in June 2022 created the Artificial Intelligence and Data Act (AIDA) that aims to regulate international and provincial trade between AI systems, this act prohibits certain actions. As said, there are many legislations that encourage the regulations of these systems but there isn't a global approach where all countries are involved.

Guide questions

- ➔ The power of AI systems is growing very fast. Were knowledge and creative jobs thought to be less exposed to AI disruption? Is this still true? Will any occupation escape the impact of AI?
- ➔ Are our societies ready to deal with AI, for jobs, human rights, civic and political participation, or ethics?
- ➔ Can education help make AI more likely to enhance workers’ abilities rather than replace them? What needs to change in education policies and practices for this to happen?
- ➔ Given that AI does is not currently present in most of the world, is it ethical or equitable to allow it to have an increasing role in managing global systems? Is there a risk that AI development will escape the regulatory power of governments?

- ➔ Can an open innovation approach for AI offer an alternative model that is more amenable to the ethical and equitable imperatives that matter for developing countries? How shall the rights issue in relation to AI and emerging technologies be addressed?
- ➔ How can international cooperation help solve these issues?

Sources suggestions

- 24 top AI statistics and Trends in 2023
  Organization: Forbes
  Date: August 25, 2023
  Link: 24 Top AI Statistics & Trends In 2023 – Forbes Advisor

- The world factbook
  Organization: CIA
  Date: January 2019
  Link: The World Factbook - The World Factbook (cia.gov)

- Artificial Intelligence worldwide statistics and facts
  Organization: Statista
  Date: Sep 21, 2023
  link:
  https://www.statista.com/topics/3104/artificial-intelligence-ai-worldwide/#editorsPicks

Delegates, the chair hopes the committee reaches a democratic and pacific solution, considering the needs of each country and cooperating with each other. It is a priority to use technology as a tool for the development of our present and future generations. The solution must seek the prevalence of the positive aspects that using artificial intelligence has, and the contributions it has for our society.

References

Wade,V.(2022.) Blueprint for AI Bill of Rights. Retrieved from: https://www.whitehouse.gov/ostp/ai-bill-of-rights/#applying

Haan, K. (2023, 25 abril). 24 Top AI Statistics and Trends in 2023. Forbes Advisor. https://www.forbes.com/advisor/business/ai-statistics/

Horgen,D.(2023.) The EU Artificial Intelligence Act. Retrieved from: https://www.artificial-intelligence-act.com/

NA.(2023.) How governments are looking to regulate AI. Retrieved from: https://www.eiu.com/n/how-governments-are-looking-to-regulate-ai/

Benedikt,J.(9 May 2023.) AI Regulation around the world. Retrieved from: https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world

Nations, U. (2023, March 29). *26th CSTD side event: The multi-faceted implications of ai*. UNCTAD. https://unctad.org/meeting/26th-cstd-side-event-multi-faceted-implications-ai

Topic B: The use of false online identities in order to carry out kidnappings or extortions

Abstract

Our daily activities lead us to expose our personal information and identity on the internet. The fact that each day people's lives are more dependent on technology makes our security vulnerable. Most of the time people are not conscious of the risk of offering their personal data. For example, when using social media, buying something, or registering on any online platform, people are exposing personal information, like phone numbers, mail, location, private photos, personal documents, and private conversations.

This phenomenon led to the creation of false online identities and identity theft. It happens when a party uses falsely created personal information, in a non-authorized way or they take control of the usernames, and passwords, to impersonate someone else. As examples of criminal actions are the creation of social media accounts: including facebook, Instagram, tiktok, and Twitter, among others, to get an individual's personal information and use it to take advantage of their own. They could also make calls to deceive with the idea of being an important institution or known person. The most common crimes that involve the use of false online identities are stealing funds, accessing confidential information, kidnapping, extortions, or engaging in tax or health insurance fraud. Through the analysis of data and statistics it has been established that kidnapping and extortions are the crimes most relevant nowadays, therefore it is necessary to know them deeply. They have been more prevalent in the past years and they lead to more types of cyber crime according to the OECD.

Policies for the protection of data differ in each country. For that, the General Data protection Regulation arose in 2018. This new regulation was the answer for the EU countries and their data protection. It was only adopted by the EU but it has served as a model for the creation of new regulations around the world. It was the case of the CCPA in California and the LGPD in Brazil, they have the same bases as in the GDPR.

Statistics and General data
Social media kidnapping statistics and information: ● The NCMEC (National Center for Missing and Exploited Children) received more than 21.7 million reports in 2020. ● According to the FBI, there were 365,348 reports of missing children. ● The majority of children accept friend requests immediately. Without caring if they know the person. ● 56% of parents expose information about their children online. ● An estimated 500,000 criminals use online platforms to target children according to the FBI. ● 1 in 4 children freely share personal information online when asked.
Internet crime report (2022) of the FBI victims of the use of false identities that are related to extortion and kidnapping: ● extortion 39,416 ● Identity Theft 27,922 ● Phishing 300,497 ● Personal Data Breach 58,859 ● BEC 21,832 ● Spoofing 20,649 ● Confidence/Romance 19,021 ● Employment 14,946 ● Government Impersonation 11,554 ● Advanced Fee 11,264 ● Lottery/Sweepstakes/Inheritance 5,650

Solutions

There are 3 most recommended actions presented by several associations and countries to contrast the use of false online identities and its effects, they are:

1- Prevention

Bases: The first solution to reduce the number of victims is to create a conscious society, having prepared individuals reduces vulnerability at the time of exposing personal data. Through knowledge and elimination of ignorance situations of extortions and kidnapping could be prevented. Involved associations and countries:

- UNODC, which has a specific program for preventing kidnapping.
- Non-governmental associations like "Maria de los Angeles foundation" in Argentina which fights against all forms of human trafficking since 2007.
- In may 2006, The US Federal Trade Commission launched "Deter, Detect, Defend" an education campaign on ID theft, personal information, and reaction when ID theft is suspected.
- Countries with education and prevention initiatives: united kingdom, united states, netherlands, australia, mexico, belgium.

2-International cooperation

Bases: International cooperation in combating false online identities is difficult because each country has a different idea about how to combat the issue and have a different view on the limits of privacy invasion, and a different system for regulation and granting jurisdiction, although it is considered that is indispensable acting through the idea that investigation and mutual legal assistance agreements are the only way to have an agile and fast answer. to the problem. Involved associations and countries:

- European Union Data Protection Directive, designed to restrict data collection since 1998.
- Safe Harbor Agreement (under the EU Data Directive) in May of 2000 United states entered into the initiative of the EU.
- The Council of Europe introduced the Budapest convention, the first international treaty on crimes committed via the Internet and other computer networks. Since 2001 till now. It has 68 parties.
- London Meeting Draft proposed to create a forum for discussion on multinational identity theft issues.

- The convention on Cybercrime provides a legal framework for international cooperation. Ii includes the global communication system of interpol as well as the national central reference points, network of investigation in more than 120 countries. Brazil, Japan and Ukraine participate providing legal assistance.
- The African Union Convention on Cyber Security and Personal Data Protection since 2014.
- The League of Arab States' Arab Convention on Combating Information Technology Offences since 2010.

3-Protection of data

Bases: Conscientizing individuals about how users are responsible for the shared data and promoting techniques to protect information like the use of passwords, recognition of apocryphal pages, avoid accessing non-official websites, understating how social media works, respecting the alignments established by websites like the age requirements, how to report identity theft, the right of people to deny proportioning any information, deleting data on internet browsers. Involved associations and countries:

- OECD-with its policy guidance on online identity theft.
- FBI, the responsible of investigation in order to generate statistics to promote the responsible exposure of data.
- All countries involved in prevention and international cooperation.

Guide questions

- ➔ Since social media privacy policies are different in each country caused by the difference in the legal regime, which tools of privacy are adopted in the delegation?
- ➔ What are the laws in the delegation that protect the integrity of individuals at the time of being victims of the use of false online identities? The national regulation on kidnapping and extortions.
- ➔ Which are the most vulnerable groups affected by false online identities?
- ➔ What programs for prevention the delegation is putting in practice?
- ➔ What consequences are applied to those who commit a crime by using a false online identity?

➔ What treaties and alliances do your delegations have in terms of international cooperation in order to reduce cybercrimes?

Sources suggestions

- Formal international cooperation mechanisms
  Organization: UNODC
  Link:
  https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html2022 IC3 Report.pdf

- Manual sobre los delitos relacionados con la identidad
  Organization: UNODC
  Link: https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

- Suplantación de la identidad digital con fines de trata de personas en facebook
  Organization: INFOTEC
  Date: January 2019
  Link: INFOTEC_MDTIC_EAB_26092019.pdf (repositorioinstitucional.mx)

- The world factbook
  Organization: CIA
  Date: January 2019
  Link: The World Factbook - The World Factbook (cia.gov)

The chair hopes the committee reaches the best solution. This will be achieved after a debate in which the delegates will present the position of their delegations on this highly relevant issue. By generating these solutions, we are closer to achieving the SDG's.

References

Action against Cybercrime. Counsil of europe. (n.d.). https://www.coe.int/en/web/cybercrime/home

Aguilar, E. (2019, January). *SUPLANTACIÓN DE LA IDENTIDAD DIGITAL CON FINES DE TRATA DE PERSONAS EN FACEBOOK*. INFOTEC. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf

A world wide problem on the World Wide Web: International Responses to ... (n.d.-a). https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1314&context=law_journal_law_policy

Cybercrime module 7 key issues: Formal International Cooperation Mechanisms. UNODC. (n.d.). https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

Identity-related crime. United Nations : Office on Drugs and Crime. (n.d.). https://www.unodc.org/unodc/es/corruption/identity-related-crime.html

-*Internet crime complaint center (IC3)*. Internet Crime Complaint Center(IC3) | Annual Reports. (n.d.). https://www.ic3.gov/Home/AnnualReports

Jacimovic, D. (n.d.). *9 shocking social media kidnapping statistics 2023*. Techjury. https://techjury.net/blog/social-media-kidnapping-statistics/

OECD policy guidance on Online Identity Theft. (2008). https://www.oecd.org/sti/consumer/40879136.pdf

Manual sobre Los Delitos Relacionados con la identidad. (n.d.-b). https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Muntingh, L. (2023, February 20). *2022 social media kidnapping statistics*. Screen and Reveal. https://screenandreveal.com/social-media-kidnapping-statistics/