Forum: United Nations Commission On Science and Technology for Development

Issue #11-01 : Addressing the regulation of Artificial Intelligence regarding its impact on the privacy and well-being of society

Student Officer: Daniel Igualada and Abel Resende

Written by: Abel Resende, Juan Estevez, Daniel Igualada, Onat Ergin

Introduction

We are at the dawn of a new era. The technological revolution is rapidly changing our lives, drastically affecting how we work, learn, and even live together. Then, the question is "How could we adapt to these drastic changes?" However, before that, these drastic changes should be defined.

Artificial intelligence is the development of a computer program designed to perform tasks typically done by humans. It involves the simulation of intelligent behavior in a machine, in response to inputs it receives. There are many ways in which this technology can be applied, but AI's broad applicability means that the potential impact of this technology on our society is very real and currently evolving at a very rapid pace. This rapid pace promises a whole new world and civilization. Yet, the main principle of AI isn't to replace human intelligence. To guarantee that technology should be developed with humanist principles and morals. For example, it should not violate privacy laws while collecting data and processing them. The ethics of Artificial Intelligence is a current debate topic and it seems like there will be discussions for quite a while.

Data collection and advertising technology have progressed a lot within years with the help of AI. For that, the European Union (EU) passed The General Data Protection Regulation GDPR) (Document ID: 2016/679) in 2016 and it was implemented in 2018. Data sets collected from consumers to be processed, analyzed, and to be used in the future or Big Data is crucial for Artificial Intelligence to develop. Therefore, there is a challenge about the relationship between privacy and AI: the tighter the privacy protection, the more difficult it may be to access considerable data sets for further work. If strong privacy laws are implemented in the future, it will restrict AI's workforce specifically in the fields related to marketing. Again, if privacy laws prevent companies from collecting too much data regarding buying decisions, AI may shift its focus from marketing to sustainable development. Instead of human manipulation and behavioral control, it may focus on education, medical applications, etc. However, AI in the marketing sector will still be used. So, regulating AI developments and thus, complying with the democratic and humanitarian frame is necessary.

Moreover, UNESCO works towards establishing that ethical frame. For example, "in terms of gender equality, we must fight against the biases in our societies to guarantee that they are not reproduced in AI applications" and "eliminating fragmentation between countries and genders, but also in terms of resources and knowledge, could enable more people to contribute to the digital transformation underway" ("Towards and Ethics").

Lastly, regulation of AI is crucial regarding the rapid developments in AI. If not regulated, possible violations of data protection laws are possible. Besides, the studies to ensure the wellbeing of society should be enhanced so the benefits of AI can be maximized.

Definition of Key Terms

Artificial Intelligence (AI)

Refers to an automated system with the ability of analyzing data and making choices autonomously. There are two different type of AI:

- **Weak AI:** A weak AI is a machine that simulates a specific human behavior.
- **Strong AI**: Is a machine able to reproduce a human behavior while learning and recording it, therefore having its own reasoning, and developing their own knowledge.

Online Privacy

Online privacy is the level of privacy protection an individual has while connected to the internet or any browser. Internet users often try to increase their online privacy by installing antivirus software, strong passwords, turning their locations and tracking off.

Online Security

Similar to online privacy, online security covers the amount of security available for a person relating to financial data, communications and preferences.

Privacy of Data

Privacy of data is the security of the information about yourself that you have in your mobile devices. This includes your photos, your documents, your contacts, your personal information and more.

Privacy Identity

Privacy of identity is the right you as a citizen of the world have of remaining anonymous online unless you willingly show it.

Privacy location

Privacy to location is the right you have of being anywhere you want without the government or any organization knowing your location. Unless you willingly allow it.

Internet

A global computer network that provides users with a variety of information, activities, and communications facilities.

General Overview

As the internet evolved and developed in the past ten years, privacy concerns increased drastically around the world. The decade's most significant internet privacy controversies redefined the relationship between multinational tech companies and governments. In 2013, the Snowden disclosures raised the world's ire due to the U.S. government accessing private data from hundreds of millions of citizens internationally. This scandal raised alarms on A.I. implementations to manage personal data and drove the creation of new regulations. American tech companies such as Microsoft and Google responded by increasing and expanding encryption and protecting their customers' data through litigation.

However, five years after the Snowden disclosures, the tech sector faced another backlash due to the Cambridge Analytica data scandal. The controversy included American technology conglomerate Facebook, and digital privacy became a highly discussed political issue worldwide. Over the years, new privacy laws started to be integrated into the political, legislative, and technological fields.

According to the United Nations Conference on Trade and Development (UNCTAD), 128 out of 194 countries have pushed legislation to secure the protection of data and privacy. Africa and Asia show a similar level of adoption, with 55% of countries having adopted such legislation, of which 23 are least developed countries. Since 2016, the regulatory and policy landscape for Artificial Intelligence has been an emerging issue in jurisdictions, including in the European Union by the European Parliament, multinational organizations such as International Telecommunication Union (ITU) and many UN organizations such as the United Nations Development Programme (UNDP) and United Nations Educational, Scientific and Cultural Organization (UNESCO).

A.I. is becoming the new humanity frontier as the technological revolution is dramatically altering the ways in which humans interact, learn and live together. According to the United Nations, the guiding principle of A.I. is not to replace human intelligence and capabilities but rather ensure it is developed through a humanist approach based on values and human rights. The upcoming A.I. revolution creates new opportunities and prospects, but due to the social and technological potential power of A.I., its development needs careful consideration.

Snowden global surveillance disclosures on private data in 2013

In June of 2013, The Guardian reported the confidential disclosures based on top-secret documentation accessed by Edward Snowden, an intelligence contractor for Booz Allen Hamilton in Hawaii. Snowden downloaded up to 1.5 million files. Much of the leaked information showed the immoral and illegal use of artificial intelligence integrations with mass surveillance programs to manage private data from millions of citizens worldwide.

The leaks between 2013 and 2014 revealed information on the collection of telephone records from millions of Verizon customers by the United States Department of Defense National Security Agency (NSA). Furthermore, The U.S.

government spied on Venezuelan, Colombian, Argentinian, Panamanian, Ecuadorian, Peruvian, Italian, French, German, Spanish, Brazilian, Qatari, and Indian citizens, companies, and government officials. Moreover, the American National Security Agency built a system capable of recording "100%" of a foreign country's phone calls with an A.I. voice intercept program called MYSTIC. Through a $79.7 million research program, the NSA is working on an A.I. quantum computer that can crack most types of encryption.

The United Kingdom Government Communications Headquarters (GCHQ) has also intercepted phone and internet communications of foreign politicians attending two G-20 meetings in London in 2009. The GCHQ tapped fiber-optic cables to collect and store global email messages, Facebook posts, internet histories, and calls and shared the data with the NSA.

Cambridge Analytica data scandal in 2018

In early 2018, American technology conglomerate Facebook and political data-analytics firm Cambridge Analytica were implicated in a massive data breach. The political data analytics firm had improperly obtained personal data from over 87 million Facebook users through the use of artificial intelligence data scraping programs. In the subsequent months, Facebook testified in the United States Congress and received a $5 billion fine by the United States Federal Trade Commission.

Major Parties Involved and Their Views

United States

The National Security Commission on Artificial Intelligence (NSCAI) was made official with President Trump’s signing of the 2019 National Defense Authorization Act (NDAA) in August of 2018. The Commission comprises 15 members, tasked with assessing the national security implications and ethical considerations of AI.

On March 1st of 2021, the NSCAI submitted its Final Report to Congress and current U.S. President Joe Biden. The report issued an urgent call to action, warning that the U.S. government is currently not adequately resourced or organized to effectively compete with other governments in regards to emerging and innovating technologies. The report also stated that the United States is not sufficiently prepared to defend against AI-enabled threats or to quickly establish AI applications for national security purposes. The report outlined a scheme to make the United States "AI-ready" by 2025.

European Union (EU)

Amidst the rapid technological development of Artificial Intelligence and a global policy context where several countries are heavily investing in AI, the EU has addressed the potential high risks it poses to safety, privacy and fundamental rights prominently. The EU has presented a proposal with strict regulations and a coordinated plan to govern the use of AI. Corporations that contravene the new regulations, could experience repercussions of a fine up to 6 percent of total global sales.

China

In 2017, the Chinese State Council released the "New Generation Artificial Intelligence Development Plan" which is a policy that elaborates on China's plan to create a domestic Artificial Intelligence industry worth roughly $150 billion in the upcoming years and to become the leading AI power by 2030. Although AI has taken a prominent role in China's national strategy, action is being taken to regulate the usage and applications of AI to an extent. In 2019, the China National Information Technology Standardisation Committee announced the plan of establishing an AI technology subcommittee; furthermore, the Big Data Security Standard Special Task Force proposed an AI security standard system. The Chinese government has strategized a specific plan for establishing a legal regime of Artificial Intelligence. The Chinese government has intentions to institute a legal, ethical and policy system of AI regulation by 2025.

Germany

Following the release of the European Union's "White Paper" on Artificial Intelligence in early 2020, the government of Germany has passively agreed with the initiative but has called for tightened AI requirements. Germany believes the criteria for "high risk" are not far reaching and clarified enough therefore they called for the tightening of the classification and requirements. The government sees the need for improvement in the area of human supervision of AI systems and mandatory high IT security standards for AI systems deemed 'high-risk'. Germany also demanded a more direct definition of when and how long data records must be stored on a mandatory basis.

Russia

In October 2019, the Office of the President released a national AI strategy including a list of objectives for the development of AI in the next 10+ years. These goals include creating appropriate standards and a regulatory system that guarantee public safety as well as stimulating the development of AI technologies. The plan also contains principles for the development and use of AI technologies such as the protection of human rights and liberties, technological sovereignty, security, transparency and integrity. On July 1st, 2020 Russia's Federal Law No. 123-FZ was established, introducing a unique legal framework for "digital sandboxes" in Moscow. This law enables companies to work on experimental AI technologies that are unregulated under current legislation. This law does come with some concerns as the law states that the personal data obtained of citizens will be at the disposal of the Moscow city government, along with the entrepreneurs, firms and legal entities registered.

Canada

In regards to Artificial Intelligence, the Canadian government has evidently prioritized funding research rather than developing regulations and governance structures. In 2017, it is estimated that the funding raised by Canadian AI companies would "exceed US$250 million". There are still concerns over the protection of personal information in relation to AI. In February of 2017,the Privacy Commissioner of Canada stated that even with the establishment of 'PIPEDA', obtaining meaningful privacy consent has become substantially difficult in the era of Artificial Intelligence and robotics. The Committee on Access to Information, Privacy and Ethics released a report in February, 2018 which issued concerns over transparency of AI decision-making, and the risk of algorithms using personal user information to "perpetuate prejudices or discriminatory practices." A vital recommendation of the report was that the Canadian government must consider establishing measures to refine algorithmic transparency.

Timeline of Events

Date	**Description of event**
September 2017	The UNICRI signed the host country agreement for the opening of its Centre for Artificial Intelligence and Robotics in The Hague", with a focus on "understanding and addressing the risks and benefits of AI and robotics from the perspective of crime and security through awareness-raising, education, exchange of information, and harmonization of stakeholders."

April 2018	Twenty-four EU Members and Norway signed the Declaration of Cooperation on AI to develop a European approach to AI including cooperation on ensuring an “adequate legal and ethical framework, building on EU fundamental rights and values, including privacy and protection of personal data”.
December 2018	Canada and France announce plans to establish a new international body, aimed at studying and steering the effects of Artificial Intelligence on people and economies globally
October 2019	The Russian Office of the President released a national AI strategy that includes a list of objectives for the development of Artificial Intelligence throughout the next 10+ years.
November 2019	During UNESCO’s 40th General conference, the organization began developing the first normative instrument on the ethics of artificial intelligence with two inter-governmental meetings scheduled for 2021 to finalize these ethical rules based on fundamental human rights.
September 2020	Engineers based across Europe came together to create the report "Addressing Ethical Dilemmas in AI: Listening to Engineers". The report details engineers’ needs and concerns in seeking routes to the development of ethical and responsible AI.
April 2021	The European Commission publishes their Proposal for a Regulation on a European approach for AI, the first-ever legal framework on AI. They also published an update to the 2018 Coordinated Plan

UN involvement, Relevant Resolutions, Treaties and Events

It's impossible for UN to impose strict restrictions on Artificial Intelligence; however, it's more convenient to secure field that AI technologies may harm ie. data protection.

- "Deeply concerned that electronic surveillance, interception of digital communications and collection of personal data may negatively impact human rights, the United Nations General Assembly has adopted a consensus resolution strongly backing the right to privacy, calling on all countries to take measures to end activities that violate this fundamental 'tenet of a democratic society' " ("General Assembly backs")
- United Nations has initiated the Global Pulse Initiative in 2016.
- European Union (EU) passed The General Data Protection Regulation GDPR) (Document ID: 2016/679) in 2016 and it was implemented in EU countries in 2018.
- The International Telecommunication Union (ITU), a United Nations specialized agency for information and communication technologies, started yearly publishing a report titled "United Nations Activities on Artificial Intelligence" in 2018:
  - United Nations Activities on Artificial Intelligence (AI) 2018
  - United Nations Activities on Artificial Intelligence (AI) 2019
  - United Nations Activities on Artificial Intelligence (AI) 2020

Past action

Artificial Intelligence has been rapidly growing and nations all over the world have not stayed behind to keep up with the new technologies and create new legislations and policies that protect citizens rights to privacy.

European Union Brussels Conference

Some of the nations which have been most active in creating a policy regarding the usage and development of AI have been the nations which make up the European Union. The EU Brussels Conference took part on February 19th of 2020. They claimed the following: "Artificial Intelligence is developing fast. It will change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine. At the same time, Artificial Intelligence (AI) entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes." (Commission President Ursula von der Leyen). The European Commission then proceeded to pass this new legislation and guidelines that users and developers would need to follow in their territory.

China's state council releases new Guidelines for the country

In July 2017, the Chinese Government released to the public their new strategy and guidelines to approach this issue. It was named the New Generation Artificial iIntelligence Development and Regulation Plan. Such a plan included regulations addressing: big data, personal information, and consumer protection. The state's government intends to establish a legal and ethical system for AI regulation by 2025. China's actions inspired many governments inAsia to take similar preventive measures.

Social Media companies

It has been evident for the past few years that social media and internet browsers have been selling our personal information to advertisers for a while now. Governments are still seeing to what extent this is correct either way

Google founder said, "Some businesses have responded by setting up internal review boards to assess the ethical issues associated with their projects that might have significant ethical consequences. Interestingly, these reviews go beyond trying to protect the human research subjects and touch on the broader question of whether the insights gained from the research might have harmful downstream consequences on a wider population." Overall it is key to know that companies have collected large amounts of information about consumers and have used it for free marketing now it up to governments to hold companies accountable and new guidelines and legislations to be made such as the U.S.A new "McCain National Defense Authorization Act (P.L. 115-232) established the National Security Commission on Artificial Intelligence" (McCain).

Possible Solutions

Over the last decade, privacy laws have continued to spread across the world. The year 2018 saw stronger privacy protections jump from Europe, across the Atlantic, and move to the Pacific, as California's legislature passed a new law that paves the way for action in the U.S capital, Washington, D.C.

However, it wasn't the geographic spread of privacy laws that characterized the decade. Possible solutions centered in Brussels, the European Union effectively embarked on a new era of privacy protection. For instance, the E.U created unique solutions that require websites to give consumers "notice and consent" rights before using their data. Europe's General Data Protection Regulation, or GDPR, provides consumers "access and control" over their data, empowering them to review their data online and edit, move or delete it under various circumstances.

Both these solutions empowered consumers and placed a burden and limitations on them to manage their data. With the volume of data sprouting, the 2020 decade will likely see a new wave of privacy protection with a different emphasis. Rather than simply empowering consumers, possible solutions may adopt new rules that regulate how businesses can use data in the first place. The new regulations will reach data brokers that are unregulated in some key markets today, as well as a focus on sensitive technologies like Artificial Intelligence, including facial recognition technology and protections against the use of data to adversely impact vulnerable populations. It is important for possible future solutions to address ethical and social dilemmas. For example, who is responsible for the conduct and actions that A.I. algorithms commit. The upcoming laws may also analyze the usage of Artificial Intelligence for mass surveillance and its possible regulations to prevent or allow the development and usage of A.I. for warfare.

Sustainable Development Goal (SDG)

Although the advancement of technology and the implementation of artificial intelligence have heavily influenced and revolutionized modern day societies, the growing crisis regarding privacy issues and the impact this has on society has, in recent years, been more proactively addressed by governments and organizations globally. Throughout the past few years, there have been various incidents worldwide that have furthered the mistrust of the public in artificial intelligence and raised the alarm on severe privacy issues facilitated by AI usage. Breaches such as the Snowden disclosures in 2013 is a prime example of this as the U.S. government had been accessing private data from hundreds of millions of citizens internationally facilitated by artificial intelligence. Through the **Sustainable Development Goal 17: Partnerships For The Goals,** nations world wide are actively collaborating with each other to tackle a variety of global issues which encompasses addressing and taking action against A.I. impact on privacy. The United Nations seeks to “Strengthen the means of implementation and revitalize the global partnership”.

Appendix

I. Data Protection and Privacy Legislation Worldwide by the UNCTAD https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

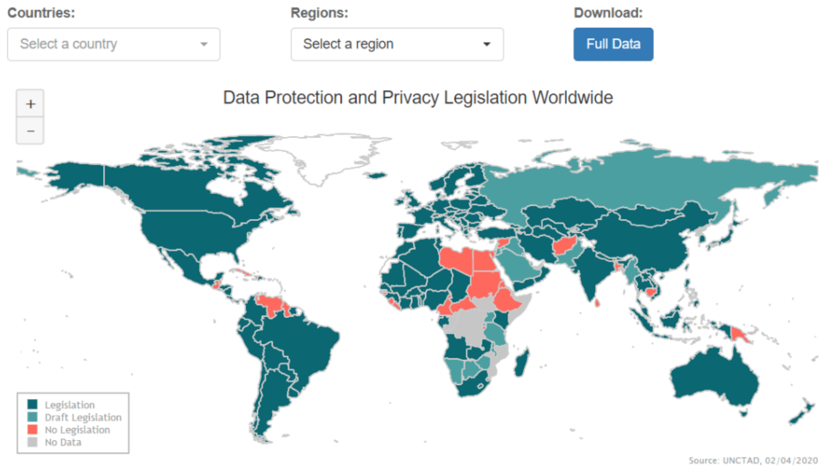
II. Towards an Ethics of Artificial Intelligence https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

III. The Guardian articles and leaks on security and liberty https://www.theguardian.com/commentisfree/series/glenn-greenwald-security-liberty

IV. "Official Legal Text." General Data Protection Regulation (GDPR), 25 May 2018, https://www.gdpr-info.eu/

V. Here you can find a list of links that take you to each countries legislation on privacy and data protection updated in 2021 https://www.lickslegal.com/post/data-protection-and-privacy-mapping-in-the-world

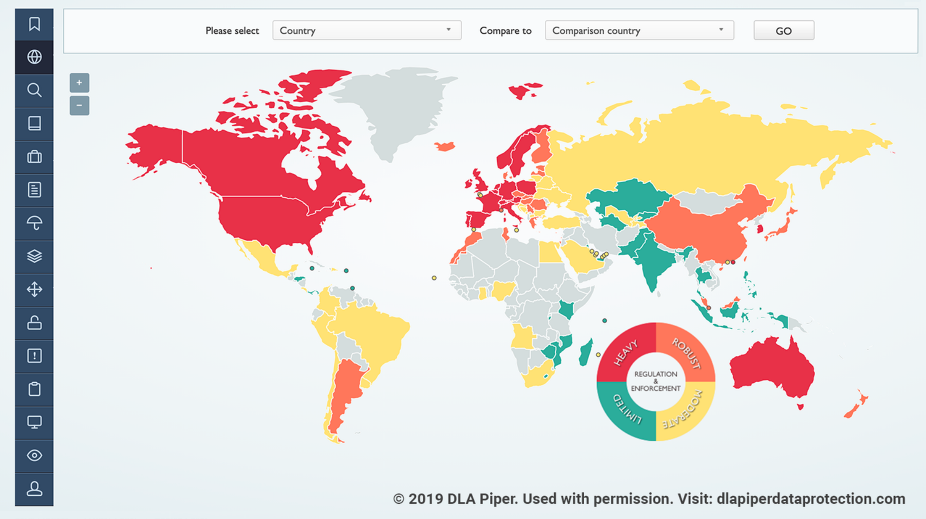
VI.



Data Protection and Privacy Legislation Worldwide

Source: UNCTAD, 02/04/2020

VII.



© 2019 DLA Piper. Used with permission. Visit: dlapiperdataprotection.com

VIII. Video explaining further the legislations by UNESCO https://en.unesco.org/interview-danilo-doneda

Bibliography

Azoulay, Audrey. "Towards an Ethics of Artificial Intelligence." United Nations, www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

"General Assembly Backs Right to Privacy in Digital Age | UN NEWS." United Nations, www.news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age

MacAskill, Ewen, et al. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained." *The Guardian*, Guardian News and Media, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout so Far." *The New York Times*, 4 Apr. 2018, www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout

"Data Protection and Privacy Legislation Worldwide." *UNCTAD*, 4 Feb. 2020, www.unctad.org/page/data-protection-and-privacy-legislation-worldwide

Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" *GDPR*, European Union, 13 Feb. 2019, www.gdpr.eu/what-is-gdpr/

Abrams, Abigail. "Here's What We Know so Far About RUSSIA'S 2016 Meddling." *Time*, Time, 18 Apr. 2019, www.time.com/5565991/russia-influence-2016-election/.

Gesley, Jenny, et al. "Regulation of Artificial Intelligence in Selected Jurisdictions." *DigitalCommons@University of Nebraska - Lincoln*, 2019, www.digitalcommons.unl.edu/scholcom/177/.

Hazlegreaves, Steph. "Cyber Security Threats against Global Governments Increase Exponentially." *Open Access Government*, 30 Oct. 2020, www.openaccessgovernment.org/cyber-security-threats-global-governments-increasing/96789/.

Kavanagh, Camino. "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft SMARTER RESPONSES?" *Carnegie Endowment for International Peace*, 28 Aug. 2019, www.carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

Liu, Wei, and at al, "Resource Guide on Artificial Resource Intelligence ." *Sustainable Development Goals*, UNESCO, Apr. 2021, https://sdgs.un.org/sites/default/files/2021-04/Resource%20Guide%20on%20AI%20Strategies_April%202021_rev_0.pdf

Saran, Samir, et al. "In Pursuit of Autonomy: AI and National Strategies." *ORF Special Report*, Observer Research Foundation, Nov. 2018, www.researchgate.net/publication/332752046_In_pursuit_of_autonomy_AI_and_national_strategies.

"UNESCO's 40th General CONFERENCE Confirms the Organization's Historic Turnaround and ITS Repositioning on Contemporary Issues." *UNESCO*, 29 Nov. 2019, https://en.unesco.org/generalconference/40/results

"Using Artificial Intelligence in Cybersecurity." *Balbix*, 18 Aug. 2020, www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.

Vought, Russel T. "Memorandum for the Heads of Executive Departments and Agencies." *Guidance for Regulation of Artificial Intelligence Applications*, 2019, www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

Wolf, Pam Greenberg; Mark. "Legislation Related to Artificial Intelligence." *National Conference of State Legislatures*, 2021, www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.