



A GLOBAL SURVEY

BY RAINE SAGRAMSINGH

FOR IEEE-USA

VER. 2019.1



Copyright © 2019 IEEE. All rights reserved. Published and hosted by IEEE-USA. Copying this material in any form is not permitted without prior written approval from IEEE/IEEE-USA.

Prepared by Raine Sagrarsingh for IEEE-USA at the request of the IEEE-USA Artificial Intelligence and Autonomous Systems Policy Committee (Chair Mina Hanna).

Corrections, comments, or suggestions should be sent to Erica Wissolik at e.wissolik@ieee.org.

This IEEE-USA publication is made possible through funding by a special dues assessment of IEEE members residing in the United States.

CONTENTS

INTRODUCTION	4
AI COUNTRY CHECKLIST	6
EUROPEAN UNION DATA PRIVACY	8
EU CYBERSECURITY	9
EUROPEAN UNION	10
DENMARK	12
ESTONIA	14
FINLAND	16
FRANCE	18
GERMANY	20
ITALY	22
SPAIN	24
SWEDEN	26
UNITED KINGDOM	28
ARGENTINA	30
AUSTRALIA	32
CANADA	34
CHINA	36
INDIA	40
JAPAN	42
KENYA	44
MEXICO	46
NIGERIA	48
RUSSIA	50
SAUDI ARABIA	52
SINGAPORE	54
SOUTH KOREA	56
TAIWAN	58
TUNISIA	60
UAE	62
ZIMBABWE	64
BIBLIOGRAPHY	66

AI

A GLOBAL SURVEY

INTRODUCTION

Artificial Intelligence (AI) potentially affects all aspects of society in both positive and negative ways. Future regulations and laws regarding the implementation of AI technologies will significantly impact how AI benefits or harms society. Public policies will play a role in encouraging innovation and mitigating possible negative effects.

U.S. policymakers will be confronted with the difficult challenge of reacting to the rapid development and deployment of these new technologies. AI is already deployed in many industries – from banking to agriculture to transportation – and the United States, like many governments, has yet to develop the legal or regulatory tools to control AI’s impact. Even more powerful technology is on the way, and it is critical to establish rules that determine how, when, and if specific technologies can be used.

The United States cannot address AI without considering the global connectedness of companies and economies, both because foreign laws will affect Americans, and because we can learn from the successes and failures of foreign governments. This situation demands that our approach to AI be coordinated with those of other nations. The United States should examine how other countries work to encourage, promote, integrate, and control emerging AI technologies. Addressing the unique public policy challenges of AI will require innovative solutions, and working with other governments will help us get there.

This report provides insight into how other countries approach AI and regulation of related technologies by providing an overview of the national AI strategies of 26 countries. It includes extant laws that address privacy, security, and most importantly, ethics in general as these concerns relate to AI.

For purposes of comparison, the information provided focuses on three areas – regulation of autonomous vehicles, data privacy, and cybersecurity. This report does not cover every country considering AI policies, but rather investigates the most relevant countries, the most innovative countries, and a few surprising/unexpected countries. We hope that the selection of nations discussed here proves to be representative, but also inspirational, as many nations struggle to understand and capture the promise of AI.

DEFINING AI

In October 2016, The Executive Office of the President’s National Science and Technology Council released a document, *Preparing for the Future of Artificial Intelligence*. [1] When addressing the question,



“What is Artificial Intelligence?” the report states, “There is no single definition of AI that is universally accepted by practitioners.”

The White House does offer definitions of Narrow AI vs. General AI. Narrow AI is a system that can complete a single or narrow set of tasks at a level equal to, or better than, human intelligence. General AI is a system able to complete all human tasks at a level equal to, or better than, human intelligence. A system with general AI should also be able to adapt to situations unforeseen at its creation, implying that the system is capable of machine learning, and has all the sensory and decision-making capabilities of a human.

The term AI encompasses many subfields. Often, the term is used as a blanket for one or more subfields. While the list of subfields is ever-growing, some of the most widely discussed include:

- Machine Learning – a computer’s ability to modify its system based off information learned from experience.

- Computer Vision – the analysis and understand of images by a computer system using algorithms.
- Robotics – computer systems that manage controls, sensors, and information processing for mechanical robotic systems.
- Natural Language Processing – the ability of a computer system to analyze and comprehend natural language and speech.
- Data Mining – the use of large datasets to find patterns or anomalies in the data and predict future outcomes.

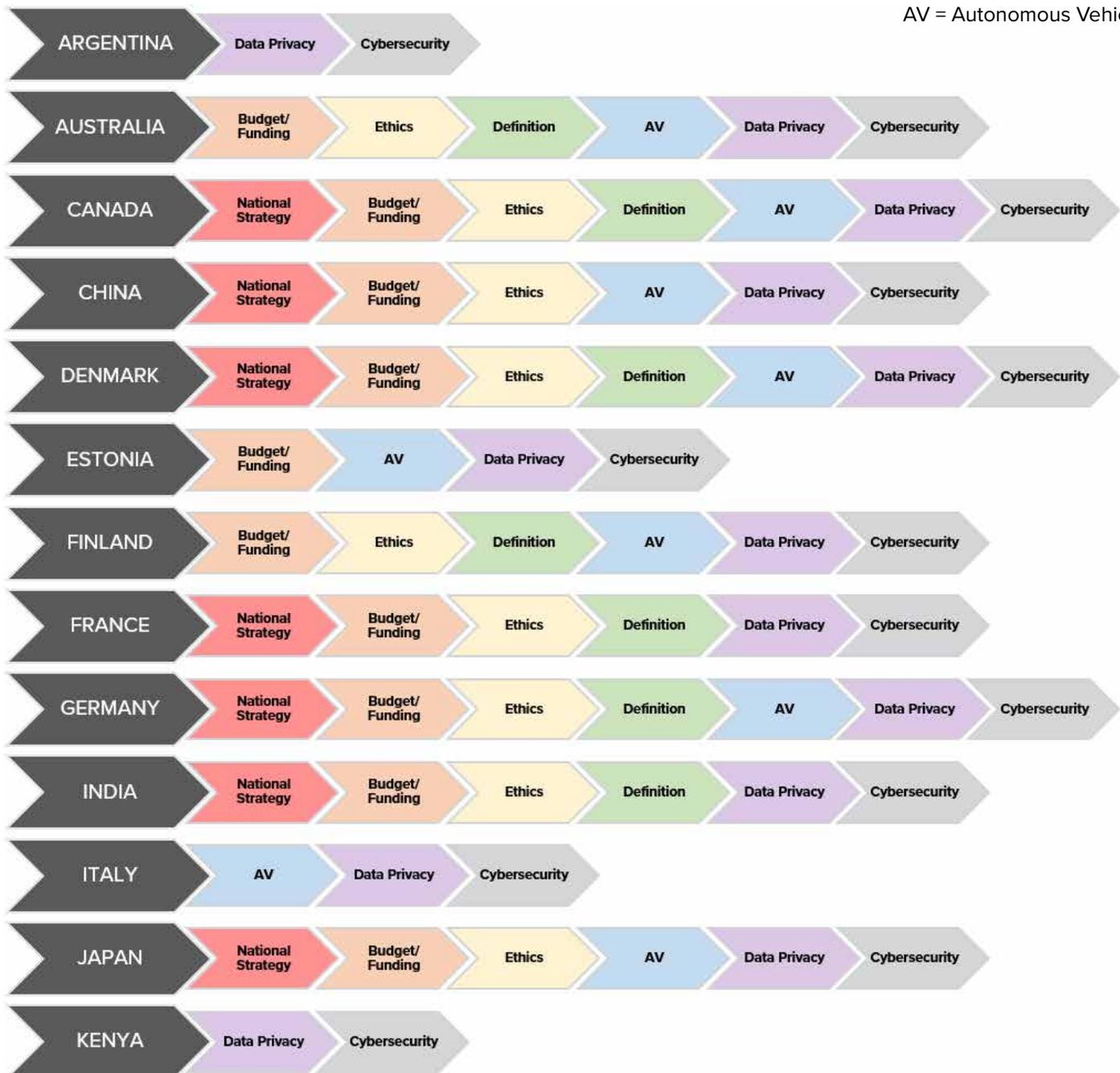
Disclaimer

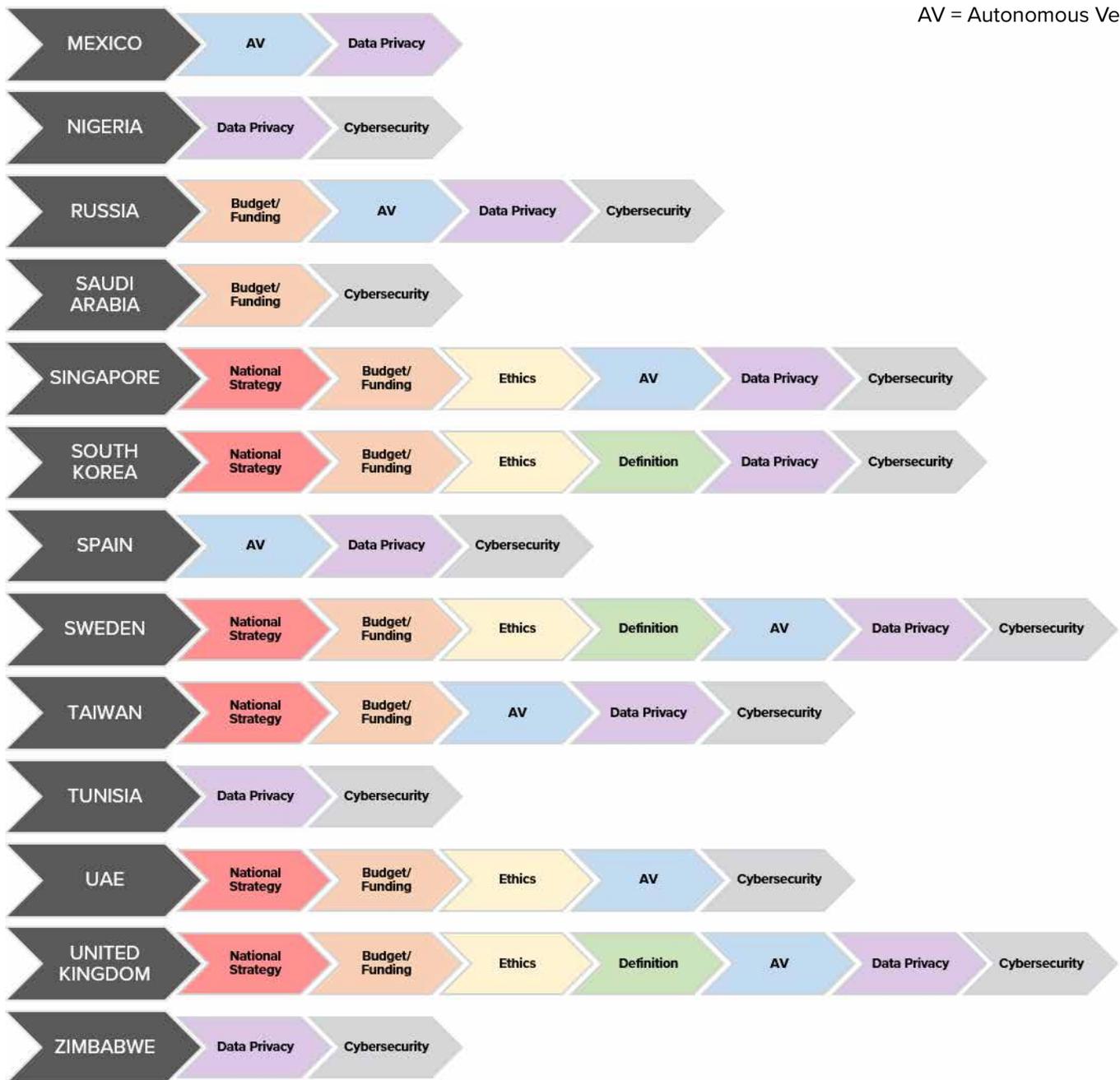
All information contained in this report is current as of publication date, and will be continually updated as the activities of these countries progress. Unless otherwise noted, all budget figures are in U.S. dollars, using mid-2019 exchange rates.

AI COUNTRY CHECKLIST

The countries covered in this survey are at different stages of development in their overall AI adoption strategies and policies. The following chart illustrates the various levels of progress attained or planned.

AV = Autonomous Vehicles





AV = Autonomous Vehicles



EUROPEAN UNION DATA PRIVACY

In May 2018, the European Union (EU) enacted the *General Data Protection Regulation* (GDPR), changing the way organizations must handle personal data in the EU. The GDPR, a directly binding and applicable policy, provides flexibility to individual member states, allowing them to adjust certain aspects of the regulation. However, the GDPR also affects individuals and businesses globally as the scope of the GDPR covers businesses that handle personal data and have a presence in the EU, as well as organizations beyond the EU that provide services to, or process, EU citizens' personal data.[2] The regulation includes areas where individual member states may make their own interpretations, leading to unique, but ideally consistent, GDPR laws in each country.[3] The GDPR includes the following principles for processing personal data [4]:

- a. Lawfulness, fairness, and transparency – data should be processed in a lawful, fair, and transparent way, with respect to the data subject;
- b. Purpose limitation – Data should be collected for specific, explicit, and legitimate purposes and should not be further processed;
- c. Data minimization – Data should be adequate, relevant, and limited to the purpose of its processing;
- d. Accuracy – Data should be accurate, and kept up-to-date, if necessary;
- e. Storage limitation – Data should be kept in a form that identifies the data subject – no longer than is necessary;
- f. Integrity and confidentiality – Data should be processed in a manner that ensures appropriate security of personal data; and
- g. Accountability – The data controller should be able to show compliance with the principles above.

The GDPR's purpose is to give people more control of their personal data, and level the playing field for businesses – by providing the same rules for obtaining, storing, and using the personal data of subjects. [5] The responsibilities of processing personal data under the GDPR require business to: [6]

- Write privacy policies in clear and straightforward language
- Obtain affirmative consent from users to process their data
- Notify users, if their data is transferred outside the EU
- Inform users, if an algorithm is used to make decisions about the user based on the personal data
- Inform users of a data breach
- Allow users to move their data to a competing service
- Provide users with access to their data, and
- Grant users the right to have their data forgotten

The European Commission addresses personal data and AI by ensuring that the GDPR will protect personal data used in AI applications. The GDPR applies to data processing using identifiable data; however, if the data is anonymized then the GDPR does not apply. It also allows automated decision-making pertaining to personal data ,provided there is justification by contract, explicit consent, or law, and that there are safeguards for the individuals involved (e.g., individuals may obtain information about the logic of the decision). [7]



EU CYBERSECURITY

In 2016, the EU adopted the first piece of cybersecurity legislation, *The Directive on Security of Network and Information Systems* (The NIS Directive). The purpose of the NIS Directive is to improve cybersecurity in the EU through preparedness, cooperation, and a “culture of security.” [8]

The NIS Directive addresses cybersecurity in three parts [9]:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities, such as performing cybersecurity exercises.
2. Cross-border collaboration: EU Member States must establish methods of cross-border collaboration, such as Computer Security Incident Response Teams (CSIRTs).
3. National supervision of critical sectors: EU Member States must supervise the cybersecurity of critical market operators in their country (energy, transport, water, health, and finance sectors).

Similar to the GDPR requirements, EU Member States must impose the NIS Directive by updating current laws, or developing new implementation laws. [10]



EUROPEAN UNION

The EU Commission implemented, *Artificial Intelligence for Europe*, in response to the European Council's urgent call to address emerging technologies such as AI. [11] The communication sets forth the need for the EU Member States to join forces and develop a European AI initiative aiming to:

- Boost the EU's technological and industrial capacity and AI adoption across the economy
- Prepare for socio-economic changes caused by AI, and
- Ensure an appropriate ethical and legal framework for using AI



NATIONAL STRATEGY:

Yes – *Artificial Intelligence for Europe* – April 2018. [12]



BUDGET/FUNDING:

The Commission plans to invest \$1.68B from 2018-2020, primarily for AI research and innovation throughout Europe.



NATIONAL FOCUS:

Joining forces among EU Member States to develop a European AI initiative.



ETHICS:

In April 2019, the EU Commission’s High-Level Expert Group on AI presented their *Ethics guidelines for trustworthy AI*. The guidelines state that trustworthy AI should follow applicable laws, follow ethical principles, and be technically and socially robust. The guidelines include seven key requirements for trustworthy AI systems [13]:

1. Human agency and oversight – maintaining ability for human intervention;
2. Technical robustness and safety – AI that is accurate, reliable, reproducible, and safe (e.g., having a plan – in case of unexpected error);
3. Privacy and data governance – respect for data privacy and protection, as well as ensuring quality, integrity and legitimized access to data;
4. Transparency – AI systems and their decisions should be explained, and humans should be aware of their interactions with AI;
5. Diversity, non-discrimination, and fairness – avoiding unfair bias and providing access to all;
6. Societal and environmental well-being – sustainable and environmentally friendly; and
7. Accountability – mechanisms for responsibility and accountability for AI systems and assessments of algorithms, data, and design processes.

DEFINITION OF AI:

“Systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals.” [14]



DENMARK

Together, the Danish Ministry of Finance, and the Ministry of Industry, Business, and Financial Affairs, released the *National Strategy for Artificial Intelligence*, calling “for Denmark to be a front-runner in responsible development and use of artificial intelligence.” [15]. The strategy includes four objectives:

1. Denmark should have a common ethical and human-centered basis for artificial intelligence.
2. Danish researchers should research and develop artificial intelligence technologies.
3. Danish businesses should achieve growth through developing and using artificial intelligence.
4. The public sector should use artificial intelligence to offer world-class services.



NATIONAL STRATEGY:

Yes – *National Strategy for Artificial Intelligence* – March 2019.



BUDGET/FUNDING:

The Danish government earmarked \$9M for 2019-2027 in support of the AI strategy, supplementing \$45M allocated to researching new technologies. [16]



NATIONAL FOCUS:

Denmark as a front-runner in AI focusing on responsible development and use.

ETHICS:

The strategy includes seven initiatives focused on ethical AI:

1. Ethical principles for artificial intelligence
2. Establishment of a Data Ethics Council
3. Security and AI (to ensure AI systems can withstand organized attacks)
4. Legal clarity on development and use of artificial intelligence
5. Transparent use of algorithms by the public sector
6. Ethically responsible and sustainable use of data by the business community
7. Danish imprint on standards for artificial intelligence

The strategy also defines six principles for AI: self-determination, dignity, responsibility, explainability, equality and justice, and development.



DEFINITION OF AI:

“Artificial intelligence is systems based on algorithms (mathematical formulae) that, by analyzing and identifying patterns in data, can identify the most appropriate solution. The vast majority of these systems perform specific tasks in limited areas, e.g., control, prediction, and guidance. The technology can be designed to adapt its behavior by observing how the environment is influenced by previous actions.” [17]

AUTONOMOUS VEHICLES

As a part of the *Danish Road Traffic Act*, Denmark allows the testing of self-driving cars through an application and approval process with the Ministry of Transportation. The individual or organization receiving the permit from the Ministry to conduct testing is liable for all damages that may occur during testing. [18]

DATA PRIVACY

GDPR Implementation Law: *Danish Data Protection Act, 2018* [19]

CYBERSECURITY

NIS Directive Implementation Law: *Danish Requirements for Security of Network and Information Systems within the Healthcare sector, ACT (no. 440/2018)* [20]



ESTONIA

Beginning in 2016, the Estonian Government Office and the Ministry of Economic Affairs and Communications began debating a new “kratt law,” aimed at addressing the implementation of AI. [21] A group of experts are tasked with developing a bill laying out the use of AI and an official national strategy.



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

\$3.3M annually, 2018-2022, to support information and communication technology (ICT) research for six sectors, including AI. [22]



NATIONAL FOCUS:

Currently debating a bill (“kratt law”) to allow development of fully autonomous information systems.

ETHICS:

No official policy on ethics. In his announcement of Estonia’s plan for an AI strategy, Marten Kaevats, Adviser, Strategy Unit of the Government Office, noted that one question which the “kratt law” expert group will address is: When implementing AI systems, who holds responsibility for decisions made by the systems? The task force will answer this question by addressing the ethical, moral and philosophical aspects of AI liability. [23]

DEFINITION OF AI:

No official definition. However, government funding of ITC research includes six focus areas that include AI specifically: artificial intelligence and machine learning; data science and big data; human-robot interaction and the Internet of Things in industrial processes; software reliability; the Internet of Smart Things; and hardware and system security and reliability. [24]



AUTONOMOUS VEHICLES

Since 2017, the testing of self-driving vehicles is legal on all public roads in Estonia, provided a human driver is able to control the vehicle and thereby be legally responsible. In 2018, after studying the entry of self-driving vehicles into Estonia's transportation system, an independent expert group on self-driving vehicles directed by the Strategy Unit of the Government Office, released a report on the risks and possibilities of self-driving cars. The expert group found that "success in implementing the change will depend on a change in attitudes and strategic steps taken at the state level, and the necessary investments in a new type of transportation infrastructure." [25]

DATA PRIVACY

GDPR Implementation Law: *The Personal Data Protection Act Implementation Act (778 SE)* passed February 2019 [26]

CYBERSECURITY

NIS Directive Implementation Law: *Cyber Security Act, 2018* [27]



FINLAND

In 2017, Finland’s Ministry of Economic Affairs and Employment published a report developed by the Steering Group of the Artificial Intelligence Programme, an ongoing working group of experts, to determine the actions necessary to ensure Finland is considered a frontrunner in AI. The report includes eight proposals to propel Finland into development and use of AI applications. [28]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

\$47M through 2027 for the Finnish Center for Artificial Intelligence (FCAI). [29]



NATIONAL FOCUS:

Becoming a frontrunner in the application of AI technology with a focus on business competitiveness, utilization of data, top-level expertise, and public services.

ETHICS:

A 2018 government report, *Work in the Age of Artificial Intelligence*, includes discussion of the intersections of AI with the economy, employment, skills, and ethics. It outlines three values of a good AI Society [30]:

1. Transparency – What and why data is collected, and the aim of the decision-making algorithms;
2. Responsibility – Decision-making by AI should not threaten the health or safety of individuals; and
3. Extensive societal benefits – AI solutions benefit all groups.

The report also lays out six public policy recommendations regarding ethical AI including, building on existing values, AI and healthcare, developing a center of excellence, promoting diversity, following current obligations (e.g., GDPR), and continually updating regulation.

Additionally, Finland is to consider the impact and growth available for AI-driven businesses, the public sector, ordinary citizens, and society – including the question of whether the country should move forward with an active or passive strategy for AI. A passive strategy would allow existing institutions to lead the implementation of AI into life and society. An active strategy would require a national strategy to regulate how AI would be used for the good of society.



DEFINITION OF AI:

“In this report, artificial intelligence refers to devices, software, and systems that are able to learn and to make decisions in almost the same manner as people. Artificial intelligence allows machines, devices, software, systems, and services to function in a sensible way, according to the task and situation at hand.” [31]

AUTONOMOUS VEHICLES

Current legislation in Finland allows trials of automated vehicles. [32] In 2019, several private companies began testing self-driving public transport buses in the Finnish city of Espoo with the aim of rolling out to Helsinki, Vantaa, and other Finnish cities in late 2019. After further testing, Finland plans to begin widespread use of a self-driving mini buses that are already used as part of the Robobus Line in Helsinki. However, it is not clear to the public how these buses will operate, once they begin service, and the extent of human intervention is unknown. [33], [34]

DATA PRIVACY

GDPR Implementation Law: *The Data Protection Act* became effective on 1 January 2019. The process for assessing and amending sector specific laws is ongoing. [35]

CYBERSECURITY

NIS Directive Implementation Law: *Transposed in 2018*. Under Finnish national legislation, industries such as online marketplaces, search engines, cloud providers, and other digital infrastructures are considered operators of essential services, and the requirements are the same as expressed in NIS Directive for digital service providers. [36]



FRANCE

The French AI strategy makes three main commitments: to support French talent in AI, to address the under-exploitation of their large centralized databases, and to establish an ethical framework for utilizing AI. The country's strategy is strongly based on the 2018 *Villani Report*, commissioned by Prime Minister Édouard Philippe; and written by a task force on artificial intelligence under the direction of Cédric Villani, mathematician and Member of Parliament. [37]



NATIONAL STRATEGY:

Yes – *Artificial Intelligence – AI for Humanity* – released March 2018. [38]



BUDGET/FUNDING:

The French government plans to invest \$1.8B in AI research through 2022. [39]



NATIONAL FOCUS:

Address underperformance in innovation, becoming a leader in AI with an emphasis on developing talent, exploiting databases, and addressing ethical issues.

ETHICS:

The French commitment to “establishing an ethical framework” prioritizes the development of fair and transparent algorithms. The government plans to organize an international group of AI experts to prepare and promote education for its citizens. The French strategy also touches on privacy and security regulation accompanying the development of AI, stating, “using aggregated data does not mean impinging on the privacy of users.” Additionally, while one of the French government's goals is to open many of the under-exploited, massive centralized government databases, there will be a European framework accompanying this activity to protect personal data. [40]

DEFINITION OF AI:

“Defining artificial intelligence (AI) is not easy. The field is so vast that it cannot be restricted to a specific area of research: it is more like a multidisciplinary program. Originally, it sought to imitate the cognitive processes of human beings. Its current objectives are to develop automatons that solve some problems better than humans, by all means available.” [41]



AUTONOMOUS VEHICLES

Currently, France requires a human operator to be behind the wheel of a vehicle. Laws surrounding product safety and liability have not yet been adapted to consider autonomous or self-driving vehicles. However, French President Emmanuel Macron announced that the government is developing regulation to allow vehicles with almost total autonomy to be tested and operated on public roads. [42]

DATA PRIVACY

GDPR Implementation Law: *Law concerning the protection of personal data*, 2018 [43]

CYBERSECURITY

NIS Directive Implementation Law: *Decree No. 2018-384*, 2018 [44]



GERMANY

Germany has a comprehensive approach to AI with a detailed national strategy for becoming global leaders in the development and use of AI technologies. The strategy has three key goals:

- Safeguarding the responsible development and use of AI;
- Integrating AI into society ethically, legally, and in a culturally appropriate way; and
- Making Germany and Europe global leaders in the development and use of AI technologies.



NATIONAL STRATEGY:

Yes – *National Strategy for Artificial Intelligence* – released November 2018. [4456]



BUDGET/FUNDING:

\$57M for 2019, with intent to make \$3.4B available by 2025, to implement the national strategy. [46]



NATIONAL FOCUS:

To be global leaders in the development and responsible use of AI, while maintaining ethical and legal standards.

ETHICS:

Germany plans to address ethics and AI through awareness, ethical and legal principles, and societal dialogue. National strategy objectives include:

- “We want to raise awareness...regarding ethical and legal limits of the use of artificial intelligence and to examine whether the regulatory framework needs to be further developed for it to guarantee a high level of legal certainty.”
- “We want to demand and foster compliance with ethical and legal principles throughout the process of developing and using AI.”
- “We will integrate AI in society in ethical, legal, cultural, and institutional terms – in the context of a broad societal dialogue and active political measures.”

The Ethics Commission on Automated Driving also released a report containing guidelines for programming automated driving systems, answering some ethical questions related to AI in vehicles. [47]



DEFINITION OF AI:

German officials base their strategy on ‘weak’ AI, distinguishing it from ‘strong’ AI.

“In highly abstract terms, AI researchers can be assigned to two groups: “strong” and “weak” AI. “Strong” AI means that AI systems have the same intellectual capabilities as humans, or even exceed them. “Weak” AI is focused on the solution of specific problems using methods from mathematics and computer science, whereby the systems developed are capable of self-optimization. To this end, aspects of human intelligence are mapped and formally described, and systems are designed to simulate and support human thinking.” [48]

AUTONOMOUS VEHICLES

In June 2017, Germany passed legislation to allow the use of highly autonomous systems in vehicles. [49] The bill includes three conditions:

1. An alert, licensed driver must be behind the wheel.
2. The car must have manual override to give control back to the driver.
3. A protocol, including appropriate lead time, is required for the vehicle to return control to the driver.

To determine liability, in case of an accident, the vehicle must have a data recorder that specifically keeps track of what or who has control at any given time. Additionally, the government plan for AVs lays out the following elements: [50]

- Automated and connected driving is an ethical imperative, if the systems cause fewer accidents than human drivers (positive balance of risk);
- Damage to property must take precedence over personal injury. In hazardous situations, the protection of human life must always have top priority;
- In the event of unavoidable accident situations, any distinction between individuals based on personal features (age, gender, physical, or mental constitution) is impermissible;
- In every driving situation, it must be clearly regulated and apparent who is responsible for the driving task: the human, or the computer;
- It must be documented and stored who is driving (to resolve possible issues of liability, among other things); and
- Drivers must always be able to decide themselves whether their vehicle data are to be forwarded and used (data sovereignty).

DATA PRIVACY

GDPR Implementation Law: *German Federal Data Protection Act* [51]

CYBERSECURITY

NIS Directive Implementation Law: *Transposed 2018* [52]



ITALY

In March 2018, the Italian Government’s Task Force on Artificial Intelligence of the Agency for Digital Italy published a white paper entitled, *Artificial Intelligence at the Service of the Citizen*. The paper includes recommendations focusing on improving services to citizens and fueling innovation. [53].



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No official budget.



NATIONAL FOCUS:

Implementing AI to improve services to citizens and businesses, and progress daily life in Italy.

ETHICS:

No official policy on ethics. The nation’s white paper discusses the ethical challenges of AI and dedicates a chapter to addressing those challenges. This chapter identifies two groups of people: doom-mongers, who fear AI, and AI enthusiasts. The Italian government’s goal is to balance these two visions, stating, “the use of AI based on algorithms of data analysis in decision-making processes related to social, health, and judicial issues... requires a thorough reflection in terms of ethics.”

DEFINITION OF AI:

No official definition. The white paper states, “What is Artificial Intelligence (AI)? There are many definitions; among them, the one of the University of Stanford, which identifies it as ‘a science and a set of computational techniques that are inspired – albeit typically operating in a different way – by the way in which human beings use their nervous system and their body to feel, learn, reason, and act’”



AUTONOMOUS VEHICLES

As a result of the 2018 budget law, Italy allows test driving of certain autonomous vehicles on specified roads. Cars are required to have a human driver on board during testing, who can take control if something goes wrong. [54]

DATA PRIVACY

GDPR Implementation Law: *DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali” (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174)* [55]

CYBERSECURITY

NIS Directive Implementation Law: Transposed in 2018. *Statutory Instrument No. 360 of 2018*. No changes to the NIS directive, with the exception of a requirement that digital service providers immediately report any data incidents to the Computer Security Incident Response Team Italia (CSIRT). Failure for non-compliance can result in an administrative fine. [56]



SPAIN

In March 2019, the Spanish government held a conference on the *Spanish Strategy for R&D+i in Artificial Intelligence*, during which the Spanish president, Pedro Sánchez, discussed the economic and societal opportunities for Spain. [57]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

Developing a national AI strategy with an emphasis on science, innovation, and universities.

ETHICS:

No official policy on ethics. In his speech, President Sanchez highlighted the need to prevent discrimination and exclusion in AI technologies, and ensure there are no biases based on gender or race. He also stated, “artificial intelligence and all its applications present infinite ethical dilemmas that we will have to deal with quickly, without attempting to shy away from them.” To do this, he recommends including writers, philosophers, and lawyers in the discussion of AI.

DEFINITION OF AI:

No official definition. President Sánchez has discussed current applications of AI and included autonomous cars, intelligent homes, virtual reality, and mass data analysis. He also referenced what he deemed to be the first AI technology; “Hal 9000’ was the first being with artificial intelligence that we saw in the cinemas, in Stanley Kubrick’s legendary film, *2001: a Space Odyssey*.”



AUTONOMOUS VEHICLES

Since November 2015, the Spanish government's Dirección General de Tráfico (DGT) regulates autonomous driving tests, allowing testing of vehicles with capabilities up to full autonomy on any road, under any condition. The government is also working on expanding rules for these vehicles, with a focus on developing insurance laws, and an overall legal framework regarding autonomous vehicles. [58]

DATA PRIVACY

GDPR Implementation Law: *The Organic Law* (Ley Orgánica, de Protección de Datos Personales y garantía de los derechos digitales) passed November, 2018. [59]

CYBERSECURITY

NIS Directive Implementation Law: *Royal Decree – Law 12/2018, September 7, on security of networks and information systems – date of application, 2018* [60]



SWEDEN

Sweden’s government outlines the nation’s approach to AI in the *National Approach to Artificial Intelligence*, which identifies to stakeholders, four “key conditions for use of AI in Sweden:” [61]

1. Education and training – increase AI knowledge and expertise ;
2. Research – basic and applied research to realize the opportunities of AI;
3. Innovation and use – promote the widespread use of AI in the private and public sectors; and
4. Framework and infrastructure – “safe, secure and favorable climate” for the use of AI.



NATIONAL STRATEGY:

Yes – *National approach to artificial intelligence* – adopted May 2018.



BUDGET/FUNDING:

Total US \$4B SEK 2015-2026, co-financing from universities, Wallenberg foundation, and industry; to the Wallenberg AI, Autonomous Systems, and Software Program (WASP), Sweden’s largest individual research program. [62]



NATIONAL FOCUS:

To become a world leader in harnessing opportunities of digital transformation, with a concentration on education, research, innovation, and infrastructure.

ETHICS:

The national strategy emphasizes the need for regulatory development balancing privacy and ethics, while also ensuring access to data to create AI applications. To do this, the Swedish Government, “needs to develop rules, standards, norms, and ethical principles to guide ethical and sustainable AI, and the use of AI.” [63]

DEFINITION OF AI:

“There is no one single, clear-cut or generally accepted definition of artificial intelligence. In general, however, AI refers to intelligence demonstrated by machines.” [64]



AUTONOMOUS VEHICLES

Trials of self-driving cars are permitted, effective July 2017, under the *Vehicle Act and Vehicle Ordinance*. A physical driver, with the ability to take control of the vehicle, must be present inside or outside of the vehicle during testing. “The ordinance...provides for fines for those who conduct trials without a permit.” [65] Jonas Bjelfvenstam, the Swedish Government’s Inquiry Chair, presented a report in March 2018, recommending the development of a new responsibility system, requirements for data storage, and increased testing of autonomous vehicles. [66]

DATA PRIVACY

GDPR Implementation Law: In April 2018, the Swedish parliament adopted a data protection Act containing provisions that supplement the GDPR. Several laws adapting sector specific data protection rules to the GDPR have also been adopted. [67]

CYBERSECURITY

NIS Directive Implementation Law: Transposed 2017. Follows NIS Directive requirements with the additional requirement that digital service providers must report any ‘data incidents’ immediately to the Civil Contingencies Agency. Failure to comply with the legislation can result in an administrative fine. [68]



UNITED KINGDOM

The UK government lays out an extensive list of policies to develop and implement AI in the policy paper, *AI Sector Deal*. The *Deal* is part of a broader UK Industrial Strategy that sets four “grand challenges” with the aim of putting the UK at the forefront of the industries of the future, and five foundations of productivity: [69]

- Place: prosperous communities across the UK;
- Business Environment: the best place to start and grow a business;
- Ideas: the world’s most innovative economy;
- People: good jobs and greater earning power for all; and
- Infrastructure: a major upgrade to the UK’s infrastructure.

The *Deal* also establishes two new government structures:

- a. an AI Council of leading figures from industry and academia to drive action, oversee implementation of the strategy, galvanize industry, and advise government, and
- b. a government Office for AI that works with the AI Council to create and deliver the strategy.



NATIONAL STRATEGY:

Yes – *AI Sector Deal* – released April 2018.



BUDGET/FUNDING:

A package of government, industry and academic contributions of ~\$1.2B, and an increase of total R&D investment to 2.4 percent of GDP by 2027. [70]



NATIONAL FOCUS:

Developing and implementing AI that boosts economic productivity and earnings in the UK.

ETHICS:

The UK Centre for Data Ethics and Innovation (CDEI), not yet a regulatory body, connects policymakers, industry, civil society, and the public to develop the right governance regime for data-driven technologies. [71] The Centre’s current priorities include a review of online targeting, to see how personal data is used to feed online targeted messages, content, and services; and a review of algorithmic bias. [72]



DEFINITION OF AI:

“Technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation.” [73]

AUTONOMOUS VEHICLES

The UK released the *Code of Practice: Automated vehicle trialling*, in February 2019, which outlines vehicle requirements, operator requirements, engagement, and general requirements for AV trials. The Code states that organizations who want to complete trials of AVs on UK roads, should engage with road and enforcement authorities, and must have: [74]

- An operator who can take control of the vehicle either in or out of the vehicle;
- A roadworthy vehicle; and
- Appropriate insurance.

The British government is currently analyzing feedback solicited from the public to improve this code. [75] Former Chancellor of the Exchequer Philip Hammond reported that “genuine driverless cars’ will be on the roads by 2021,” [76] and the Department of Transport confirmed that they are on-track to meet that commitment. [77]

DATA PRIVACY

GDPR Implementation Law: *The UK Data Protection Act, 2018* [78]

CYBERSECURITY

NIS Directive Implementation Law: *The Network and Information Systems Regulation, 2018* [79] Additionally, the *National Cyber Security Strategy 2016 to 2021*, sets out the government’s plan to make Britain secure and resilient in cyberspace.



ARGENTINA

While the Argentinian government has not yet published an official national strategy on AI, the “*Buenos Aires Declaration*” – the result of the first forum on *Artificial Intelligence and Internet of Things in Smart Sustainable Cities in Latin America* held in May 2018, by the Ministry of Modernization of Argentina – outlines the action items for Argentina regarding AI and the Internet of Things (IoT). The declaration innovatively views AI as a way to improve communities – cities – rather than individuals or businesses. [80]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

Using AI for the development of Smart Sustainable Cities, with a concentration on the Internet of Things.

ETHICS:

No official policy on ethics. The *Buenos Aires Declaration* states that, “The lack of regulation in data collection and ownership means that it is often up to the data collectors to determine the volumes and types of data being collected, making it their responsibilities [sic] to decide how to utilize those data. Consensus, accountability, inclusiveness, and transparency are at the center of developing an ethical framework that can build and sustain a trusting relationship.”

DEFINITION OF AI:

No official definition. The *Buenos Aires Declaration* states that the following technologies are subsets of AI and IoT: distributed computing, machine and deep learning, big data analysis, smart sensors, automation, and analytics.



AUTONOMOUS VEHICLES

Argentina has not issued regulations related to driverless vehicles.

DATA PRIVACY

Since 2000, the Argentina Personal Data Protection Act has protected personal data. [81] The country is, however, moving away from this law, and in 2018, President Mauricio Macri submitted a bill (Bill No. MEN-2018-147-APN-PTE) to the Argentine National Congress to align Argentinian data protection law with the General Data Protection Regulation (GDPR). [82] If approved, the bill will implement the following:

- A data subject is required to be a person;
- Eliminate the requirement of the registration of databases containing personal data;
- Processing of personal data requires the data subject's consent;
- Organizations must notify the data protection authority of data breaches;
- Require an impact analysis, when the data processor intends to treat personal data in such a way that entails a high risk of affecting the data subject's rights; and
- Public agencies, organizations processing sensitive data, and those participating in big data activities, are required to appoint a data protection officer.

CYBERSECURITY

Cybersecurity is not highly regulated in Argentina. In 2011, Resolution No. 580/2011 of the Executive Office of the Cabinet of Ministers ("Chief of Staff") created the *National Program for Critical Infrastructures for Information and Cybersecurity*. The program promotes protection of infrastructure and private sector organizations. Organizations may participate voluntarily in this program. Additionally, Decree 577/2017 created the Argentinian Cybersecurity Committee in 2017 to create a regulatory framework, create a national plan on cybersecurity, and educate the public about cybersecurity. [83]



AUSTRALIA

Australia views AI from a decidedly economically-centric perspective, seeing AI as a way to help Australian businesses become more competitive. Therefore, their public policies tend to be designed to help private companies gain access to AI technology, and to use that technology to solve specific business problems.



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

\$1.3B budgeted 2018-2030 for the National Research Infrastructure (NRI), of which \$20M is for R&D to develop the AI and machine learning capabilities of businesses and workers. [84]



NATIONAL FOCUS:

Artificial intelligence for Australian businesses and workers with a concentration on AI related research projects and a national ethics framework.

ETHICS:

In April 2019, the Department of Industry, Innovation, and Science released *Artificial Intelligence: Australia's Ethics Framework*. This discussion paper refers to eight core principles that Australia will use as a guide for organizations to develop and use AI ethically:

- Generate net-benefits
- Do no harm
- Regulatory and legal compliance
- Privacy protection
- Fairness (without discrimination)
- Transparency and explainability
- Contestability (a person can challenge the use of algorithms that impact them)
- Accountability

The framework focuses on three key issues – data governance, automated decisions, and predicting human behavior – and how they affect AI. [85] The national budget includes funding for Cooperative Research Centre Projects focusing on AI, and a national ethics framework to address standards and codes of conduct for adopting the technology in Australia.



DEFINITION OF AI:

Australia does not have an agreed definition of artificial intelligence; however, a number of definitions inform and guide the government's policy work on AI in various contexts, to accommodate different nuances. For example, Data61, Australia's leading digital research network, writes programs that learn to improve themselves using vast amounts of data and in some cases, not much data at all, defines AI as a range of technologies that exhibit some characteristics of human intelligence. [86]

For the purposes of designing civilian applications of AI with ethical and inclusive values, the Australian government defines AI as, "A collection of interrelated technologies, used to solve problems autonomously and perform tasks to achieve defined objectives, without explicit guidance from a human being." [87]

AUTONOMOUS VEHICLES:

While some vehicles on Australian roads are equipped with driver assistance, partial automation, and parking assistance, current Australian regulation does not recognize automated systems within the legal framework. Therefore, regardless of the level of vehicle automation, even when a vehicle is operated autonomously, the responsibility for compliance with traffic laws falls on the human in control.

In November 2017, the Australian National Transport Commission outlined regulations regarding "proper control" of vehicles with varying levels of automation. The regulations addressed levels of automation ranging from no automation – fully human driven, with some active safety systems – to partial automation for short periods, but with a human driver performing some tasks. At all levels of automation, the human is solely responsible for full operation of the vehicle, and must keep at least one hand on the steering wheel. [88]

DATA PRIVACY:

The Australian Privacy Principles (APPs) as codified in *The Privacy Act 1988*, lay out the requirements for personal data processing, including an individual's right to transact anonymously or use a pseudonym while online, as well as a right to access and correct information; maintenance of quality and security of personal information; and disclosures of purpose and use of personal information. [89]

CYBERSECURITY:

The *Corporations Act 2001* requires directors to "exercise powers and duties with the care and diligence that a reasonable person would." If a director ignores a real threat of an incident, they are liable for not protecting their systems. [90]

The *Security of Critical Infrastructure Act 2018* regulates critical infrastructure and requires the following: [91]

- A Register of Critical Infrastructure Assets – the register will build a clearer picture of critical infrastructure ownership and control in high-risk sectors, and support more proactive management of the risks these assets face;
- An information gathering power – the Secretary of the Department of Home Affairs will have the power to obtain more detailed information from owners and operators of assets in certain circumstances, to support the work of the center; and
- A Ministerial directions power – the Minister for Home Affairs will have the ability to direct an owner or operator of critical infrastructure to do, or not do, a specified thing to mitigate against a national security risk – where all other mechanisms to mitigate the risk have been exhausted.



CANADA

The Canadian government is focusing on ensuring that the societal impact of AI technologies is as benign as possible. Canada is investing heavily in research and developing domestic experts in the new technologies, as well as aggressively thinking through the ethics of AI development and deployment. Their national strategy – a global first – outlines four major goals: increase the number of AI researchers and graduates; establish major centers for AI in Edmonton, Montreal, and Toronto; lead discussions on economic, ethical, policy, and legal implications of advances in AI; and support national research on AI. [92]



NATIONAL STRATEGY:

Yes – *Pan-Canadian Artificial Intelligence Strategy* – released March 2017.



BUDGET/FUNDING:

\$93.3M through FY-2022. [93]



NATIONAL FOCUS:

Promoting AI research and thought leadership on economic, ethical, policy and legal implications of AI advances.

ETHICS:

The Treasury Board of Canada Secretariat addressed the ethical implications through the following guiding principles: [94]

1. Understand and measure the impact of using AI by developing and sharing tools and approaches;
2. Be transparent about how and when we are using AI, starting with a clear user need and public benefit;
3. Provide meaningful explanations about AI decision-making, while also offering opportunities to review results and challenge these decisions;
4. Be as open as we can by sharing source code, training data, and other relevant information; all while protecting personal information, system integration, and national security and defense; and
5. Provide sufficient training, so that government employees developing and using AI solutions have the responsible design, function, and implementation skills needed to make AI-based public services better.



DEFINITION OF AI:

“The term artificial intelligence (AI) encompasses a broad range of technologies and approaches. Two general approaches to AI are worth distinguishing. One approach uses predefined models to accomplish goals; the other relies on machine learning to train a system to accomplish goals. There are two well-known techniques in machine learning. To define them at a very high level, they are deep learning, which uses very large artificial neural networks; and reinforcement learning, which uses a reward and punishment structure. The intent of this paper is to discuss accountability, as it applies broadly to AI; while recognizing that certain ethical issues that have become associated with AI, most notably explainability, relate most directly to deep learning.” [95]

AUTONOMOUS VEHICLES

Testing autonomous vehicles is currently allowed. All trial vehicles are required to have data recording and to share that data with provincial, territorial, or federal regulators, in the case of an incident investigation. These regulations are outlined in the Canadian Department of Transport’s *Guidelines for Trial Organizations for Testing Highly Automated Vehicles* (2018). [96]

DATA PRIVACY

Canada’s federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), governs the collection, use, disclosure, and management of personal information, and includes requirements related to accountability, data subject consent, limits on use and retention, and accuracy of personal information. [97]

- Openness: An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
- Individual Access: Upon request, individuals must be informed of the existence, use, and disclosure of their personal information, and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information; and have it amended, as appropriate.
- Challenging Compliance: Individuals shall be able to challenge an organization’s compliance with the above principles. Their challenge should be addressed to the person accountable for the organization’s compliance with PIPEDA, usually their Chief Privacy Officer.

CYBERSECURITY

PIPEDA requires organizations to adopt physical and technological safeguards to protect personal information aligned with the sensitivity of that information. Additionally, PIPEDA’s updated *National Cyber Security Strategy* (2018) includes the following themes: protecting Canadians from cybercrime, responding to threats, defending critical government and private sector systems, leading development and innovation in cybersecurity, and advancing cyber security in Canada. [98]



CHINA

China sees AI as a central pillar of its long-term political and military strategy, and a key technology that will strengthen its economy, allowing China to become a world-power. The government is investing heavily in all aspects of AI research, including knowledge computing, swarm intelligence, autonomous unmanned systems, and natural language processing.



NATIONAL STRATEGY:

Yes – *A New Generation Artificial Intelligence Development Plan* – released July 2017.



BUDGET/FUNDING:

The national spending on AI is unknown to the public but two regional governments have promised \$14.7B each. [99]



NATIONAL FOCUS:

World-leading levels of AI by 2030 – with a focus on innovation, smart economy, safety, military-civilian integration, and infrastructure.

ETHICS:

The Development Plan states that China will develop laws, regulations, and ethical norms promoting AI development. [100] To promote this development, action items include:

- Launching research on AI behavior science and ethics, and other issues;
- Establishing an ethical and moral multi-level judgment structure and human-computer collaboration ethical framework;
- Developing an ethical code of conduct and R&D design for AI products;
- Strengthening the assessment of the potential hazards and benefits of AI; and
- Building solutions for emergencies in complex AI scenarios.

Additionally, the ethics committee of the Chinese Association for Artificial Intelligence, China's only state-level AI association, will develop draft ethics guidelines. [101]



DEFINITION OF AI:

No official definition. The Development Plan lists the following related disciplines of AI: “After sixty years of evolution, especially in mobile Internet, big data, supercomputing, sensor networks, brain science...AI’s development has accelerated, displaying deep learning, cross-domain integration, man-machine collaboration, the opening of swarm intelligence, autonomous control...big data-driven cognitive learning, cross-media collaborative processing, and man-machine collaboration – strengthened intelligence, swarm integrated intelligence, and autonomous intelligent systems have become the focus of the development of AI...the development a new generation of AI and related disciplines, theoretical modeling, technological innovation, hardware and software upgrades, etc.” [102]

China’s leadership, including the President of the People’s Republic of China, Xi Jinping, has expressed the goal of being a global leader in AI – ensuring independence from needing resources, or expertise, from other nations. Their strategy includes a stronger focus on military use of AI than many of the other national strategies, drawing concern about the ethics and use of these technologies.

China has already spurred debate over the ethical implementation and use of AI systems. Their widespread mass surveillance systems and facial recognition have enabled a social credit system, which can limit an individual’s access to many things, including bank loans and public transportation tickets. [103]



CHINA (CONT'D)

The 2017 Development Plan states that China will take advantage of strategic opportunities, gain a “first-mover” advantage, and become a global power in science and technology. The overall focus of the Plan is to be the first to achieve, and therefore be world leaders in the development and use of AI technologies. The Plan has three strategic objectives, each of which is given a deadline:

STEP	DEADLINE	MAIN OBJECTIVE	AREA OF INTEREST	GOAL
1	2020	Technology and application of AI in step with globally advanced levels	New generation of AI theories and technologies	Achieve important progress in theories and core technology
			AI industry competitiveness	Enter the first echelon internationally
			AI ethical norms, policies, laws, and regulations	Initial establishment
2	2025	Some technologies and applications achieve world-leading level	New generation of AI theories and technologies	Initial establishment
			AI industry competitiveness	Enter the global high-end value chain
			AI ethical norms, policies, laws, and regulations	Established with the formation of AI security assessment and control capabilities
3	2030	China’s AI theories, technologies, and applications achieve world-leading levels	New generation of AI theories and technologies	Formation of more mature system
			AI industry competitiveness	Reach world-leading levels
			AI ethical norms, policies, laws, and regulation,	Constructed more comprehensively



AUTONOMOUS VEHICLES

Current Chinese regulation requires autonomous cars to be tested on private roads before being tested in limited public locations. All vehicles must also have a person in the vehicle who is able to take control of the system. To assure safety and security of autonomous vehicles, the Chinese government has expressed interest in improving communication systems and intelligent roads. [104]

DATA PRIVACY

The Chinese *Personal Information Security Specification* regulates data privacy of Chinese citizens as an imperative of national security. Personal information (PI) controllers must, among other things: [105]

- Bear responsibility for damage to the lawful rights and interests of the PI subject;
- Process PI for legal, justified, necessary, and specific purposes;
- Obtain authorized consent from the PI subject, after expressly providing the PI subject with the purpose, method, scope, and rules of the processing;
- Process only the minimum types and quantity of PI necessary for the purposes for which the authorized consent is obtained from the PI subject;
- Be open and transparent about the scope and purposes of PI processing; and
- Provide the PI subject with the means to access, correct, and delete the PI; to withdraw consent; and to close accounts..

CYBERSECURITY

The 2017 Chinese *Cybersecurity Law of the People's Republic of China* aims to ensure cybersecurity and protect the rights and interest of Chinese citizens. The law applies to “network operators” and “operators of critical information infrastructure.” These operators are required to follow procedures to protect their networks based on cybersecurity standards detailed in the law. The State also monitors cybersecurity and receives early warning of incidents. [106]



INDIA

The Indian Nation Strategy is robust and addresses many of the current societal concerns regarding AI, including: intellectual property, data privacy and security, and ethics. Their goal – “#AIforAll” [107] – is to ensure that AI technologies provide economic, societal, and inclusive growth for their nation.



NATIONAL STRATEGY:

Yes – *National Strategy for Artificial Intelligence* – released June 2018.



BUDGET/FUNDING:

\$480M for 2018-2019 to ‘digital India,’ which includes the disciplines of: AI, machine learning, Internet of Things, 3D printing, and blockchain. [108]



NATIONAL FOCUS:

Addressing barriers to ensure AI benefits five societal needs: healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation.

ETHICS:

India’s National Strategy discusses, “Ethics, Privacy, Security, and Artificial Intelligence,” and focuses on fairness and transparency. Fairness addresses the inherent biases in data and algorithms of AI technologies, and aims to identify, assess the impact of, and reduce biases. Transparency refers to the explainability of algorithms and systems to ensure that more than the inputs and outputs are understood. Of particular importance: machine learning technologies that continually update their processes.



DEFINITION OF AI:

“AI is a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend, and act. Thus, computer vision and audio processing can actively perceive the world around them by acquiring and processing images, sound and speech. The natural language processing and inference engines can enable AI systems to analyze and understand the information collected. An AI system can also take action through technologies such as expert systems and inference engines, or undertake actions in the physical world. These human capabilities are augmented by the ability to learn from experience and keep adapting over time. AI systems are finding ever-wider application to supplement these capabilities across enterprises, as they grow in sophistication. Irrespective of the type of AI being used, however, every application begins with large amounts of training data.” [109]

AUTONOMOUS VEHICLES

Current regulation in India – the *Motor Vehicles Act, 1988* – does not allow fully automated systems, or the testing of autonomous vehicles in India. [110]

DATA PRIVACY

India’s Information *Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*, state that “whenever a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining a reasonable security to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected.” [111] Additionally, in 2018, the Ministry of Electronics and Information Technology (MeitY) submitted for vetting, the still pending draft of the *Personal Data Protection Bill, 2018*, to the Indian law ministry. [112]

CYBERSECURITY

The *National Cyber Security Policy, 2013* [113] includes 13 strategies to create a secure and resilient cyberspace in India:

- A. Creating a secure cyber ecosystem
- B. Creating an assurance framework
- C. Encouraging open standards
- D. Strengthening the regulatory framework
- E. Creating mechanisms for security threat early warning, vulnerability management, and response to security threats
- F. Securing E-Governance services
- G. Promotion of Research & Development in cyber security
- H. Reducing supply chain risks
- I. Human resource development
- J. Creating cyber security awareness
- K. Developing effective public private partnerships
- L. Information sharing and cooperation
- M. Prioritized approach for implementation



JAPAN



The Japanese Prime Minister established Japan’s Strategic Council for AI Technology, with representatives from industry, academia, and government, in April 2016. Their priorities are developing solutions for social issues, economic growth, social contributions, and information security.



NATIONAL STRATEGY:

Yes – *Artificial Intelligence Technology Strategy* – released March 2017.



BUDGET/FUNDING:

\$720M in AI related spending for FY 2018. [114]



NATIONAL FOCUS:

Use of AI for societal and economic improvement in four priority areas: productivity, health, mobility, and information security.

ETHICS:

The strategy states that the government plans to address “opportunities for examination” of the following ethical aspects of AI technologies:

- intellectual property rights;
- personal information protection; and
- promotion of open data.

DEFINITION OF AI:

No official definition. The national strategy states:

“As a result of promotion of machine learning, starting with deep learning, advancement of accumulation of enormous amounts of data on the Internet, acceleration of communication speed due to broadband, and the popularization of compact, high-performance computers – such as smartphones – research and development of artificial intelligence (AI) technology has progressed. Domains in which AI can be used and applied have also expanded, and a social change, known as the “Fourth Industrial Revolution,” is beginning. The AI technology that is currently progressing is specialized AI technology for carrying out specialized tasks, and is used only to supplement human capabilities. Based on the progression of AI technology, various inferences have become possible from past data, image recognition, language recognition, etc.”



AUTONOMOUS VEHICLES

In 2019, the government approved amendments to the *Road Transport Vehicle Act* that permit highly automated vehicles on public roads. The amendments include requirements for special equipment on the vehicles, regulation of testing vehicles, and accident liability. [115]

DATA PRIVACY

The *Japanese Act on the Protection of Personal Information* (APPI, 2003) requires among other things, that businesses handling personal information state the purpose for how information is used; businesses handling personal information implement measures to secure personal data; and businesses handling personal information do not provide personal data to a third party without consent of the data subject. [116]

CYBERSECURITY

The *Basic Act on Cybersecurity* requires national and local governments, businesses related to critical infrastructure, and cyber-businesses to take measures to improve cybersecurity. It also requires the government to: establish uniform cybersecurity standards for government agencies; improve cooperation between organizations on cybersecurity; reorganize the Information Security Policy Council; and support the legal authority of the National Security Information Center. [117]



KENYA

Kenya focuses its research and development efforts on a specific AI technology – blockchain – with the goal of using this technology to make their government more efficient. [118] In March 2018, the government established the Kenyan Distributed Ledgers and Artificial Intelligence Task Force to evaluate proposals for deploying blockchain technology.



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

AI and blockchain technology to improve government efficiency.

ETHICS:

No official policy on ethics, although policymakers are reacting to AI's potential to violate privacy. For example, Furhat, a social robot featured at the 2019 World AI Show (a summit for AI and machine learning in Nairobi) can converse with humans, mimic common facial expressions, and is currently deployed in Swedish schools. To address worry over the potential for privacy violations with these types of robots, Jerome Ochieng – the Principal Secretary for ICT and Innovation for the Ministry of Information and Communication Technology Authority – said Kenya should employ mechanisms that will safeguard citizens' privacy and also ensure AI technologies are deployed ethically. [119]

DEFINITION OF AI:

No official definition.



AUTONOMOUS VEHICLES

Kenya does not regulate autonomous vehicles.

DATA PRIVACY

The *Kenya Data Protection Bill 2018* requires every data controller or data processor to ensure that personal data is collected and handled according to specific requirements, including: a guarantee that subjects have a right of privacy; data managed lawfully, fairly, and in a transparent manner; data is not transferred outside Kenya, unless there is proof of adequate data protection laws by the recipient country; and that data is only released to a third party with the consent of the data subject. [120]

CYBERSECURITY

To promote the Kenyan Government's commitment to cybersecurity, their *National Cybersecurity Strategy* [121] includes four strategic goals:

1. Enhance the nation's cybersecurity posture in a manner that facilitates the country's growth, safety, and prosperity.
2. Build national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs.
3. Foster information sharing and collaboration among relevant stakeholders, to facilitate an information-sharing environment focused on achieving the Strategy's goals and objectives.
4. Provide national leadership by defining the national cybersecurity vision, goals, and objectives, and coordinating cybersecurity initiatives at the national level.



MEXICO

The Mexican government views AI through a public service lens, aiming to more effectively deliver public services using AI technologies. In June 2018, the British Embassy in Mexico, in collaboration with the National Digital Strategy Office (NDSO) of Mexico, released a report entitled, *Towards an AI Strategy in Mexico: Harnessing the AI Revolution*. [122] The report includes recommendations to the Mexican government that are based on interviews with experts across government, private industry, and academia, as well as predictions of AI's impact on the Mexican labor market.



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

AI to promote: the government and public services; data and digital infrastructure; research and development; skills and education; and ethics.

ETHICS:

No official policy on ethics. The NDSO report recommends the creation of a Mexican AI Ethics Council – composed of ethicists and business leaders – to address concerns that AI might increase the effectiveness of harmful things. It recommends building on the work of professional organizations, government, academia, and industry to:

- set guidelines and limits which reflect Mexican values; and
- award a quality mark for AI companies who abide by the standards.

DEFINITION OF AI:

No official definition. The NDSO report refers “to machines, and generally computer systems, that can simulate the processes of natural intelligence displayed by humans. These processes include learning, reasoning, and self-correction. The phrase ‘artificial intelligence’ is now an umbrella term that refers to a broad range of research approaches and technologies.” [123] The report also refers to ‘weak’ or narrow AI and ‘strong’ or general AI – Narrow AI completing one task; while general AI performs all cognitive tasks.



AUTONOMOUS VEHICLES

Current regulation does not necessarily prohibit autonomous vehicles. However, most jurisdictions require drivers to maintain two hands on the wheel when driving on highways or bridges. [124]

DATA PRIVACY

The 2010 *Federal Law for the Protection of Personal Data Held by Private Parties* requires transparency, purpose limitation, consent, and loyalty – in other words, the data collector should process personal data in a way that protects the interests and privacy of the data subject. [125]

CYBERSECURITY

No specific laws exist in Mexico related to cybersecurity responsibility, or liability of personnel and directors. Also, no obligation to report incidents or potential incidents to authorities currently exists; and authorities cannot require minimum protective measures for organizations.



NIGERIA

Nigeria's current AI research is focused on deploying domestically produced technologies. In August 2018, the government established the Agency for Robotics and Artificial Intelligence, which sees AI as, potentially, an area where Nigeria could develop a global competitive edge in high-tech.



NATIONAL STRATEGY:

No official strategy, but Nigeria plans to develop an action plan to accelerate AI, machine learning, and robotics, and inspire local tech hubs.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

Establishing an agency for robotics and AI to advance knowledge, usability and growth in those areas.

ETHICS:

No official policy on ethics.

DEFINITION OF AI:

No official definition.

AUTONOMOUS VEHICLES

No current regulation of autonomous vehicles. However, in 2018, the Nigerian Air Force launched their first indigenous UAV. A Facebook post states that the UAV, called Tsaigumi, includes the following capabilities [126]:

- Day and night operations;
- An operational endurance in excess of 10 hours;
- A mission radius of 100km; and
- A muffled engine.



DATA PRIVACY

The Nigerian National Information and Technology Development Agency (NITDA) released guidelines for data protection that include the following requirements for obtaining personal data: [127]

1. Data must be lawfully processed, and can be processed only if one of the following is true:
 - The Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes;
 - Processing is necessary for the performance of a contract to which the Data Subject is party; or to take steps at the request of the Data Subject, prior to entering into a contract;
 - Processing is necessary for compliance with a legal obligation to which the Controller is subject;
 - Processing is necessary to protect the vital interests of the Data Subject, or of another natural person; or
 - Processing is necessary for the performance of a task carried out in the public interest; or in exercise of an official public mandate vested in the controller.
2. Data must be collected and processed in accordance with specific, legitimate, and lawful purpose consented to by the Data Subject; provided that:
 - A further processing may be done only for archiving, scientific research, historical research, or statistical purposes for public interest; and
 - Any person or entity carrying out or purporting to carry out data processing, under the provision of this paragraph, shall not transfer any Personal Data to any person.
3. Data must be adequate, accurate, and without prejudice to the dignity of human person.
4. Data must be stored only for the period within which it is reasonably needed.
5. Data must be secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.

CYBERSECURITY

Nigeria's *Cybercrimes (Prohibition and Prevention etc.) Act, 2015* addresses 36 cyber offenses, including offenses against critical national information infrastructure, unlawful interceptions, cyber terrorism, identity theft, and system interference. The objectives are to promote cyber security, protect critical national information infrastructure, and provide a unified framework for the prosecution of cybercrimes. [128]



RUSSIA

Russia released a draft *National Strategy for Artificial Intelligence (AI) Development in Russia* in June 2019. A final version is due in October 2019. The country’s goal is to be a global leader in the development of AI that will “support growth in prosperity and quality of life of the population, stimulate economic development, and ensure national security and law enforcement.” The Analytical Center for the Government of the Russian Federation held an expert discussion to solicit feedback on the draft to be considered before the final approval by the Cabinet of Ministers. [129]

At a March 2018 conference, the Russian government gathered domestic and international developers and users at a conference which resulted in a 10-point AI plan. The plan includes the following points, but is not currently an official strategy: [130]

- Form an AI and Big Data consortium
- Gain automation expertise
- Create a state system for AI training and education
- Build an AI lab
- Establish a National Center for Artificial Intelligence
- Monitor global AI development
- Hold AI war games
- Check for AI compliance
- Discuss AI proposals at domestic military forums
- Hold an annual AI conference



NATIONAL STRATEGY:

DRAFT – *National Strategy for Artificial Intelligence (AI) in Russia*
– released June 2019.



BUDGET/FUNDING:

\$287M for research centers and start-ups, \$145M to develop products, services and platforms, and \$287M for technology. [131]



NATIONAL FOCUS:

Leading AI development to support quality of life, economic development, and national security.

ETHICS:

No official policy on ethics, however, the 10-point plan for AI states that Russian public-private partnerships should monitor global AI development and include an understanding of the impacts of AI through a “social sciences” lens. [132]



DEFINITION OF AI:

No official definition. However, the 10-point plan included the following sub-fields: big data analysis, analytical algorithms and programs, automated systems, robotics, image recognition, training and imitating the human thought process, complex data analysis, and assimilation of new knowledge. [133]

AUTONOMOUS VEHICLES

Regulation No. 1415, Conducting an Experiment in Testing the Use of Highly Automated Vehicles on Public Roads, released November 2018, permits testing of driverless cars on regular roads. Autonomous vehicles must have both a “pilot” in the vehicle and continuous data recording; video recording must be made available to the government upon request. The vehicles must also be identified as autonomous, with a large letter “A.” The owner of the vehicle assumes all liability for any accident, if another party is not found to be responsible. [134]

DATA PRIVACY

Under the *Data Protection Act, No. 152 FZ (DPA)*, organizations are required, among other things, to obtain consent when collecting and processing personal data, and ensure protections for personal data transferred out of Russia.

Additionally, “If the data controller is a legal entity, it is required to appoint a data protection officer.” [135]

CYBERSECURITY

In July 2017, Russia adopted the *Federal Law on the Security of Critical Information Infrastructure of the Russian Federation*. The law established principles for critical information infrastructure security. Due to the critical nature of these services for the economy, they must possess protection measures against cyberattack and must register with the Federal Service for Technical and Export Control (FSTEK). [136]



SAUDI ARABIA

In April 2016, Crown Prince Mohammad bin Salman announced the *Saudi Vision 2030* – a plan to reduce Saudi Arabia’s dependence on oil, diversify its economy, and develop public service sectors such as health, education, infrastructure, recreation, and tourism. [137] The plan includes development of Neom, a planned cross-border city (26,000 square kilometers) in the Tabuk Province of northwestern Saudi Arabia. Neom is to become an unparalleled smart city. Additionally, Saudi Arabia is the first country to grant citizenship to a robot, which is legally named Sophia. [138]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

The government has invested \$3B in building the infrastructure to ensure AI-readiness and leadership in AI use. [139] The government plans to invest \$500B in Neom. [140]



NATIONAL FOCUS:

Developing the smart city, Neom, to enable integration of resident medical files, household electronics, and transport into IoT systems.

ETHICS:

No official policy on ethics, although ethics is a consideration in the development of Neom. Dr. Ahmed Al Theneyan, the Deputy Minister of Technology, Industry, and Digital Capabilities, stated, “We’re embracing AI and exploring how to use it in an innovative, responsible, and ethical way that will advance our Vision 2030 objectives.” [141]

DEFINITION OF AI:

No official definition. *Saudi Vision 2030* includes discussion of IoT and blockchain, but does not formally define them.

AUTONOMOUS VEHICLES

Saudi Arabia does not currently regulate autonomous vehicles on public roads; however, driverless vehicles are a part of the plan for developing Neom. [142]



DATA PRIVACY

Saudi Arabia does not have specific data protection laws, however there is data protection under Sharī'ah principles. The international law firm, Latham & Watkins states, “Sharī'ah principles protect each individual's right to privacy and prohibit any invasions thereon. Under Sharī'ah principles, disclosure of secrets is prohibited, except inter alia, where the owner of the relevant secret agrees to such disclosure, or if the public interest requires so.” [143]

AI AND THE INTERSECTION OF STATE LAW AND SHARĪ'AH

Many discussions of religion and AI revolve around the ethics and principles of religion, and how to implement theology into AI systems. It is particularly important to assess how AI and religious beliefs interact, where religious law is in effect, such as in many Muslim countries that follow Sharī'ah. Of the Muslim countries where Islam is the official religion, Saudi Arabia employs one of the strictest interpretations of Sharī'ah. This has raised a number of questions, including:

- If AI systems are programmed to follow Sharī'ah, will they be programmed to be Muslim? What exactly would that mean?
- Is it against Sharī'ah to have strong AI (i.e., systems that are able to think like humans)?
- Robots, such as Sophia (see above), can be citizens. Can they also be a part of Islam?

Additionally, AI systems based on natural language and text normally need a machine-readable corpus that is typically over one million words. The Quran has less than 80,000 words. [144] To augment the Quran and develop AI systems that can understand and interpret religious texts, researchers may need to include knowledge, wisdom, and law from the Muslim population. This addition to the dataset will have inherent biases; and likely, it will have contradictions in the interpretation of the Quran.

CYBERSECURITY

The *Saudi Anti-Cyber Crime Law* [145] combats cybercrimes with the purpose of enhancing information security, protecting rights regarding legitimate use of computer and information systems, protecting public interest and protecting the national economy. Maximum imprisonment periods and fine amounts fluctuate depending upon the type of cybercrime. For example:

1. Spying on, interception, or reception of data transmitted through an information network, or a computer, without legitimate authorization (\leq 1-year term and \$134,000);
2. Illegally accessing bank or credit data, or data pertaining to ownership of securities – with the intention of obtaining data, information, funds, or services offered (\leq 3-year term and \$534,000);
3. Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter, or redistribute private data (\leq 4-year term and \$800,000);
4. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network, or computers (\leq 5-year term and \$300,000); and
5. Unlawful access to a web site or an information system directly, or through the information network; or any computer – with the intention of obtaining data jeopardizing the internal or external security of the State, or its national economy (\leq 10-year term and \$1.3 million).



SINGAPORE

The National Research Foundation (NRF), a department of the Prime Minister's Office that develops policies and strategies for research and development, launched *AI Singapore*, an initiative designed to enable Singapore to use AI to address societal challenges through scientific innovation and expanded production of AI in industry. [146]



NATIONAL STRATEGY:

Yes – *AI Singapore* – released May 2017.



BUDGET/FUNDING:

The NRF will invest up to \$150M through 2022 in *AI Singapore*.



NATIONAL FOCUS:

“... catalyze, synergize, and boost Singapore's AI capabilities to power future, digital economy” with three pillars – AI research, AI innovation, and AI technology.

ETHICS:

Singapore's Infocomm Media Development Authority (IMDA) developed three initiatives to address ethics, privacy, and security: [147]

1. Advisory Council on the Ethical Use of AI and Data
 - a. Develop ethics standards
 - b. Publish advisory guidelines/codes of practice for voluntary adoption by industry
 - c. Establish a Legal and Technical Expert Panel
2. Discussion paper by the Personal Data Protection Commission (PDPC) on responsible development and adoption of AI
 - a. Discussion on possible AI and Data Governance frameworks for industry
 - b. Two key principles
 - i. Decisions made by, or with the assistance of AI, should be explainable, transparent, and fair to consumers
 - ii. AI systems, robots, and decisions should be human-centric
3. Research program on the governance of AI and data use



DEFINITION OF AI:

No official definition. In a 2019 Grant Call, *AI Singapore* produced a guide outlining different types of AI: [148]

- Explainable AI
 - Designing AI systems and/or solutions that can explain their own decisions/recommendations.
 - Understanding ‘black-box’ AI systems: To develop theories and methods for explainable AI.
- Robust AI
 - Designing AI systems and/or solutions that are able to address misinformation presented: To detect misinformation and determine the veracity of information. An example is AI able to perform fact checking.
 - Designing AI systems and/or solutions that are able to learn well with noisy data, and infer robustly on unseen scenarios.
 - Designing AI systems and/or solutions that are resilient to attacks, data poisoning, and unknown threats.
- Interactivity between AI and Humans
 - Designing AI systems and/or solutions that are able to bridge the gap in interactivity between human and AI systems: Current AI systems and solutions lack user-friendliness. This may hinder the deployment of AI in real world contexts. An example is to incorporate human social aspects when designing AI systems. Another example is to guide AI systems with human collective intelligence.

AUTONOMOUS VEHICLES

An amendment to the *Road Traffic Act*, 2004, [149] regulates trials of autonomous vehicles. The act allows approved trials on public roads, as long as the persons running the trial have sufficient liability insurance. *Technical Reference 68* (TR 68), released in early 2019, guides development and deployment of autonomous vehicles in Singapore. [150] This is one of the first set of standards.

DATA PRIVACY

Singapore’s 2012 *Personal Data Protection Act* [151] regulates transparency, lawful processing, limits on use and transfer of information.

CYBERSECURITY

The 2018 *Cybersecurity Act* [152], is the nation’s legal framework addressing cybersecurity, particularly in regards to critical information infrastructure. The act has four key objectives:

- Strengthen the protection of the Critical Information Infrastructure (CII) against cyber-attacks;
- Authorize Singapore’s Cyber Security Agency to prevent and respond to cybersecurity threats and incidents;
- Establish a framework for sharing cybersecurity information; and
- Establish a light-touch, licensing framework for cybersecurity service providers.



SOUTH KOREA



South Korea strives to be a world leader in AI within five years. The country focuses their research and development on three categories: human resources, technology, and infrastructure. South Korea will also develop six graduate schools for AI and computer software.



NATIONAL STRATEGY:

Yes — the *Artificial Intelligence R&D Strategy* — released May 2018.



BUDGET/FUNDING:

\$1.95B investment in AI R&D through 2022. [153]



NATIONAL FOCUS:

Securing AI talent, development of AI technology, and infrastructure to support AI start-ups and small- and medium-sized entities.

ETHICS:

The *Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society* (2016), includes the following recommendation: “Establish human-centered ethics to govern data-collection processes and AI algorithms.” [154]

DEFINITION OF AI:

“AI technology encompasses intelligent software and hardware technologies, basic sciences (brain science and industrial mathematics), and other such technologies that are capable of performing human cognitive functions (language, voice recognition, visual perception, emotional support, etc.). At present, Intelligent IT is understood mainly as a weak form of AI that merely simulates human cognitive functions in limited areas of human activity. It is not yet a strong form of AI that is capable of replacing all human tasks requiring intelligence based on creative learning and decision-making.” [155]



AUTONOMOUS VEHICLES

The South Korean government plans to regulate self-driving cars, with a focus on insurance systems, observation, and location information collection, transfer of control, liability in accidents, and a simplified license system. [156] South Korea also has plans to build K-City, a 360,000 square meter site used to test autonomous vehicles. The Ministry will invest \$11 million in the project, which will have highway, downtown, suburban, parking, and community facilities. [157]

DATA PRIVACY

The *Personal Information Protection Act, 2011* (PIPA) requires information processors to inform a subject of the purpose of data collection and to obtain consent from the data subject; limits how much personal information is collected and how it is used; and requires a personal information processor to have a privacy officer. [158]

CYBERSECURITY

South Korea regulates cybersecurity via PIPA (see above), as well as the *Act on the Protection of Information and Communications Infrastructure* (PICIA), and the *Act on the Promotion of IT Network Use and Information Protection* (The Network Act). [159] The Network Act protects personal information and improves IT network security. It also prohibits access to a network system by an unauthorized individual. The PICIA protects against attacks on information and communications infrastructure, including hacking, viruses, and denial of service.



TAIWAN

Taiwan has been a leader in information and communications technology (ICT) and semiconductor technology for several decades. The country’s goal is to supplement that momentum and success with AI, making the country a valuable global partner in intelligent systems. Taiwan presents their vision for AI as, “innovation, collaboration, and inspiration.” [160]



NATIONAL STRATEGY:

Yes — *AI Taiwan* — released January 2018.



BUDGET/FUNDING:

Between \$304.4M-\$338.3M, to be allocated annually. [161]



NATIONAL FOCUS:

Integrating AI to develop “smart” technology, particularly in the fields of ICT and semiconductors, to promote industrial transformation.

ETHICS:

No official policy on ethics.

DEFINITION OF AI:

No official definition.

AUTONOMOUS VEHICLES

In May 2019, the Executive Yuan approved the *Unmanned Vehicle Technology Innovation and Experiment Act*. [162] The Act promotes a secure environment for R&D of unmanned vehicle technology. Organizations must apply to run experiments, and include descriptions of testing, analysis of applicability, expected benefits of testing, plans for insurance coverage, and potential risks – among other things.

DATA PRIVACY

The Personal Information Protection Act (PIPA) [163] regulates the “collection, processing, and use” of personal information in Taiwan. There are two separate sections for information collection, processing, and use by Government and non-Government agencies, outlined on the following page:



GOVERNMENT AGENCIES	NON-GOVERNMENT AGENCIES
<p>Government agencies may collect personal information – only – when there is a specific purpose, and it is within the scope of job functions, consent has been given, or the rights and interests of the data subject are not harmed.</p>	<p>Non-government agencies may collect personal information only when (1) there is a specific purpose or; (2) it is in accordance with law; there is a contractual relationship between the Parties, the information has been publicized legally, it is necessary for public interests, consent has been given by the subject, or the rights and interests of the Party are not harmed.</p>
<p>Personal information can be used outside of the scope of its collection only if one of the following is true: it is in accordance with law, it is necessary for national security or promotion of public interests, it is to prevent harm to the subject, it is to prevent harm on the rights and interests of other people, it is necessary for public interests, such use may benefit the subject, or consent has been given by the subject.</p>	<p>Personal information can be used outside of the scope of its collection only if one of the following is true: it is in accordance with law, it is necessary to promote public interests, it is to prevent harm to the subject, it is to prevent harm to other people, such use may benefit the subject, or consent has been given by the subject.</p>
<p>Government agencies may publicize the following items for inquires:</p> <ul style="list-style-type: none"> • Name of personal information file • Name of the government agency keeping the personal information • Basis and purpose of keeping the file • Classification of personal information 	<p>When transmitting personal information internationally, the government authority in charge may limit its action, if the transmission: involves major national interests, opposes a national treaty or agreement, is made to a country lacking proper regulations, or is made through any method where this Law is not applicable.</p>
<p>Government agencies should have personnel to ensure security and avoid information being stolen, altered, damaged, destroyed, or disclosed</p>	<p>The non-government agency should adopt proper security measures to prevent information from being stolen, altered, damaged, destroyed, or disclosed</p>
<p>---</p>	<p>For the non-government agency that violates the provisions of this Law, one of the following actions may be ordered jointly with a fine: forbid the collecting, processing, or use of the personal information; demand the deletion of the personal information files already processed; confiscate or destroy the personal information illegally collected; publicize the violation case, the name of the non-government agency, and the name of the person in charge.</p>

CYBERSECURITY

Taiwan’s *Information and Communication Security Management Act*, effective 1 January 2019, requires government agencies and organizations involved with critical infrastructure to implement cybersecurity measures. These agencies and organizations are also required to notify competent authorities of incidents involving cybersecurity. [164]



TUNISIA

In April 2018, the Tunisian government held the *National AI Strategy: Unlocking Tunisia's Capabilities Potential* workshop, with the intent to join, “the AI race to secure a respectable place and a proactive role commensurate with its capabilities, ambitions, and vision of AI as a knowledge-intensive sector; and a lever of sustainable and equitable development ...” Tunisia hopes to spark a scientific, technological, and industrial revolution for socio-economic development. [165]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

Producing a national AI strategy, as a lever of sustainable and equitable development.

ETHICS:

No official policy on ethics. The Tunisian National Agency for Scientific Research Promotion (ANPR) aspires to play a proactive role in the development and implementation of AI, but acknowledge it must be done, “without forgetting about the ethical challenges posed by this emerging technology.” [166]

DEFINITION OF AI:

No official definition.



AUTONOMOUS VEHICLES

No current regulation on autonomous vehicles.

DATA PRIVACY

Tunisia's National Authority for the Protection of Personal Data (INPDP) introduced a draft law on the protection of personal data in March 2018. The draft was created in accordance with the GDPR [167] but has yet to be passed [168]. Current *Law No. 63 – 2004 on the Protection of Personal Data* regulates data privacy and requires obtaining consent to the access and use of personal data, and limits how personal data is collected and transferred. [169]

CYBERSECURITY

The *Electronic Security Law* requires organizations related to national telecommunications to annually audit their computer systems and network. Additionally, the Network and Information Security Agency (NISA) requires public or private entities to report an attack, intrusion, or disruption, if it will likely affect another network. NISA also has the authority to require these entities to implement measures to protect their networks, in the event of a cyber attack. [170]



In 2017, the United Arab Emirates launched a five-decade government plan known as, “UAE CENTENNIAL 2071.” [171] As part of that plan, the UAE also developed the *National Artificial Intelligence Strategy 2031* to boost government performance. The UAE hopes to position itself as a global leader in AI by 2031, and to develop an integrated system that employs AI technologies in “vital areas,” including transportation, health, space, renewable energy, water, technology, education, environment, and traffic. [172]

The UAE Strategy presents five themes to achieve the country’s objectives: [173]

- The formation of the UAE AI Council;
- Workshops, programs, initiatives, and field visits to government bodies;
- Develop capabilities and skills of all staff operating in the field of technology; and organize training courses for government officials;
- Provide all services via AI, and the full integration of AI, into medical and security services; and
- Launch a leadership strategy, and issue a government law, on the safe use of AI.



NATIONAL STRATEGY:

Yes — *UAE AI 2031 Strategy* —
October 2017.



BUDGET/FUNDING:

\$408.4M in new schools featuring
labs for robotics, AI, health, and
environment. [174]



NATIONAL FOCUS:

Developing a smart government
with emphasis on “vital areas.”

ETHICS:

The Smart Dubai initiative presents *AI Ethics, Principles, & Guidelines* as: [175]

- Fair – Demographic fairness, fairness in design, fairness in data, fairness in algorithms, and fairness in outcomes;
- Transparent – Identifiable by humans, traceability of cause or harm, and auditability by the public;
- Accountable – Apportionment of accountabilities, accountable measures for mitigating risks, and appeals procedures and contingency plans; and
- Explainable – Process explainability, outcomes explainability, explainability in non-technical terms, and channels of explainability.

Smart Dubai also includes a self-assessment tool for developers to determine the ethics level of their systems and platforms. [176]



DEFINITION OF AI:

No official definition. AI deployable technologies include: deep learning, cognitive cities, image and video content, recognition, speech recognition, predictive APIs, emotional recognition, gestural computing. [177]

AUTONOMOUS VEHICLES

The Dubai Future Foundation, in conjunction with Dubai's Roads and Transport Authority Launched, the *Dubai Autonomous Transportation Strategy*. [178] By 2030, Dubai hopes to make autonomous, 25 percent of vehicles, thereby cutting transportation costs, reducing environmental pollution, improving transportation safety, and increasing individual productivity by saving time.

The strategy's four main pillars are individuals, technology, legislative structure, and infrastructure – with a focus on metro, bus, and taxi sectors.

DATA PRIVACY

The UAE does not have standalone data privacy legislation; however, in April 2019, the Telecommunications Regulatory Authority (TRA) released a Regulatory Policy on the Internet of Things (IoT). [179]. This policy outlines three key principles for data storage that IoT service providers must follow:

- Purpose limitation – Data should be collected for specified, explicit, and legitimate purposes and not further processed;
- Data minimization – Data should be adequate, relevant, and limited to what is necessary for the purposes for which it is processed; and
- Storage limitation – Data should only be kept in a format that identifies the data subject for as long as necessary, for the purposes for which it was processed.

CYBERSECURITY

The Telecommunications Regulatory Authority established the *UAE National Cyber Security Strategy (NCSS)* to protect personal information and communications of the UAE's citizens. The NCSS focuses on, among other things, “preparing and preventing” by ensuring compliance to the UAE's cyber security standards; fostering collaboration with international bodies; and building national capability by educating the workforce and promoting research. [180]



ZIMBABWE

Zimbabwe's government currently has no official national AI strategy. In early 2019, the country partnered with a Chinese-based startup on a facial recognition project to aid the development of smart cities. Nigel Sheima Muguza, an official with the special advisor to the presidency, stated that the Zimbabwean government will “[contribute to] the building of national artificial intelligence.” [181]



NATIONAL STRATEGY:

No official strategy.



BUDGET/FUNDING:

No current budget.



NATIONAL FOCUS:

Becoming a middle-income country by 2030, and implementation of a nation facial recognition project moving toward smart cities.

ETHICS:

No official policy on ethics. The proposed facial recognition project initially will be used for security purposes, disaster response, and traffic control. The government has not addressed the ethics of AI.

DEFINITION OF AI:

No official definition.



AUTONOMOUS VEHICLES

Currently no regulation on autonomous vehicles.

DATA PRIVACY

See Cybersecurity below.

CYBERSECURITY

In early 2019, after two years of deliberation, the government of Zimbabwe approved the *Cybercrime and Cybersecurity Bill of 2017*. [182] The bill combines several pieces of legislation, including the *Electronic Transactions and Electronic Commerce Bill*, *Data Protection Bill*, and the *Computer Crime and Cybercrime Bill*. [183] Some of the offenses considered to be cybercrimes are those related to computer systems, computer data, data storage, data codes and devices; those related to electronic communications and materials; offenses against children; and cyber-related terrorism and sabotage.

BIBLIOGRAPHY

- [1] Executive Office of the President, National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, [Accessed: 16 September 2019].
- [2] J. Gesley, In Custodia Legis: Law Librarians of Congress, *Personal Data Protection and the EU GDPR*, 25 May 2018, <https://blogs.loc.gov/law/2018/05/personal-data-protection-and-the-eu-gdpr/>, [Accessed: 25 August 2019].
- [3] European Commission, *GDPR Implementation: Updated State of Play in the Member States (11/04/2019)* <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 25 August 2019]
- [4] EUR-Lex, Access to European Union Law, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>. [Accessed: 25 August 2019].
- [5] European Commission, *EU Data Protection Rules*, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. [Accessed: 25 August 2019].
- [6] European Commission, *A New Era for Data Protection in the EU: What Changes after May 2018*, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf. [Accessed: 25 August 2019].
- [7] European Commission, *Mythbusting: General Data Protection Regulation, January 2019*, https://ec.europa.eu/commission/sites/beta-political/files/100124_gdpr_factsheet_mythbusting.pdf, [Accessed: 25 August 2019].
- [8] “The Directive on Security of Network and Information Systems (NIS Directive),” *Digital Single Market - European Commission*, 5 July 2016. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>. [Accessed: 12 August 2019].
- [9] European Union Agency for Cybersecurity, *NIS Directive*, <https://www.enisa.europa.eu/topics/nis-directive>, [Accessed: 25 August 2019].
- [10] *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [11] All EU member states were encouraged to develop their own national AI strategies by mid-2019. “European AI Strategies: Where Do Member States Stand, and Where Are They Headed?” *Center for Data Innovation*, 4 April 2019, <https://www.datainnovation.org/2019/04/european-ai-strategies-where-do-member-states-stand-and-where-are-they-headed/>. [Accessed: 27 May 2019].
- [12] European Commission, *Communication Artificial Intelligence for Europe*, April 2018, <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>, [Accessed: 25 August 2019].
- [13] *Digital Single Market - European Commission*, “Ethics Guidelines for Trustworthy AI,” 08 April 2019, <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. [Accessed: 11-May-2019].
- [14] European Commission, *Communication Artificial Intelligence for Europe*, April 2018, <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>, [Accessed: 25 August 2019].
- [15] *Strategy for Denmark’s Digital Growth*, <https://eng.em.dk/media/10554/digital-strategy-fact-sheet.pdf>. [Accessed: 12 August 2019].

- [16] The Danish Government, *National Strategy for Artificial Intelligence*, p. 20, 2019. https://eng.em.dk/media/13081/305755-gb-version_4k.pdf, [Accessed 12 August 2019].
- [17] Ibid. The Danish Government, *National Strategy for Artificial Intelligence*.
- [18] Kennedys Law LLP, *Danish parliament adopts new legislation on self-driving cars*, <https://www.kennedyslaw.com/thought-leadership/article/danish-parliament-adopts-new-legislation-on-self-driving-cars>. [Accessed: 12 August 2019].
- [19] IT Governance, Data Protection “Danish Data Protection Act (DDPA) 2018” <https://www.itgovernance.eu/da-dk/eu-gdpr-compliance-dk>. [Accessed: 14 August 2019].
- [20] *NIS Implementation Tracker*, European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [21] Kaevats, Marten, National Digital advisor of Estonia, “*Estonia considers a ‘kratt law’ to legalise Artificial Intelligence (AI)*,” <https://medium.com/e-residency-blog/estonia-starts-public-discussion-legalising-ai-166cb8e34596> [Accessed 12 August 2019]
- [22] The Information Technology Foundation for Education (HITSA), “Estonian Government to Allocate Three Million Euros Annually to Support IT Research,” <https://www.hitsa.ee/about-us/news/estonian-government-to-allocate-three-million-euros-annually-to-support-it-research>. [Accessed 12 August 2019].
- [23] “Estonia will have an artificial intelligence strategy,” *Government Office of Estonia*. <https://www.riigikantselei.ee/en/news/estonia-will-have-artificial-intelligence-strategy>. [Accessed: 12 August 2019].
- [24] The Information Technology Foundation for Education (HITSA), “Estonian Government to Allocate Three Million Euros Annually to Support IT Research,” <https://www.hitsa.ee/about-us/news/estonian-government-to-allocate-three-million-euros-annually-to-support-it-research>. [Accessed 12 August 2019].
- [25] *Government Office of Estonia*, “Final report: self-driving vehicles on Estonian roads may signal the end of traffic deaths,” <https://www.riigikantselei.ee/en/news/final-report-self-driving-vehicles-estonian-roads-may-signal-end-traffic-deaths>, [Accessed: 12 August 2019].
- [26] “*Riigikogu passed 27 Acts and two Resolutions.*” <https://www.riigikogu.ee/en/sitting-reviews/riigikogu-passed-27-acts-two-resolutions/> [Accessed: 12 August 2019].
- [27] European Union Agency for Cybersecurity, *NIS Directive*, <https://www.enisa.europa.eu/topics/nis-directive>, [Accessed: 25 August 2019].
- [28] Ministry of Economic Affairs and Employment of Finland, *Finland’s Age of Artificial Intelligence: Turning Finland into a leading country in the application of artificial intelligence Objective and recommendations for measures*, http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y [Accessed: 12 August 2019].
- [29] University of Helsinki, “Significant boost for AI research from the Academy of Finland,” 08-Jan-2019. <https://www.helsinki.fi/en/news/data-science-news/significant-boost-for-ai-research-from-the-academy-of-finland>. [Accessed: 14 August 2019].
- [30] Ministry of Economic Affairs and Employment of Finland, *Work in the Age of Artificial Intelligence: Four Perspectives on the Economy, Employment, Skills and Ethics*, p.49. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160980/TEMjul_21_2018_Work_in_the_age.pdf. [Accessed: 12 August 2019].

- [31] Ministry of Economic Affairs and Employment of Finland, *Finland's Age of Artificial Intelligence: Turning Finland into a Leading Country in the Application of Artificial Intelligence: Objectives and Recommendations for Measures*, p. 15. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y [Accessed: 12 August 2019].
- [32] Finnish Transportation Agency, NVF Digitalization committee meeting, 8 February 2017. *Connected and Automated Driving: Finnish Government Initiatives and Pilots*. http://www.nvfnorden.org/library/Files/FI_Status%20report_Ilkka%20Kotilainen.pdf. [Accessed: 13 August 2019].
- [33] L. Stinson, "Muji's self-driving bus is hitting the streets this spring," *Curbed*, 14-Mar-2019. <https://www.curbed.com/2019/3/14/18265298/muji-self-driving-bus-gacha-finland>. [Accessed: 13 August 2019].
- [34] Novinite.com, Sofia News Agency, "Autonomous Vehicles in Public Transport in Finland," <https://www.novinite.com/articles/189056/Autonomous+Vehicles+in+Public+Transport+in+Finland>. [Accessed: 13 August 2019].
- [35] European Commission, *GDPR Implementation: Updated State of Play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [36] In European Union law, transposition is a process by which the European Union's member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary legislation,,, or secondary legislation. *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [37] Villani, C. *For a Meaningful Artificial Intelligence – Toward a French and European Strategy*. https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf, [Accessed: 13 August 2019]
- [38] The Villani Mission. *AI for Humanity; French Strategy for Artificial Intelligence*. <https://www.aiforhumanity.fr/en/> [Accessed: 13 August 2019].
- [39] N. Vinocur, "Macron's €1.5 billion plan to drag France into the age of artificial intelligence," *POLITICO*, 27-Mar-2018. <https://www.politico.eu/article/macron-aims-to-drag-france-into-the-age-of-artificial-intelligence/>. [Accessed: 13 August 2019].
- [40] The Villani Mission. *AI for Humanity; French Strategy for Artificial Intelligence*. <https://www.aiforhumanity.fr/en/> [Accessed: 13 August 2019].
- [41] Ibid. "Introduction," [Accessed: 13 August 2019].
- [42] Autovista Group, "France to amend legislation for autonomous vehicle trials." <https://autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials>. [Accessed: 13 August 2019].
- [43] European Commission, *GDPR Implementation: Updated State of Play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [44] In European Union law, transposition is a process by which the European Union's member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary legislation or secondary legislation. *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [45] Federal Ministry of Education and Research, Federal Ministry for Economic Affairs and Energy, and Federal Ministry of Labour and Social Affairs, "Artificial Intelligence Strategy." Nov.2018. <https://www.de.digital/DIGITAL/Redaktion/EN/Meldungen/2018/2018-11-16-federal-government-adopts-artificial-intelligence-strategy.html> [Accessed: 13 August 2019]

- [46] J. Delcker, “Germany’s €3B plan to become an AI powerhouse,” *POLITICO*, 14-Nov-2018. <https://www.politico.eu/article/germanys-plan-to-become-an-ai-powerhouse/>. [Accessed: 21-Apr-2019].
- [47] Federal Ministry of Transport and Digital Infrastructure, “Federal Government adopts action plan on automated driving.” <https://www.bmvi.de/SharedDocs/EN/PressRelease/2017/128-dobrindt-federal-government-action-plan-automated-driving.html>. [Accessed: 13 August 2019].
- [48] *Artificial Intelligence Strategy*, p. 4. https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf [Accessed: 13 August 2019]
- [49] Autovista Group, “The state of autonomous legislation in Europe,” <https://autovistagroup.com/news-and-insights/state-autonomous-legislation-europe> [Accessed: 13 August 2019]
- [50] Federal Minister of Transport and Digital Infrastructure, “Federal Government adopts action plan on automated driving.” <https://www.bmvi.de/SharedDocs/EN/PressRelease/2017/128-dobrindt-federal-government-action-plan-automated-driving.html>. [Accessed: 15 August 2019].
- [51] Covington, *Inside Privacy*, “German Bundestag approves 2nd German Data Protection Adaptation Act (“2nd DSAnpUG”): Summary of significant changes for German data protection laws.” <https://www.insideprivacy.com/eu-data-protection/german-bundestag-approves-2nd-german-data-protection-adaptation-act-2nd-dsanpug-summary-of-significant-changes-for-german-data-protection-laws/> [Accessed: 13 August 2019]
- [52] In European Union law, transposition is a process by which the European Union’s member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary legislation or secondary legislation. *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [53] The Agency for Digital Italy, *Artificial Intelligence at the Service of Citizens*. <https://ia.italia.it/assets/whitepaper.pdf>. [Accessed: 13 August 2019].
- [54] “Italy takes first steps with self-driving plans,” *Automotive News Europe*, 08-Aug-2018. <https://europe.autonews.com/article/20180815/ANE/180809790/italy-takes-first-steps-with-self-driving-plans>, [Accessed: 21 April 2019].
- [55] European Commission, *GDPR Implementation: Updated State of Play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [56] In European Union law, transposition is a process by which the European Union’s member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary legislation or secondary legislation. *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [57] “La Moncloa. 04/03/2019. Speech by President of the Government at close of the conference on the Spanish Strategy for R&D+i in Artificial Intelligence [President/Speeches].” <http://www.lamoncloa.gob.es/lang/en/presidente/intervenciones/Paginas/2019/20190304intelligence.aspx>. [Accessed: 13 August 2019].
- [58] “Spain works toward framework for autonomous driving,” *Automotive News Europe*, 08-Aug-2018. <https://europe.autonews.com/article/20180815/ANE/180809786/spain-works-toward-framework-for-autonomous-driving>. [Accessed: 13 August 2019].
- [59] European Commission, *GDPR Implementation: Updated State of play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [60] *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].

- [61] Ministry of Enterprise and Innovation, *National Approach to Artificial Intelligence*. <https://www.government.se/491fa7/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf>. [Accessed: 13 August 2019].
- [62] Wallenberg AI, Autonomous Systems, and Software Program (WASP), “62 WASP AI Positions.” <http://wasp-sweden.org/wasp-ai-positions/>. And, Knut and Alice Wallenberg Foundation, *Strategic Grants*, <https://kaw.wallenberg.org/en/strategic-grants>. [Both accessed: 21-Apr-2019].
- [63] Ministry of Enterprise and Innovation, *National Approach to Artificial Intelligence*, p.10. <https://www.government.se/491fa7/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf>. [Accessed: 15 August 2019].
- [64] In Swedish, p.4. *Artificiell intelligens i svenskt näringsliv och samhälle, (Artificial intelligence in Swedish business and society). Interim Report 12 February 2018, Reg. no 2017-05616*, https://www.vinnova.se/contentassets/55b18cf1169a4a4f8340a5960b32fa82/vr_18_08.pdf; or in English, Ministry of Enterprise and Innovation, *National Approach to Artificial Intelligence*, p.4. <https://www.government.se/491fa7/contentassets/fe2ba005fb49433587574c513a837fac/national-approach-to-artificial-intelligence.pdf>. [Accessed: 15 August 2019].
- [65] Ministry of Enterprise and Innovation, Government Offices of Sweden. “Government paves the way for self-driving vehicles,” 04-May-2017. <https://www.government.se/articles/2017/05/government-paves-the-way-for-self-driving-vehicles/>. [Accessed: 13 August 2019].
- [66] Ibid.
- [67] European Commission, *GDPR Implementation: Updated State of Play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [68] In European Union law, transposition is a process by which the European Union’s member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary legislation or secondary legislation. *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [69] Department of Business, Energy, and Industrial Strategy and Department for Digital, Culture, Media and Sport, *AI Sector Deal*. <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal>. [Accessed: 13 August 2019].
- [70] Ibid.
- [71] Centre for Data Ethics and Innovation, Department for Digital, Culture, Media, & Sport <https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei>. [Accessed: 13 August 2019].
- [72] Centre for Data Ethics and Innovation, Department for Digital, Culture, Media, & Sport. *Centre for Data Ethics (CDEI) 2-Year Strategy*, <https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-cdei-2-year-strategy/centre-for-data-ethics-cdei-2-year-strategy>. [Accessed: 13 August 2019].
- [73] HM Government, *Industrial Strategy: Building a Britain Fit for the Future*, p. 256. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf [Accessed: 13 August 2019]
- [74] HM Government Department of Transport, Centre for Connected and Autonomous Vehicles, “Code of Practice: Automated Vehicle Trialling,” February 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776511/code-of-practice-automated-vehicle-trialling.pdf, [Accessed: 12 September 2019].

- [75] Department for Transport, Department for Business, Energy & Industrial Strategy, and Centre for Connected and Autonomous Vehicles, “Automated Vehicle Trialling Code of Practice: Invitation to Comment,” 8 May 2019, <https://www.gov.uk/government/consultations/automated-vehicle-trialling-code-of-practice-invitation-to-comment>, [Accessed: 12 September 2019].
- [76] R. Cellan-Jones, BBC, “Robots on the road – how close is our driverless future?” 20 May 2019. <https://www.bbc.com/news/technology-48334449>, [Accessed: 12 September 2019].
- [77] L Kolirin, CNN, “Driverless cars will be on UK roads by 2021, says government,” 6 February 2019, <https://www.cnn.com/2019/02/06/uk/driverless-cars-scli-gbr-intl/index.html> [Accessed: 12 September 2019].
- [78] European Commission, *GDPR Implementation: Updated State of Play in the Member States*. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30306> [Accessed 14 August 2019]
- [79] *NIS Implementation Tracker*. European Cybersecurity Organization, DIGITALEUROPE. <https://www.digitaleurope.org/resources/nis-implementation-tracker/> [Accessed: 12 August 2019].
- [80] Ministerio de Modernizacion, Republic of Argentina. *1st Forum Artificial Intelligence and Internet of Things in Smart Sustainable Cities in Latin America*. <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180530/Documents/BuenosAires-Declaration-English-Final.pdf>. [Accessed: 13 August 2019].
- [81] Michalsons. “How the GDPR Changed the *Argentina Personal Data Protection Act*.” <https://www.michalsons.com/blog/argentina-personal-data-protection-act/25090> [Accessed: 13 August 2019]
- [82] President of Argentina, *Draft Personal Data Protection Bill*. <https://free.dataguidance.com/laws/argentina-draft-bill-for-a-law-on-the-protection-of-personal-data/> [Accessed: 13 August 2019]
- [83] A. Furman, M de Artaza, and F. Zappa, *The Law Reviews*, “Argentina: The Privacy, Data Protection, and Cybersecurity Law Review - Edition 5.” <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175618/argentina>. [Accessed: 11-May-2019].
- [84] Australian Government, Ministers for the Department of Industry, Innovation, and Science. *Budget 2018 - New Opportunities and Jobs for Australian Industry*. <https://www.minister.industry.gov.au/ministers/cash/media-releases/budget-2018-new-opportunities-and-jobs-australian-industry> (Accessed 14 August 2019)
- [85] Department of Industry, Innovation, and Science, Australian Government. “Artificial Intelligence: Australia’s Ethics Framework” <https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/>. [Accessed: 14 August 2019].
- [86] C. Dickeson, Global Digital Policy, Strategy Policy Division, Department of Industry, Innovation, and Science, E-mail to IEEE-USA, 16 August 2019.
- [87] Australian Government, Department of Industry, Innovation, and Science, *Artificial Intelligence: Australia’s Ethics Framework*, p.14. https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf [Accessed: 14 August 2019]
- [88] Australian Government, National Transport Commission, “National enforcement guidelines for automated vehicles,” November 2017. [https://www.ntc.gov.au/Media/Reports/\(10EB8512-5852-575D-96E9-CA20497EB1FC\).pdf](https://www.ntc.gov.au/Media/Reports/(10EB8512-5852-575D-96E9-CA20497EB1FC).pdf). [Accessed: 14 August 2019].
- [89] Office of the Australian Information Commissioner, “Australian Privacy Principles.” </privacy-law/privacy-act/australian-privacy-principles>. [Accessed: 11-May-2019].

- [90] Baker McKenzie, “Duties and liabilities of directors of Australian companies,” 2017. https://www.bakermckenzie.com/-/media/files/locations/australia/bk_australia_dutiesliabilitiesofdirectors_dec17.pdf?la=en. [Accessed: 11-May-2019].
- [91] Australian Government, “Security of Critical Infrastructure Act 2018.” <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018>. [Accessed: 14 August 2019].
- [92] In 2017, the Government of Canada appointed CIFAR – a Canadian-based global charitable organization that “convenes extraordinary minds to address the most important questions facing science and humanity” – to develop and lead the development of, “the world’s first national AI strategy.” Canadian Institute for Advanced Research, *CIFAR Pan-Canadian Artificial Intelligence Strategy*, <https://www.cifar.ca/ai/pan-canadian-artificial-intelligence-strategy> [Accessed 15 August 2019]
- [93] UNESCO Media Services, “Canada first to adopt strategy for artificial intelligence,” 22 November 2019, http://www.unesco.org/new/en/media-services/single-view/news/canada_first_to_adopt_strategy_for_artificial_intelligence/.
- [94] Treasury Board of Canada Secretariat, “Responsible use of artificial intelligence (AI),” 22 November 2018, <https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai.html>, [Accessed: 21 April 2019].
- [95] Canadian Institute for Advanced Research, *ACCOUNTABILITY IN AI: Promoting Greater Social Trust, Theme Paper for the G7 Multi-stakeholder Conference on Artificial Intelligence: Enabling the Responsible Adoption of AI December 6, 2018*. https://www.cifar.ca/docs/default-source/ai-society/g7-accountabilityinai.pdf?sfvrsn=66bdfdc2_6 [Accessed: 15 August 2019].
- [96] T. Canada, “Testing Highly Automated Vehicles in Canada,” 27-Jun-2018. https://www.tc.gc.ca/en/services/road/safety-standards-vehicles-tires-child-car-seats/testing-highly-automated-vehicles-canada.html#_TOC_250004. [Accessed: 21-Apr-2019].
- [97] Office of the Privacy Commissioner of Canada, “PIPEDA Fair Information Principles,” 16-Sep-2011. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/, [Accessed: 15 August 2019]
- [98] Public Safety Canada, “National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age,” Modified 28 May 2019. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrtg/index-en.aspx>. [Accessed: 15 August 2019]
- [99] G. Allen, Center for a New American Security, “Understanding China’s AI Strategy; Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security,” 6 February 2019, <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>. [Accessed: 15 August 2019].
- [100] New America, “Full Translation: China’s ‘New Generation Artificial Intelligence Development Plan’ (2017),” <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>. [Accessed: 15 August 2019].
- [101] Xinhuanet, “AI association to draft ethics guidelines,” 9 January 2019, http://www.xinhuanet.com/english/2019-01/09/c_137731216.htm, [Accessed; 15 August 2019].
- [102] New America, “Full Translation: China’s ‘New Generation Artificial Intelligence Development Plan’ (2017),” <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>. [Accessed: 15 August 2019].

- [103] Z. Jiaquan, South China Morning Post, “From drones to social credits, 10 ways China watches its citizens,” 04-Aug-2018. <https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china>. [Accessed: 15 August 2019].
- [104] Reuters, Technology News, “China lays out self-driving rules in global race” China Daily, 12 April 2018, <https://www.reuters.com/article/us-autos-selfdriving-china/china-lays-out-self-driving-rules-in-global-race-china-daily-idUSKBN1HK04J 13-Apr-2018>, Accessed 15 August 2019]
- [105] M. Shi, S. Sacks, and Q. Chen, New America, 8 February 2019, “Translation: China’s Personal Information Security Specification,” <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/>. [Accessed: 15 August 2019].
- [106] R. Creemers, P., and G. Webster, New America, “*Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017)*,” 29 June 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>. [Accessed: 15 August 2019].
- [107] National Institution for Transforming India (NITI Aayog), “The Premier Policy ‘Think Tank’ of the Government of India,” *National Strategy for Artificial Intelligence: Discussion Paper*, June 2018, https://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf, [Accessed 15 August 2019].
- [108] S. Mukherjee, Inc42 Media, 1 February 2018, “Budget 2018: Indian Govt. Allocates \$480 Mn Towards AI, ML, and IoT,” <https://inc42.com/buzz/budget-2018-ai-ml/>, [Accessed: 15 August 2019].
- [109] National Institution for Transforming India (NITI Aayog), “The Premier policy ‘Think Tank’ of the Government of India,” *National Strategy for Artificial Intelligence: Discussion Paper*, June 2018, p.12, https://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf, [Accessed 15 August 2019].
- [110] S. Dwivedi & R. Jhunjhunwala, ETAuto.com, from *The Economic Times*, “Opinion: The Future of Autonomous Vehicles in India – Steering the Legal Issues: AVs would mean better road and transport infrastructure, town planning, network and wireless connectivity in India,” 14 July 2018, <https://auto.economictimes.indiatimes.com/news/industry/the-future-of-autonomous-vehicles-in-india-steering-the-legal-issues/64985989>. [Accessed: 15 August 2019].
- [111] Mondaq, S.S. Rana & Co. Advocates, “India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,” 5 September 2017, <http://www.mondaq.com/india/x/626190/data+protection/Information+Technology+Reasonable+Security+Practices+And+Procedures+And+Sensitive+Personal+Data+Or+Information+Rules+2011>, [Accessed: 15 August 2019].
- [112] S. Agarwal, *The Economic Times*, “Personal Data Protection Bill: Only after New Government Takes Over,” 4 January 2019, <https://economictimes.indiatimes.com/tech/internet/personal-data-protection-bill-only-after-new-government-takes-over/articleshow/67374919.cms>. [Accessed: 15 August 2019].
- [113] Department of Electronics and Information Technology, Ministry of Communication and Information Technology, *National Cyber Security Policy, 2013*, http://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf, [Accessed: 25-May-2019].
- [114] Kyodo, “Japan’s budget for AI to be less than a fifth of that planned by U.S. and China,” *The Japan Times Online*, 25 February 2018, <https://www.japantimes.co.jp/news/2018/02/25/business/tech/japanese-government-spending-ai-less-20-u-s-china/#.XVW3YC3Mzok>, [Accessed: 15 August 2019].
- [115] K. Ogawa, “Japan revamps laws to put self-driving cars on roads; Drivers will be allowed to look at smartphones while operating level 3 vehicles,” *Nikkei Asian Review Online*, <https://asia.nikkei.com/Politics/Japan-revamps-laws-to-put-self-driving-cars-on-roads>. [Accessed: 15 August 2019].

- [116] S. Umeda, “Online Privacy Law: Japan,” Law Library, Library of Congress, <https://www.loc.gov/law/help/online-privacy-law/2012/japan.php>, [Accessed: 15 August 2019].
- [117] Ibid., S. Umeda.
- [118] “Kenya Govt Sets up Blockchain & Artificial Intelligence Taskforce!” *The Kenyan WallStreet*, 16 January 2018, <https://kenyanwallstreet.com/kenya-govt-sets-blockchain-artificial-intelligence-taskforce/>, [Accessed: 15 August 2019].
- [119] “Kenya Not Ready for New Tech,” *Kenyan Tribune Online*, 22 March 2019, <https://kenyantribune.com/kenya-not-ready-for-new-tech-the-standard/>, [Accessed: 15 August 2019]
- [120] Ministry of Information, Communications and Technology, Kenyan Government, “*The Data Protection Bill, 2018*,” <http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf>. [Accessed: 15 August 2019].
- [121] Ministry of Information, Communications and Technology, Kenyan Government, *Feel Safe Online, NATIONAL CYBERSECURITY STRATEGY 2014*, <http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf>, [Accessed: 15 August 2019].
- [122] British Embassy Mexico City and National Digital Strategy Office, Government of Mexico, *Towards An AI Strategy in Mexico; Harnessing the AI Revolution*, <http://go.wizeline.com/rs/571-SRN-279/images/Towards-an-AI-strategy-in-Mexico.pdf>. [Accessed: 15 August].
- [123] Ibid. p. 9.
- [124] Baker & McKenzie International, *Global Driverless Vehicle Survey 2018*, https://www.bakermckenzie.com/-/media/files/insight/publications/2018/03/global-driverless-vehicle-survey-2018/mm_global_driverlessvehiclesurvey2018_mar2018.pdf. [Accessed: 15 August]
- [125] “International Comparative Legal Guides,” *International Comparative Legal Guides International Business Reports*. <https://iclg.com/practice-areas/data-protection-laws-and-regulations/mexico>. [Accessed: 25-May-2019].
- [126] “PRESS RELEASE: CLARIFICATIONS OF MISCONCEPTIONS ABOUT NIGERIAN AIR FORCE FIRST INDIGENOUS OPERATIONAL UNMANNED AERIAL VEHICLE KNOWN AS TSAIGUMI” Nigerian Air Force HQ, 16 February 2018, <https://es-la.facebook.com/hqnigerianairforce/posts/2038669959679278>. [Accessed: 15 August 2019].
- [127] National Information Technology Development Agency (NITDA, NIGERIA DATA PROTECTION REGULATION 2019, <https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf>. [Accessed: 15 August 2019]
- [128] Computer Emergency Response Team, Nigeria, *Cyber Crimes (Prohibition, Prevention, etc.) Act 2015, Explanatory Memorandum*, https://www.cert.gov.ng/file/docs/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf. [Accessed: 15 August 2019].
- [129] Analytical Center for the Government of the Russian Federation, “Expert Community Discusses National AI Strategy,” 24 June 2019, <http://ac.gov.ru/en/events/022650.html>, [Accessed: 28-Aug-2019].
- [130] “Here’s How the Russian Military Is Organizing to Develop AI,” *Defense One*, <https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/>. [Accessed: 21-Apr-2019].
- [131] “Russia: Expect a National AI Roadmap by Midyear,” *Nextgov.com*, <https://www.nextgov.com/emerging-tech/2019/01/russia-expect-national-ai-roadmap-midyear/154046/>. [Accessed: 21-Apr-2019].
- [132] “Here’s How the Russian Military Is Organizing to Develop AI,” *Defense One*, <https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/>. [Accessed: 21-Apr-2019].

[133] Ibid.

[134] “Russia: Government Begins Testing Driverless Cars,” *Global Legal Monitor*, Library of Congress, 18 January 2019, <http://www.loc.gov/law/foreign-news/article/russia-government-begins-testing-driverless-cars/>. [Accessed: 25 August 2019]

[135] “Law in Russia - DLA Piper Global Data Protection Laws of the World,” <https://www.dlapiperdataprotection.com/index.html?t=law&c=RU>. [Accessed: 27-May-2019].

[136] “Russia - The Privacy, Data Protection, and Cybersecurity Law Review - Edition 5 - The Law Reviews.” <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175638/russia>. [Accessed: 27-May-2019].

[137] Kingdom of Saudi Arabia, <https://vision2030.gov.sa/en>, [Accessed 25 August 2019].

[138] “Artificial Intelligence in Saudi Arabia,” *Arab News*, 23-Feb-2019. <http://www.arabnews.com/node/1457086>. and <https://www.neom.com>, [Accessed: 25 August 2019]

[139] C. Jewell, Communications Division, WIPO, *Saudi Arabia embraces AI-driven innovation*, https://www.wipo.int/wipo_magazine/en/2018/05/article_0002.html. [Accessed: 25 August 2019].

[140] “Artificial Intelligence in Saudi Arabia,” *Arab News*, 23-Feb-2019. <http://www.arabnews.com/node/1457086>. [Accessed: 25 August 2019].

[141] C. Jewell, Communications Division, WIPO, *Saudi Arabia embraces AI-driven innovation*, https://www.wipo.int/wipo_magazine/en/2018/05/article_0002.html. [Accessed: 25 August 2019].

[142] “Saudi-backed Vision Fund invests in GM’s driverless car program,” *Arab News*, 31-May-2018, <http://www.arabnews.com/node/1313171/business-economy>. [Accessed: 21-Apr-2019].

[143] N. Al-Fawzan and O. Elsayed, “Data Protection in the Kingdom of Saudi Arabia - a Primer,” p. 2.

[144] E. Atwell, C. Brierley, K. Dukes, M. Sawalha, and A.-B. M. Sharaf, “An Artificial Intelligence approach to Arabic and Islamic content on the internet,” 2011.

[145] Kingdom of Saudi Arabia, Bureau of Experts at the Council of Ministers, *Anti-Cyber Crime Law*, Translation of Saudi Laws, 2009, https://www.citc.gov.sa/en/RulesandSystems/CITCSys/Docs/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf, [Accessed: 25 August 2019].

[146] National Research Foundation, Prime Minister’s Office, Singapore, AI Singapore, <https://www.nrf.gov.sg/programmes/artificial-intelligence-r-d-programme>. [Accessed: 25 August 2019].

[147] Infocomm Media Development Authority, Singapore Government, <https://www2.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2018/composition-of-the-advisory-council-on-the-ethical-use-of-ai-and-data>, [Accessed: 25 August 2019].

[148] AI Singapore Research Programme, National University of Singapore, *AI SINGAPORE RESEARCH PROGRAMME GRANT CALL*, <https://www.aisingapore.org/wp-content/uploads/2019/01/AI-Spore-Research-Prog-Administrative-Guidelines-21Jan2019.pdf>, [Accessed: 25 August 2019].

[149] “Road Traffic Act - Singapore Statutes Online.” <https://sso.agc.gov.sg/Act/RTA1961>. [Accessed: 25-May-2019].

[150] “Joint Media Release by the Land Transport Authority (LTA), Enterprise Singapore, Standards Development Organization & Singapore Standards Council - Singapore Develops Provisional National Standards to Guide Development of Fully Autonomous Vehicles | Press Room | Land Transport Authority,” <https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=8ea02b69-4505-45ff-8dca-7b094a7954f9>. [Accessed: 25-May-2019].

- [151] Singapore; *Data Protection 2019*, International Comparative Legal Guides, <https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore>. [Accessed: 25 August 2019].
- [152] “Cybersecurity Act,” *Cyber Security Agency*. <http://www.csa.gov.sg/legislation/cybersecurity-act>. [Accessed: 25-May-2019].
- [153] Synced, *Medium*, “South Korea Aims High on AI, Pumps \$2 Billion into R&D,” <https://medium.com/syncedreview/south-korea-aims-high-on-ai-pumps-2-billion-into-r-d-de8e5c0c8ac5>, [Accessed; 25 August 2019].
- [154] Government of the Republic of Korea, Interdepartmental Exercise, *Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society: Managing the Fourth Industrial Revolution*, p.56, <http://www.msip.go.kr/dynamic/file/afieldfile/msse56/1352869/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf>, [Accessed 25 August 2019].
- [155] *Ibid.* p. 6.
- [156] G. Olano, “South Korea to create roadmap on self-driving cars,” *Insurance Business*, <https://www.insurancebusinessmag.com/asia/news/breaking-news/south-korea-to-create-roadmap-on-selfdriving-cars-115960.aspx>, [Accessed: 21-Apr-2019].
- [157] J.P. Tomas, Enterprise IoT Insights, *South Korea completes works in K-City autonomous driving testing zone*, <https://enterpriseiotinsights.com/20181212/connected-cars-2/south-korea-completes-works-kcity-autonomous-driving-testing-zone>. [Accessed: 25 August 2019].
- [158] GDPR matchup: South Korea’s *Personal Information Protection Act*. (n.d.). Retrieved May 25, 2019, from <https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/>
- [159] “Korea: Cybersecurity 2019 - International Comparative Legal Guides,” *International Comparative Legal Guides International Business Reports*. <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/korea>. [Accessed: 25-May-2019].
- [160] *AI Taiwan: Innovation, Collaboration and Inspiration*, <https://ai.taiwan.gov.tw>. [Accessed: 25 August 2019].
- [161] “AI Taiwan.pdf.” <http://www.jaist.ac.jp/~bao/AI/OtherAIstrategies/AI%20Taiwan.pdf>. [Accessed: 25 August 2019].
- [162] K.Y.H. Wang, Baker McKenzie, *Taiwan Recently Enacted the Unmanned Vehicle Technology Innovation Experiment Regulations While Gearing Up for Autonomous Vehicles*, <https://www.bakermckenzie.com/en/insight/publications/2019/02/taiwan-recently-enacted-the-unmanned>, [Accessed: 25 August 2019].
- [163] “Personal Information Protection Act,” *Laws & Regulations Database of The Republic of China*, <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>. [Accessed: 25 August 2019].
- [164] L. Zhang, “Taiwan: New Cybersecurity Law Takes Effect,” 30 January 2019, *Global Legal Monitor*, Library of Congress, <https://www.loc.gov/law/foreign-news/article/taiwan-new-cybersecurity-law-takes-effect/>, [Accessed: 26-May-2019].
- [165] Agence Nationale de la Promotion de la Recherche Scientifique, République Tunisienne, Ministère de l’Enseignement Supérieur et de la Recherche Scientifique, *National AI Strategy: Unlocking Tunisia’s capabilities potential*, <http://www.anpr.tn/national-ai-strategy-unlocking-tunisias-capabilities-potential/>, [Accessed: 25 August 2019].
- [166] *Ibid.*
- [167] “INPDP_Accueil.” <http://www.inpdp.nat.tn/>. [Accessed: 26-May-2019].

- [168] “Now more than ever, Tunisians need a functioning Data Protection Authority,” *Access Now*, 25-Feb-2019. <https://www.accessnow.org/now-more-than-ever-tunisians-need-a-functioning-data-protection-authority/>. [Accessed: 26-May-2019].
- [169] *Organic Act n°2004-63 of July 27th 2004 on the protection of personal data*, <https://media2.mofo.com/documents/The+Organic+Act+2004-63.pdf>. [Accessed: 25 August 2019].
- [170] R. Ferchiou and A. Larbi, “Tunisia: Cybersecurity 2019,” *International Comparative Legal Guides International Business Reports*, 16-Oct-2018. <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/tunisia>. [Accessed: 27-May-2019].
- [171] Ministry of Cabinet Affairs and The Future, United Arab Emirates, <https://uaecabinet.ae/en/details/news/mohammed-bin-rashid-launches-five-decade-government-plan-uae-centennial-2071>. The vision for the plan may be viewed at: <https://area2071.ae/our-vision/>. [Accessed: 26 August 2019].
- [172] Ministry of Cabinet Affairs and The Future, United Arab Emirates, <https://uaecabinet.ae/en/details/news/uae-cabinet-adopts-national-artificial-intelligence-strategy-2031>, [Accessed: 26 August 2019]
- [173] UAE Government, <https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/uae-strategy-for-artificial-intelligence>, [Accessed: 26 August 2019].
- [174] The National, *Sheikh Mohammed bin Rashid announces Dh1.5bn ‘new generation of UAE schools’*, 4 March 2019, <https://www.thenational.ae/uae/education/sheikh-mohammed-bin-rashid-announces-dh1-5bn-new-generation-of-uae-schools-1.832941>, [Accessed: 26 August 2019].
- [175] Smart Dubai is an initiative of, “His Highness Sheikh Mohammed Bin Rashid Al Maktoum, Vice-President & Prime Minister of the UAE, and Ruler of Dubai, to make Dubai the happiest city on Earth.” <https://www.smartdubai.ae/about-us>, [Accessed 25 August 2019].
- [176] *Smart Dubai: AI Ethics Principles & Guidelines*, <https://www.smartdubai.ae/initiatives/ai-principles-ethics>, [Accessed: 26-May-2019].
- [177] *AI Everything*, an annual global AI summit hosted by the Dubai government, <https://ai-everything.com/about-ai-everything/>, [Accessed: 26 August 2019].
- [178] Dubai Future Foundation, *Dubai’s Autonomous Transportation Strategy*, <https://www.dubaifuture.gov.ae/our-initiatives/dubais-autonomous-transportation-strategy/>, [Accessed: 26-May-2019].
- [179] Telecommunications Regulatory Authority, United Arab Emirates, “Regulatory Policy - Internet of Things (IoT),” <https://www.tra.gov.ae/en/about-tra/telecommunication-sector/regulations-and-ruling/details.aspx#description>, [Accessed: 26 August 2019].
- [180] “National Cyber Security Strategy of the UAE - The Official Portal of the UAE Government.” <https://www.government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cyber-security-strategy-of-the-uae>. [Accessed: 26-May-2019].
- [181] T. Karombo & Commentary, “Zimbabwe is trying to transform itself into a leading tech hub with China’s help,” 15 June 2018, *Quartz Africa*, <https://qz.com/africa/1306520/zimbabwe-needs-china-for-its-tech-and-ict-ambitions/>. [Accessed: 25 August 2019].
- [182] *CYBERCRIME and CYBERSECURITY BILL, 2017*, <https://t792ae.c2.acecdn.net/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf>. [Accessed: 25-May-2019].
- [183] S. Karombo, Zimbabwe fast-tracks cybercrime legislation, *itWebAfrica*, 31 January 2019, <http://www.itwebafrica.com/security/887-zimbabwe/245414-zimbabwe-fast-tracks-cybercrime-legislation>, [Accessed: 26 August 2019].



IEEE★USA

IEEE-USA
2001 L St NW Suite 700
Washington, D.C. 20036
<https://ieeusa.org>