



GLOBAL STANDARDS ON **ARTIFICIAL INTELLIGENCE**

A report on global legislation &
policy positions governing
AI technology

December 2020

Rahul Rai & Shruti Aji Murali

The authors are practicing advocates with a special focus on technology and antitrust/competition law, and may be reached at

rahulrai@gschambers.org & shrutiajimurali@gmail.com

| | |
|-------------------------------------|-----------|
| TABLE OF ABBREVIATIONS | 10 |
| INTRODUCTION | 14 |
| Methodology | 15 |
| DEFINITION OF AI | 16 |
| INDIA | 18 |
| USA..... | 18 |
| CHINA..... | 19 |
| CANADA | 21 |
| UK..... | 21 |
| FRANCE | 23 |
| GERMANY..... | 23 |
| RUSSIA | 24 |
| ISRAEL..... | 24 |
| DENMARK..... | 25 |
| EU | 25 |
| AUSTRALIA..... | 26 |
| JAPAN | 26 |
| SINGAPORE..... | 27 |
| SOUTH KOREA..... | 28 |
| SWEDEN | 29 |
| FINLAND..... | 29 |
| SPAIN | 29 |
| NORWAY | 30 |
| ESTONIA..... | 30 |
| THE NETHERLANDS..... | 31 |
| UAE..... | 31 |
| HONG KONG | 32 |
| TRANSPARENCY | 33 |
| MATURITY INDEX | 36 |

| | |
|-------------------------------|-----------|
| INDIA | 37 |
| USA..... | 37 |
| CHINA..... | 38 |
| CANADA | 38 |
| UK..... | 39 |
| FRANCE..... | 40 |
| GERMANY..... | 40 |
| RUSSIA | 40 |
| DENMARK..... | 41 |
| EU | 41 |
| AUSTRALIA..... | 42 |
| JAPAN | 43 |
| SINGAPORE..... | 43 |
| SOUTH KOREA..... | 44 |
| SWEDEN | 44 |
| FINLAND..... | 44 |
| SPAIN | 45 |
| NORWAY | 45 |
| ESTONIA..... | 46 |
| THE NETHERLANDS..... | 46 |
| UAE..... | 47 |
| HONG KONG | 47 |
| INTEROPERABILITY | 49 |
| MATURITY INDEX..... | 52 |
| INDIA | 53 |
| USA..... | 54 |
| CHINA..... | 54 |
| CANADA | 55 |
| UK..... | 55 |
| FRANCE..... | 56 |
| GERMANY..... | 56 |
| ISRAEL..... | 57 |

| | |
|----------------------|----|
| DENMARK..... | 57 |
| EU | 57 |
| AUSTRALIA..... | 58 |
| SINGAPORE..... | 59 |
| SOUTH KOREA..... | 59 |
| SWEDEN | 59 |
| FINLAND..... | 60 |
| SPAIN | 60 |
| NORWAY | 60 |
| ESTONIA..... | 61 |
| THE NETHERLANDS..... | 61 |
| UAE..... | 62 |
| HONG KONG | 62 |

PRIVACY & CONSENT63

| | |
|----------------------------|-----------|
| MATURITY INDEX..... | 65 |
| INDIA | 66 |
| USA..... | 68 |
| CHINA..... | 70 |
| CANADA | 71 |
| UK..... | 73 |
| FRANCE | 74 |
| GERMANY..... | 74 |
| ISRAEL..... | 75 |
| DENMARK..... | 76 |
| EU | 77 |
| AUSTRALIA..... | 78 |
| SINGAPORE..... | 80 |
| SOUTH KOREA..... | 81 |
| SWEDEN | 82 |
| FINLAND..... | 83 |
| SPAIN | 84 |
| NORWAY | 84 |

| | |
|-----------------------|----|
| ESTONIA | 86 |
| THE NETHERLANDS | 86 |
| UAE | 87 |
| HONG KONG | 88 |

NETWORK SECURITY.....89

| | |
|------------------------------|-----|
| MATURITY INDEX.....91 | |
| INDIA | 92 |
| USA..... | 93 |
| CHINA..... | 94 |
| CANADA | 95 |
| UK..... | 96 |
| FRANCE | 97 |
| GERMANY..... | 97 |
| ISRAEL..... | 98 |
| RUSSIA | 98 |
| DENMARK..... | 99 |
| EU | 99 |
| AUSTRALIA..... | 101 |
| JAPAN | 102 |
| SINGAPORE..... | 103 |
| SOUTH KOREA..... | 103 |
| SWEDEN | 104 |
| FINLAND..... | 104 |
| SPAIN | 105 |
| NORWAY | 105 |
| ESTONIA..... | 106 |
| THE NETHERLANDS..... | 107 |
| UAE..... | 107 |
| HONG KONG | 107 |

ETHICS & HUMAN RIGHTS109

| | |
|-------------------------------|-----|
| MATURITY INDEX.....113 | |
| INDIA | 114 |

| | |
|----------------------|-----|
| USA..... | 115 |
| CHINA..... | 116 |
| CANADA | 117 |
| UK..... | 118 |
| FRANCE | 119 |
| GERMANY..... | 119 |
| RUSSIA | 120 |
| DENMARK..... | 120 |
| EU | 121 |
| AUSTRALIA..... | 122 |
| JAPAN | 123 |
| SINGAPORE..... | 124 |
| SOUTH KOREA..... | 125 |
| SWEDEN | 126 |
| FINLAND..... | 126 |
| SPAIN | 127 |
| NORWAY | 127 |
| ESTONIA..... | 128 |
| THE NETHERLANDS..... | 128 |
| UAE..... | 129 |
| HONG KONG..... | 129 |

INTELLECTUAL PROPERTY RIGHTS 131

| | |
|----------------------------|------------|
| MATURITY INDEX..... | 136 |
| INDIA | 137 |
| USA..... | 137 |
| CHINA..... | 139 |
| CANADA | 140 |
| UK..... | 141 |
| FRANCE | 141 |
| GERMANY..... | 142 |
| ISRAEL..... | 143 |
| RUSSIA | 144 |

| | |
|-----------------------|-----|
| DENMARK..... | 144 |
| EU | 144 |
| AUSTRALIA..... | 146 |
| JAPAN | 146 |
| SINGAPORE..... | 147 |
| SOUTH KOREA..... | 147 |
| SWEDEN | 148 |
| FINLAND..... | 148 |
| SPAIN | 149 |
| NORWAY | 150 |
| ESTONIA..... | 150 |
| THE NETHERLANDS | 150 |
| UAE..... | 151 |
| HONG KONG | 151 |

CIVIL LIABILITY..... **152**

| | |
|----------------------------|------------|
| MATURITY INDEX..... | 154 |
| INDIA | 155 |
| USA..... | 155 |
| CHINA..... | 156 |
| CANADA | 156 |
| UK..... | 156 |
| FRANCE | 157 |
| GERMANY..... | 157 |
| RUSSIA | 157 |
| ISRAEL..... | 158 |
| DENMARK..... | 158 |
| EU | 158 |
| AUSTRALIA..... | 160 |
| JAPAN | 160 |
| SINGAPORE..... | 160 |
| SOUTH KOREA..... | 161 |
| SWEDEN | 161 |

| | |
|----------------------|-----|
| FINLAND | 161 |
| SPAIN | 162 |
| NORWAY | 162 |
| ESTONIA..... | 162 |
| THE NETHERLANDS..... | 163 |
| UAE..... | 163 |
| HONG KONG | 163 |

AUTONOMOUS VEHICLES..... 164

| | |
|----------------------|-----|
| MATURITY INDEX..... | 167 |
| INDIA | 168 |
| USA..... | 168 |
| CHINA..... | 169 |
| CANADA | 170 |
| UK..... | 171 |
| FRANCE | 172 |
| GERMANY..... | 173 |
| ISRAEL..... | 173 |
| RUSSIA | 174 |
| DENMARK..... | 174 |
| EU | 175 |
| AUSTRALIA..... | 176 |
| JAPAN | 177 |
| SINGAPORE..... | 177 |
| SOUTH KOREA..... | 178 |
| SWEDEN | 179 |
| FINLAND..... | 179 |
| SPAIN | 180 |
| NORWAY..... | 180 |
| ESTONIA..... | 181 |
| THE NETHERLANDS..... | 181 |
| UAE..... | 182 |
| HONG KONG | 182 |

AUTONOMOUS WEAPONS 184

| | |
|----------------------|-----|
| MATURITY INDEX..... | 187 |
| INDIA | 188 |
| USA..... | 189 |
| CHINA..... | 190 |
| CANADA | 190 |
| UK..... | 191 |
| FRANCE | 191 |
| GERMANY..... | 192 |
| ISRAEL..... | 193 |
| RUSSIA | 193 |
| DENMARK..... | 194 |
| EU | 194 |
| AUSTRALIA..... | 195 |
| JAPAN | 196 |
| SOUTH KOREA..... | 196 |
| SWEDEN | 196 |
| FINLAND..... | 197 |
| NORWAY | 197 |
| ESTONIA..... | 198 |
| THE NETHERLANDS..... | 198 |



TABLE OF ABBREVIATIONS

| Abbreviation | Full form |
|------------------------|---|
| ACCC | Australian Competition and Consumer Commission |
| ADS | Automatic Driving System |
| Advisory Council | Advisory Council for the Ethical Use of AI and Data |
| AEVA | Automated and Electronic Vehicles Act 2018 |
| AI | Artificial Intelligence |
| AI Executive Order | (US) Executive Order on Maintaining American Leadership in Artificial Intelligence, 2019 |
| AIA | Algorithmic Impact Assessment |
| AIDP | (Chinese) New Generation Artificial Intelligence Development Plan |
| AIHLEG | EU High-Level Expert Group on Artificial Intelligence |
| AIV | Advisory Council on International Affairs |
| APT | Advanced and persistent threats |
| C-ITS | Co-operative Intelligent Transport Systems initiative |
| CCAV | Centre for Connected and Autonomous Vehicles |
| CCMTAs | Canadian Council of Motor Transport Administrators |
| CCW | Convention on Certain Conventional Weapons |
| CDPA | The (UK) Copyright, Designs and Patents Act 1998 |
| CGW | Computer Generated Works |
| CII | Computer Implemented Innovations |
| CMAPS | Crime Mapping, Analytics and Predictive Systems |
| CNIL | Commission Nationale de l'Informatique et des Libertés or the National Commission for Information and Liberty |
| CRI | Computer Related Inventions |
| CS Strategy | UK Interim Cyber Security Science and Technology Strategy |
| Cybersecurity Strategy | Danish National Strategy for Cyber and Information Security |
| DCMS | UK Department for Digital, Culture, Media and Sports |
| DGT | Spanish Directorate General of Traffic |
| DIA | Discrimination Impact Assessment |
| Digital Economy | Russian national program called 'Digital Economy of Russian Federation' |
| DPMA | German Patent and Trademark Office |

| Abbreviation | Full form |
|------------------------------|---|
| EDIA | Ethical Data Impact Assessment |
| Enhanced Elements and Values | Enhanced Data Stewardship Accountability Elements for Data Processing Activities, such as AI and ML, that Directly Impacts People and Data Stewardship Values |
| ENISA | EU Agency for Cybersecurity |
| EPO | European Patent Office |
| EU EU | European Union |
| Framework | Hong Kong Ethical Accountability Framework |
| GDPR | General Data Protection Regulation |
| German National Strategy | German National Strategy for AI |
| GGE | Group of Governmental Experts on LAWS |
| GPAI | Global Partnership on AI |
| HITL | Human in the Loop |
| ICBM technologies | IoT, cloud computing, big data analysis, and mobile technologies |
| INCD | Israel National Cyber Directorate |
| INCIBE | Spanish National Cybersecurity Institute |
| IoT | Internet of Things |
| IPA | Intelligent Process Automation |
| IPOS | Intellectual Property Office of Singapore |
| IPRs | Intellectual Property rights |
| JPO | Japan Patent Office |
| KIPO | Korean Intellectual Property Office |
| LAWS | Lethal Autonomous Weapon Systems |
| MIC | Ministry of Internal Affairs and Communication of Japan |
| MOLMOP | (Israeli) National Council for Research and Development |
| Indian AI Report | UAE Aayog's report on the National AI Strategy |
| NATO | North Atlantic Treaty Organization |
| NHTSA | US National Highway Traffic Safety Administration |
| NIST | US National Institute of Standards and Technology |
| NSTC | US National Science and Technology Council |

| Abbreviation | Full form |
|-----------------------|--|
| NTC | Australian National Transport Commission |
| NTF | EU New Technologies Formation |
| OECD | Organization for Economic Co-operation and Development |
| OECD Principles on AI | OECD Principles for AI, Robustness, Security and Safety |
| OPSOC | Ottawa Police Strategic Operations Centre |
| PCPD | Hong Kong Privacy Commissioner for Personal Data |
| PDPC | (Singapore) Personal Data Protection Commission |
| PDPO | Hong Kong's Personal Data (Privacy) Ordinance |
| PLDF | EU Product Liability Directive Formation |
| POM | Process Oversight Model |
| PRH | Finnish Patent and Registration Office |
| R&D | Research & development |
| R&D Guidelines | Draft AI Research and Development Guidelines |
| Regulations | Beijing Guidance on Accelerating Road Testing for Self-Driving Vehicles (Trial) and Beijing Implementing Rules for Managing Road Testing for Self-Driving Vehicles (Trial) |
| RTA | Singapore Road Traffic Act |
| SRI | Software related inventions |
| UAE | United Arab Emirates |
| UK | United Kingdom |
| US DoD | US Department of Defense |
| USA / US | United States of America |
| USCO | US Copyright Office |
| USPTO | US Patent and Trademark Office |
| WIPO | World Intellectual Property Organisation |
| WIPO Discussion Paper | WIPO published a Draft Discussion Paper on IP and AI in December 2019 |
| XAI | explainable AI |



INTRODUCTION

Although Artificial Intelligence (**AI**) is generally seen as a technology of the future, it has already entered our day-to-day lives in many ways. Since much of this technology is created and built upon by the private sector, the legal framework governing AI or the repercussions of actions taken by AI may not be clear in many cases. Developments in this respect have not been uniform across the world. Some countries have been at the forefront of research & development (**R&D**) in AI-based technologies and applications, not just in the private sector but also in government functioning. As such, these countries have started to grapple with questions of law and policy in the AI space sooner than others.

Globally, there appears to be a broad consensus on the general ethical principles by which AI-based technology should function and the ways in which AI intersects with existing legal frameworks such as privacy, liability, and intellectual property rights (**IPRs**). However, at present, the technology itself appears to be too nascent, for any global standard to emerge. Nevertheless, key sectors in which some developments have occurred from a policy-setting perspective include healthcare, targeted advertising and autonomous vehicles.

Methodology

This report reviews the law and policy governing various aspects in which AI intersects or is likely to intersect with existing legal rights and obligations, across 22 jurisdictions.

The issues chosen span areas that affect individual users such as the right to privacy and other human rights, to systemic issues such as network security and interoperability with AI systems. The report also focuses on two kinds of AI applications that are already being used to varying degrees across the world – autonomous vehicles and autonomous weapons.

The jurisdictions reviewed were a cross-section of countries at various stages of development. Jurisdictions such as the United States of America (**USA**), the European Union (**EU**), United Kingdom (**UK**), France, Germany, China, South Korea, Japan, etc. are at

the forefront of AI R&D. This is reflected in the advanced level of policy discussion and legislation that accounts for the impact of AI technology in some way. However, other countries such as India, Russia, the United Arab Emirates (**UAE**), Israel, etc. are generally not as far ahead in terms of developing AI based technology and legislating for them.

In terms of the range of policy and legal developments, this paper tracks stated / reported policy positions or discussions which have been initiated by government or public bodies, through to more concrete policy positions and legislation.

Every chapter introduces the issue with an overview of the range of policy positions and current research, including by global multilateral agencies (such as the United Nations, and Organization for Economic Co-operation and Development (**OECD**)), academic papers and conferences. Developments in each country are then tracked against this broad global outlook.

Every chapter also includes a maturity index that ranks each country from level 1 to level 5, in increasing order of "maturity".

Countries are ranked at level 1 if there has been no consideration or discussion of an issue at all. Level 2 indicates preliminary discussions, academic or public consultation on issues relating to AI, although there may not be a clearly formulated policy position. Countries ranked at Level 3 have developed a clear policy position, with concrete statements through a strategy document or guidelines published by a government department or public authority. However, these may merely indicate consideration of the issue at hand (e.g., stating the need to achieve interoperability across AI systems) rather than concrete decisions or methods for achieving a particular policy goal or position (e.g., prescribing a particular standard or methodology to achieve interoperability across social networks or data collected by public authorities), which would be ranked at Level 4. The highest level or rank would be reserved for jurisdictions that have formalized a stated policy into law, rather than merely providing guidance or recommendations. Admittedly, very few jurisdictions can be said to have reached this level of maturity on AI-related issues, given the nascence of the subject matter.

DEFINITION OF AI

The concept of AI was conceived in 1956 with the publication of the academic paper, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence'.¹ The document is considered to be the founding basis for the definition of AI. As with any regulatory regime, the definition of the subject is a crucial first step to delineating its scope and influence. In the case of AI, which is a rapidly evolving field, the need for an appropriate definition is even greater. Although developments in AI technology have rapidly emerged across the world, most countries do not have a specific regulatory regime as yet. In most cases, there appear to be broad road maps or strategies that provide guidance on areas of further research. Within these documents, AI has broadly been defined as encompassing any technology that can approximate human intelligence. Further categorisations of AI are done on the basis of (a) the range of subjects covered by the technology – i.e., specific of 'weak' AI which is applied to a specific data set; and general or 'strong' AI which is not limited to any particular kinds of data; or (b) the type of technology or processes that use AI – e.g., machine learning, robotics, pattern recognition, etc.

Broadly, AI can be classified into the four categories set out below:²

Thinking humanly -

"the exciting new effort to make computers think... machines with minds, in the full and literal sense..." (John Hageland, 1985)

"[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning..." (Richard Bellman, 1978)

Thinking rationally -

"The study of mental faculties, through the use of computational models" (Charniak & McDermott, 1985)

"The study of the computations that make it possible to perceive, reason, and act" (Winston, 1992)

Acting humanly -

"The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990)

"The study of how to make computers do things at which, at the moment, people are better" (Rich & Knight, 1991)

"Computational intelligence is the study of the design of intelligent agents." (Poole et al., 1998)

"AI... is concerned with intelligent behaviour in artifacts.." (Nilsson, 1998)

In his paper "On Defining Artificial Intelligence" Pei Wang (2019) defines intelligence as "the capacity of an information-processing system to adapt to its environment while operating with insufficient knowledge and resources."³ In a 2020 response to comments on the 2019 definition, he notes that while stakeholders in the field of AI do not want to spend all their time debating definition, this issue currently does not draw sufficient attention. He notes that many of the current debates on AI can be traced back to "different understandings of intelligence".⁴

In the following chapter, we consider the definition of AI in different jurisdictions and the approach adopted by the regulatory regimes in defining it. Given that the definition of AI is drawn from research and the state of technology, this chapter does not include a maturity index.

1. McCarthy, J., Minsky, M. L., et al., "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", AI Magazine, August 1955, available at <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>

2. Doris Salazar, "Artificial intelligence: From Turing test to the Dream of Emulating Human Brain", 6 October 2016, available at <http://innovacion.uas.edu.mx/artificial-intelligence-from-turing-test-to-the-dream-of-emulating-human-brain/?lang=en>

3. Wang, P, "On Defining Artificial Intelligence", Journal of Artificial General Intelligence, 2019, Volume 10 Issue 2, pages 1–37, available at <https://content.sciendo.com/downloadpdf/journals/jagi/10/2/article-p1.pdf>

4. Wang P, "On Defining Artificial Intelligence – Author's Response to Commentaries", Journal of Artificial General Intelligence, 2020, Volume 11 Issue 2, pages 73-86, available at <https://content.sciendo.com/downloadpdf/journals/jagi/11/2/article-p1.xml#page=16>.

INDIA

As per the NITI Aayog's report on the National AI Strategy (**Indian AI Strategy**),⁵ AI is a constellation of technologies that enables machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act, while acknowledging the largely accepted definition of AI outlined by scientists such as John McCarthy, Alan Turing and Marvin Minsky. The National AI Report highlights that an AI system can also take action in the physical world through technologies such as expert systems and inference engines.

The Indian AI Strategy further divides AI in various categories like weak AI, strong AI, narrow AI, general AI and superintelligence. Weak AI is understood to be "simulated" thinking and is a system which appears to behave intelligently but doesn't have any kind of consciousness of its own actions. Strong AI, on the other hand, describes "actual" thinking, i.e., behaving intelligently, thinking as human does, with a conscious, subjective mind. Narrow AI is limited to a single task or a set number of tasks (such as Deep Mind's AlphaGo, the first computer program to defeat a professional human Go player⁶), whereas general AI, describes an AI which can undertake a wide range of tasks in various environments, making it closer to human intelligence. Finally, superintelligence is a term used to refer to general and strong AI at the point at which it surpasses human intelligence, if that occurs in the future.

USA

In 2016, the National Science and Technology Council (**NSTC**) committee on AI published its report⁷ on preparing for the future of AI and while it acknowledged that there is no single definition of AI that is universally accepted by the practitioners, it identified the following four features:

1. Systems that think like humans (e.g., cognitive architectures and neural networks)
2. Systems that act like humans (e.g., pass the Turing test via natural language processing (**NLP**), knowledge representation, automated reasoning and learning)
3. Systems that think rationally (e.g., logic solvers, inference and optimization);
4. Systems that act rationally (e.g., intelligent software agents and embodied robots that achieve goals via perception, planning, reasoning, learning, communicating, decision-making, and acting)

Aside from this, the John S. McCain National Defence Authorization Act⁸ defines AI as including:

1. Any artificial system that performs tasks under varying and unpredictable circumstance without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

5. NITI Aayog, "National Strategy for Artificial Intelligence, #AIForAll", June 2018, available at <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>

6. "AlphaGo: The Story so Far", available at <https://deepmind.com/research/case-studies/alphago-the-story-so-far>

7. National Science and Technology Council, "Preparing for The Future of Artificial Intelligence", October 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

8. Section 238 of the John S. McCain National Defense Authorization Act for fiscal year 2019, available at <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>

3. An artificial system designed to think or act like a human, Including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Further, the Executive Order on Maintaining American Leadership in Artificial Intelligence, February 2019 (**AI Executive Order**)⁹ defined the term 'artificial intelligence' to the full extent of Federal investments in AI, to include: R&D of core AI techniques and technologies; AI prototype systems; application and adaptation of AI techniques; architectural and systems support for AI; and cyber-infrastructure, data sets, and standards for AI.¹⁰

CHINA

In July 2017, China issued the 'New Generation Artificial Intelligence Development Plan' (**AIDP**)¹¹. While it does not have a set definition of AI, it mentions the following theories of AI as areas for further research:

1. Big data intelligence theory: Research new data-driven and knowledge-driven AI methods, theories and methods for sensing computing theory with NLP, images and figures at the core, comprehensive deep reasoning and creative AI theories and methods, basic theories and frameworks on smart decision-making with incomplete information, data-driven common AI data models and theories, etc.
2. Cross-media sensing and computing theory: Research sensing that exceeds human visual abilities, active visual sensing and computing aimed at the real world, auditory sensing and computing of natural acoustic scenes, language sensing and computing in an environment of natural interaction, human sensing and computing aimed at asynchronous orders, autonomous learning aimed at smart media sensing, and urban omni-dimensional smart sensing and reasoning engines.
3. Hybrid and enhanced intelligence theory: Research hybridization and convergence of humans and machines; behavioural strengthening through human-machine smart symbiosis and brain-machine coordination; intuitive machine reasoning and causal models; associative recall models and knowledge evolution methods, complex data and task blended and enhanced intelligence learning methods, cloud robotics coordination computing methods, and situational comprehension and human-machine group coordination in real-world environments.
4. Swarm intelligence theory: Research swarm intelligence structural theory and organizational methods, swarm intelligence incentive mechanisms and emergence mechanisms, swarm intelligence learning theories and methods, common swarm intelligence computing paradigms and models.
5. Autonomous coordination and control, and optimized decision-making theory: Research coordination sensing and interaction aimed at autonomous unmanned systems, coordination, control and optimized decision-making aimed at autonomous and unmanned systems, knowledge-driven human-machine-object triangular coordination and interoperability theories.

9. Executive Order on Maintaining American Leadership in Artificial Intelligence (2019), available at: <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>

10. Section 9(a) of the Executive Order 13859 announcing the American AI Initiative, available at <https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf>

11. China's 'New Generation Artificial Intelligence Development Plan', 2017, available at <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> The purpose of the plan is to set out a road map for research in the field of AI.

6. High-level machine learning theory: Research basic statistical learning theories, reasoning and decision-making under uncertainty, distributed learning and interaction, learning while protecting privacy, small-sample learning, deep intensive learning, unsupervised learning, semi-supervised learning, active learning and other such learning theories and efficient models.
7. Brain-inspired intelligence computing theory: Research theories and methods on brain-inspired sensing, brain-inspired learning, and recall mechanisms; computing blends, brain-inspired complex systems, brain-inspired control, etc.
8. Quantum intelligent computing theory: Explore cognitive quantum models and intrinsic mechanisms, research efficient quantum intelligence models and algorithms, high-performance and high-bitrate quantum AI processors, real-time quantum AI systems that can exchange information with the outside world, etc.

The findings of the research under the plan will feed into the definition of AI for the proposed regulatory regime. Additionally, the document highlights the strategy adopted to build a next-generation AI key general technology system, which would focus on making algorithms the core; data and hardware the foundation; and upping capabilities in sensing and recognition, knowledge computing, cognitive reasoning, executing motion and human-machine interface the emphasis; in order to form openly compatible, stable and mature technological systems.

1. Knowledge computing engine and knowledge service technology: Key breakthroughs in knowledge processing, deep search, and visual interactive core technology; realization of automatic acquisition of incrementally growing knowledge; possession of concept discernment, object discovery, attribute prediction, evolutionary knowledge modelling, and relationship discovery capabilities; the formation of multi-billion-scale, multi-source, multi-disciplinary, multi-data type, and cross-medium knowledge maps.
2. Cross-medium analytical reasoning technology: Key breakthroughs in cross-medium unified indicators; relational understanding and knowledge mining; knowledge map structure and learning; knowledge evolution and reasoning; intelligent description and generation, etc., technology; realization of cross-medium knowledge indicators, analysis, mining, reasoning, evolution, and utilization; and construct analytic reasoning engines.
3. Key swarm intelligence technology: Key breakthroughs on the basis of the popularization of the internet, mass collaboration, knowledge resource management, and open sharing, etc., technologies. Building frameworks to display swarm intelligence knowledge. Realize the integration and strengthening of swarm intelligence-based knowledge acquisition and swarm intelligence under open development conditions. Support swarm perception, cooperation, and evolution at a national, tens-of-millions scale.
4. New architecture and new technology for hybrid and enhanced intelligence: Key breakthroughs in human-machine interaction for perception and execution integration models, new types of intelligent computing-fronted sensors, common use hybrid architecture, etc., core technologies. Build autonomous, environmentally adaptable hybrid enhanced intelligent systems, human-machine hybrid enhanced intelligent systems and support environments.
5. Intelligent technologies of autonomous unmanned systems: Key breakthroughs in autonomous unmanned system computing architecture, complex situational environment perception and understanding, real-time accurate positioning, adaptable, intelligent navigation in complex environments, etc., general technologies. Unmanned and autonomously controlled systems including automobiles, ships, automatic driving in traffic, etc., intelligent technologies. Develop service robots, special-purpose robots, etc., core technologies and support unmanned system application and manufacturing development.
6. Intelligent virtual reality modelling technology: Key breakthroughs in intelligent modelling technology for virtual counterparts. Increasing the sociality, diversity, and lifelike quality of virtual reality intelligent counterpart behaviour. Realize the organic integration, high efficiency, and interactivity of virtual reality and augmented reality, etc., technologies.
7. Intelligent computing chips and systems: Key breakthroughs in high energy efficiency, reconfigurable brain-inspired

computing chips and brain-inspired visual sensor systems with computational imaging capabilities. Research and develop high-efficiency brain-inspired neural network architectures and hardware systems with autonomous learning capabilities. Realize brain-inspired intelligent systems with multimedia sensory information understanding, intelligence growth, and common-sense reasoning capabilities.

8. NLP technology: Key breakthroughs in natural language grammar logic, word-concept symbols, and deep semantic analysis core technologies. Advance effective human-machine communication and free interaction. Realize multi-style, multi-language, multi-domain natural language intelligent understanding and automated [results] generation.¹²

CANADA

In 2015, the Canadian Information and Communications Technology Council released a White Paper on AI¹³ which defines it as "the human-like intelligence exhibited by machines or software". These machines or software can reason, plan, learn, perceive and process information like the human mind and thus facilitate human life. AI enables machines or the in-built software to behave like human beings which allows these devices to perceive, analyse data, reason, talk, make decisions and act. There are several ideas, systems and technologies that have been developed in the world of AI. however, these are not called AI systems or products; rather, they are referred to by their specific functions, such as smart graphics, machine learning, e-commerce and so forth. This phenomenon is known as the "AI effect".¹⁴

In 2019, the Montreal Declaration for Responsible AI,¹⁵ which is an initiative of the Université de Montréal under CIFAR's Pan-Canadian Artificial Intelligence Strategy, defines AI as a process of "simulating certain learning processes of human intelligence, learning from them and replicating them...These cognitive skills form the basis for other skills such as choosing among several possible actions to reach a goal, interpreting an image or a sound, predicting behavior, anticipating an event, diagnosing a pathology and more."¹⁶

UK

The official definition of AI by the UK government, published in 2019, is as "a research field spanning philosophy, logic, statistics, computer science, mathematics, neuroscience, linguistics, cognitive psychology and economics. AI can be defined as the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence."¹⁷

13. Information and Communication Technology Council, "Artificial Intelligence in Canada Where Do We Stand?", April 2015, available at <https://www.ictc-ctic.ca/wp-content/uploads/2015/06/AI-White-paper-final-English1.pdf>

14. Think Automation, "What is the AI Effect and is it set to happen again?", available at <https://www.thinkautomation.com/bots-and-ai/what-is-the-ai-effect-and-is-it-set-to-happen-again/>

15. Montréal Declaration for Responsible Development of Artificial Intelligence, available at <https://www.montrealdeclaration-responsibleai.com/the-declaration>

16. Montréal Declaration for Responsible Development of Artificial Intelligence: Part 1 – Co-Construction Approach and Methodology, available at https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_eb775ce43d3b46fe90c89da583e9744d.pdf

17. Office for Artificial Intelligence, "Guidance: A Guide to Using Artificial Intelligence in the Public Sector", June 2019, available at <https://www.gov.uk/government/publications/understanding-artificial-intelligence/a-guide-to-using-artificial-intelligence-in-the-public-sector>

The Industrial Strategy¹⁸ released by the UK government in November 2017 lays out the plan for industrial growth and also projects AI to be one of the main drivers of the economy. It defines AI as ‘technology with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation.’ It further defines machine learning as ‘a type of AI that allows computers to learn rapidly from large datasets without being explicitly programmed’ and a ‘data-driven economy’ as being ‘a digitally connected economy that realises significant value from connected, large-scale data that can be rapidly analysed by technology to generate insights and innovation’.

A report¹⁹ by the Select Committee on Artificial Intelligence, House of Lords, has added to the definition used by the UK Government in its Industrial Strategy White Paper. It states that AI can be viewed as ‘narrow’ or ‘general’ in scope. Artificial general intelligence refers to a machine with broad cognitive abilities, which is able to think, or at least simulate convincingly, all of the intellectual capacities of a human being, and potentially surpass them—it would essentially be intellectually indistinguishable from a human being. Narrow AI systems perform specific tasks which would require intelligence in a human being and may even surpass human abilities in these areas. However, such systems are limited in the range of tasks they can perform.

Another study on Growing the Artificial Intelligence industry in the UK²⁰ commissioned by the Business and Cultural Secretary of UK states that AI is ‘a set of advanced general purpose digital technologies that enable machines to do highly complex tasks effectively’. Further it highlights the definition of AI used by the Engineering and Physical Science Research Council that describes AI as ‘technologies that aim to reproduce or surpass abilities (in computational systems) that would require ‘intelligence’ if humans were to perform them. These include: learning and adaptation; sensory understanding and interaction; reasoning and planning; optimisation of procedures and parameters; autonomy; creativity; and extracting knowledge and predictions from large, diverse digital data’. In discussing the various applications and usage of AI, it notes that AI actually comprises a set of complementary techniques that have developed from statistics, computer science and cognitive psychology.

Another government report²¹ published in 2016, notes that the range of different statistical techniques that fall under the general term ‘artificial intelligence’ have emerged over a long time from many different research fields within statistics, computer science and cognitive psychology. It acknowledges that authors from different disciplines tend to make distinctions between terms like ‘machine learning’ and ‘machine intelligence’, using them to refer to related but distinct ideas. It also brings to light the difference between the ‘unsupervised’ and ‘supervised’ algorithms that are used in machine learning; while the former is a learning algorithm with an un-labelled set of data, the latter involves using a labelled data set to train a model, which can then be used to classify or sort a new, unseen set of data (for example, learning how to spot a particular person in a batch of photographs). Finally, it mentions deep learning as a sub-set of machine learning that depends on using layers of non-linear algorithmic processes to find patterns or classify data.

18. Secretary of State for Business, Energy and Industrial Strategy, “Industrial Strategy: Building Britain for future”, November 2017, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730048/industrial-strategy-white-paper-web-ready-a4-version.pdf

19. Select Committee of Artificial Intelligence, House of Lords, “AI in the UK: ready, willing and able?”, April 2018, available at <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

20. Professor Dame Wendy Hall and Jerome Presenti, “Growing the Artificial Intelligence industry in the UK”, 15 October 2017 available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

21. Government Office for Science, “Artificial Intelligence: Opportunities and Implications for the Future of Decision Making”, February 2016, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf

FRANCE

In December 2018, the Commission Nationale de l'Informatique et des Libertés (National Commission on Computer Technology and Civil Liberties or **CNIL**) published a report²² on societal and ethical stakes related to new digital technologies. The report was commissioned by the French Government and extensively discussed the issue of defining AI and algorithms. It defines algorithms as 'the description of a finite and unambiguous sequence of steps (or instructions) for producing results (output) from initial data (input).' The report draws from the definition of AI by Marvin Minsky and Alan Turing to say that AI is "the science of making machines do things that would require intelligence if done by men".²³ Furthermore, it also attempts to explain the concept of machine learning and deep learning to give reader a better idea of the AI technology in general.

In a report²⁴ prepared by the French Member of Parliament and mathematician Cedric Villani, the discipline of AI is acknowledged to have a wide scope, but that fundamentally, it is a programme whose ambitious objective is to understand and reproduce human cognition; creating cognitive processes comparable to those found in human beings. The French President's AI for Humanity Strategy Initiative²⁵ draws from this definition of AI, noting that the field is so vast that it cannot be restricted to a specific area of research. While originally, it sought to imitate the cognitive processes of human beings, its current objectives are to develop automations that solve some problems better than humans, by all means available. Another report on AI and work²⁶ discussed the issue of defining AI and laid out the broad contours of the technology that need to be considered in this process, such as machine learning and statistical learning. The report considers 'strong AI' as one that can be equated to human intelligence. It mentions how AI brings together a range of fields including logical reasoning, knowledge representation, and NLP and that its main applications at present are connected with advances in machine-learning techniques, deep learning in particular, which usually requires availability of big data, for these to be factored in while defining AI. Furthermore, it attempts to draw the line between generic technology and AI and AI and robotics so that the technology can be better understood for the purpose of defining it.

GERMANY

In November 2018, the Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and Energy, and the Federal Ministry of Labour and Social Affairs prepared a national strategy²⁷ for AI based on the nationwide online consultation. The strategy acknowledges that there is no definition of AI which generally valid or used consistently by all stakeholders. However, for the purpose of the national strategy it divides the AI in two parts namely 'strong AI' and 'weak AI'. While 'strong AI' means that AI systems have the same intellectual capabilities as humans, 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-optimisation. It further mentions that the government has oriented the national strategy to the use of AI to solve specific problems (i.e., 'weak AI'), comprising the following systems:

22. CNIL, "How Can Humans Keep The Upper Hand? The Ethical Matters Raised By Algorithms And Artificial Intelligence", December 2017, available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

23. French Government, "#FranceIA: The National Artificial Intelligence Strategy is Underway", January 2017, available at <https://www.gouvernement.fr/en/franceia-the-national-artificial-intelligence-strategy-is-underway>

24. Cedric Villani, "For a Meaningful Artificial Intelligence: Towards a French and European Strategy", March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

25. AI for Humanity, available at <https://www.aiforhumanity.fr/en/>

26. Salima Benhamou and Lionel Janine, "Artificial Intelligence and Work", March 2018, available at https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-report_-artificial-intelligence-and-work-finalweb-21122018.pdf

27. Federal Government, "National Strategy for Artificial Intelligence", 2018, available at <https://www.ki-strategie-deutschland.de/home.html>

1. Deduction systems, machine-based proofs: deduction of formal statements from logical expressions, systems to prove the correctness of hardware and software;
2. Knowledge-based systems: methods to model and gather expertise; software to simulate human expertise and to support experts (previously designated "expert systems"); to some extent coupled with psychology and cognitive sciences;
3. Pattern analysis and pattern recognition: inductive analytical processes in general, machine learning in particular;
4. Robotics: autonomous control of robotic systems, i.e., autonomous systems;
5. Smart multimodal human-machine interaction: analysis and "understanding" of language (in conjunction with linguistics), images, gestures and other forms of human interaction.

RUSSIA

The National Strategy²⁸ on AI released by Russia in October 2019, lays down a 20-year plan for the development of infrastructure and regulations for AI. This document defines AI as referring to technological solutions that can simulate the cognitive functions of a person and get results comparable at least to the results of human intellectual activity. The National Strategy focuses on machine learning as the core of concept of AI. It states that machine learning is characterized by a number of specific features: first, in order for a computing system to seek an unbiased solution, it is necessary to introduce a representative, relevant, and correctly labelled dataset; second, neural network operating algorithms are extremely difficult to interpret, and consequently, the results of their operation may be subject to human doubt and may be rejected by the user.

Much like the approach taken by many other nations, it bi-furcates the technology into two kinds, 'weak AI' and 'strong AI'. It categorises the machine learning (as mentioned above) as weak AI. It defines 'strong AI' as being 'the creation of an artificial general intelligence (strong artificial intelligence) that is able, like a person, to solve various problems, to think, to interact, and to adapt to changing conditions is a complex scientific and technical problem, the resolution of which lies at the crossroads of different spheres of scientific knowledge – natural science, engineering, social studies, and the humanities.'

ISRAEL

The interim report²⁹ commissioned by the National Council for Research and Development (**MOLMOP**) at the Ministry of Science and Technology, Israel defined AI as a 'method for programming computers to enable them to carry out tasks or behaviours that would require intelligence if performed by humans'. Further, the report also explains the 'smart robotics' that indicates a link between robots or actuators in the physical world and AI and re-iterates the attributes of 'Smart Autonomous Robots' as given by EU. Following are the cited attributes:

1. AI acquires autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and trades and analyses data;

28. Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation, October 2019, available at https://cset.georgetown.edu/wp-content/uploads/t0060_Russia_AI_strategy_EN-1.pdf

29. Dr. Daphne Getz, Oshrat Katz, et al., "Artificial Intelligence, Data Science, and Smart Robotics", September 2018, available at https://www.neaman.org.il/Files/Summary-ENG-Artificial-Intelligence-Data-Science-and-Smart-Robotics_20190103155717.804.pdf

2. AI is self-learning (optional criterion);
3. AI has a physical support;
4. AI adapts its behaviors and actions to its environment.

DENMARK

The National Strategy for Artificial Intelligence,³⁰ published in March 2019, relies heavily on the definition given by the OECD and the EC and states 'Artificial intelligence is systems based on algorithms (mathematical formulae) that, by analysing 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 behaviour by observing how the environment is influenced by previous actions.' The strategy also considers the basic uses of AI in its definition and says 'Artificial intelligence is used in a number of areas, e.g., search engines, voice and image recognition, or to support drones and self-driving cars. Artificial intelligence can be a crucial element to increase productivity growth and to raise the standard of living in the years to come.'

EU

In 2018, the European Commission (**EC**) came out with an approach on AI for European countries in the form of a communication.³¹ The communication defines AI as follows: '...systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.' It also clarified that 'AI-based systems can be purely software-based, acting in the virtual world (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g., advanced robots, autonomous cars, drones or Internet of Things (**IoT**) applications).

Following this, the High-Level Expert Group on AI came up with a paper³² to expand the scope of this definition to clarify various aspects of the technology. The updated definition of AI provided in this paper is as follows: 'Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.

As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).'

30. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", March 2019, available at https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

31. EC, "Communication on Artificial Intelligence for Europe", April 2018, available at <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>

32. High Level Expert Group on Artificial Intelligence, "A Definition of Artificial Intelligence: Main Capabilities and Scientific Discipline", April 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>

AUSTRALIA

In a consultation paper³³ by the Department of Industry, Innovation and Science released in 2018, the term 'general AI' has been explained to mean any technology that replicates human intelligence, and that such general AI is an unlikely prospect in the coming decade. The paper identifies the target of the policy to be 'narrow AI' technologies that are already incredibly sophisticated at handling specific tasks like automated vehicles and medical AI technology. In another paper³⁴ commissioned by the Australian Government and prepared by the Commonwealth Scientific and Industrial Research Organisation, AI was defined 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.'

JAPAN

Japan's Strategic Council of AI Technology came out with a report on AI technology strategy on 31 March 2017³⁵ that lays down the nation's roadmap for the development and regulation of AI. The report acknowledges that the prevalent form of AI is specialized AI technology for carrying out specialized tasks and is used only to supplement human capabilities. It mentions that based on the progression of AI technology, various inferences have become possible from past data, image recognition, language recognition, etc. By using and applying AI technology as a service based on data, the capabilities of human beings are drawn out to the fullest extent, human society becomes abundant, including sustainability of society and approaches to social issues such as environmental problems, and economic and industrial benefits are yielded. The report also includes IoT in the scope of AI that needs regulation.

In July 2017, the Ministry of Internal Affairs and Communication of Japan released draft guidelines³⁶ on research and development of AI. It defines AI as a concept that collectively refers to the AI systems and AI software. AI software means software that has functions to change its own outputs or programs in the process of the utilization, by learning data, information, or knowledge; or by other methods (e.g., machine learning software). AI systems have been defined as systems that incorporate AI software as a component (e.g., robots and cloud systems that implement AI software).

Japan's Council for the Social Principles of Human Centric AI³⁷ defines AI as a system that realizes an intelligent function. It notes that although AI in recent years has been based on machine learning, especially deep learning, AI related technology is rapidly developing, and the definition of AI is not limited solely to technology used for AI.

33. Dawson D, Schleiger E, et al, "Artificial Intelligence: Australia's Ethics Framework", 2019 available at: [https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf](https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting-documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf)

34. Data61 and the Department of Industry, Innovation and Science, "Australia's Artificial Intelligence Roadmap", November 2019, available at: <https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap>

35. Strategic Council for AI Technology, "Artificial Intelligence Technology Strategy", March 2017, available at <https://www.nedo.go.jp/content/100865202.pdf>

36. (Japanese) Ministry of Internal Affairs and Communication, "Draft AI R&D Guidelines for International Discussions", July 2017, available at https://www.soumu.go.jp/main_content/000507517.pdf

37. Council for Social Principles of Human-centric AI, "Social Principles of Human-centric AI", February 2019, available at <https://www8.cao.go.jp/cstp/english/humancentrictai.pdf>

SINGAPORE

The Singapore National AI Strategy Paper defines AI as the capability to simulate intelligent, human-like behaviour in computers.³⁸ The scope of AI has also been considered in the context of data privacy legislation. In 2013, the Singapore government established the Personal Data Protection Commission (**PDPC**) to enforce the Personal Data Protection Act, 2012. The PDP Commission is the authority for the matters related to data and AI. In June 2018, the PDPC came up with a discussion paper³⁹ on fostering responsible development of AI. The paper looks into the responsible use of the technology from the stakeholder's side and therefore defines terms like 'AI developers', that includes developers of application systems that make use of AI technology; 'user companies' that includes companies that make use of AI solutions in their operations. This could be a backroom operation (e.g., processing applications for loans) or a front-of-house service (e.g., e-commerce portal or ride-hailing app). The term can also refer to companies that sell or distribute devices or equipment that provide AI-powered features (e.g., smart home appliances). However, it does not specifically define AI technology itself.

The paper also adopts a process model to describe different phases in AI deployment. The process thus adopted has been divided in three phases that are:

1. Data preparation: In this raw data is formatted and cleansed so that accurate conclusions can be drawn.
2. Algorithms: Then the algorithms are applied for analysis. This includes statistical models, decision trees and neural networks. The results are examined, and the algorithms are re-iterated till the model produces the desired results.
3. Chosen model: The final model is used to produce probability scores that can be incorporated into applications to make decisions, solve problems and trigger actions.

The report identifies that the applicability of AI regulatory framework may be different for different stakeholders. Therefore, 'it is necessary to consider both the AI value chain and the technology deployment process in discussing the development of the AI governance framework.'

The PDPC also released the second edition of Model AI Governance Framework⁴⁰ that gives a definition of AI, and as per the model, AI 'refers to a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation, and/or classification). AI technologies rely on AI algorithms to generate models. The most appropriate model(s) is/are selected and deployed in a production system.' Though it should be noted the definition was said to be neither authoritative nor exhaustive.

38. (Singapore) Smart Nation Digital Governance Office, "National Artificial Intelligence Strategy: Advancing our Smart Nation Strategy", November 2019, available at https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4

39. (Singapore) Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI", June 2018, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD--050618.pdf>

40. (Singapore) Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework, Second Edition", January 2020, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

SOUTH KOREA

South Korea is one of the frontrunners in the robotics industry. In 2008, the National Assembly of South Korea enacted the Intelligent Robot Development and Promotion Act⁴¹ to establish and promote a policy on the sustainable development of the intelligent robot industry. According to Article 2(1) of the Intelligent Robot Development and Promotion Act, the term “intelligent robot” means a mechanical device that perceives the external environment for itself, discerns circumstances, and moves voluntarily.

The South Korean Ministry of Science, ICT and Future Planning published a Mid-to-Long-Term Master Plan in Preparation for the Intelligent Information Society,⁴² which defines ‘Intelligent IT’ as a technology that is capable of performing the highly complex functions of human intelligence by combining the “intelligence” of AI with the “information” provided by data-processing and network technologies, such as IoT, cloud computing, big data analysis, and mobile technologies (referred to collectively as **ICBM technologies**). It also mentions that the 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.). It further explains that the ‘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. With regards to data processing and network ICBM technologies, it says that these are essential ICTs that generate, collect, transmit, store, and analyze data that are crucial to the development, enhancement, and dissemination of AI technology.

Finally, the plan enlists four characteristics of the Intelligent IT for a better understanding of the scope of the definition of AI and Intelligent IT. Following are the characteristics as listed by the plan,

1. Automatic decision-making: Machines become capable of performing the highly complex and intelligent tasks involved in decision-making independently, thereby accelerating automation.
2. Real-time responses: ICBM technologies carry out a series of related tasks (e.g., data gathering/analysis and deduction) instantly to provide real-time responses and actions.
3. Automatic evolution: Machines utilize their deep-learning experiences to evolve independently, achieving astronomical improvements in performance.
4. Storage of all kinds of data: Even data that were impossible to store and use in the past (e.g., biological and behavioural information, amorphous data, etc.) can now be made useful through the machine-learning process.

According to the Korean National AI Strategy Paper of March 2020, AI has been defined as “a science and technology that performs human intellectual functions with machines.”⁴³

41. Translated text of the Intelligent Robots Development and Distribution Promotion Act, 2008, available at http://elaw.klri.re.kr/eng_service/lawView.do?hseq=39153&lang=ENG

42. Government of South Korea, “Mid-To Long-Term Master Plan in Preparation for Intelligent Information Society”, 2017, available at: https://english.msis.go.kr/cms/english/pl/policies2/_icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

43. Ministry of Science and ICT, “National Strategy for Artificial Intelligence”, March 2020, available at https://www.msis.go.kr/cms/english/pl/policies2/_icsFiles/afieldfile/2020/03/23/National%20Strategy%20for%20Artificial%20Intelligence_200323.pdf

SWEDEN

The Ministry of Enterprise and Innovation of Sweden published the 'National Approach to Artificial Intelligence'⁴⁴ that refers to AI as 'a broad field that encompasses many technologies, not least machine learning and deep learning'. It further acknowledges the self-evolving nature of the technology and notes that AI is distinguishable from other automation methods on the basis of its ability to earn and become smarter over time.

In 2017, the Government of Sweden commissioned a report⁴⁵ to carry out a mapping study and analysis of how AI and machine learning are used in Swedish industry, public sector and society, and the potential that could be realised by boosting the use thereof. The report acknowledges that there is no clear-cut definition of AI, but for the purposes of the report, AI is defined as 'the ability of a machine to imitate intelligent human behaviour. AI also denotes the area of science and technology that aims to study, understand and develop computers and software with intelligent behaviour.'

FINLAND

In a report⁴⁶ published by Ministry of Economic Affairs and Employment of Finland, AI is defined as devices, software and systems that are able to learn and to make decisions in almost the same manner as people. AI allows machines, devices, software, systems and services to function in a sensible way according to the task and situation at hand.

SPAIN

Spain released its National AI Strategy in 2019⁴⁷ through Ministry of Science, Innovation and Universities, which borrows the definition of AI provided by John McCarthy in his seminal paper of 1956 on AI i.e. - 'the science and engineering of making machines that behave in a way we would call intelligent if humans had that behaviour'. It further highlights that even though AI is an area of computer science, it shared techniques with other disciplines such as mathematics and statistics or cognitive sciences, and is also increasingly interdisciplinary, with synergies with biology, philosophy, the world of law, psychology, sociology and economics.

44. (Swedish) Ministry of Enterprise and Innovation, "National Approach to Artificial Intelligence", 2018, available at <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

45. Vinnova, "Artificial Intelligence in Swedish Business and Society – Analysis of Development and Potential", 2017, available at https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf

46. (Finland) Ministry of Economic Affairs and Employment, "Finland's Age of Artificial Intelligence: Turning Finland into a Leading Country in the Application of Artificial Intelligence", 2017, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf

47. Ministry of Science, Innovation and Universities, "Spanish RDI Strategy in Artificial Intelligence", 2019, available at https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_EN.PDF

NORWAY

The National Strategy⁴⁸ for AI of Norway addresses the issue of definition rather extensively.⁴⁹ AI is divided into ‘weak’ and ‘strong’ versions, depending on the processes of decision making and machine learning. It states that the machine learning algorithms usually learn in three different ways that are as follows:

1. Supervised learning: the algorithm is trained with a dataset where both input data and output data are given, using which it builds a model. The model then is capable of making a decision based on input data.
2. Non-supervised learning: the algorithm is fed only a dataset without a ‘solution’ and must find patterns in the dataset which then can be used to make decisions about new input data. Deep learning algorithms can be trained using non-supervised learning.
3. Reinforcement learning: the algorithm builds its model based on non-supervised learning but receives feedback from the user or operator on whether the decision it proposes is good or bad. The feedback is fed into the system and contributes to improve the model.

Another report⁵⁰ commissioned by the Norwegian Data Protection Authority describes AI as ‘the concept used to describe computer systems that are able to learn from their own experiences and solve complex problems in different situations – abilities we previously thought were unique to mankind.’ It further differentiates between AI, machine learning and deep learning for a better understanding of the concept.

Finally, the Norwegian Board of Technology⁵¹ explains the process of machine learning to give a better idea of the working and programming of such systems.

ESTONIA

In May 2019, Estonia’s Taskforce on AI released a report⁵² laying down the roadmap for country’s AI policy and initiatives. While acknowledging that no consensus has yet been reached in defining AI, the report defines AI as ‘systems that exhibit intelligent behaviour by analysing their environment and making decisions that are independent to a certain extent to meet certain objectives.’

48. Norwegian Ministry of Local Government and Modernisation, “National Strategy for Artificial Intelligence”, January 2020, available at: https://www.regjeringen.no/contentassets/1feb8bb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

49. Norway borrows from the position adopted by High-Level Expert Group on Artificial Intelligence set up by the EC.

50. Datatilsynet (Norwegian Data Protection Authority), “Artificial intelligence and Privacy”, January 2018, available at: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>

51. Norwegian Board of Technology, “Artificial Intelligence: Opportunities, challenges and a plan for Norway”, 2018, available at <https://teknologiradet.no/wp-content/uploads/sites/105/2018/11/Al-and-machine-learning-1.pdf>

52. (Estonian) Ministry of Economic Affairs and Communication, “Report of Estonia’s AI Taskforce”, 2019, available at <https://www.kratid.ee/in-english>

THE NETHERLANDS

The Dutch Artificial Intelligence Manifesto⁵³ released by the Special Interest Group on Artificial Intelligence in 2018 defines AI as systems that are 'capable of sensing their environment, learn from and reason about it, and change it based on advanced decision making'. The manifesto identifies seven AI foundational areas in which the Dutch AI community has made and is expected to make important contributions, which are:

1. Agents & Robotics: developing autonomous computer systems acting in (either digital or physical) environments in order to achieve their design objectives.
2. Computer Vision: obtaining a visual understanding of the world.
3. Decision Making: planning and scheduling, heuristic search and optimization.
4. Information Retrieval: technology to connect people to information, e.g., in the form of search engines, recommender systems, or conversational agents.
5. Knowledge Representation & Reasoning: representing information computationally, and processing information in order to solve complex reasoning tasks.
6. Machine Learning: learning from data (using e.g., neural networks also known as 'deep learning' and/or statistical techniques).
7. NLP: Extracting information and knowledge about the world from (large amounts of) spoken, written, and signed natural language, enabling human-machine communication, and supporting multilingual human-human communication.

The National Strategic Action Plan⁵⁴ for AI acknowledges that a general definition of AI doesn't exist and borrows the definition given by the EC, i.e., 'AI refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.'

UAE

The National AI Strategy⁵⁵ of the UAE does not specifically define AI but lists out the focus areas of the government for its development. These are - education, transportation, energy, space and technology.

53. (Dutch) Special Interest Group on Artificial Intelligence, "Dutch Artificial Intelligence Manifesto", 2018, available at <http://ii.tudelft.nl/bnvki/wp-content/uploads/2018/09/Dutch-AI-Manifesto.pdf>

54. (Dutch) Ministry of Economic Affairs and Climate Policy, "Strategic Action Plan for Artificial Intelligence", 2019, available at: <https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence>

55. Government of the UAE, "UAE Artificial Intelligence Strategy 2031", 2017, available at: <http://www.uaeai.ae/en/>

HONG KONG

In 2019, the Hong Kong Monetary Authority along with PwC⁵⁶ published a research paper to foster discussion about AI in the context of the banking sector. The objectives of this paper included understanding better how AI works, given its impact as a disrupter of many corporate industries. The report notes that the goal of AI is to allow computers to mimic human intelligence so that they can learn, sense, think and act in order to achieve automation and gain analytic insights. To achieve the same, AI systems use two computation approaches: (a) rule-based: where the AI 'learns' using pre-defined rules and knowledge, and 'thinks' by inferring logical causes and effects according to 'if-then-else' rules; and (b) non-rule based: where the AI 'learns' with machine learning algorithms and 'thinks' using trained AI models.

56. Hong Kong Monetary Authority and PwC, "Reshaping Banking with Artificial Intelligence", 2019, available at https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf



TRANSPARENCY

One of the long-standing concerns about the growing ubiquity of AI systems relates to understanding how AI really “works”, from which emerges a resistance to incorporating AI into various aspects of human life. This has led researchers and regulatory regimes to give careful thought to the “explainability” of AI systems. With recent instances of AI systems acting unprompted or in ways that may be unintelligible to the layperson,⁵⁷ stakeholders have started questioning the kind of decisions to be left to AI systems, and the way in which these decisions are made.

Moreover, informed consent – another foundational principle for ethical AI – is predicated on the user understanding the technology and its impact.⁵⁸ Transparency in AI systems, therefore, enables humans to understand what is happening in AI models and ensures that advanced or AI-powered algorithms are thoroughly tested, explainable and aligned with the principles of ethical conduct.⁵⁹ Methods and guidelines to ensure that AI is fair, accountable and transparent is now one of the most crucial areas of AI research and has made way for an almost separate area of research referred to as “explainable AI” (XAI).⁶⁰ The goal with XAI is to avoid black box algorithms, i.e. AI systems that are not explainable due to the complexity of the algorithm’s structure and/or use of algorithms that rely on geometric relationships that humans cannot visualize,⁶¹ as a prerequisite to hold systems accountable. The urgency of the issue of transparency varies depending on the nature of the technology. For instance, rule-based AI systems, which function on the basis of rules programmed into the algorithm by humans or expert-based AI systems, which dip into a knowledge pool created by human experts, are

less “autonomous” in their decision making. The scope of their operation and possible outcomes or decisions are circumscribed by a knowledge base created by humans, which makes them more predictable. Transparency and explainability becomes more difficult where AI systems “learn” and develop rules for functioning autonomously, as with deep learning AI systems.

The issue of avoiding or solving the black box problem has become even more complex, as technologies that use deep learning using programmable neural networks are deployed in fields as varied as targeted online purchasing recommendations to autonomous vehicles. The advantage of deep learning algorithms is the ability of such systems to “learn” by interpreting a continuous stream of data to identify links and connections that are of value without human guidance; since the decision is made autonomously by the AI system itself, the question of the process and basis for these machine made decisions would have a profound impact on the “value” of such decisions to human beings and society.⁶² Another question to be considered is whether designing transparency into such AI systems would negatively affect the accuracy of the outcomes of such systems at all. It has been suggested that interpretable AI systems should be considered the standard, especially where the system is used to make high stakes decisions, rather than assuming that the “black box” problem is a necessary feature of deep learning AI systems.⁶³

In May 2019, the OECD recommended the adoption of certain principles for responsible stewardship of trustworthy AI. One of the principles that were also later adopted by the G-20 countries in June 2019 was that of

57. BBC News, “Amazon scrapped ‘sexist’ AI tool”, 2018, available at <https://www.bbc.com/news/technology-45809919>; Oscar Schwartz, “In 2016, Microsoft’s Racist Chatbot revealed the Dangers of Online Conversation”, 2019, available at <https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation>; and Gerald Sauer, “A Murder Case Tests Alexa’s Devotion to your Privacy”, Wired, 2017, available at <https://www.wired.com/2017/02/murder-case-tests-alexa-devotion-privacy/>

58. Felzmann, H. and Villaronga, E. F. et al., “Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns”, Big Data & Society, Volume 6 Issue 1, 2019, available at: <https://doi.org/10.1177/2053951719860542>

59. Deloitte, “Transparency and Responsibility in Artificial Intelligence: A Call for Explainable AI”, 2019, available at: <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovation-bringing-transparency-and-ethics-into-ai.pdf>

60. Joy Lu, Dokyun Lee (DK) et al, “Good Explanation for Algorithmic Transparency”, November 2019, available at: <https://ssrn.com/abstract=3503603>

61. Yavar Bathaei, “The Artificial Intelligence Black Box and the Failure of Intent and Causation”, Harvard Journal of Law & Technology, Volume 31 Issue 2, 2018 available at: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaei.pdf>

62. Davide Castelvecchi, “Can We Open the Black Box of AI?”, 2016, available at <https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731>

63. Cynthia Rudin and Joanna Radin, “Why are we using Black Box Models in AI when we don’t need to? A Lesson from an Explainable AI Competition”, 2019, available at <https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/5>

'transparency and explainability'. The recommendations state that the AI actors should commit to transparency and responsible disclosure regarding AI systems. It emphasised that to this end, they should provide meaningful information, appropriate context and must foster the general understanding of the AI systems so that those affected by the outcome of an AI system must know about it and are able to challenge the outcomes if the same are adverse.

In the light of the above, it becomes imperative for regulatory regimes to devise guidelines in order to make AI more transparent and hence accountable for the decisions it makes. Even though research has shown that achieving transparency in AI systems depends on the stakeholders interacting with the system, and therefore the process of achieving the same can

vary on a case-by-case basis,⁶⁴ many countries have incorporated the requirement for transparency as a high-level principle in their national strategies for AI, while exploring options for practical implementation of transparency and explainability in business.

A recent attempt at practical application of this principle relates to the recommendation by Saidot (a Finnish company that works in the space of AI transparency) of the creation of an AI Register, which is a "standardised, searchable and archivable way to document the decisions and assumptions that were made in the process of developing, implementing, managing and ultimately dismantling an algorithm." The concept of the AI Register links the principles of openness and accountability in democracy to similar principles relating to AI systems, by creating public AI registers for the cities of Helsinki and Amsterdam.⁶⁵

64. Ibid at 2.

65. Meeri Hatja et al, "Public AI Registers: Realising AI Transparency and Civic Participation in Government Use of AI" (white paper), September 2020, available at https://uploads-ssl.webflow.com/5c8abedb10ed656ecfb65fd9/5f6f334b49d5444079726a79_AI%20Registers%20-%20White%20paper%201.0.pdf

MATURITY INDEX TRANSPARENCY



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation



INDIA

Maturity index – 3/5

The Indian AI Strategy⁶⁶ gives due importance to the concept of transparency in AI. It proposes the establishment of Ethics Council at every Centre of Research and Excellence (one of the two tier structure that the strategy proposes for research in AI) for developing a FAT (Fairness, Accountability and Transparency) framework, for the purpose of adhering to standard practices while developing AI tools and products. The strategy also explicitly addresses the problem of the 'black box phenomenon' and highlights the importance of XAI for an increased transparency with respect to decisions made by AI systems while balancing the need to protect the IP in AI systems from the developers' point of view.

USA

Maturity index – 3/5

A report⁶⁷ on the future of AI released by the White House in 2016, heavily focused on the problem of anonymity in decision-making by the AI systems and mentioned that transparency concerns relate not only to the data and algorithms involved, but also on the potential to have some form of explanation for any AI-based determination. It also highlighted the need for development of international standards for the same reason and established country's commitment towards the same.

The National AI R&D Strategic Plan of 2016⁶⁸ divides the overall strategy in eight parts out of which Strategy 4 emphasizes the need for explainable and transparent systems that are trusted by their users, perform in a manner that is acceptable to the users, and can be guaranteed to act as the user intended. Pursuant to this, an update⁶⁹ released in 2019 on the research and development strategy brings up the issue of transparency in the design of the AI systems recommends that the researchers must learn how to design these systems so that their actions and decision-making are transparent and easily interpretable by humans, and thus can be examined for any bias they may contain, rather than just learning and repeating these biases. It also specifically broaches the issue of explainability of decisions made by AI systems in the healthcare sector where doctors need explanations to justify a particular diagnosis or a course of treatment and hence, urges the researchers to improve the explainability of AI systems.

For instance, hospitals in the US have been using algorithms to match organ donors to patients since the mid-2000s. Thus far, these algorithms have had significant human supervision or intervention in its decision-making. Going forward, however, it is possible for the AI system itself to weigh in on the decision-making process, balancing various ethical principles to arrive at the most "suitable" decision. The success or effectiveness of such systems would likely depend on the information provided on relevant ethical considerations in organ donor scenarios.⁷⁰

66. NITI Aayog, "National Strategy for AI: #AI for All", June 2018, available at: <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>

67. Committee on Technology, National Science and Technology Council, "Preparing for the Future of Artificial Intelligence", October 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

68. Networking and Information Technology Research and Development Subcommittee, National Science and Technology Council, "The National Artificial Intelligence Research and Development Strategic Plan", October 2016, available at: https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf

69. Networking and Information Technology Research and Development Subcommittee, National Science and Technology Council, "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update", June 2019, available at: <https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf>

70. Corinne Purtil, "How AI changed Organ Donation in the US", Quartz, September 2018, available at <https://qz.com/1383083/how-ai-changed-organ-donation-in-the-us/>.

In December 2020, the US President issued an executive order on promoting the use of trustworthy AI in the federal government.⁷¹ This executive order lists principles for the use of AI, including the importance of AI systems being understandable, responsible, traceable and transparent. It also directs the creation of a common policy for implementation by government agencies, the creation of a list of use cases by each government agencies of AI systems to improve their functioning and initiatives to attract AI implementation expertise within government agencies.⁷²

CHINA

Maturity index – 3/5

The AIDP⁷³, released in 2017 discusses the research and development of security evaluation tools for AI algorithms and platforms. Apart from this, the Governance Principles⁷⁴ for a New Generation of Artificial Intelligence released by the Chinese government incorporates the controllability of AI as one of the principles and mentions that AI systems should continuously improve transparency, explainability, reliability, and controllability, and gradually achieve auditability, supervisability, traceability, and trustworthiness. In May 2019, the Beijing Academy of Artificial Intelligence, an organisation backed by the Chinese Ministry of Science and Technology and Beijing Municipal Government released the Beijing AI Principles⁷⁵ that mentions that the research and development of AI must observe the principle of 'controlling risks' and directs that continuous efforts should be made to improve the maturity, robustness, reliability, and controllability of AI systems, so as to ensure the security for the data, the safety and security for the AI system itself, and the safety for the external environment where the AI system deploys.

CANADA

Maturity index – 4/5

In February 2018, the Standing Committee on Access to Information, Privacy and Ethics released a report reviewing the Personal Information and Protection of Electronic Documents Act that laid significant emphasis on the transparency of algorithms. The report defines algorithmic transparency as a situation 'when users have complete information about the workings of the AI programs behind the websites they visit, the data they collect and how they are used'. This places algorithmic transparency high in the list of priority areas in the process of developing AI systems and models. The report recommends that the Government of Canada should consider implementing measures to improve algorithmic transparency.

Canada also has a mechanism to address the issue of algorithmic transparency in automated decision-making systems used in public administration. In a directive⁷⁶ issued in February 2019, the Canadian government made it mandatory to complete the 'Algorithmic Impact Assessment' before the deployment of any automated decision system for administrative

71. Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, 3 December 2020, available at <https://www.whitehouse.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/>

72. Office of Science and Technology Policy, "Promoting the Use of Trustworthy Artificial Intelligence in Government", December 2020, available at <https://www.whitehouse.gov/articles/promoting-use-trustworthy-artificial-intelligence-government/>

73. State Council of People's Republic of China, "Notice on the Issuance of the New Generation Artificial Intelligence Development Plan", July 2017, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>

74. National New Generation Artificial Intelligence Governance Expert Committee, Ministry of Science and Technology, "Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence", June 2019, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/>

75. Beijing Academy of Artificial Intelligence, "Beijing AI Principles", May 2019, available at: <https://www.baai.ac.cn/blog/beijing-ai-principles>

76. Government of Canada, "Directive on Automated Decision-Making", February 2019, available at: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>

purposes. The government also provides a model for Algorithmic Impact Assessment in the form of a questionnaire⁷⁷ for the users to assess the algorithms.

UK

Maturity index – 4/5

In a report⁷⁸ commissioned by the Business and Cultural secretary of UK emphasised that the decisions which affect people and are made on the basis that decisions based on data analysis data should be fair and should be demonstrably fair. It relies on the transparency principle set forth by the Data Protection law of UK and the General Data Protection Regulation (**GDPR**) of EU to underscore the importance of transparency in automated decision-making systems and recommends that the Information Commissioner's Office and the Alan Turing Institute should develop a framework for explaining processes, services and decisions delivered by AI, to improve transparency and accountability.

In another report in 2019,⁷⁹ the Government Office for Science mentions the importance of transparency in the functioning of AI systems. In relation to maintaining anonymity, it notes that simply sharing static code provides no assurance that it was actually used in a particular decision, or that it behaves in the way its programmers expect on a given dataset, when deployed in the real world. To this effect it proposes an end-justifies-means approach to the problem and proposes that identifying desirable purposes and understanding whether the system achieves this intended end, be given as much importance as understanding the technicalities of the underlying algorithm. In addition to these, a report⁸⁰ by Select Committee of AI and another recommendatory report⁸¹ by the All-Party Parliamentary Group further buttress the importance of explainability of AI systems to make the decision making by them more transparent.

In another review of online targeting⁸² by the Centre for Data Ethics and Innovation, it was noted that though the consumers are not averse to the idea of targeted advertising or customised online experiences, the lack of transparency in the operation of the AI systems to use data unknowingly collected reduces public trust in AI systems. It also notes that in order to fully comply with the OECD standards for transparency in AI, a host of measures need to be implemented, such as opening up data repositories to researchers engaged in public policy research, requiring platforms to host publicly accessible archives for online political advertising, etc.

77. Government of Canada, "Algorithmic Impact Assessment v0.7", available at: <https://open.canada.ca/aia-eia-js/?lang=en>

78. Professor Dame Wendy Hall and Jérôme Pesenti, "Growing the Artificial Intelligence Industry in the UK", October 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

79. Government for Science, "Artificial Intelligence: Opportunities and Implications for the Future of Decision Making", November 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf

80. Select Committee on Artificial Intelligence, House of Lords, "AI in the UK: Ready, Willing and Able?", April 2018, available at: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

81. All-Party Parliamentary Group on Artificial Intelligence, "Findings 2017", October 2018, available at: http://www.appg-ai.org/wp-content/uploads/2017/12/appgai_2017_findings.pdf

82. Online targeting consists of a host of practices used to analyse information about people and then customise their online experience.

FRANCE

Maturity index – 3/5

A report⁸³ published by CNIL in December 2017 emphasized that the subjects of bias, discrimination and exclusion warrant particular vigilance, irrespective of whether the bias in question is intentional or unintentional. As a means to identifying and addressing bias, the report notes that it is important that the AI systems are explainable and transparent. It states that with the rise of machine learning algorithms, the designers themselves are also steadily losing the ability to understand the logic behind the results produced. The report proposes creating a framework that reverses or addresses the phenomenon of diminishing accountability which algorithms and AI are tending to encourage. Further, it recommends institution of soft law instruments such as reachability of the people whose data is being used to the algorithmic system controllers to get hold of relevant information and explanations. The current President of France Emmanuel Macron has also expressed⁸⁴ his support for the algorithmic transparency in AI as a core democratic principle.

GERMANY

Maturity index – 3/5

The German National Strategy for AI⁸⁵ acknowledges the problem of anonymity that prevails in the working of an AI system at large. It mentions that as a general rule the transparency, predictability, non-discriminatory nature and verifiability of AI systems need to be ensured in the development, coding, introduction and use of AI systems (including training and application data). Further, it brings to focus the requirement of implementation of this rule especially in automated processes that prepare decisions or draw conclusions that are implemented directly without any human interaction. In the light of this, the strategy commits the nation to the promotion of research regarding explainability and accountability of algorithm-based forecasting and decision-making systems.

RUSSIA

Maturity index – 3/5

The National Strategy⁸⁶ for AI of Russia released in October 2019 enlists transparency as one of the 'Basic Principles of the Development and Use of Artificial Intelligence Technologies', which is required to be considered when developing AI systems. The principle of transparency is defined as 'the intelligibility of artificial intelligence, work and the process whereby it achieves results, as well as non-discriminatory access by the users of products that have been created on the basis of AI technologies to information about the AI operating algorithms employed in these products'.

83. National Commission for Information and Liberty, "How Can Humans Keep the Upper Hand?", December 2017, available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

84. Electronic Privacy Information Centre, "French President: Algorithmic Transparency Key to National Strategy", April 2018, available at <https://epic.org/2018/04/french-president-algorithmic-t.html>

85. The Federal Government of Germany, "Artificial Intelligence Strategy", November 2018, available at: https://ec.europa.eu/knowledge4policy/publication/germany-artificial-intelligence-strategy_en

86. Office of the President of the Russian Federation, "Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation", October 2019, available at: https://cset.georgetown.edu/wp-content/uploads/t0060_Russia_AI_strategy_EN-1.pdf

DENMARK

Maturity index – 3/5

Denmark's 2019 National Strategy⁸⁷ for AI lays down the framework for regulating AI, and as a part of its initiative to establish ethical principles for AI, it emphasises the principle of explainability. According to the strategy, explainability means that you can describe, control and restore data, underlying logics and consequences of the use of AI. The Danish Strategy Paper notes that explainability is not full transparency of the algorithms, as it also balances the need to protect business interests. However, it mentions that the public authorities have a special responsibility to ensure openness and transparency in the use of algorithms.

EU

Maturity index – 4/5

The EC is one of the first to have adopted regulations to govern the use and development of AI. The Communication on Artificial Intelligence⁸⁸ released by the EC in 2018 for the European Parliament was amongst the first set of recommendations that mentioned the importance of XAI and transparent algorithms. Even though the communication sets the research and development in XAI as an agenda in its 'Beyond 2020' focus, it still acknowledged the need for the same to be incorporated in the ethics guidelines that it envisaged.

In April 2019, the High-Level Expert Group on AI released its Ethics Guidelines⁸⁹ for Trustworthy AI that highlighted the importance of transparency and listed it as one of the seven key requirements that AI systems should meet in order to be trustworthy. As per the guidelines, this requirement is closely linked with the principle of explicability and encompasses transparency of elements relevant to an AI system: the data, the system and the business models. Apart from the traceability and explainability of AI decision making, it highlighted that the users must be aware of the information that is being used by AI systems and the same must be communicated to them, making 'communication' an indispensable part of the requirement of transparency. This principle was reiterated in the communication⁹⁰ released by the EC on 'Building Trust in Human Centric Artificial Intelligence' in April 2019. In June 2019, the High-Level Expert Group on AI issued a further set of recommendations on 'Policy and Investment Recommendations for Trustworthy AI',⁹¹ which suggested that a general responsibility to disclose that data being collected and analysed by a system is non-human should be attributed to the deployers of AI systems and that this goes hand-in-hand with ensuring the transparency of AI systems.

On 17 July 2020, the High-Level Expert Group completed its mandate by issuing a new tool, i.e. the final Assessment List for Trustworthy AI.⁹² This tool – available as a document⁹³ and a web-based tool⁹⁴ - offers a practical, dynamic and accessible checklist for developers and deployers of AI, who seek to implement the Ethics Guidelines. The goal of the

87. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", March 2019, available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

88. EC, "Communication Artificial Intelligence for Europe", April 2018, available at: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>

89. High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy Artificial Intelligence", April 2019, available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

90. EC, "Communication on Building Trust in Human Centric Artificial Intelligence", April 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>

91. High-Level Expert Group on Artificial Intelligence, "Policy and Investment Recommendations", June 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>

92. EC, "Final Assessment List for Trustworthy AI", July 2020, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342

93. EC, "Assessment List for Trustworthy AI Checklist", July 2020, available as https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342

94. European AI Alliance, "ALTAI – The Assessment List on Trustworthy Artificial Intelligence" (web tool), available at <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence>

checklist is to ensure that users benefit from AI without exposure to unnecessary risks, through a set of concrete steps for self-assessment. In respect of transparency, the checklist specifically considers items that relate to the traceability of the processes and data used by the AI systems, explainability of both the technical process and reasoning behind the decision-making of the AI system and whether the limitations of the AI systems' capabilities have been communicated to the user. These three elements are all considered integral to improving transparency, with a view to building greater trust in AI systems.⁹⁵ Along with the checklist, the High-Level Expert Group also issued a report that builds on the Policy and Investment Recommendations by offering possible implementation recommendations in three specific sectors – the public sector, healthcare and manufacturing & the IoT.⁹⁶

A white paper⁹⁷ released in 2020 by the EC on developing excellence and trust in AI urged the legislative framework to address the problem of opacity that exists in AI systems with regards to decision making. In connection with the white paper, the EC also noted that opacity of algorithms led to difficulty in ascertaining liability when AI systems are used.⁹⁸ It argues that humans may not need to understand every single step of the decision-making process, but as AI algorithms grow more advanced and are deployed in critical domains, it is imperative for human beings to understand how decisions have been reached. In particular, this is crucial where AI systems are used in ex-post mechanisms of enforcement, as it will allow the enforcement authorities the possibility to trace the responsibility of AI systems' behaviours and choices.

AUSTRALIA

Maturity index – 4/5

A discussion paper⁹⁹ prepared by the government on Australia's AI ethics framework includes transparency and explainability of AI technology as one of the core principles. The discussion paper focuses more on the aspect of the information that is used by AI systems to reach a decision, rather than algorithmic transparency which focuses on sharing knowledge of the process that underlie decision making by AI systems. The paper rejects the idea of a 'black box' algorithm, wherein the workings of AI are kept secret and are unknowable by users, especially in matters of public interest. It recommends various solutions to the problem of opacity, such as explainable technology, regular testing and regulations that require transparency and fairness in an AI system.

The report highlights that advanced AI systems such as neural networks are not possible to be understood by a layman; however, the input data can be explained, the outcomes from the system can be monitored, and the impacts of the system can be reviewed internally or externally, to achieve transparency in a meaningful way. Therefore, transparency does not necessarily mean only understanding the way an algorithm reaches a particular decision. As a solution, the framework propounds the concept of Human in the Loop (**HITL**) which means incorporating human oversight over automated technologies, including exception control, optimisation and maintenance of automated decision systems to ensure that errors are addressed, and humans remain accountable.

Another report¹⁰⁰ commissioned by Government of Australia in November 2019 considered the problem of black box as one of the three main challenges in making AI trustworthy in the minds of people. The report also considers transparency as one of the main principles that must be incorporated while developing the regulations for AI.

95. Requirement #4 of the Assessment List on Trustworthy Artificial Intelligence.

96. EC, "Sectoral Considerations on the Policy and Investment Recommendations, July 2020, available at <https://futurum.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-sectoral-considerations-policy-and-investment-recommendations-trustworthy-ai>

97. EC, "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust", February 2020, available at: https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

98. EC, "Commission Report on Safety and Liability Implications of AI, Internet of Things and Robotics", February 2020, available at: https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en

99. Dawson D, Schleiger E, et al, "Artificial Intelligence: Australia's Ethics Framework. Data61 CSIRO", 2019, available at: https://consult.industry.gov.au стратегic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

100. Data61 CSIRO, "Artificial Intelligence: Solving Problems, Growing the Economy and Improving our Quality of Life", November 2019, available at: <https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap>

JAPAN

Maturity index – 4/5

In March 2017, the Advisory Board on Artificial Intelligence and Human Society released its report¹⁰¹ analysing the issues to be considered by the government of Japan while making regulations on AI. It called for further research to ensure AI technologies are controllable and transparent by explaining the processes and logic of calculations that can have social implications. A novel issue that was raised with respect to explainability by the report was about the transfer of control from machines to humans in emergencies; the report argues that explainability becomes all the more crucial in such cases, and there needs to be a smooth transfer of control in the human hands at an individual level.

The Draft AI guidelines¹⁰² released by the government in July 2017 lists transparency as one of the main principles concerning the sound development of AI networking and the promotion of the benefits of AI systems. The guidelines emphasise the importance of developers looking into the verifiability of inputs and outputs of AI systems, as well as the explainability of the judgment of AI systems to a reasonable extent, to promote better public understanding and trust, including among users of AI systems.

SINGAPORE

Maturity index – 4/5

A discussion paper¹⁰³ on AI and personal data released by the PDPC, the nodal authority for data protection and AI in Singapore, set out the basis for a regulatory framework governing AI. It approaches the issue of transparency and explainability from the point of view of inculcating trust towards AI systems. It underscores that policies and regulations that promote explainability, verifiability and transparency as clear baseline requirements can build consumer trust in AI systems deployed in various sectors. It suggests that explainability should be accounted for by AI developers in the process of design itself, which would help to explain to users how their AI solutions function. Traceability of the decisions by AI systems is another measure that the paper argues to be incorporated in every organisational governance structure.

Pursuant to the publication of the discussion paper, the PDPC issued the Model Artificial Intelligence Governance Framework¹⁰⁴ that also includes transparency and explainability as one of the guiding principles for the development of AI. According to the framework, organisations using AI in decision-making should ensure that the decision-making process is explainable, transparent and fair. It also encourages organisations to take a risk-based approach in making a two-fold assessment: first, identifying the features or functionalities that have the greatest impact on stakeholders; and second, identifying which of these measures will be most effective in building trust with their stakeholders. It suggested that explainability is sufficiently essential as a principle that it should be incorporated as part of the organisation's AI deployment process, through the following practices:

1. Documenting how the model training and selection processes are conducted, the reasons for which decisions are made, and measures taken to address identified risks will enable the organisation to provide an account of the decisions subsequently.

101. Advisory Board on Artificial Intelligence and Human Society, "Report on Artificial Intelligence and Human Society" (Unofficial translation), March 2014, available at: https://www8.cao.go.jp/cstp/tyousakai/ai/summary/aisociety_en.pdf

102. The Conference toward AI Network Society, "Draft AI R&D Guidelines for International Discussions", July 2017, available at: https://www.soumu.go.jp/main_content/000507517.pdf

103. (Singapore) Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI", June 2018, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD---050618.pdf>

104. (Singapore) Personal Data Protection Commission and Infocomm Media Development Authority, "Model Artificial Intelligence Governance Framework (Second Edition)", January 2020, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

2. Incorporating descriptions of the solutions' design and expected behaviour into product or service descriptions and system technical specifications documentation demonstrates accountability to individuals and/or regulators.
3. Using supplementary explanation tools that are helpful for explaining AI models, especially models that are less interpretable (also known as "black box" systems).

SOUTH KOREA

Maturity index – 2/5

The South Korean National Strategy for AI¹⁰⁵ notes that transparency is among the basic ethical principles and norms on the basis of which discussions between the government and the private sector should be had in respect of the direction in which AI development takes place in the country. The Mid-to-Long-term Master Plan in Preparation for the Intelligence Information Society¹⁰⁶ also highlights the importance of enhancing understanding in intelligent IT as an important part of building trust in AI. Aside from the above broad policy statements, there do not appear to be any specific developments in South Korea in respect of transparency in AI.

SWEDEN

Maturity index – 3/5

A report¹⁰⁷ on AI by Sweden's national innovation agency, Vinnova mentions the importance of transparency in AI systems to ensure ethical conduct by the technology. The National Strategy¹⁰⁸ for AI released by the government gives due regard to transparency and recommends that the same must be included in the ethics framework for AI of the country, as a means to develop greater trust towards AI deployment. In considering the use of AI, the National Strategy considers transparency as an important aspect of maintaining the rule of law, ascribing liability where AI systems are used and inculcating greater public trust.

FINLAND

Maturity index – 3/5

The report¹⁰⁹ published by Ministry of Economic Affairs and Employment of Finland acknowledges that transparency, accountability and extensively notable societal benefit constitute the general principles of a good AI society. This sentiment and intent have been elaborated in a subsequent report¹¹⁰ which discusses transparency as crucial in AI that supplements

105. Ministry of Science and ICT, "National Strategy for Artificial Intelligence", March 2020, available at https://www.msit.go.kr/cms/english/pl-policies2/_icsFiles/afieldfile/2020/03/23/National%20Strategy%20for%20Artificial%20Intelligence_200323.pdf

106. Government of South Korea, "Mid- To Long-Term Master Plan in Preparation for Intelligent Information Society", 2017, available at: https://english.msit.go.kr/cms/english/pl-policies2/_icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

107. Vinnova, "Artificial intelligence in Swedish Business and Society - Analysis of Development and Potential", May 2018, available at: https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf

108. Government Offices of Sweden, "National Approach to Artificial Intelligence", 2018, available at: <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

109. (Finland) Ministry of Economic Affairs and Employment, "Finland's Age of Artificial Intelligence", December 2017, available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

110. Ministry of Economic Affairs and Employment Ministry, "Work in the Age of Artificial Intelligence", September 2018, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160980/TEMJul_21_2018_Work_in_the_age.pdf

decision-making of public organizations where citizen's statutory rights and obligations may be affected. In such scenarios, it is imperative to understand the extent of structural bias borne out of underlying data since machines are not normative learners and unlike humans that assume ultimate legal and moral responsibility for their decisions – the same cannot be attributed to any AI software.

The final report¹¹¹ of Finland's Artificial Intelligence Programme 2019 assumes a novel perspective and states that it is more about trust in AI than a need for transparency, explaining this with the example of how one may not understand how calls are transmitted across continents over 4G networks but there is unwavering trust in the data communication systems and parties operating them. However, it maintains that the basis of building of such trust remains transparency, accountability and reliability.

SPAIN

Maturity index – 4/5

In February 2020, the Spanish Data Protection Authority issued guidelines on compliance with data protection law in the context of AI,¹¹² which considered multiple aspects of AI regulation, including of the importance of protecting privacy and implementing the rights granted to citizens under the EU's GDPR. In this context, the guidelines discuss methods of risk assessment, which include privacy impact assessments for high-risk categories of data (as laid out in the GDPR) and measures to increase transparency in the use of AI systems. The guidelines note that the obligation to be transparent is crucial to AI based processing, and it should be designed in a way that enables data subjects to become aware of the capabilities, context and impact of AI based solutions, as well as the existence of third parties in the processing methodology, among other things. It notes that transparency is not a momentary obligation, but must be considered throughout the life cycle of AI systems, including design, certification, training, decision making, etc. The guidelines consider the appointment of a data protection officer, as per the GDPR, to be a helpful measure in introducing transparency, as it allows data subjects to get information from a single source that is obligated under law to protect the data subjects' interest.

NORWAY

Maturity index – 4/5

The Norwegian National Strategy for Artificial Intelligence¹¹³ extensively discusses the need for AI systems to be transparent and explainable, stating that "transparency, explainability and cautious testing" are the "fundamental principles" to turn to for guidance when considering the consequences of autonomous decisions made by AI. The National Strategy mentions "transparency" as one of the ethical principles for AI and emphasizes on 'traceability' which facilitates auditability and explainability, as crucial to allow individuals an insight into how a decision that affects them was made. This stance on transparency is reiterated by Norway's Law Commission on the Public Administration Act which states that while "automation can promote equal treatment and consistent implementation of regulations", transparent and explainable systems are necessary to ensure that the AI algorithm's judgement is comparable to human judgment as far as possible in respect of reasonability, soundness and trustworthiness.

111. Ministry of Economic Affairs and Employment Ministry, "Leading the Way into the Age of Artificial Intelligence", June 2019, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf

112. Agencia Espanola Proteccion Datos, "RGPD Compliance of Processing that Embed Artificial Intelligence: An Introduction", February 2020, available at https://www.aepd.es/sites/default/files/2020-02/adequacion-rgpd-ia-en_0.pdf

113. Norwegian Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence", available at: https://www.regjeringen.no/contentassets/1febbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

In 2018, a report published by the Norwegian Board of Technology entitled “Artificial Intelligence – Opportunities, Challenges and a Plan for Norway”¹¹⁴ presents an interesting and important argument against absolute transparency by considering the clash between transparency and security of AI. It notes that the process of making an AI algorithm transparent exposes it to malicious use which can compromise the purpose and intent of the system, and therefore, should be considered when looking into the ways in which transparency can be introduced via regulation.

ESTONIA

Maturity index – 3/5

Estonia has been at the forefront of implementing AI in governance and public services. The Report of the Estonia AI Taskforce¹¹⁵ (2019) set out the Estonian government’s plan for integrating AI systems into its public and private sectors, which sets out a list of ethical principles related to AI, of which the principle of clarity or transparency is one. It also specifically considers transparency in the context of imputing liability for actions taken by AI, and for the sake of clarity notes that such responsibility should lie with the relevant government body that implemented the AI solution.¹¹⁶

THE NETHERLANDS

Maturity index – 3/5

The Dutch AI Manifesto,¹¹⁷ released in 2018, lists “opacity” in AI systems as one of the multidisciplinary challenges that the rollout of AI will face, including in terms of regulation. The manifesto states that AI systems should be socially aware to support collaboration, explainable to be transparent and responsible to promote accountability for decision making. In order to promote transparency, the manifesto notes that further research is required into models that are more open to explanation, techniques and models for generating satisfactory explanations, and intelligible user interfaces for interacting with human users. It notes that the main challenge is how to develop advanced AI systems which can explain their rationale for how they perform sophisticated tasks.

The Strategic Action Plan for AI, 2019¹¹⁸ released by the Netherlands government also contains recommendations to tackle opacity in AI systems. It directs Ministry of the Interior and Kingdom Relations and the Association of Netherlands Municipalities to experiment with AI, with a focus on ethics by design and algorithm transparency. It notes that the Innovation Centre for Artificial Intelligence is carrying out research on explainable and transparent AI, and further that in collaboration with other government organisations, the Ministry of the Interior and Kingdom Relations is conducting two experiments with AI, focusing on transparency of algorithms. Apart from this, the Ministry of the Interior and Kingdom Relations is also setting up a transparency lab for government organisations, where knowledge is exchanged in the areas of transparency, explainability and accountability.

In an interesting application of the principle of transparency, the city of Amsterdam recently collaborated with the city of Helsinki to launch public “AI registers”, which were developed in collaboration with Saidot.ai,¹¹⁹ a Finnish company

114. Norwegian Board of Technology, “Artificial Intelligence – Opportunities, Challenges and a Plan for Norway”, 2018, available at: <https://teknologiradet.no/wp-content/uploads/sites/105/2018/11/AI-and-machine-learning-1.pdf>

115. (Estonian) Ministry of Economic Affairs and Communication, “Report of Estonia’s AI Taskforce”, 2019, available at <https://www.kratid.ee/in-english>

115. Id, page 39.

117. Special Interest Group on Artificial Intelligence, “Dutch Artificial Intelligence Manifesto”, September 2019, available at: <http://ii.tudelft.nl/bnvki/wp-content/uploads/2018/09/Dutch-AI-Manifesto.pdf>

118. Ministry of Economic Affairs and Climate Policy, “Strategic Action Plan for Artificial Intelligence”, October 2019, available at: <https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence>

119. See, <https://www.saidot.ai>

UAE

Maturity index – 3/5

The UAE's Artificial Intelligence Guide, 2020,¹²² a part of its National Program for Artificial Intelligence touches upon the subject of transparency with respect to AI and its use in companies. It recommends that companies evaluate corporate policy to ensure the right guidelines are in place for any AI implementation to be ethical, fair, accountable, transparent and explainable. The intention of the recommendation was to ensure that the AI solution is not only innovative but also delivers human benefit and happiness.

This outlook on AI explainability is supplemented by the Ethical AI Toolkit¹²³ published by the Dubai Data Establishment, Smart Dubai Office in 2019 which defines guiding principles for ethical AI focusing on four domains: ethics, security, humanity, and inclusiveness. Within the purview of 'ethics', the AI systems are expected to be fair, transparent, accountable, and understandable.

HONG KONG

Maturity index – 4/5

Hong Kong's Personal Data (Privacy) Ordinance (**PDPO**),¹²⁴ which governs data privacy, includes transparency as one of its core principles. However, while the PDPO is technology neutral, the difficulties of giving effect to the principle of transparency in substance, in the light of AI technology was acknowledged.

The Hong Kong Privacy Commissioner for Personal Data (**PCPD**), which enforces data protection law in Hong Kong, commissioned a study to achieve ethical and fair processing of data,¹²⁵ which contains a set of principles known as the "Enhanced Data Stewardship Accountability Elements for Data Processing Activities, such as AI and ML, that Directly Impacts People (**Enhanced Elements**) and Data Stewardship Values (**Values**). The report notes that technology such as AI should be built and deployed to serve human interest, and not hinder it through lack of explainability or by violating data privacy rights. It also highlights the difficulties with transparency in the context of AI, because it may not be possible to understand the purpose for data-collection beforehand in the case of big data, and black box algorithms are opaque, complicated and users may not be able to discern the true reasoning for decision making undertaken automatically by AI systems. The Enhanced Elements and Values have been propounded with the purpose of addressing these issues, which include being transparent about processes and the data stewardship values that organisations use to design or deploy AI systems, through effective communication, documentation and setting up accountability systems such as Privacy Impact

120. City of Amsterdam, "City of Amsterdam Algorithm Register", available at <https://algoritmeregister.amsterdam.nl/en/ai-register/>

121. Natalia NygrenModjeska, "AI Registers: Finally, a Tool to increase Transparency in AI/ML", KD Nuggets, December 2020, available at <https://www.kdnuggets.com/2020/12/ai-registers-transparency-ml.html>

122. Ministry of State for Artificial Intelligence, "National Program for Artificial Intelligence: AI Guide", 2020, available at: https://ai.gov.ae/wp-content/uploads/2020/02/AIGuide_EN_v1-online.pdf

123. Smart Dubai, "AI Ethics, Principles and Guidelines", 2019, available at: https://www.smartdubai.ae/pdfviewer/web/viewer.html?file=https://www.smartdubai.ae/docs/default-source/ai-ethics-resources/ai-ethics.pdf?sfvrsn=a9081451_8

124. Text of the Personal Data (Privacy) Ordinance, 1996, available at <https://www.elegislation.gov.hk/hk/cap486?pmc=1&m=1&pm=0>

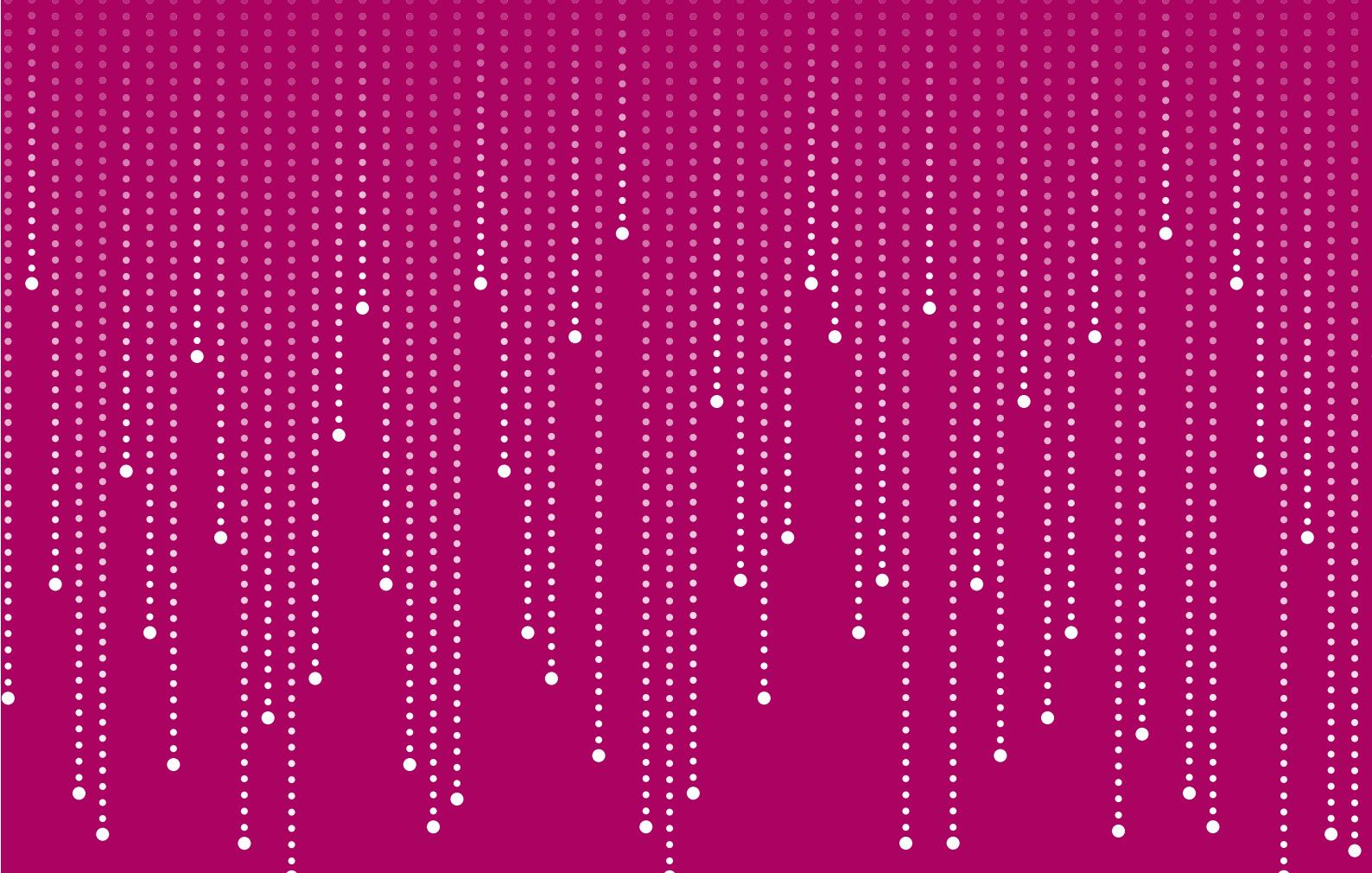
125. The Information Accountability Foundation, "Ethical Accountability Framework for Hong Kong, China", October 2018, available at https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf

Assessments and Ethical Data Impact Assessments.¹²⁶

The report also discusses a Process Oversight Model which provides a set of comprehensive actions that companies working in the AI ecosystem should incorporate to ensure that these systems are respectful, beneficial and fair. Of these actions, transparency of process was included as an important one.¹²⁷

126. Id, page 22.

127. Id, page 31.



INTEROPERABILITY

Interoperability can be defined as the ‘the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together’.¹²⁸ It refers to the ability of two or more systems or components to exchange information, and to use or analyse the information that has been exchanged.¹²⁹ However, technological interoperability requires that the format in which data is generated or stored is standardized and that interconnected systems have the ability to read, analyse or make use of the transmitted information.¹³⁰

There are multiple levels or layers of interoperability – (a) foundational interoperability, where the data is transmitted by one system and received by another, but not interpreted; (b) structural interoperability, which standardizes the format of receiving data across multiple systems; and (c) semantic interoperability, which ensures that data flowing between two or more systems can be interpreted at the receiving end (relying on the two underlying layers).¹³¹ This makes it imperative for regulatory regimes to standardise the way in which data is received, processed, or both, by multiple systems, in order to fully harness the power of AI across systems. This may be done through archetypes or templates that are comprehensive and evidence-based, created by domain experts.¹³² Interoperability may also be technical or non-technical: the former includes communications, electronics, applications, and multi-database interoperability, while the latter considers organisational, operational, process, cultural and coalition interoperability.

Some of the key benefits of interoperability in AI systems include the ease of processing large amounts of data

(or big data), precision of outcomes or outputs so processed and timeliness of processing. In a sector such as healthcare, these elements are crucial to improve the quality of decision-making by healthcare professionals. Interoperability also increases the value of existing networks – something that can increase manifold with AI. There are also social benefits to interoperability, whereby a user expends less effort to use various platforms than if each of them was distinct. However, the transmission and interpretation of data from one system to another (or multiple others) gives rise to concerns relating to privacy and data protection, as rights need to be balanced with the interest or benefits accruing from interoperability. From a competition perspective, interoperability through the imposition of standards by regulatory authorities or incumbents in a sector could potentially keep new entrants out, or exclude innovations that are not based on the industry standard.¹³³

The OECD principles on AI¹³⁴ have also included interoperability as a principle to increase transparency and promote ethical use of AI going forward; developing industry standards internationally is a recognised priority,¹³⁵ and this is seen as an ongoing project at the international level by various participant countries. The North Atlantic Treaty Organization (**NATO**) is also reportedly working towards establishing interoperability standards and norms for the use of AI in military and defence. NATO’s recently set up Innovation Board is responsible for coordinating on-going AI related work across NATO member countries, in an attempt to arrive at a shared vision of how to use AI in military applications.¹³⁶

128. Cambridge Business English Dictionary, “Interoperability”, available at <https://dictionary.cambridge.org/dictionary/english/interoperability>

129. IEEE 1990 quoted in Berankova M., Kvasnicka R., & Houska M., “Towards the definition of knowledge interoperability”, 2nd International Conference on Software Technology and Engineering, 2010, available at https://www.researchgate.net/publication/224184937_Towards_the_definition_of_knowledge_interoperability

130. Urs Gasser, “Interoperability in the Digital Ecosystem”, July 2015, available at: <http://dx.doi.org/10.2139/ssrn.2639210>

131. Cabot Solutions, “Interoperability and AI - A Symbiotic Relationship for Healthcare”, 22 August 2019, available at <https://www.cabotsolutions.com/interoperability-and-ai-a-symbiotic-relationship-for-healthcare>

132. L Potgieter, “Semantic Interoperability: Are You Training your AI by Mixing Data Sources that Look the Same but Aren’t?”, 2018, available at <https://www.kdnuggets.com/2018/10/semantic-interoperability-training-ai-mixing-different-data-sources.html>

133. C Marsden and R Nicholls, “Interoperability: A solution to regulating AI and Social Media platforms”, October 2019, available at <https://www.sciencedirect.com/science/article/pii/S1066212319300449>

134. OECD, “OECD Principles on AI”, May 2019, available at <https://www.oecd.org/going-digital/ai/principles/>

135. OECD, “Recommendation of the Council on Artificial Intelligence”, May 2019, available at <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

136. Erica Pepe, “NATO and Collective Thinking on AI”, November 2020, available at <https://www.iiss.org/blogs/military-balance/2020/11/nato-artificial-intelligence>

Apart from national and international government efforts to introducing interoperability, there have also been private industry-led efforts in this regard. For instance, in February 2020, 50 organizations (which included Google, AT&T, Amazon, etc.) developed a common standard for the use of AI in healthcare, under the aegis of the Consumer Technology Association.¹³⁷ This standard received accreditation by the American National Standards Institute, and covers definitional aspects of AI and associated technologies in healthcare, including assistive intelligence, synthetic data, remote patient monitoring, etc.¹³⁸ The goal of this project

was to arrive at a common understanding between manufacturers and deployers of AI based technology, and support interchangeability / interoperability between products and systems. This is expected to help the creators, deployers and users of AI systems understand them better and use them more efficiently.¹³⁹

In the chapter below, we examine the regulatory regime governing interoperability of AI in various countries, and whether or how such regulations propose to or have navigated some of the issues arising from the move towards increasing interoperability.

137. Riya Anandwala and Danielle Cassagnol, "CTA Launches First-Ever Industry-Led Standard for AI in Healthcare", February 2020, available at <https://www.cta.tech/Resources/Newsroom/Media-Releases/2020/February/CTA-Launches-First-Ever-Industry-Led-Standard>

138. Consumer Technology Association, "Definitions / Characteristics of Artificial Intelligence in Healthcare (ANSI/CTA-2089.1)", February 2020, available at https://shop.cta.tech/collections/standards/products/definitions-characteristics-of-ai-in-health-care?_ga=2.57103209.231402224.1608601539-1730171033.1608601539

139. Samantha McGrail, "New Standard Launched for Artificial Intelligence in Healthcare", March 2020, available at <https://hitinfrastructure.com/news/new-standard-launched-for-artificial-intelligence-in-healthcare>

MATURITY INDEX INTEROPERABILITY



Level 1

No Discussion

South Korea

Level 2

Preliminary
Discussions

India, USA, China, Canada, France, Israel, Denmark,
Singapore, Sweden, Finland, Spain, Norway

Level 3

Established Policy
Position

UK, Germany, Australia, The Netherlands,
United Arab Emirates, Hong Kong

Level 4

Policy
Recommendation

EU, Estonia

Level 5

Implementation into
Legislation



INDIA

Maturity Index – 2/5

The Indian AI Strategy¹⁴⁰ does not expressly address the issue of interoperability between the AI systems. However, it does recognise that interoperability of big data in specific sectors is the key to development of those sectors. The two broad application areas of AI interoperability that have been discussed in the said report are as follows:

1. Language: Native Language NLP for diverse Indian languages and its integration with technology. In such initiatives, co-funding by the Government would also enable enforcement of standards across development of data sets, thereby allowing interoperability at a large scale.
2. Healthcare: The Government aims at leveraging technology to improve healthcare facilities through the National eHealth Authority which will strategise eHealth adoption, define standards and a framework for the health sector, and put in place electronic health record exchanges. It also propounds the concept of Integrated Health Information Program to provide electronic health records to all citizens of India while making existing health records interoperable or accessible across multiple systems.

The report also recommends creation of large foundational annotated data sets for the availability of general data corpora which can be applied across product functions, and can serve to provide a ready source of data for AI systems to use.

Further, in 2019, the Ministry of Electronics and Information Technology¹⁴¹ has highlighted the need to develop and implement standards for data formats to ensure that data provided is operable in common AI platforms and frameworks used by AI researchers.

The report of the Expert Committee chaired by Justice B N Srikrishna on Data Protection¹⁴² also makes an important recommendation on interoperability in the context of data protection and managing consent by individuals to data fiduciaries. The report refers to 'consent dashboards' through which individuals can manage the consent that they have given to various data fiduciaries for using their data. As mentioned in the White Paper¹⁴³ released by the Expert Committee on Data Protection, interoperability and standardization of the data consented to be shared and held by the data controller is the key to convenient tracking and access to such data. Leading from such policy recommendations, Section 23 of the Data Protection Bill, 2019¹⁴⁴ provides for a consent manager, who is a data fiduciary and is required to facilitate the gain, withdrawal, review and management of consent from a data principal (i.e., the source of data) on an accessible, transparent and interoperable platform.

140. NITI Aayog, "National Strategy for Artificial Intelligence, #AIForAll", 2019, available at: <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>. P.39

141. Ministry of Electronics and Information Technology, "Report Of Committee - A On Platforms and Data On Artificial Intelligence", July 2019, available at https://meity.gov.in/writereaddata/files/Committee_A-Report_on_Platforms.pdf

142. Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", 27 July 2018 available at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

143. Committee of Experts under the Chairmanship of Justice Srikrishna, "White Paper of the Committee of Experts on a Data Protection Framework for India", available at: https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

144. The Personal Data Protection Bill, 2019, available at: https://prsinIndia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf

USA

Maturity Index – 2/5

In the USA, the regulatory priority has been to create standards or formats for the procurement and storage of data to promote interoperability in various sectors, with a view to maintaining flexibility, inclusivity and security from malicious attacks. For instance, the United States Core Data for Interoperability¹⁴⁵ is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange. Apart from this, the US National Institute of Standards and Technology (**NIST**), tasked with the development of standards across sectors, released a plan in 2019 for federal engagement in developing technical standards and related tools to facilitate interoperability.¹⁴⁶ NIST has acknowledged the wide-ranging impact of AI, and the need to develop it in a trustworthy manner to ensure reliability, safety and accuracy. As a part of this endeavour, NIST is participating in the creation of international standards that ensure innovation, public trust and confidence in systems that use AI technologies.¹⁴⁷

Besides this, Section 5(a)(iv) of the AI Executive Order¹⁴⁸ provides for identification of data and models for consideration for increased public access. It further acknowledges the need for data documentation and formatting, including the need for interoperable and machine-readable data formats.

CHINA

Maturity Index – 2/5

China has accorded great importance to the standardization of AI for the purpose of interoperability. The State Council's AIDP,¹⁴⁹ for which AI standardization serves as an important support guarantee, proposed the following:

1. 1strengthening the AI standards framework system
2. adherence to the principles of security, availability, interoperability, and traceability;
3. gradually establishing and improving the basic commonality, interoperability, industrial applications, cyber security, privacy protection, and other technical standards for AI.

Additionally, the Ministry of Industry and Information Technology in its Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018-2020),¹⁵⁰ pointed out that it is necessary to establish an AI industry standard specification system, and establish and improve technical standards such as common foundations, interoperability, and industrial applications, while building AI product evaluation systems.

145. The Office of the National Coordinator for Health Information Technology, "United States Core Data for Interoperability, Version 1", available at: <https://www.healthit.gov/isa/sites/isa/files/2020-03/USCDI-Version1-2020-Final-Standard.pdf>

146. NIST, "U.S. Leadership in AI: A Plan For Federal Engagement In Developing Technical Standards And Related Tools", 2019, available at: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

147. See, <https://www.nist.gov/topics/artificial-intelligence>

148. Executive Order on Maintaining American Leadership in Artificial Intelligence, 2019, available at <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>

149. People's Republic of China, "New Generation Artificial Intelligence Development Plan", available at: <https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/>

150. Ministry of Industry and Information Technology, "Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018-2020)", December 2017, available at <https://super-ai.diascreative.net/three-year-action-plan-for-promoting-development-of-a-new-generation-artificial-intelligence-industry-20182020>

CANADA

Maturity Index – 2/5

Canada is committed to a level data playing field and the promotion of transparency, portability, and interoperability across domains; in pursuance of which, experts from government, industry and civil society have established a ‘Canadian Data Governance Standardization Collaborative’¹⁵¹ with the aim of developing a data standards roadmap. The group, overseen by the Standards Council of Canada, aims to deliver a “comprehensive and consensus-based standardisation roadmap and a concrete set of recommendations” on data governance by the end of 2020.

UK

Maturity Index – 2/5

Like in most countries, the UK has considered data interoperability in AI primarily in the healthcare sector. In September 2018, the Department for Health and Social Care published a code of conduct¹⁵² relating to the use of data-driven health and care technology. One of the commitments of the government was to improve interoperability and openness, using application programming interfaces and public data standards, so that products are interoperable.

Interoperability is also addressed as a part of the bundle of rights under data privacy, in compliance with the EU GDPR. The right to data portability and interoperability is overseen by the Information Commissioner’s Office, which secures the right to data portability or the right to allow individuals to obtain and reuse their personal data for their own purposes across different services; and moving, transferring or copying personal data from one IT environment to another in a way that does not affect its security or usability.¹⁵³

For example, a report on Online Targeting by the UK Centre for Data Ethics and Innovation,¹⁵⁴ has considered the issue of interoperability in the context of online targeting by social media platforms and search engines. The report acknowledges the benefits of online targeting, i.e., that content is more personalised and operates as a filter for the massive amounts of information found online, that it is already a major driver of economic value, and will continue to be used in innovative ways as technology continues to develop. In calling for greater transparency and accountability, the report calls for limited regulation that empowers the user and protects vulnerable groups. In this regard, the report notes that stakeholders called for “simple and digestible consent mechanisms and easy to use, accessible settings which would ideally be interoperable between platforms or services” as an important step towards creating robust and user-friendly systems, over which users have greater control. This includes measures to protect autonomy and privacy, identify risky behaviours, identify vulnerable groups (for example, age), etc. The report also predicts the rise of data intermediaries, which would lead the charge towards developing interoperability standards and act as an alternate regulatory mechanism pending government regulation, while rebalancing power towards the user. It recommends that public policy support the development of these intermediaries, given the volume of personal data that is available and continues to be shared online.

151. Standards Council of Canada, “Canadian Data Governance Standardization Collaborative”, 2019, available at <https://www.scc.ca/en/flagships/data-governance>

152. Department of Health and Social Care, “Guidance: Code of Conduct for Data-Driven Health and Care Technology”, 2019, available at <https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology>

153. The Information Commissioner’s Office, “The Right to Data Portability”, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>

154. Centre for Data Ethics and Innovation, “Online Targeting: Final Report and Recommendations”, 4 February 2020, available at <https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations>

FRANCE

Maturity Index – 2/5

In the National Strategy on AI,¹⁵⁵ emphasis has been laid on the need to develop and implement standards, tests and measurement methods to make AI technology more secure, reliable, useable and interoperable. Since data is the raw material of AI, and the emergence of new uses and applications depends on it, an aggressive policy aimed at promoting data access, as well as its circulation and sharing has also been recommended.

GERMANY

Maturity Index – 2/5

A well-rounded approach to AI and Interoperability can be observed in the case of German initiatives and policy. First addressing the need of standardisation in development of AI, the Federal Government of Germany in its National Strategy for AI¹⁵⁶ proposed the following initiatives:

1. Funding for the development of data standards and formats to encourage EU-wide collaborations;
2. Funding for experts, particularly from SMEs and start-ups in order to support their participation in international standardisation processes;
3. Developing a roadmap on AI standardisation to review existing standards for AI compatibility.

In addition to this, the German AI strategy aims to develop the requisite infrastructure to ensure better connectivity of the network and interoperability of data. To this effect, it proposes the following initiatives:

1. Improving data sharing facilities by providing open access to governmental data and improving infrastructure for access to Earth observation data;
2. Building a trustworthy data and analysis infrastructure based on cloud platforms, upgraded storage and computing capacity; and
3. Setting up a National Research Data infrastructure to provide science-driven data services to research communities.

Furthermore, in January 2018, representatives of companies, large corporations, universities, research organizations, certification bodies, ethics experts and the German Federal Office for Information Security joined together to form the interdisciplinary DIN Working Committee "Artificial Intelligence" with the purpose of developing a comprehensive approach to AI. The committee's task is to develop standards and best practices for AI tools, processes and applications while also working on open standards and specifications for a thorough understanding of AI.

155. Cedric Villani, "For a Meaningful Artificial Intelligence: Towards a French and European Strategy", 2018, available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

156. The (German) Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and Energy, and the Federal Ministry of Labour and Social Affairs, "Artificial Intelligence Strategy", November 2018, available at https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf

ISRAEL

Maturity Index – 2/5

While the concept of interoperability has not been directly touched upon despite Israel's thought leadership in the field of AI, the interim report¹⁵⁷ commissioned by the National Council for Research and Development (**MOLMOP**) at the Ministry of Science and Technology, emphasizes that the government must provide coordination and leadership in order to promote the creation of shared standards and encourage their widespread use in government, academia, and industry. The intent and effect of this emphasis on 'shared standards' can be directly linked to allowing and enabling interoperability among systems as the AI community (users, industry, academia, and government) matures and advances.

DENMARK

Maturity Index – 2/5

The Strategy for Denmark's Digital Growth¹⁵⁸ released in 2018, underlines the importance of standardisation of data and further explains that uniformity and proper documentation makes it easier for companies and institutions to use public data. In view of the same, the government aims to promote the use of common public standards for data and interfaces.

As per the National Strategy for AI¹⁵⁹ released in March 2019, the government will implement the following initiatives to better data sharing infrastructure and further facilitate interoperability of data:

1. Common Danish language resource
2. Better access to public-sector data
3. More data in the cloud for AI
4. Improved access to data outside Denmark for Danish businesses and researchers.

EU

Maturity Index – 2/5

Adopted in March 2017, the European Interoperability Framework¹⁶⁰ is part of the Communication (COM(2017)134) from the EC that gives specific guidance on how to set up interoperable digital public services. It offers forty-seven concrete recommendations on how to improve governance of the interoperable activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts.

Besides this, the EU Rolling Plan for Information and Communication Technology (**ICT**) Standardisation forms part of a short-to-medium-term work programme in ICT standardisation. It provides for a bridge between EU policies and standardisation activities in ICT, allowing for increased convergence of standardisation makers' efforts towards European policy goals.

157. Dr. Daphne Getz, Oshrat Katz, et. al., "Artificial Intelligence, Data Science, and Smart Robotics – First Report Summary", September 2018, available at: https://www.neaman.org.il/Files/Summary-ENG-Artificial-Intelligence-Data-Science-and-Smart-Robotics_20190103155717.804.pdf

158. Ministry of Industry, Business and Financial Affairs, "Strategy for Denmark's Digital Growth", 2018, available at https://eng.em.dk/media/10566/digital-growth-strategy-report_uk_web-2.pdf

159. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", 2019, available at https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

160. EC, "European Interoperability Framework", 2017, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF

The European Strategy on Data,¹⁶¹ released by the EC in February 2020, mentions that ‘data interoperability and quality, as well as their structure, authenticity and integrity are key for the exploitation of the data value, especially in the context of AI deployment’. As per the report, the lack of interoperability of data is a hurdle to ensuring seamless integration and development of efficient AI systems. As such, that should encourage the application of standard, shared and compatible formats and protocols for gathering and processing data from different sources, in a coherent and interoperable manner across sectors and vertical markets.

On 15 December 2020, the EC announced¹⁶² a proposal for a new framework of rules to govern the digital space, comprising the Digital Services Act¹⁶³ and the Digital Markets Act.¹⁶⁴ The new proposal considers the responsibilities of digital platforms, including potentially mandating inter-app compatibility and making their services interoperable with competitors.¹⁶⁵

AUSTRALIA

Maturity Index – 3/5

In June 2019, Standards Australia (an independent, non-government standards organisation of Australia) started a consultation process¹⁶⁶ with key Australian stakeholders across industry, government, civil society and academia to examine how standards can support AI in Australia. In September, 2019, it released a roadmap¹⁶⁷ for standardisation of AI in the country and laid down the purpose and recommendation for standardising technology around AI.

Additionally, the Digital Continuity 2020 Policy¹⁶⁸ calls for information, systems and processes to be interoperable by 31 December 2020. As per the policy, government agencies will have interoperable information, systems and processes that meet standards for short and long-term management, improve information quality and enable information to be found, managed, shared and re-used easily and efficiently.

161. EC, “A European Strategy for Data”, 2020, available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

162. EC, “Europe fit for the Digital Age: Commission Proposes New Rules for Digital Platform”, 15 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

163. EC, “The Digital Services Act: Ensuring a Safe and Accountable Online Environment”, December 2020, available at https://ec.europa.eu/info/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

164. EC, “The Digital Markets Act: Ensuring Fair and Open Digital Markets”, December 2020, available at <https://ec.europa.eu/!Rd39Mp>

165. Emma Beswick, “Five Reasons Why the Digital Services Act and Digital Markets Act Matter”, December 2020, available at <https://www.euronews.com/2020/12/15/five-reasons-why-the-digital-services-act-and-digital-markets-act-matter>

166. Standards Australia, “Developing Standards for Artificial Intelligence: Hearing Australia”, June 2019, available at [https://www.standards.org.au/getmedia/aeaa5d9e-8911-4536-8c36-76733a3950d1/Artificial-Intelligence-Discussion-Paper-\(004\).pdf.aspx](https://www.standards.org.au/getmedia/aeaa5d9e-8911-4536-8c36-76733a3950d1/Artificial-Intelligence-Discussion-Paper-(004).pdf.aspx)

167. Standards Australia, “An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard”, 2020, available at <https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx>

168. National Archives of Australia, “Digital Continuity 2020 Policy”, 2015, available at <https://www.naa.gov.au/information-management/building-interoperability>

SINGAPORE

Maturity Index – 2/5

The Singaporean National Strategy on AI¹⁶⁹ lists definition and promulgation of common data standards to ensure data interoperability as one of the key thrusts. It states that to facilitate data interoperability, the Government will work with companies in key sectors to define and promulgate a set of common data standards for the sector (e.g., standards for health records across restructured hospitals, private GPs and research institutes).

SOUTH KOREA

Maturity Index – 1/5

While there does not appear to be any specific regulation or policy to facilitate interoperability of data for AI systems, the Mid-To Long-Term Master Plan in Preparation for Intelligent Information Society¹⁷⁰ published by the South Korean Ministry of Science, ICT and Future Planning provides for creation of a super-connected, data- and service-centered network environment, and proposes to launch interdepartmental test projects for real-time, super-connected network services linking intelligent networks with other industries (self-driving cars, intelligent robots, drones, smart homes, etc.).

SWEDEN

Maturity Index – 2/5

During the period October 2017 to June 2019, Swedish industry worked together on a project under the name “LCDM Project”. The aim of the project was to conduct a feasibility study to explore the possibilities of establishing a standardized data exchange between different IT support systems in a facility's life cycle. The project has also worked on how Swedish industry takes the next step into the digital transformation, aiming to find solutions to Swedish industrial interoperability, as a part of the Strategic Innovation Program Process Industrial IT and Automation, a joint venture of Vinnova, Formas and the Swedish Energy Agency.¹⁷¹

Sweden's National Approach to Artificial Intelligence¹⁷² highlights that AI standards have the potential to promote technical, semantic, legal and other forms of interoperability both within and between companies and public institutions, and to contribute to greater clarity for users and consumers.

169. Smart Nation and Digital Government Office, “The National Artificial Intelligence Strategy”, 2019, available at <https://www.smarnation.gov.sg/why-Smart-Nation/NationalAIStrategy>

170. Government of South Korea, “Mid-To Long-Term Master Plan in Preparation for Intelligent Information Society”, 2017, available at: https://english.mst.go.kr/cms/english/pl/policies2/_icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

171. Swedish Industrial Interoperability Association, “LCDM Project”, available at <http://seiia.se/>

172. Government Offices of Sweden, “National Approach to Artificial Intelligence”, 2018, available at: <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

FINLAND

Maturity Index – 2/5

In October 2017, the Finnish Ministry of Economic Affairs and Employment published a National AI Strategy titled Finland's Age of Artificial Intelligence.¹⁷³ The strategy gives due importance to interoperability and calls it a key requirement for digitalisation, robotisation and AI. As a result, it proposes to launch a neural network study as part of the Joint Metadata and Information Management programme. The study will look into the ability of AI to create the semantic interoperability of data in place of manual determination work and symbolic modelling.

The Helsinki Institute of Information and Technology and the Ministry of Transportation and Communication are also facilitating a community run alliance named 'Mydata',¹⁷⁴ which combines industry needs with data and digital human rights. The core idea is to let individuals remain in control of their data. It also makes data easily accessible to the individuals making it more interoperable and easier to manage, while paving the way for prospective entrants to innovate in data management services.

SPAIN

Maturity Index – 2/5

Spain's Ministry of Science, Innovation and Universities came up with National AI Strategy¹⁷⁵ in 2019. The report discusses various sectors that can benefit with the use of AI, and emphasises that AI can improve the performance of Public Administrations by ensuring interoperability between administrations and generate automated administrative procedures.

The National Interoperability Framework,¹⁷⁶ a dedicated report on the subject of interoperability in AI was created by the Spanish government in 2010. It addressed requirements in relation to the implementation of interoperability principles, dimensions, agreements and governance, plus other issues related to interoperability, such as standards, common infrastructures and services, reuse of applications, electronic signature, and electronic documents.

NORWAY

Maturity Index – 2/5

The National Strategy for Artificial Intelligence,¹⁷⁷ released by Norwegian Ministry of Local Government and Modernisation considers interoperability as one of the major challenges in the way of implementation of a nationwide AI strategy. Therefore, it aims to achieve semantic interoperability in its legislation to make it easier to be read by machines and used for artificial intelligence.

173. Ministry of Economic Affairs and Employment, "Finland's Age of Artificial Intelligence", 2017, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

174. See, <https://mydata.org/finland/>

173. Ministry of Economic Affairs and Employment, "Finland's Age of Artificial Intelligence", 2017, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

174. See, <https://mydata.org/finland/>

175. Spanish RDI Strategy In Artificial Intelligence, available at: http://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_EN.PDF

176. Government of Spain, "Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope", available at: <https://administracionelectronica.gob.es/ctt/resources/Soluciones/145/Descargas/Spain-National-Interoperability-Framework-NIF-English-version.pdf>

177. Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence", available at https://www.regjeringen.no/contentassets/1feb8bb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

ESTONIA

Maturity Index – 4/5

The Estonian IT Interoperability Framework¹⁷⁸ has been developed by the government to make data more accessible and interoperable to the citizens. It aims at creating open standards to ensure universality in the data sets. This facilitates the transformation of institution-based public administration into a service-centred one, where all citizens can communicate with the state without knowing anything about its hierarchical structure and division of roles.

Estonia has also put in place one of the most ambitious interoperability programs in the world called the X-Road.¹⁷⁹ It connects different information systems that may include a variety of services. It can also write to multiple information systems, transmit large data sets and perform searches across several information systems simultaneously. The report of Estonia's Task Force on AI,¹⁸⁰ also called the #Kratt report, gives significant importance to the use of AI in ensuring interoperability.

It proposes to create and test the interoperability of kratts and the concept of a personal virtual assistant. Further it suggests updating the semantic interoperability framework that would meet current and future needs, including for kratt projects, to evaluate and improve data quality.

THE NETHERLANDS

Maturity Index – 3/5

The Dutch government employs a national e-government reference architecture, as well as an evolving list of open standards. While this is not specific to the development of AI, interoperability is clearly a priority. Besides this, a research paper¹⁸¹ makes the case that Netherlands follows an interoperability agenda; the Standardization Forum identified seven cross-cutting concerns that constitute the Dutch Interoperability Agenda. The seven concerns are as follows:

1. Open Standards
2. Governance of Interoperability
3. Authentication and authorization
4. Service Concepts
5. Financial arrangements
6. Systematic Semantics
7. Treating Data

178. Ministry of Economic Affairs and Communications, "Estonian IT Interoperability Framework", 2011, available at: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS07_04_06A_Forum_Estonian_IT_Interop_Framework_05.pdf

179. E-Estonia, "Interoperability Services", 2017, available at <https://e-estonia.com/solutions/interoperability-services/>

180. (Estonian) Ministry of Economic Affairs and Communication, "Report of Estonia's AI Taskforce", 2019, available at <https://www.kratid.ee/in-english>

181. Arendsen and Zwienink, "Setting the Dutch E-Government Interoperability Agenda: A Public-Private Partnership", 2010, available at: https://www.researchgate.net/publication/232707994_Setting_the_Dutch_E-Government_Interoperability_Agenda_A_Public-Private_Partnership/citation/download

UAE

Maturity Index – 3/5

The UAE Smart Data Principles and Standards¹⁸² sets out the core standards around data classification, exchange and quality to ensure UAE data is reliable, interoperable and fit-for-purpose. The UAE Smart Data Framework outlines a common basis for managing data that enables interoperability and exchange among entities. It draws on the European Interoperability Framework's guidance on use of open standards to drive data interoperability, and on other relevant open standards, including those developed by ISO and W3C.

HONG KONG

Maturity Index – 3/5

The Government of Hong Kong has put in place a National Interoperability Framework¹⁸³ that defines a collection of specifications aimed at facilitating the interoperability of Government systems and services. It supports the Government's strategy of providing client-centric joined-up services by facilitating the interoperability of technical systems between Government departments, as well as between Government systems and those used by the public (including citizens and businesses).

182. Digital UAE, "The UAE Smart Data Principle and Standards", February 2019, available at: <https://u.ae/en/about-the-uae/digital-uae/data/data-operability>

183. Office of the Government Chief Information Officer, "The Interoperability Framework for e-Government (Version 19)", 2020, available at https://www.occio.gov.hk/en/our_work/infrastructure/e_government/if/doc/s18.pdf

PRIVACY & CONSENT



With the widespread use of social media and IoT, there have been increasing concerns over data leaks,¹⁸⁴ control over content and political influence of social networks. This has led investigations into how social media platforms collect and use personal data, which in turn has reduced the level of trust users have in such platforms and digital services.

While privacy has been universally acknowledged as a fundamental right,¹⁸⁵ one of the foremost regulatory challenges is to protect individual privacy. Increasingly, big data analytics and machine learning techniques are being used to draw insights using the vast amount of unstructured data available on the internet.¹⁸⁶ At present, most jurisdictions recognise the right to privacy as being an offshoot from the right to life and dignity. Any discourse on right to privacy though must also factor in the possible benefits to the society from AI, in terms of greater convenience, tailored solutions and efficiency gains in business.

AI systems can now engage in automated decision-making that have wide-spread political, economic and social impact. The 'echo chamber' effect on social media platforms has come to prominence recently and is a product of profiling through the scrutiny of personal data and preferences, with AI technologies.¹⁸⁷ Therefore, regulatory regimes across the globe have attempted to find a balance between the need to protect/uphold the right to privacy while ensuring that the potential benefits of big data analytics and AI does not get negated.

Most data protection legislations define personal information as data points that identify an individual or a device, which may include identifiers such as biometric

data, address, bank account details, location, government identification numbers, and genetic data. In this context, data protection regulations in various jurisdictions have charted out a series of data protection rights, which include the right to transparent communication and information, the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the obligation to notify recipients, the right to data portability, the right to object and the right to not be subject to automated decision-making.

To address the potential erosion of privacy by AI, there have been calls for data privacy laws to buttress provisions relating to informed consent, perceptibility or explainability of decision-making by machines and the enforcement of protections against creating or exacerbating bias.¹⁸⁸ In most cases, regulators and governments have sought to encourage companies developing AI to account for these data protection rights in the design of the AI system itself. Given the nature of AI and increasingly limited human intervention in AI systems, it would be difficult to regulate the outcomes (whether intended or not) of AI once these systems are in place. There also appears to be widespread consensus on prioritizing the use of anonymised data, where possible. Data privacy regulations and policy statements also recommend conducting regular privacy impact assessments of AI systems, to maintain oversight of the functioning of AI and allowing for course-correction where required. Some countries have also provided model impact assessment tools, and examples of less intrusive machine learning models. However, it remains to be seen as to how far countries uphold the principles of privacy in the face of the significant potential benefits that could arise from widespread adoption of AI systems.

184. Carole Cadwalladr, "Fresh Cambridge Analytica leak 'shows global manipulation is out of control'", The Guardian, January 2020, available at <https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation>

185. Article 12 of Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights recognise right to privacy as a basic human right.

186. Karl Manheim and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy", Yale Journal of Law and Technology, October 2018, available at: <https://ssrn.com/abstract=3273016>

187. Dirk Helbing et al., "Will Democracy Survive Big Data and Artificial Intelligence?", Scientific American, 25 February 2017, available at <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>

188. Supra note 182.

MATURITY INDEX

PRIVACY & CONSENT



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation

India, USA, China, Canada, France,
Israel, Denmark, Australia, South Korea,
Sweden, Norway, The Netherlands, UAE

UK, Germany, EU, Singapore,
Finland, Spain, Estonia, Hong Kong



INDIA

Maturity Index – 3/5

In India, the right to privacy has been recently recognised as a fundamental right emerging primarily from Article 21 of the Constitution, in the Justice K.S. Puttaswamy (Retd.) v. Union of India verdict.¹⁸⁹ In this case, the Supreme Court considered the legality of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (**Aadhar Act**). However, barring certain provisions, the Supreme Court held that the Aadhaar Act, as a whole, served a legitimate purpose, is proportionate, and thereby comprises a reasonable exception to the 'right to privacy'. In this context, the Supreme Court recognised that the scope of the right to privacy was to include "intrusion with an individual's physical body, informational privacy and privacy of choice." The Supreme Court also noted that the right to control the dissemination of personal information is an aspect of the right to privacy, and that every individual should have the right to be able to control the image of themselves portrayed to the world as well as the commercial use of their identity.¹⁹⁰ The Supreme Court recognised the following principles (drawing from European law) for the protection of data: principles of consent, purpose and storage limitation, data differentiation, data exception, data minimization, substantive and procedural fairness and safeguards, transparency, data protection and security.¹⁹¹ The current Indian legislative framework governing data protection is quite disparate and there are about 50 existing legislations¹⁹² that could have an impact on data protection. The main legislative framework governing the transfer of personal data is governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**SPD Rules**).¹⁹³ The SPD Rules were issued under Section 43A of the Information Technology Act, 2000 (**IT Act**) which holds a body corporate liable for compensation for any negligence in implementing and maintaining reasonable security practices and procedures while dealing with sensitive personal data or information. The SPD Rules define personal information to mean any information relating to a natural person which either directly or indirectly, is capable of identifying such person. The SPD Rules define specific categories of "sensitive personal data or information", and mandate that (i) any body corporate collecting such information shall obtain specific consent in writing, (ii) specify the purpose for which such data is being collected and (iii) only collect such information if it is for a lawful purpose connected with the activities of such body corporate and where the collection of such data is considered necessary for that purpose. Prior consent is also required before such sensitive personal data or information is shared with a third party. Moreover, provisions such as Section 66E, Section 72 and Section 72A of the IT Act set out the obligation to seek consent and impose punishments for persons who share data or publish data without consent.

In August 2017, the Union Ministry of Electronics & Information Technology (**MEITY**) constituted an Expert Committee to study and identify key data protection issues and recommend methods to address them. The Expert Committee led by Justice Srikrishna released its report in July 2018¹⁹⁴ and set out several recommendations to protect data privacy in the context of emerging AI and big data applications, proposing the Personal Data Protection Bill, 2019 (**PDP Bill**).¹⁹⁵ Some of the salient features of the PDP Bill are as follows:

It governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.

Personal data is defined as being data which pertains to characteristics, traits or attributes of identity, which can be used

189. Writ Petition (Civil) no 494 of 2012, available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

190. Paragraph 81, supra note 170.

191. Paragraph 187, supra note 170.

192. Annexure C of the Report by the Expert Committee chaired by Justice Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", July 2018, available at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

193. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, available at [https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511\(1\).pdf](https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf)

194. Supra note 173.

195. Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

to identify an individual and characterises some data as sensitive personal data. This definition includes financial data, biometric data, caste, religion or political beliefs, and can be expanded upon by the government.

It defines a data fiduciary as an entity or individual who decides the means and purpose of processing personal data, which is subject to a specific clear and lawful purpose. Moreover, the processing of personal data is subject to collection and storage limitations. Data fiduciaries are also required to ensure transparency and accountability through data encryption, ensuring that data is not misused, and providing for complaint redressal mechanisms to individuals.

The PDP Bill sets out rights of individuals, or the data principal, which include seeking confirmation from the data fiduciary on whether their personal data has been processed, seeking correction of inaccurate, incomplete, or out-of-date personal data, have personal data transferred to any other data fiduciary in certain circumstances and restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

Under the PDP Bill, personal data can only be processed if consent is provided by the data principal, except where it is required by the State to provide benefits to the individual, legal proceedings or to respond to a medical emergency. It requires that the consent provided be free, informed, specific, clear and capable of being withdrawn.

Finally, the PDP Bill proposes the establishment of a Data Protection Authority which may take steps to protect interests of individuals, prevent misuse of personal data, and ensure compliance with the Bill.

The framework of the PDP Bill – while being technology agnostic - acknowledges the growing influence of AI in various provisions. For example, it defines “harm” as specifically including discriminatory treatment or “denial of a service, benefit or good resulting from an evaluative decision about the data principal” and also “any observation or surveillance that is not reasonably expected by the data principal”. It allows the Data Protection Authority to expand this definition. While it also grants several data rights to the individual, it does not go so far as the EU’s GDPR to grant specific rights that would allow for opting out of automated decision making (and the obligation on the part of the data fiduciary to inform the individual of automated decision-making) – which is one of the most contentious outcomes of AI systems today. Nevertheless, the PDP Bill does impose an obligation on data fiduciaries to put in place a “privacy by design” policy, which has at its core, the protection of the data principal against harm as well as ensuring transparency and maintaining security. Significant data fiduciaries are a separately defined group of data fiduciaries that may be identified by the data protection authority on the basis of the volume or sensitivity of data that they deal with; these data fiduciaries have an obligation to undertake a data protection impact assessment to ensure that their systems for data protection are sound and are in compliance with the obligations under the PDP Bill. Interestingly, the PDP Bill specifically calls for social media intermediaries to be identified as significant data fiduciaries if they meet certain conditions. It remains to be seen how effectively this obligation can be used to leverage the protection of privacy rights, especially as the thinking, development and implementation of AI systems in a multitude of sectors evolves.¹⁹⁶

The Indian AI Strategy brings to attention various issues with regards to the privacy, such as data collection without proper consent, privacy of personal data, inherent selection biases and resultant risk of profiling and discrimination, and non-transparent nature of AI solutions. The paper also presents various ways to deal with challenges with regards to privacy, which include the following:

1. establish a data protection framework with legal backing;
2. establish sectoral regulatory frameworks;
3. benchmark national data protection and privacy laws with international standards;
4. encourage AI developers to adhere to international standards;
5. encourage self-regulation;
6. invest and collaborate in privacy preserving AI research; and
7. spread awareness.

¹⁹⁶. Amber Sinha and Elonnai Hickok, “The Srikrishna Committee Data Protection Bill and Artificial Intelligence in India”, The Centre for Internet and Society, 3 September 2018, available at <https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india>

USA

Maturity Index – 3/5

While there is no single federal law governing privacy or data protection in the USA similar to the GDPR in Europe, there are certain sector specific legislations that deal with data privacy at the federal level and the state level. Some of the key federal legislations are:

1. The US Privacy Act of 1974,¹⁹⁷ which governs the manner in which US government agencies deal with data;
2. Health Insurance Portability and Accountability Act,¹⁹⁸ which covers personally identifiable healthcare information
3. Children's Online Privacy Protection Act,¹⁹⁹ which regulates personal information that relates to minors;
4. Telephone Consumer Protection Act,²⁰⁰ which deals with tele-marketing;
5. CAN-SPAM Act,²⁰¹ which deals with spam email; 6. Gramm-Leach-Bliley Act²⁰² which deals with data security and privacy in the context of the banking and financial sector;

At the state level, several states such as California,²⁰³ Massachusetts,²⁰⁴ New York,²⁰⁵ Hawaii,²⁰⁶ Maryland²⁰⁷ and North Dakota²⁰⁸ have sought to create laws that address consumer protection in the context of online behaviour.²⁰⁹ The California Consumer Privacy Act, 2018 (**CCPA**) is similar to the GDPR in its scope and the rights granted to consumers, and has been the basis for the other state legislations in the US that deal with data privacy. The CCPA protects information such as purchasing history, browsing and search history, and inferences drawn from personally identifiable information. This definition captures information that is capable of being associated with a California resident, household or device, which is a broader definition than simply looking at natural persons, as in most other jurisdictions. It also grants individual rights, which includes the right against discrimination and the right to opt-out, rather than an explicit requirement to obtain consent prior to collection of data, unlike in other jurisdictions.²¹⁰ Effective from 1 January 2020, California's cybersecurity law²¹¹ also requires implementing security features for IoT devices and chatbots, ensuring that the information collected through

197. Privacy Act of 1974, available at: <https://www.justice.gov/opcl/privacy-act-1974>

198. The Health Insurance Portability and Accountability Act (HIPAA), available at: <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>

199. The Children's Online Privacy Protection Act, available at: <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>

200. Telephone Consumer Protection Act, 47 U.S.C. §227 et seq., available at <https://www.fcc.gov/sites/default/files/tcpa-rules.pdf>

201. Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003, 15 U.S.C. §§7701-7713 and 18 U.S.C. §1037. available at <https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf>

202. Gramm-Leach-Bliley Act of 1999, available at: <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>

203. The California Consumer Privacy Act, 2018, available at http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&divison=3.&title=1.81.5.&part=4.&chapter=&article=

204. Massachusetts Data Privacy Bill, available at <https://malegislature.gov/Bills/191/SD341>

205. New York Privacy Bill, available at <https://www.nysenate.gov/legislation/bills/2019/s5642>

206. Hawaii Privacy Bill, available at https://www.capitol.hawaii.gov/session2019/bills/SB418_.pdf

207. Maryland Online Consumer Protection Bill, available at <http://mgaleg.maryland.gov/mgawebsite/legislation/details/sb0613?ys=2019rs>

208. North Dakota Data Protection Bill, available at <https://www.legis.nd.gov/assembly/66-2019/bill-actions/ba1485.html>

209. Andy Green, "The Complete Guide to Privacy Laws in the US", 29 March 2020, available at <https://www.varonis.com/blog/us-privacy-laws/>

210. Supra note 166.

211. California's Cybersecurity law, SB-327, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

these routes cannot be manipulated or used to influence purchasing decisions and political behaviours. Notably, some of these legislations have a size-of-business threshold value that needs to be crossed before the obligations apply.²¹²

In 2016, the National Privacy Research Strategy²¹³ (**NPRS**) was released by the National Science and Technology Council, to respond to the challenges to privacy arising from large-scale deployment of information technology systems and big data. The NPRS recognises that massive data collection, processing and retention are a challenge to the right to privacy, while also recognising that large scale data analytics are a necessary step for AI to progress in the development of science, engineering and medicine. The NPRS characterises privacy as a combination of the concept of subjects (i.e. an individual or a group of individuals, their identity, autonomy and privacy desires), data (i.e. data and derived information about these individuals and groups), actions (i.e. data collection, processing, analysis and retention practices; controls that constrain these practices and the impact of such actions on individuals, groups and society) and context (i.e. the context in which interactions between subjects, data and actions take place and the risk of harm that arises in each case).²¹⁴ The NPRS uses the idea of context to essentially signify the purpose for which data is shared, and the fact that the use of data outside this purpose could result in a perceived privacy violation by individuals and communities. The NPRS also considers how to provide for transparency in data use, collection and retention, given that traditional notice and choice frameworks have proven inadequate to meaningfully consider that informed consent has been given. It considers that methods of providing consent need to match up to the complexity and minuteness of information being collected, processed and retained.²¹⁵

In this context, the NPRS proposes the following points as research priorities:²¹⁶

1. fostering a multidisciplinary approach to privacy research and solutions;
2. understanding and measuring privacy desires and impacts;
3. developing system design methods to incorporate privacy desires, requirements and controls;
4. increasing transparency of data collection, sharing, use and retention;
5. providing assurances that information flows and use are consistent with privacy rules;
6. developing approaches for remediation and recovery from actual or perceived privacy violations; and
7. reducing privacy risks of analytical algorithms, especially those that analyse and predict human behaviour and performance, which could result in restrictions of opportunities, benefits, etc.

In addition, the U.S. Government Accountability Office released a report²¹⁷ in January 2019 expressing concern about the lack of a comprehensive national internet privacy law, with particular concern over “the collection, use, and sale or other disclosure of consumers’ personal information.” However, despite the calls for a national legislation that governs and protects data privacy, the US appears to be moving in the direction of prioritising innovation and exploring the power of AI systems rather than first setting up a legislative framework that would safeguard individual interests. This approach is

212. Supra note 192.

213. National Science and Technology Council, “National Privacy Research Strategy”, June 2016 available at: <https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf>

214. Paragraph 2.2, supra note 192.

215. Paragraph 2.3.2, supra note 192.

216. Sections 3.1 to 3.5, supra note 192.

217. USA Government Accountability Office, “Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility”, January 2019, available at: <https://www.gao.gov/assets/700/696446.pdf>

visible in the AI Executive Order²¹⁸, which focuses on objectives such as – promoting sustained investment in R&D in AI; enhancing access to high-quality and fully traceable federal data, models and computing resources to increase the value of such resources to AI R&D (while maintaining security, safety, privacy and confidentiality provisions under applicable laws); reducing barriers to the use of AI technologies; develop and implement an action plan to protect the US's advantage in AI and technology critical to its national security and economic interests.

It is also possible that the US may prefer that data privacy protections emerge through self-regulation by industry, which would allow for a balancing of competing interests by industry players themselves, rather than as an imposition by the government.²¹⁹ However, as a counter, Democratic lawmakers in the US introduced the Algorithmic Accountability Act (**AA Act**) in the House of Representatives in April 2019, as a specific measure to guard against discriminatory, unethical use of AI that could threaten security and privacy. This legislation would require companies to consider accuracy, fairness, bias, discrimination, privacy and security of AI systems, especially where they deal with sensitive personal information. Unlike existing data privacy legislation at the federal level, the AA Act is sector agnostic and instead focuses on covering all machine learning processes. With respect to protecting privacy in the case of sensitive data, the AA Act proposes auditing for privacy and security risks through impact assessments.²²⁰

With the increased scrutiny of big tech firms from an antitrust and privacy perspective, it is likely that any regulation aimed at AI will focus on the manner in which these companies store, secure and share user data. The US House Judiciary Committee issued its report²²¹ on competition in digital markets, concluding a years-long investigation. It notes that the dominance of digital platforms distorts competition, reduces consumer choice and has "undermined Americans' privacy". It specifically highlights the importance of data collection as a means for online platforms to maintain dominance, and states that the erosion of consumer privacy is "the best evidence of platform market power". Subsequently, in its recent filings against Facebook and Google, the Federal Trade Commission,²²² in coordination with several state attorneys-general, contended that Facebook was weakening users' privacy, because it does not face any competition as a social media platform, an argument that has limited precedent in the anti-trust world.²²³

CHINA

Maturity Index – 3/5

The PRC Cybersecurity Law, 2016²²⁴ (**Cybersecurity Law**) was the first national-level law to address cybersecurity and data privacy protection in China. In addition to the Cybersecurity Law, there are accompanying guidelines and regulations which elaborate on key concepts. These include:

218. Executive Office of the President, Executive Order 13859 of 11 February 2019, "Maintaining American Leadership in Artificial Intelligence, available at <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>

219. Supra note 168.

220. Michael Scherman, et al, "US Lawmakers propose Algorithmic Accountability Act intended to regulate AI", April 2019, available at <https://www.mccarthy.ca/fr/node/57481>

221. US House of Congress Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations", October 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

222. Text of the complaint by the State of New York et al. v. Facebook, Inc., 9 December 2020, available at https://ag.ny.gov/sites/default/files/facebook_complaint_12.9.2020.pdf

223. Ben Brody, "The FTC's Antitrust Case Against Facebook Stakes out New Ground", Bloomberg Businessweek, December 2020, available at <https://www.bloomberg.com/news/articles/2020-12-16/facebook-fb-antitrust-case-has-much-different-goal-than-google-s-googl>

224. Cybersecurity Law, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>

1. Personal Information Security Specification (PIS Specification),²²⁵
2. Guidelines on Internet Personal Information Security Protection;²²⁶ and
3. Draft National Standard of Information Security Technology²²⁷

The PIS Specification and other guidelines cover key issues such as data transfers, sensitive personal information and data subject rights. While these guidelines are not legally binding, they explain China's approach towards data privacy. In November 2019, an updated draft of the amended PIS Specifications were published, which proposed new amendments. The Cybersecurity Law, read along with the various guidance papers and regulations, set out a data protection regime that is quite similar in approach to the GDPR.

The PIS Specification defines sensitive personal information as being personal information, which, if disclosed or abused, would adversely impact the data subject (for example, personal identification number, individual biometric information, bank account number, etc.). The Cybersecurity Law requires that the express consent of the individual be obtained where their personal data is collected and used.²²⁸ Moreover, it provides for specific rights to the data subject (or the person from whom information is collected), which include the right to access their data, correction of data, the right to request deletion in case of a data breach, de-registration of account, etc. The amended PIS Specifications now abolish 'bundled' consent, which means that separate consent is likely to be required for each purpose for which data is collected.²²⁹ This would include situations such as targeted advertising. The Cybersecurity Law also imposes the burden of protecting the privacy of data collected and used on the corporation or organization collecting it, including for any data breaches, unauthorized uses, accidental losses and destruction of data.²³⁰

CANADA

Maturity Index – 3/5

In Canada, the Personal Information Protection and Electronic Data Act²³¹ (**PIPEDA**) governs data privacy. It recognises that rules are required to govern the collection, use and disclosure of personal information in a manner that recognises the privacy of the individual, while also balancing the need of organizations to collect, use and disclose such personal information for reasonable purposes. PIPEDA applies to the private sector as well as to the personal information of employees of federally regulated businesses such as banking, airlines and telecommunications.²³²

Personal information is defined as being information about an identifiable individual. PIPEDA permits the collection, use and disclosure of personal information only for "reasonable" purposes. With respect to consent, it specifies that consent would

225. Personal Information Security Specification (PIS Specification), available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/>

226. Guidelines on Internet Personal Information Security Protection, available at <https://www.sesec.eu/app/uploads/2017/08/SESEC-Translation-2017-China-Personal-information-Protection-Compliance-en.pdf>

227. Draft National Standard of Information Security Technology, available at <https://www.huntonprivacyblog.com/2019/11/14/china-issues-updated-draft-amendments-to-information-security-technology-specification/>

228. Articles 22, 41 and 42 of the Cybersecurity Law.

229. DLA Piper, "China: Navigating China: Further Developments in PRC Data Privacy Regulations", 5 November 2019, available at <https://blogs.dlapiper.com/privacymatters/navigating-china-the-digital-journey/>

230. DLA Piper, "Data Protection Laws of the World: China", December 2019, available at <https://www.dlapiperdataprotection.com/index.html?t=law&c=CN>

231. (Canadian) Personal Information Protection and Electronic Data Act, 2000, available at: <https://laws-lois.justice.gc.ca/pdf/P-8.6.pdf>

232. Other government institutions are governed by the Privacy Act, 1985.

be considered valid only if the individual giving consent can be reasonably expected to understand the nature, purpose and consequences of the collection, use and disclosure of such personal information. The collection of personal information without consent is also permissible in some cases – e.g., where obtaining consent is not in the interest of the individual, where it cannot be obtained in a timely manner, where it is required to investigate a breach of contract or contravention of law, in legal proceedings, etc.

Schedule I of the PIPEDA lists the various principles that must be enforced for the protection of personal information. These principles contribute to a fairly robust set of regulations that protect the interest of the individual providing personal information. The principles are set out below –

1. accountability – placed on the organization which has personal information under its control;
2. identifying purposes – where the organization collecting personal information is required to identify the purpose for collecting such information either before or at the time of collection;
3. consent – where the knowledge and consent of the person providing personal information is required for the collection, use and disclosure of personal information. Here, the Schedule specifies that consent may be obtained at a later stage, in cases where the purpose for collection of data was not previously identified. It also requires that the consent obtained be “meaningful”, i.e., the purpose(s) of collection must be stated in a way that the individual can reasonably understand how the information collected may be used or disclosed. The Schedule also permits individuals to withdraw consent at any time, subject to legal/contractual restrictions and the provision of reasonable notice;
4. limiting collection of personal information to only such data that is necessary for the purposes identified by the organization, and that data may be collected in a “fair and lawful” manner;
5. limiting use, disclosure and retention – which requires that the use and disclosure of personal information collected can only be for the purposes previously specified by the organization, and that it is retained for only as long as it may be necessary;
6. accuracy – the information collected should be accurate, up to date and complete as far as possible, especially in the interest of minimizing the possibility that inappropriate information be used to make a decision about an individual;
7. safeguards – personal information is required to be protected by safeguards appropriate to the sensitivity of the information, to ensure that there is no unauthorized use, theft, disclosure, copying, or modification;
8. openness – organizations are required to make readily available details about their practices and policies relating to the management of personal information, in a form that is easily understood;
9. individual access – individuals should have access to the personal information that exists, has been collected and used by organizations, upon request;
10. challenging compliance – individuals have the right to challenge compliance by an organization of the above principles.

The Digital Privacy Act, 2018²³³ introduced data breach notification requirements as an amendment to PIPEDA, to make it more comprehensive and allowing users a greater degree of transparency regarding their data.

²³³. Graham Greenleaf, “Global Data Privacy Laws 2019: 132 National Laws & Many Bills” 2019, Privacy Laws & Business International Report, 2019, available at <https://ssrn.com/abstract=3381593>

In January 2020, the Office of the Privacy Commissioner (**OPC**) launched a consultation on the appropriate regulation of AI, recognising that the existing framework for data protection is inadequate. It identifies several areas where PIPEDA should be enhanced and has sought public views on these privacy principles. Of these, the OPC favours the adoption of a rights-based approach in the law through explicit mention, whereby data protection rules are applied as a means to protect the right to privacy as a fundamental right. The OPC also proposes the creation of a right that specifically objects to automated decision-making, and not to be subject to decisions based solely on automated decision making (requesting human intervention), subject to certain exceptions. This appears to be in line with the GDPR. It also proposes increased transparency and the right to an explanation where individuals are subject to automated processing, to bring greater specificity to the existing principle of openness and transparency in PIPEDA. This would include measures such as conducting Privacy Impact Assessments including the impact of AI and public filings for algorithms. The OPC also recommends that “privacy by design” be a legal requirement in all phases of data processing, including collection of data, to ensure that there are no adverse consequences to the right to privacy and other human rights. Another important issue highlighted by the OPC is to consider how purpose specification and data minimization can be complied with in the context of AI. Recognizing that access to vast and broad amounts of data is key to the working of AI systems and also that it is not always possible to identify the purpose of information collection in advance, the OPC notes that it is important to consider alternate ways of data processing while still complying with these principles that are key to the protection of the right to privacy. With respect to the requirement to obtain meaningful consent in PIPEDA, the OPC notes that the current model of consent may not be viable in the context of AI, following from the issue of inability to identify a purpose for data collection at the time of collection. In order to explore viable alternatives, the OPC proposes exploring emerging consent technologies and personal information management systems where the goal is to preserve human agency and meaningfully inform individuals about the manner of deployment of AI systems. The OPC has also proposed alternate grounds to consent, where for instance, an exception may be provided to the prior consent requirement where the AI system has been deployed for a socially beneficial purpose. Another solution could be de-identifying or anonymising data, where meaningful consent cannot be obtained.²³⁴

UK

Maturity Index – 3/5

The Data Protection Act, 2018²³⁵ which implements the GDPR in the UK (**UK**), controls how personal information is used by organisations, businesses or the government. It provides for data protection principles that are required to be followed by every person or organization responsible for using personal data. The data protection principles require that information is:

1. used fairly, lawfully and transparently;
2. used for specified, explicit purposes;
3. used in a way that is adequate, relevant and limited to only what is necessary;
4. accurate and, where necessary, kept up to date;
5. kept for no longer than is necessary; and
6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

The Information Commissioner’s Office (**ICO**) is the independent body entrusted with the job of “upholding information

234. The Office of the Privacy Commissioner of Canada, “A Regulatory Framework for AI: Recommendations for PIPEDA Reform”, November 2020, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/

235. The Data Protection Act, 2018, available at: <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

rights in the public interest, promoting openness by public bodies and data privacy for individuals".²³⁶ The ICO considered the implications of big data analytics and AI systems on data protection in a report in September 2017,²³⁷ stating that privacy is an enabling right and not an end in itself. Therefore, embedding privacy and data protection into big data analytics would help to "promote societal benefits such as dignity, personality and community" as well as promoting "organizational benefits such as creativity, innovation and trust". The ICO recognised that data protection requirements in current legislation are not conducive to application to big data analytics. In its report, it considered various tools and approaches that could be used to protect privacy while not stemming the flow of innovation in AI. These tools include the use of anonymised data where big data analytics does not actually require personal information, conducting privacy impact assessments and "privacy by design".²³⁸ The ICO also considered that the principles of transparency and meaningful consent could still be adhered to in the case of AI systems by modifying traditional consent provisions to provide meaningful privacy notices at various stages of a big-data project (as inferences and linkages become clearer). As a guiding principle for the development of AI systems and algorithms, the ICO recommends that private actors implement innovative techniques to create auditable machine learning algorithms, to ensure that any autonomous decision made through algorithms remains explainable, and can be held accountable for bias, errors or discrimination.

FRANCE

Maturity Index – 3/5

France's Data Protection Act, 2018²³⁹ (**DPA**) replaced earlier legislation to support and comply with the provisions of the GDPR.²⁴⁰ The DPA enhanced the rights of individuals by introducing a general right to control the use of personal data. The DPA states that all data processing must be done fairly, lawfully and for legitimate purposes, and that only the minimum amount of data necessary is collected. The DPA also outlines several rights of data subjects, including the right to know the identity of the data controller, the purpose of the processing and their rights to collect or transfer the data. While the French legislation does not specifically consider the impact of AI, it does grant data subjects the right not to be subject to automated decision-making, except where this right pertains to special categories of personal data (i.e. information pertaining to racial or ethnic origin, political opinions, religion, trade union membership, genetic data, biometric data, data pertaining to health or sex life and sexual orientation), if the processing is justified by public interest and authorized by the French data protection agency, the Commission Nationale de l'Informatique et des Libertés.

GERMANY

Maturity Index – 3/5

The Federal Data Protection Act 2017²⁴¹ (**BDSG**) is the applicable data privacy law that outlines the general obligations of personal data collectors and processors. Apart from implementing the GDPR in Germany, the BDSG provides for specific rules applicable to data processing in employment, the appointment of a data protection officer, credit checks and profiling.

236. The Office of the Information Commissioner, available at <https://ico.org.uk/>

237. The Office of the Information Commissioner, "Big Data, Artificial Intelligence, Machine Learning and Data Protection", 4 September 2017, available at <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

238. Ibid, paragraph 210.

239. Law no. 2016-1321 of 7 October 2016, available at: https://www.legifrance.gouv.fr/affichTexte.do?sessionid=2EEDDC53AA4334B2F421EFAD13113A7B.tpdila23v_1?cidTexte=JORFTEXT000033202746&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFC0NT000033202743%20

240. Privacy & Information Security Law Blog, "New French Data Privacy Act and Implementing Decree Take Force", June 2019, available at <https://www.huntonprivacyblog.com/2019/06/13/new-french-data-protection-act-and-implementing-decree-take-force/>

241. Federal Data Protection Act, 2014, available at <https://germanlawarchive.iuscomp.org/wp-content/uploads/2014/03/BDSG.pdf>

In addition to this, the BDSG also contains laws regarding subject rights, transferring personal data, informed consent, etc. Germany also has specific data privacy laws that relate to issues such as telemedia, or specific sectors such as banking and energy.

The AI strategy formulated by the Federal Government of Germany in 2018²⁴² considers the impact of AI on data privacy regulation, among other forms of regulation. In the strategy paper, the government reiterates its commitment to ensuring that the use of AI does not undermine fundamental democratic values and rights that include the right to privacy and control over personal data. The strategy paper undertakes to review existing regulations at the national and European level to ensure that data protection laws are transparent, predictable and verifiable, especially in the context of algorithm-based prognosis and decision-making applications. The strategy paper recognises that values such as transparency, predictability, non-discrimination and verifiability in AI systems need to be accounted for and incorporated into algorithms in the creation and development process itself. In particular, this is highlighted as an important requirement in automated decision-making processes, where decisions are implemented without any human interaction. The scope for discrimination and bias arises even in cases where there is no decision making per se, such as robot journalism. In this context, the German government expressed its intention to consider setting up institutions or engaging with private sector bodies to audit and verify algorithmic decision-making to prevent improper use, discrimination and negative impacts on society. The strategy paper envisages the development of auditing standards and impact assessment standards to achieve these goals and considers a requirement to disclose all elements of the AI decision-making process to such monitoring bodies without having to disclose any commercial secrets.²⁴³ With Germany at the forefront of AI research as well as in the championing of liberal democratic values in Europe, it remains to be seen how the German Federal Government's stated strategy comes to fruition.

ISRAEL

Maturity Index – 3/5

While the Basic Law: Human Dignity and Liberty sets out the fundamental right to privacy, data security and privacy in Israel is governed by the Protection of Privacy Law of 1981²⁴⁴ (**PPL**) supplemented by the Protection of Privacy Regulation (Data Security),²⁴⁵ 2017 (**PPR**).

Similar to other countries, the Basic Law and the PPL together focus on transparency, the lawful basis for processing data, limiting data use, minimizing data, and individual rights. Section 11 of the PPL provides that for the entry and usage of the data in the 'database', the person to whom the information relates, must be furnished with a notice that clearly states whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent. It must also include the purpose for which the information is requested, to whom the information must be delivered and for what purpose. Apart from this section 23B of PPL prohibits the imparting of information by a public body unless it has been published by lawful authority, or the person to whom it relates has consented to its being imparted.

While the consent provisions are given by the PPL, the PPR provides safeguards for the protection of data by fixing responsibilities and duties on the data controller. The scheme of the PPR is such that the data controller is required to grant permissions and authorizations for the grant of access to the data user. The PPR does not use the term 'data subject' or 'data principle' as in other jurisdictions to indicate the person whose data is being used. The definitions of 'data' and

242. German Federal Government, "Artificial Intelligence Strategy", November 2018, available at https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf

243. Ibid, Section 3.9.

244 .The Privacy Protection Law, 1981, available at <https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf>

245. The Protection of Privacy Regulation (Data Security) 2017, available at: https://www.gov.il/en/Departments/legalInfo/data_security_regulation

'database' given in the PPL indicate that the database provisions apply only to databases containing information about natural persons.

While Israel does not appear to have published any policy positions on the protection of the right to privacy in the face of fast paced developments in AI, recent reports have indicated that it is willing to push the use of AI systems in defence to identify and control the spread of COVID-19.²⁴⁶ The push towards the use of AI systems in healthcare has been supported by the fact that Israel has legal requirements to provide inclusive health insurance to its entire population, thereby creating one of the most comprehensive personal health databases at the national level in any country. The Israeli government has been promoting digital health initiatives, through the use of de-identified and anonymised data arising not out of any clear legislation, but through a directive by the Ministry of Health. At present, the directives permit the primary use of personal medical data (for treatment of the data subject), and can also collate and analyse this data for secondary uses for the public good, but only if it is anonymised and with express consent.²⁴⁷ More generally, the Israeli government has set up a committee to formulate a national AI strategy, which was due to issue its report and findings by January 2020. The committee noted that AI systems would have a wide-ranging effect on the economy and society and identifies agriculture as a potential focus sector.²⁴⁸

DENMARK

Maturity Index – 3/5

Data privacy in Denmark is regulated by the Danish Data Protection Act, 2018 (**DDPA**).²⁴⁹ The DDPA supplements and implements the GDPR in Denmark²⁵⁰ and contains provisions relating to data processing, the disclosure of personal data, the right of access, the designation of a data protection officer, limits on consent, prohibitions on data transfers, administrative penalties and more. It is enforced by the Danish Data Protection Agency.

On the questions of the use of personal data or sensitive data to feed into AI systems and its interplay with the protection of the right to privacy, the Danish Data Protection Agency does not appear to have formally presented a position favouring either AI or securing the right to privacy,²⁵¹ although the DDPA is in line with the GDPR. However, in a White Paper on a common public sector digital architecture,²⁵² one of the principles outlined by the Agency for Digitization, Ministry of Finance has been to ensure that trust, security and privacy is achieved by incorporating, information security and protection of privacy by design in the digital solution.

246. Sejuti Das, "Israel Converts AI Cyber-Security Defence System to Predict Coronavirus Outbreak Locations", Analytics India Magazine, March 2020, available at <https://analyticsindiamag.com/israel-converts-ai-cyber-security-defense-system-to-predict-coronavirus-outbreak-locations/>; William Douglas Heaven, "Israel is Using AI to flag High-Risk COVID-19 Patients", MIT Technology Review, April 2020, available at <https://www.technologyreview.com/2020/04/24/1000543/israel-ai-prediction-medical-testing-data-high-risk-covid-19-patients/>

247. Global Legal Insights, "AI, Machine Learning and Big Data 2020", available at <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/israel>

248. Uri Berkovitz, "Israel's National AI Plan Unveiled", Globes Israel Business News, November 2019, available at <https://en.globes.co.il/en/article-israels-national-ai-plan-unveiled-1001307979>

249. Data Protection Act, 2018 (Law No. 502 of 23 May 2018), formerly the Danish Act on Processing of Personal Data Law (Act No. 429 of 31 May 2000), available at: <https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf>

250. The Danish Data Protection Act, 2018, available at <https://www.itgovernance.eu/da-dk/eu-gdpr-compliance-dk>

251. Alan Charles Raul (Ed.), "The Privacy, Data Protection and Cybersecurity Law Review: Edition 6", The Law Reviews, October 2020, available at <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210046/denmark>

252. Steering Committee for Data and Architecture, "The Digitally Coherent Public Sector: White Paper on a Common Public Sector Digital Architecture", June 2017, available at https://arkitektur.digst.dk/sites/default/files/white_paper_on_a_common_public-sector_digital_architecture_pdfa.pdf

EU

Maturity Index – 3/5

The GDPR²⁵³ formulated by the EC in 2016, came into effect in 2018 and has been possibly the most wide-ranging impact on data privacy laws across the world. In stark contrast to the US approach, the GDPR reflects the European preference for a strong rights-based approach and is directly binding on all EU member states. Pursuant to the enactment of the GDPR, each EU member state was required to update or streamline its data protection laws with the framework established in the GDPR.²⁵⁴

The main themes of the GDPR are control, transparency and accountability. It lays down the rules relating to the protection of the personal data of natural persons and sets out the fundamental rights and freedoms of natural persons in respect of the protection of personal data.²⁵⁵ It defines “personal data” as meaning any information relating to an identified or identifiable natural person, which includes information such as names, identification numbers, location data, etc.²⁵⁶ It also sets out core principles relating to the processing of personal data which are:

1. lawfulness, fairness and transparency;

2. purpose limitation;

3. data minimization

4. accuracy

5. storage limitation; and

6. integrity and confidentiality.²⁵⁷

The GDPR also grants data subjects or individuals the following rights: data protection rights, which include the right to transparent communication and information (Art. 12-14), the right of access (Art. 15), right to rectification (Art. 16), right to erasure (Art.17), right to restriction of processing (Art.18), obligation to notify recipients (Art. 19), right to data portability (Art.20), the right to object (Art.21) and the right to not be subject to automated decision-making (Art. 22).

As with other data protection legislations, the GDPR is technology agnostic, and does not explicitly refer to AI. However, with respect to the right to consent, the GDPR has an opt-in system and the modalities of an express consent provision in the context of AI is unclear. The GDPR consent provision requires that that data subject be made aware of the (limited) purpose for which the data is being collected, and only upon such consent being obtained, can such data be used. AI systems do not function in a linear manner, and come to inferences and potentially, decisions from vast quantities of disparate information. However, per the GDPR, the data subject has the right to opt out against automated decision-making and can request human intervention as well as an explanation for how automated decision making takes place.

In April 2018, the EC published the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for

253. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

254. Supra note 167, page 168.

255. Article 1 of the GDPR.

256. Article 4(1) of the GDPR.

257. Article 5(1) of the GDPR.

Europe (AI Communication).²⁵⁸ In the AI Communication, the EC notes that the GDPR ensures a high standard of personal data protection, as the rights and obligations contained in it protect data by design and by default. It also notes that the GDPR considers the issue of decision-making based solely on automated processing, including profiling. In such cases, data subjects have the right to be provided with meaningful information about the logic involved in the decision, as well as the right not to be subject solely to automated decision-making, except in certain situations. Without discussing specifically how these would balance the issue of privacy vis-à-vis the benefits of AI systems, the AI Communication merely states that it would await the application of these provisions in the context of AI. However, based on the wording of the provision, the restriction applies only when the decision is based solely on automated processing (which includes profiling), which produces legal effects or significantly affects the data subject. Moreover, the right to access of information related to data processing also applies only when the provisions of Article 22 are met. Nevertheless, where automated decision making involves the processing of personal data, all GDPR provisions apply – including, for instance, the principles of fair and transparent processing. Another issue is the way in which the right to explanation as contained in the GDPR would apply in the context of AI. The right to explanation requires the provision of “meaningful information about the logic involved”, which could potentially be limited to information about the algorithmic method, rather than the actual logic used in the decision-making process by the AI system. This may not truly fulfil explainability and transparency in the truest sense.²⁵⁹

While further explanation/guidance and enforcement experience is required to fully understand how the GDPR would affect the growth of AI systems, it is clear that the intention of the EU is to have the principles of transparency, accountability and protection of the right to privacy ingrained into the design of AI at the very beginning, so that tools and systems can be developed around these ideas rather than be shoehorned in at a later stage (which may not be possible).

On 15 December 2020, the EC proposed²⁶⁰ a new framework of rules to govern the digital space, comprising the Digital Services Act²⁶¹ and the Digital Markets Act.²⁶² This builds on the GDPR, with the ostensible goal of protecting consumers and their fundamental rights (including the right to privacy) better, as well as ensuring that digital markets are more open and fair. The new proposal considers the sets out several obligations for digital platforms that operate as “gatekeepers”, including that they cannot mix data collected from their business consumers with that collected from individual users, as well as preventing automatic sign-ins across platforms. Both these steps are likely to help limit the automatic collection of user data and user profiling, without express consent and awareness on the part of the user. It also prohibits platforms from gathering data about their business customers, which has typically been used by platforms to create their own competing products/services. The Digital Markets Act also buttresses users’ rights to data portability and accessibility free of charge and on a real-time basis.²⁶³

AUSTRALIA

Maturity Index – 3/5

Australia's key privacy law, the Federal Privacy Act, 1988²⁶⁴ (**FPA**) governs both the public and the private sector and lists

258. EC, “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence in Europe”, April 2018, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625

259. Kalliopi Spyridaki, “GDPR and AI: Friends, Foes or Something in Between?”, SAS Insights, available at https://www.sas.com/en_in/insights/articles/data-management/gdpr-and-ai-friends-foes-or-something-in-between-.html

260. EC, “Europe fit for the Digital Age: Commission Proposes New Rules for Digital Platform”, 15 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

261. EC, “The Digital Services Act: Ensuring a Safe and Accountable Online Environment”, December 2020, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

262. EC, “The Digital Markets Act: Ensuring Fair and Open Digital Markets”, December 2020, available at <https://europa.eu/!Rd39Mp>

263. Cory Doctorow and Christoph Schmon, “The EU’s Digital Markets Act: There is a Lot to Like, but Room for Improvement”, Electronic Frontier Foundation, December 2020, available at <https://www.eff.org/deeplinks/2020/12/eus-digital-markets-act-there-lot-room-improvement>

264. Privacy Act, 1988, available at: <https://www.legislation.gov.au/Details/C2017C00283>

13 principles referred to as the Australian Privacy Principles (**APPs**). The APPs govern standards, rights and obligations around the collection, use and disclosure of personal information, which is defined as any information or opinion that could identify or reasonably identify a person, which could include names, addresses, phone numbers, sensitive information such as racial or ethnic origin, political beliefs, trade union membership, credit information, employee record information, IP addresses, etc.

The APPs²⁶⁵ address the following issues: (a) open and transparent management of personal information; (b) anonymity and pseudonymity; (c) collection of solicited personal information; (d) dealing with unsolicited personal information; (e) notification of the collection of personal information; (f) circumstances for the use or disclosure of personal information; (g) use of personal information for direct marketing under certain conditions; (h) protection of personal information before cross-border disclosure; (i) limited circumstances in which organizations may adopt, use or disclose government related identifiers; (j) requirement to ensure personal information is accurate, up to date and complete; (k) requirement for organizations collecting information to take reasonable steps to protect personal information from misuse, interference, loss, unauthorized access, etc.; (l) individual's right to access personal information; and (m) responsibility of the organization holding personal information to correct such information, where required. The APPs are intended to be technology neutral, flexible and principles-based, and therefore applicable to AI as well.

The FPA provides specific rights to individuals to opt out of the collection of personal information for direct marketing, protecting information such as criminal records, employment information, participation in political activities, etc.²⁶⁶ Further, the FPA and APPs also note that consent is an exception to the prohibition against collection and handling of personal information. Consent under the FPA is express or implied consent, where it is given voluntarily, the individual is adequately informed in advance, and has the capacity to understand and communicate their consent. Consent must also be current and specific, especially where it concerns an individual's sensitive information.²⁶⁷

In April 2019, the Australian Government's Department of Industry, Science, Energy and Resources issued a discussion paper,²⁶⁸ looking into the way in which AI should be designed, developed and deployed in Australia. This included draft AI ethics principles, and highlighted various issues arising from the use of AI systems, such as the necessity for data collection at the core of AI, which affects the potentially competing privacy interest. It also emphasises the need for ensuring that decision-making by AI does not result in discrimination or bias and notes that with the development of AI tracking biometric data, facial recognition, gait analysis, etc. it is necessary to understand how privacy works in today's world.²⁶⁹ The paper suggests a number of mechanisms which can be used to mitigate the dangers of AI in a "toolkit" which includes impact assessments, risk assessments, development of best practice guidelines, industry standards, mechanisms to monitor and improve AI, etc.²⁷⁰

Upon receipt of comments on the draft ethics principles, a final set of 8 ethics principles were published,²⁷¹ which are meant to be used when designing AI systems, to "achieve better outcomes, reduce the risk of negative impact and practice the highest standards of ethical business and good governance." Among other things, the principles require that AI systems

265. Office of the Australian Information Commissioner, "Australian Privacy Principles: Quick Reference", available at <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/>

266. Office of the Australian Information Commissioner, "Your Privacy Rights", available at <https://www.oaic.gov.au/privacy/your-privacy-rights/>

267. Office of the Australian Information Commissioner, "Australian Privacy Principles: Guidelines – Chapter B: Key Concepts", July 2019, available at <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#consent>

268. Dawson and Schleiger, "Artificial Intelligence: Australia's Ethics Framework", Data61 CSIRO, Australia, 2019 available at https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

269. Ibid, page 7.

270. Ibid, page 8.

271. Department of Industry, Science, Energy and Resources, Australian Government, "AI Ethics Principles", available at <https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>

should respect and uphold privacy rights and data protection, ensuring data security. The principles recommend ensuring proper data governance and management to protect data privacy. For example, by using data anonymisation where required. It goes on to state that the outcomes in terms of connections and inferences arising from the use of AI systems should be sound and assessed in an ongoing manner.²⁷²

The Office of the Australian Information Commissioner (the authority that governs privacy laws in Australia) (**OAIC**) also submitted its comments on the AI ethics framework, setting out its recommendations for how the existing privacy framework should be adapted to fit privacy concerns in the digital age.²⁷³ The OAIC believes that AI amplifies existing challenges to protecting privacy, and therefore, highlights the importance of increasing accountability of AI systems through transparency, building in privacy by design and putting in systems for third party certification, audits, regulatory oversight, etc. to build public trust in AI systems. The OAIC also notes that in order to enable meaningful individual management of privacy rights, as anticipated under the FPA, it is essential for businesses and governments to operate transparently and accountably in their information handling practices and ensure that these are accessible and understandable.²⁷⁴

On February 2020, the Australian Government kickstarted an investigation into digital platforms by directing a five-year inquiry by the Australian Competition and Consumer Commission (**ACCC**). The scope of the inquiry includes the study of practices by digital platforms or data brokers that may result in consumer harm.²⁷⁵ On 23 October 2020, the ACCC published an interim report,²⁷⁶ which focused inter alia, on online private messaging services and the effect of data collection on greater personalization of products and services online. It considers the use of data to offer personalized pricing to users and the impact of this practice on consumer welfare.²⁷⁷ It also looked at private messaging services' policies for signing up, features, etc. to consider whether these data collection mechanisms caused any harm to consumers. It noted that many privacy policies were typically "long, complex, vague and difficult to navigate"; that there were inconsistencies in descriptions of fundamental concepts, which is likely to cause confusion for consumers; and generally permitted extensive data collection.²⁷⁸ The report concludes that the extensive data practices of online private messaging, search and social media platforms increases the risks of harms occurring to consumers. These harms include an increased risk of profiling and decrease in privacy. Decreased privacy and control over consumer data could result in data breaches of personal or financial information, unsolicited targeted advertising and identify fraud.²⁷⁹

SINGAPORE

Maturity Index – 4/5

The Personal Data Protection Act, 2012 (**PDPA**)²⁸⁰ governs data privacy in Singapore. Under the PDPA, personal data refers to "data, whether true or not, about an individual who can be identified from that data". The PDPA sets out rules for the

272. Ibid.

273. Office of the Australian Information Commissioner, "Artificial Intelligence: Australia's Ethics Framework – Submission to the Department of Industry, Innovation and Science and Data61", June 2019, available at <https://www.oaic.gov.au/engage-with-us/submissions/artificial-intelligence-australias-ethics-framework-submission-to-the-department-of-industry-innovation-and-science-and-data-61/>

274. Ibid.

275. Australian Competition and Consumer Commission, "Digital Platform Services Inquiry 2020-2025", available at <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025>

276. Australian Competition and Consumer Commission, "Digital Platform Services Inquiry: September 2020 Interim Report", 23 October 2020, available at <https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Service%20Inquiry%20-%20September%202020%20interim%20report.pdf>

277. Ibid, section 6.4.3.

278. Ibid, section D.10.

279. Ibid, section D.4.2

280. The Personal Data Protection Act 2012 (No. 26 of 2012), available at: <https://sso.agc.gov.sg/Act/PDPA2012>

collection, use, disclosure and care of personal data. It also recognises individual rights such as the right to protect their personal data, right to access and correct personal data, etc. The PDPA necessitates prior user consent for the collection, use and disclosure of personal data (with some limited exceptions). It also requires organizations to disclose the purpose for which they are collecting, using and disclosing personal data; organizations may also only collect data for purposes which would be considered appropriate to a reasonable person. The PDPA provides individuals the right to withdraw consent, and organizations are required to inform the individual accordingly about the consequences of the withdrawal of consent and cannot prohibit the individual from withdrawing consent.

In 2019, Singapore launched its Model AI Governance Framework (**Framework**)²⁸¹ which translates ethical principles that form the basis of the PDPA and other guidance into practical recommendations. Specifically, on automated decision making, the Framework notes that it is necessary to determine the level of human oversight on AI systems that automate decision making by weighing the commercial benefits (e.g., consistency in decision making) with the risks such as bias. It notes that determining the appropriate level of human involvement in AI-augmented decision making is typically an iterative process and should be revisited often depending on the circumstances and impact, which can be documented through a risk impact assessment. It lists methods such as (a) human-in-the-loop, where a human merely relies on intelligent systems to help with decision making, by providing recommendations or information, but is ultimately responsible for making the decision; (b) human-over-the-loop, where a human is involved in a supervisory capacity only and can step in if the AI model encounters undesirable events. The Framework recommends that companies consider both the severity and probability of harm (which could vary by circumstance, function and sector), when considering which model to adopt.

SOUTH KOREA

Maturity index – 3/5

The Personal Information Protection Act, 2011²⁸² (**PIPA**) is the main legislation that governs data protection and privacy rights in South Korea.²⁸³ PIPA defines personal information as any information that identifies a living individual or can be combined with other information to do so.²⁸⁴ In January 2020, amendments to PIPA clarified the difference between personal data, pseudonymised data and anonymised data, which is excluded from the scope of personal data.²⁸⁵

PIPA imposes obligations such as the requirement of organizations to disclose to individuals what data they propose to collect, the purpose for which it is collected, how long this data will be used or retained, etc. If any data is proposed to be shared with a third party, specific consent must be obtained, while also explaining the objectives of the third party for collecting the data. It also imposes a requirement on organizations collecting information to limit such information collection to the extent necessary for the purposes of processing and not go beyond this. It mandates that organizations make their privacy policies public and guarantee individuals the right to access their personal information.²⁸⁶

PIPA also clarifies the rights of individuals in relation to the processing of their personal information, which includes the right to be informed of processing of their information, the right to consent (including a choice on the scope of their

281. Personal Data Protection Commission Singapore, "Model Artificial Intelligence Governance Framework: Second Edition", January 2020, available at <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

282. Personal Information Protection Act, 2011, available at <http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf>

283. By way of an amendment in 2020, the provisions on personal data protection in the Act on the Promotion of Information and Communications Network Utilization and Information Protection, 2001 (available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiyp6mf0AhWt8HMBHZk5DWIOFjAegQIAhAB&url=https%3A%2F%2Fwww.privacy.go.kr%2Fcmm%2Ffms%2FfileDown.do%3FatchFileId%3DFILE_000000000830762%26fileSn%3D0&usg=AOvVaw35VyPS6BudLoCRFdOn30r) were deleted.

284. Article 2(1), PIPA.

285. Chris Kang et al, "South Korea: Korea introduces major amendments to data privacy laws", 2 March 2020, available at <https://www.mondaq.com/privacy-protection/898830/korea-introduces-major-amendments-to-data-privacy-laws>

286. Article 3, PIPA.

consent), the right to confirm processing, the right to demand access to the personal information that has been collected for processing and the right to suspend processing of their personal information. PIPA also grants data subjects the right to make corrections, delete or destroy their personal information and to obtain appropriate redress for any damage that arises out of the processing of personal information in a prompt and fair procedure.²⁸⁷

With the recent amendments introducing the concept of pseudonymised data, PIPA now permits the use of such data to generate statistical information, for scientific research or for public record keeping without the need of individuals' consent. However, this information is not permitted to be used for commercial or business purposes. The 2020 amendments also allow for the use, without further specific consent, of personal information, where the new purpose is within a scope reasonably related to the original purpose of collection of information.²⁸⁸

With respect to the interface with AI, the Korean Ministry of Science, ICT and Future Planning published a report setting out its Artificial Intelligence Information Industry Development Strategy in 2016 (**Korean AI Strategy**).²⁸⁹ In the Korean AI Strategy, the government states its national vision to realise a human-centred intelligent information society. Overall, the Korean AI Strategy focuses on recognising the strengths and benefits that arise from having AI systems underlying various industries and sectors. It also looks at establishing a "data-based" society, with a centralized data management system that would facilitate machine learning, while differentiating between private information, non-identifying information and general information. It notes that this segregation would help to assuage fears over privacy infringement.²⁹⁰ However, it also notes that with the development of intelligent IT, it is necessary for policymakers to improve privacy protection requirements.²⁹¹

SWEDEN

Maturity index – 3/5

Sweden's Personal Data Act (1998:204)²⁹² was replaced by the Swedish Data Protection Act (2018:218) and the Swedish Data Protection Regulation (2018:219) to govern alongside the EU's GDPR. The data privacy legislation regulates data protection principles, the legal bases for processing personal data, rules around special category data and transparency requirements, in line with the GDPR.

In 2018, the Ministry of Enterprise and Innovation issued a report on the National Approach to Artificial Intelligence,²⁹³ which acknowledged the transformative nature of AI, while at the same time noting the need to create a framework that allows for the "safe, secure and favourable climate for digitisation and harnessing the opportunities of AI." It highlighted the need to ensure the collection of high-quality data that feeds into automated systems, as well as appropriate frameworks to balance the fundamental needs of privacy, ethics, trust and social protection. The paper notes that the ways in which private parties are able to implement the strong privacy protections set out in the GDPR will determine the success of Sweden's ability to manage the benefits and risks of AI. It also notes the need to develop standards and guidelines to pave the way

287. Article 4, PIPA.

288. Bae, Kim and Lee LLC, "Data Protection and Privacy 2020: South Korea", Chambers & Partners Trends and Developments, March 2020, available at <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/south-korea/trends-and-developments/05894>

289. Ministry of Science, ICT and Future Planning, "Artificial Intelligence Information Industry Development Strategy", 2016, available at https://english.mst.go.kr/cms/english/pl/policies2/_icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

290. Ibid, page 34.

291. Ibid, page 63.

292. Swedish Data Protection Act (2018:218), available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfatningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

293. "Government Offices of Sweden, "National Approach to Artificial Intelligence", 2018, available at: <https://www.regeringen.se/4aa638/contentassets/a6488cccbc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

for innovations in AI, and that it is key for Sweden to take part in the wider European effort to develop in these areas, while implementing the necessary structures nationally.²⁹⁴

The Swedish government has also set up the Committee for Technological Innovation and Ethics (**KOMET**) in August 2018, with the goal of helping to “identify policy challenges, contribute to reducing uncertainty surrounding existing regulations, and accelerate policy development.”²⁹⁵ KOMET currently has an industry focus on precision medicine, connected industries and autonomous vehicles, vessels and systems. It is due to submit its report and recommendations by March 2021.

FINLAND

Maturity index – 4/5

In Finland, data privacy is governed by the Personal Data Act, 1999 (FPDA).²⁹⁶ The FPDA mandates that personal information may be gathered only if it can be shown by the party collecting the information that there is a clear purpose for collection, and disallows using the data for any purpose other than those stated beforehand. The FPDA requires user consent prior to data gathering, while requiring the party collecting such data to provide the user with a data file that describes not just the gathering process but also the purpose behind gathering such data. Furthermore, as per the FPDA, in case the data is being collected for personalized marketing or e-mail marketing and the database is limited to basic user information and contact information, certain specific restrictions apply.

In 2017, Finland released a strategy paper,²⁹⁷ which sets out the Finnish government’s plan to ensure the deployment of AI in the public and private sector for the wellbeing of society at large, noting that Finnish society already has the essential prerequisites for the successful utilization and adaptation of AI systems. Nevertheless, the report notes that the application of AI requires new types of security solutions and related legislation and that the protection of individuals and privacy must be guaranteed.²⁹⁸

In December 2018, the Finnish government published a Government Report on Information Policy and Artificial Intelligence²⁹⁹ which outlines the progress being made in deploying AI systems in healthcare, transport, bioengineering, etc. The report also calls for legislation to consider what kinds of functions can be automated or performed by AI systems, and which still require human intervention. It notes that the efficient use of information, with both private and public bodies using the same standards and best practices, is the key to successfully deploying AI systems in Finland. It highlights that in order to use AI in the best services of its people, it is necessary to ensure access to data while taking care of consideration such as privacy. The report refers to the concept of “My Data”, where the individual is at the centre of the system that is based on the exchange of personal data as a valuable resource in the data economy. Such a system would grant the individual total control over how their data is treated or used, while providing them with the best possible capabilities to understand their own wellbeing and to take action to enhance it as required. If an individual’s data is held by a third party and they cannot make use of it, it would not fall under the category of “My Data”. Finland has used the “My Data” approach in the transport, communication and education sectors. On the basis of this experience, the report notes that the fundamentals

294. Ibid, page 10.

295. Committee for Technological Innovation and Ethics, “About Us”, 2018, available at <https://www.kometinfo.se/in-english/about-us/>

296. Personal Data Act, 1999, available at: <http://www.finlex.fi/en/laki/kaannokset/1999/19990523>

297. Ministry of Economic Affairs and Employment, “Finland’s Age of Artificial Intelligence: Turning Finland into a leading country in the application of artificial intelligence”, 18 December 2017, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y

298. Ibid, page 26.

299. Government of Finland, “Government Report on Information Policy and Artificial Intelligence: Ethical Information Policy in the age of Artificial Intelligence”, December 2018, available at https://vm.fi/documents/10623/7768305/VM_Tiepo_selonteko_070219_ENG_WEB.pdf/89b99a8e-01a3-91e3-6ada-38056451ad3f/VM_Tiepo_selonteko_070219_ENG_WEB.pdf/VM_Tiepo_selonteko_070219_ENG_WEB.pdf

for a sound data economy lie in managing the roles and responsibilities for all stakeholders within such an economy. If these responsibilities are determined through legislation which is based on widely accepted ethical principles, it is possible to develop a responsible information culture, providing the basis for sound technology and AI systems.³⁰⁰

SPAIN

Maturity index – 4/5

The Protection of Personal Data and the Guarantee of Digital Rights legislation (PDGDR) was passed in December 2018.³⁰¹ The law is modelled after GDPR with a purpose of incorporating the GDPR disciplines in the Spanish domestic legal framework. Data protection and privacy are separate fundamental rights under Spanish law, and both are derived from the right to human dignity. Apart from the PDGDR, there are sector specific legislations that deal with data protection and privacy as well.³⁰²

The digital rights guaranteed to citizens under the PDGDR are: general rights (applicable to all citizens) such as the right to digital testament, to a digital education or to digital security; specific rights involved in the provision of information such as the right to rectification or updating information over the internet, the right to be forgotten, etc., and specific rights over the use of technologies in the context of employment, which look at issues such as video surveillance, use of digital devices, as well as the digital disconnection right, which guarantees employees' leave, break time and holidays.

The Spanish data protection authority has published guidelines on multiple issues, including the use of anonymising data or using open data in big data projects, as a privacy measure. Most recently the agency published a report on how AI systems can be compliant with GDPR requirements, including by providing recommendations at different stages of the AI life cycle.³⁰³

NORWAY

Maturity index – 4/5

Norway's Personal Data Act, 2018 (**NPDA**)³⁰⁴ implements the GDPR in Norway, and is supported by existing legislation on certain specific areas such as the use of cookies,³⁰⁵ targeted marketing³⁰⁶ and several legislations and guidelines pertaining to the healthcare sector.

The NPDA defines personal data as any information relating to an identified or identifiable natural person, through identifiers such as name, ID number, location data, etc. This is to be distinguished from "sensitive personal data" which

300. Ibid, page 18-19.

301. Ministry of Finance, "Data Protection", September 2020, available at <https://www.hacienda.gob.es/en-GB/EI%20Ministerio/Paginas/DPD/dpd.aspx>

302. For example, Law of Information Society Services and Electronic Commerce (Law No. 24/2002), available at: <https://www.global-regulation.com/translation/spain/1450967/law-34-2002%252c-of-11-july%252c-services-of-the-society-of-information-and-electronic-commerce.html>; and Law 9/2014 on Telecommunications, available at: <https://www.global-regulation.com/translation/spain/1452763/law-9-2014%252c-of-9-may%252c-general-telecom.html>

303. Agencia Espanola Proteccion Datos, "RGPD Compliance of Processes that Embed Artificial Intelligence: An Introduction" (translated text), February 2020, available at https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia-en_0.pdf

304. Advokatfirmaet Wiersholm AS, "Data Protected – Norway", March 2020, available at <https://www.linklaters.com/en/insights/data-protected/data-protected---norway>

305. The Electronic Communications Act, 2003 (translated text), available at <https://www.wipo.int/edocs/lexdocs/laws/en/no/no085en.pdf>

306. The Marketing Control Act, 2009, available at <https://www.forbrukertilsynet.no/english/the-marketing-control-act>

is the equivalent of “special categories of personal data” identified under the GDPR, that deal with racial or ethnic origin, political beliefs, trade union membership, health data, data pertaining to sexual orientation, etc. The NPDA incorporates the key principles of data privacy as set out in the GDPR, which include the requirement that personal data be processed in a lawful, transparent and fair manner; that personal data may only be lawfully processed if it is obtained through prior, specific, informed and unambiguous consent from the individual; in the context of processing sensitive personal data, explicit consent is required, and it also needs to be shown that such processing is required in the context of employment law or in relation to legal claims; the principles of purpose limitation, data minimization, retention for a limited and necessary time period; maintenance of accurate and up-to-date information, etc. Similarly, as under the GDPR, the NPDA allows data subjects to exercise several rights, which include the right to access data, right to rectify errors, the right to be forgotten, the right to object to or restrict processing, the right to data portability, the right to withdraw consent and the right to object to marketing and automated decision making.

Norway also requires that in some cases of high-risk processing, businesses are required to consult with the Norwegian Data Processing Authority before they undertake any processing activity, and in these cases the authority has the power to impose specific regulations on prior authorization and consultation.³⁰⁷

In respect of the interplay between AI and privacy laws, the Norwegian Data Processing Authority released a report in January 2018³⁰⁸ that discusses the privacy implications of AI, with the imperative to protect the right to privacy of the individual. It notes that privacy laws are key to promoting public trust that their information is being handled responsibly, which is an important step in deploying AI systems. It highlights that accountability is the fundamental basis of data protection in the context of AI developments and applications, as in the GDPR. The report examines the tools specified in the GDPR to ensure accountability on the part of data processors and data controllers – privacy by design and the implementation of data protection impact assessments. It notes that both these principles are key to ensuring that the right to privacy is considered and accounted for in the process of developing AI systems. The report also studies and recommends methods for good data protection in AI, such as:

1. reducing the need for training data (i.e. the vast sums of data required for machine learning) through the use of methods such as generative adversarial networks which generate synthetic data; federated learning, which distributes the site of learning to various local clients and then aggregates any changes to the model at the central level, without having to share local user data; and matrix capsules which are a new variant of neural networks that require significantly lesser data than previous methods;³⁰⁹
2. methods that protect privacy without reducing the data basis, which includes cryptology techniques such as differential privacy, homomorphic encryption, transfer learning, etc. all of which are methods that allow for AI systems to benefit from the use of vast databases but at a higher, aggregated level, without compromising on the quality of analysis; and
3. methods to avoid the “black box” issue, which pertains to the lack of transparency or explainability of AI algorithms.³¹⁰

The report also recommends that these approaches and others be considered by developers of AI systems, as well as businesses that would deploy these systems, to ensure that the right to privacy is given due importance throughout the lifecycle of AI systems.³¹¹

307. Gry Hyvindsen and Emily Weitzenboeck, “Norway: Data Protection Laws and Regulations 2020”, The International Comparative Legal Guides, March 2020, available at <https://iclg.com/practice-areas/data-protection-laws-and-regulations/norway>

308. The Norwegian Data Protection Authority, “Artificial Intelligence and Privacy”, January 2018, available at https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf

309. Ibid, page26.

310. Ibid, page 27-28.

311. Ibid, page 29.

ESTONIA

Maturity index – 4/5

Data privacy in Estonia is primarily regulated by the Personal Data Protection Act, 2019 (**EPDPA**)³¹² which is the national legislation supporting the enforcement of the GDPR. As in the GDPR, the regulatory regime in Estonia covers the rights of data subjects, the principles of accountability, purpose limitation, data minimization, etc. as well as the necessity to obtain consent for the collection and processing of personal data.

However, Estonia has also been at the forefront of implementing AI in governance. The Report of the Estonia AI Taskforce, 2019³¹³ set out the Estonian government's plan for integrating AI systems into its public and private sectors. In this regard, the report notes that there is no need for the introduction of a new legislation to integrate AI systems, especially in the public sector; but that it would be sufficient to amend existing legislation on the basis of the proposals set out in the report.³¹⁴ In respect of data protection and privacy, the report notes that personal data can be used for processing by AI for legal procedures, and in all other cases, where consent has been obtained from the data subject. The report notes that the data protection legislation and GDPR are technology neutral and therefore are applicable to the processing of data using AI. However, it notes the difficulties of collecting data using AI where the purpose originally specified when obtaining consent no longer applies. In order to overcome this difficulty, the report recommends the use of the principle of data minimization, and also to review the quality of data being collated. As an example of implementation of automated decision making, the report highlights the process of imposing fines for speeding pursuant to traffic legislation in Estonia. The report notes that similar legal regulations will be needed in other sectors if AI systems are to be introduced in other sectors.³¹⁵

THE NETHERLANDS

Maturity index – 3/5

The Dutch Personal Data Protection Act³¹⁶ was superseded by the framework of the GDPR in the Netherlands in the field of data privacy. In October 2019, the government also released a Strategic Action Plan for AI,³¹⁷ which sets out its priorities and the steps proposed to be taken to put the Netherlands at the forefront of AI implementation in Europe. The Strategic Action Plan for AI lists as one of its priorities, securing the fundamental rights of citizens through legal and ethical frameworks, both at the European level and in the Netherlands to make sure that companies and public organizations abide by ethical guidelines in the implementation of AI applications. In November 2019, the Dutch Data Protection Authority also published its supervision and enforcement priorities for the period of 2020-2023; these include trade in data (or data monetization practices), digital government (including enhancing data security in public institutions and ensuring compliance with data security laws by public institutions) and AI & algorithms (development of monitoring systems for AI applications using personal data).³¹⁸

312. Personal Data Protection Act, 2019, available at <https://www.riigiteataja.ee/akt/104012019011>

313. (Estonian) Ministry of Economic Affairs and Communication, "Report of Estonia's AI Taskforce", 2019, available at https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_486454c9f32340b28206e140350159cf.pdf

314. Id.

315. Ibid, page 40-41.

316. Netherlands Enterprise Agency, "Protection of Personal Data", <https://business.gov.nl/regulation/protection-personal-data/>

317. Government of the Netherlands, "Strategic Action Plan for Artificial Intelligence" (summary), 2019, available at <https://www.government.nl/binaries/government/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence/Strategic+Action+Plan+for+Artificial+Intelligence+Summary.pdf>

318. Dutch Data Protection Authority, "Focus Dutch Data Protection Authority 2020-2023: Data Protection in a Digital Society", November 2019, available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap-dataprotectie_in_een_digitale_samenleving_gb_wtk.pdf

UAE

Maturity index – 3/5

Data privacy in the UAE is guaranteed by the Federal Law No. 5 of 2012 on Combating Cybercrimes,³¹⁹ which makes it illegal to disclose any information obtained by electronic means, if such information was obtained in an unauthorised manner. The law attaches criminal liability to the use of an electronic information system, or any information technology means to offend another person or to attack or invade their privacy.

In addition to the above, the Telecommunications Regulatory Authority (**TRA**) implements the Internet Access Management (**IAM**) policy, 2017³²⁰, in coordination with licensed internet service providers (**ISPs**) in the UAE.³²¹ The TRA's guidelines for ISPs include:

1. a clear privacy policy stating the information that is proposed to be collected, the purpose for data collection and its proposed use. The privacy policy is also required to inform users as to how their information could be made available to the public. Notably, the regulations require that explicit consent be obtained where data collected is proposed to be shared with a third party.
2. collection and processing of sensitive user data is to be done in a secure manner (e.g., by use of SSL/encryption technologies to prevent illegal collection of usernames, credit card information and banking information).
3. the ISP must "request the user to provide only the necessary information for service", placing a responsibility on both the ISP and the user.
4. ISPs are to refrain from collecting addresses and contact information of visitors for the purpose of sale or publication.³²²

Separately, the IAM Regulatory Policy³²³ defines information that invades the privacy of users as "prohibited content",³²⁴ which is required to be blocked as per the procedure specified. Information that invades the privacy of users includes any internet content which:

1. has tools for phone tapping, espionage, theft or publication of private information or tracking, recording or intercepting communications or conversation without right;
2. exposes news, photos or comments related to the private or family life even if it is true if publishing the same shall harm the concerned person in publication. In addition, this includes disclosure of a secret that may harm a person's reputation, wealth or trade name or the publication of something intended to threaten or forcing him to pay money or provide benefit to others or be deprived of freedom to work;
3. relates to medical examinations, medical diagnosis, medical treatment or care or medical records.

319. Federal Decree-Law no. (5) of 2012 on Combating Cybercrimes, available at: http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf

320. Telecommunication Regulatory Authority, "Internet Guidelines", January 2019, available at <https://www.tra.gov.ae/en/about-tra/information-and-e-government-sector/internet-guidelines/details.aspx#pages-67186>

321. Digital UAE, "Data and Privacy Protection in the UAE", October 2019, available at <https://u.ae/en/about-the-uae/digital-uae/data-data-and-privacy-protection-in-the-uae>

322. Telecommunication Regulatory Authority, "Internet Guidelines", January 2019, available at <https://www.tra.gov.ae/en/about-tra/information-and-e-government-sector/internet-guidelines/details.aspx#pages-67186>

323. Telecommunication Regulatory Authority, "Internet Access Management Regulatory Policy", 2017, available at <https://www.tra.gov.ae/en/about-tra/information-and-e-government-sector/internet-guidelines/details.aspx#documents>

324. Ibid, Annex 1.

4. allows access to private information illegally including those related to addresses and phone numbers of individuals or which allows disturbing others such as spam messages; and
5. confidential information of public corporations in the UAE.

HONG KONG

Maturity index – 3/5

Hong Kong's PDPO³²⁵ was originally issued in 1996 and was one of the first comprehensive data protection regulations in Asia. It has been subsequently amended and updated to deal with issues such as direct marketing, and cybersecurity. Schedule 1 of the PDPO contains 6 data protection principles - these include rules on the purpose and method for collecting personal data; accuracy and duration of retention of personal data; the use of personal data; maintaining the security of personal data; ensuring information on data protection and processing policies; and providing access to personal data to the data subject or individual.³²⁶

The enforcement agency under the PDPO, i.e., the Privacy Commissioner for Personal Data (**PCPD**) has published several guidance notes on issues affecting the privacy of personal data that have arisen as a result of technological innovations, such as targeted advertising, the use of search engines, cookies, online tracking, cloud computing and employee monitoring. In each case, the PCPD provides specific guidelines on how the data protection principles under the PDPO are applicable, in order to keep the privacy of personal data protected.³²⁷

While the longstanding enforcement practice of the PCPD demonstrates that Hong Kong does consider the right to privacy a priority, the way in which these principles apply to AI systems must be evaluated. For instance, the requirement of explicit consent, the principles of use limitation and transparency are all difficult to comply with in the context of AI systems. In order to better understand these implications, the PCPD commissioned a study to achieve ethical and fair processing of data.³²⁸ This report sets out the "Enhanced Data Stewardship Accountability Elements for Data Processing Activities, such as AI and ML, that Directly Impacts People (**Enhanced Elements**) and Data Stewardship Values" (**Values**). The Enhanced Elements inter alia, define data-stewardship values that are meant to be translated into organizational policies and processes for ethical data processing. It advocates an "ethics by design" approach in data analytics and data-use design processes so that the benefits of advanced data processing activities accrue not just to the organization but society at large. It recommends using Ethical Data Impact Assessments (**EDIA**) where data use is likely to impact people in a significant manner; conducting internal reviews to ensure that EDIAs are conducted with integrity and competency and to confirm that the issues raised through the assessment have been addressed. It suggests increasing transparency about processes and where possible, ensure the widest possible social benefit. Finally, it prioritizes demonstrating the soundness of internal processes to regulatory authorities.³²⁹ The Data Stewardship Values that are required to be championed by companies include being "Respectful, Beneficial and Fair".³³⁰ The model EDIA and Process Oversight Model described in the guidance report are meant to constitute a practical framework that is interoperable with other privacy and data protection regimes, including the GDPR.

325. The Personal Data (Privacy) Ordinance, 1996, available at <https://www.elegislation.gov.hk/hk/cap486?pmc=1&m=1&pm=0>

326. Schedule 1 of the PDPO.

327. Alan Charles Raul (Ed.), "The Privacy, Data Protection and Cybersecurity Review: Edition 7", October 2020, available at <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210040/hong-kong>

328. The Information Accountability Foundation, "Ethical Accountability Framework for Hong Kong, China", October 2018, available at https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf

329. Ibid, page 22-23.

330. Ibid, page 24-27.

NETWORK SECURITY



The roll-out of AI systems has now moved beyond merely R&D, as many public and private organisations across the world have begun deploying AI systems in key sectors like healthcare and banking. This has led to the sobering realisation that the availability of data that allows for AI systems to function efficiently and provide valuable insights can also skew in a way that could be harmful, whether intentional or unintentional.³³¹ Given data is the currency that lends value to AI systems, any manipulation or misuse of data could lead to extremely damaging outcomes. The extent of harm could vary, but even the misuse of AI in social media or advertising (much less healthcare or banking) can have far-reaching effects. This is to say nothing of how AI can be actively used to commit crimes. Ensuring network security or secure systems for the collection, storage, and use of data is essential to the safe and productive use of AI systems in society.³³²

On the other hand, AI may also hold the answers to a more secure internet. A report that surveyed 85 executives across enterprises found that 69% believed that cybersecurity breaches cannot be stopped without the use of AI. Further, 73% of the enterprises are testing the use of AI in cybersecurity.³³³ The development of AI systems, therefore, also provides methods to solve the complex problems that cannot be solved by traditional systems based on fixed algorithms.³³⁴

The policy challenges for regulatory regimes therefore stem from the lack of research in the uses of AI systems and their impact on cybersecurity. However, as cyber-attacks are on the rise, some countries have moved towards considering network security as an issue when regulating the use of AI. One of the main approaches that have emerged is to incorporate security systems

right from the design and development of AI – i.e., a ‘security by design’ approach. This approach does not just focus on mitigation or counterattacks after the fact, but develops the AI system in a way that is prepared to withstand such attacks.³³⁵

Another policy challenge concerns the development of standards and certification procedures for AI systems. Many believe that the standards and certification procedures must focus on improving the reliability of the AI systems by guiding users towards in-house development of AI protection systems, training them with adversarial data and constant monitoring.³³⁶ At the global level, the OECD Principles for AI, Robustness, Security and Safety (**OECD Principles on AI**) mention robustness as a principle, which requires that AI developers work to manage risk at every level of development of AI to make it as secure as possible. Further, they must also ensure that they can trace data sets being used by AI systems, the process for selecting data and the decisions that are being taken by the systems. This will help in ensuring that AI systems can “withstand or overcome adverse conditions, including digital security risks”.³³⁷

In the light of the above, the instant report captures various regulatory and policy decisions of various countries with respect to the intersection of AI and cybersecurity. While there do not appear to be many existing wide-ranging frameworks or policies, some jurisdictions have recently responded to specific instances by introducing executive action and proposals for tightening cybersecurity, especially on account of greater economic dependence on cyberspace with the COVID-19 pandemic.

331. Lin, Tom C. W., “Artificial Intelligence, Finance, and the Law”, Fordham Law Review, Volume 88 Issue 531, November 2019, available at: <https://ssrn.com/abstract=3480607>

332. Charlotte Tschider, “Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age”, DENV. U. L. REV. Volume 96 Issue 87, February 2018, available at <https://ssrn.com/abstract=3129557>

333. Louis Columbus, “Why AI is Future of Cybersecurity”, Forbes, July 2019, available at: <https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#3e8da2e7117e>

334. Nadine Wirkutis and Hadas Klein, “Artificial Intelligence in Cybersecurity”, Cyber, Intelligence and Security, Volume 1 Issue 1, January 2017, available at: <https://www.inss.org.il/wp-content/uploads/2017/03/Artificial-Intelligence-in-Cybersecurity.pdf>

335. Maria Korolov, “How Secure are your AI and Machine Learning Projects?”, September 2019, available at: <https://www.csoonline.com/article/3434610/how-secure-are-your-ai-and-machine-learning-projects.html>

336. Mariarosaria Taddeo, Tom McCutcheon and Luciano Floridi, “Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword”, November 2019, available at <https://www.nature.com/articles/s42256-019-0109-1?proof=trueHere>

337. Principle 1.4, “OECD Principles for AI, Robustness, Security and Safety”, 2019, available at: <https://oecd.ai/dashboards/ai-principles/P8>

MATURITY INDEX

NETWORK SECURITY



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation



INDIA

Maturity Index – 4/5

The Indian AI Strategy³³⁸ mentioned security issues as one of the barriers to be addressed to achieve the benefits of deployment of AI systems. The strategy proposes that R&D on AI security concerns should be the prerogative of various Centres of Research Excellence to be established at various premier higher education institutions. Besides this, it recommends the development of and adherence to standards on cybersecurity.

The issue of cybersecurity found a specific mention in the report³³⁹ prepared by Committee D constituted by Ministry of Electronics and Information Technology, to examine the cybersecurity, safety, legal and ethical issues related to AI. The report focuses on various challenges that countries face, such as an increase in the potential impact of intrusion and physical manifestations of online security threats through manipulation of IoT and through social media platforms. The report further brings to light the capability of AI to excel at 'speed, scale and scope' and how this should be harnessed to handle emerging security threats. The report looks at the use of AI to strengthen such security systems, and notes that as "predictive analytics gains ground, mathematics, machine learning and AI will be baked more into security solutions". Emerging technologies could help with identifying new areas of vulnerabilities, develop methods to adapt and react to attacks, glean insights from cyberattacks and adapt them for use across other systems and networks.

The main difficulty in developing greater network security, according to the report, is to avoid goal misspecification, overcome complex and uncertain environments, unforeseen conditions and controlling the system's behaviour once it is deployed. It also notes that maintaining cordial human-machine interactions and standard-setting is key to better cybersecurity. In terms of a best practice, the report advocates considering network security throughout the AI development cycle. The report also discusses areas of further research such as data privacy, encryption schemes and AI mechanisms that increase the robustness of network security. The report sets out recommendations to develop a better and more secure cyber network:

1. Development of techniques and tools which use AI to defend against attacks more effectively, and identification of new types of vulnerabilities in AI-based applications. It also recommends international collaboration on this issue.
2. Organising AI-based cybersecurity challenges to identify talent and new ideas to further support technology development.
3. Developing anonymisation infrastructure to allow for large data sets to be made available for analysis and development, including sensitising and educating public agencies that hold useful data to safely share the data with AI developers for public good.
4. Sharing of best practices between private and public institutions, with government support through procurement practices.
5. Developing a National Resource Centre to take up the activities listed above, as a nodal agency for cybersecurity and other related issues such as safety, ethical and legal issues.

On 16 December 2020, the Cabinet Committee on Security, Government of India announced the "National Security Directive on Telecom Sector", which mandates telecom service providers to purchase equipment from trusted sources, which is to be declared by the government. The directive is to be followed by rules from the National Cyber Security Coordinator, the designated authority responsible for implementation, on the methodology to designate trusted sources.³⁴⁰

338. NITI Aayog, National Strategy for Artificial Intelligence #AIforALL, June 2018, available at: <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>

339. Ministry of Electronics and Information Technology, "Report of Committee – D on Cyber Security, Safety, Legal and Ethical Issues", December 2019, available at: https://meity.gov.in/writereaddata/files/Committees_D-Cyber-n-Legal-and-Ethical.pdf

340. Press Trust of India, "Govt Announces National Security Directive on Telecom Sector for secure networks", 16 December 2020, available at <https://www.livemint.com/news/india/govt-announces-national-security-directive-on-telecom-sector-for-secure-networks-11608121644450.html>

USA

Maturity Index – 4/5

The AI Executive Order³⁴¹ tasked the NIST with developing ‘a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies.’ Pursuant to this, NIST prepared a response³⁴² to the AI Executive Order laying down the plan and areas in which NIST will work to achieve the goals listed in the AI Executive Order. Two of the crucial areas in which NIST intends to develop standards are safety and security to improve the trustworthiness of AI systems among users. In this regard, it notes that standards to maintain the trustworthiness of systems include guidance and requirements for accuracy, explainability, resiliency, safety, reliability, objectivity and security. It states that while network security standards exist, the utility and applicability of these standards should be considered before new standardisation is initiated. It highlights the benefits of technical standard setting, which would provide a clear framework for the design of AI systems that can be easily integrated with other technologies, adoption of best practices for cybersecurity and safety, and adherence to a variety of different technical specifications that maximise their utility. The report also acknowledges that the process of standardisation on aspects such as security is in its formative stages and would benefit from research to provide a strong technical basis for development.

In March 2020, the NSTC’s Networking and Information Technology Research and Development Subcommittee organised an AI and Cybersecurity workshop to assess the key research challenges and opportunities in these areas. An important aspect of the agenda, apart from analysing the use of AI in cybersecurity, was to examine ways to improve the security of AI networks i) by understanding vulnerabilities of the AI systems and ii) to improve the resilience of AI methods and algorithms to various forms of attacks. The report³⁴³ resulting from the workshop points out that there is a need for specification and verification of the AI systems, which means the ability of an AI system to specify what a system is expected to do and how it should respond to an attack. The report states that further research is required on architectural structures and analysis techniques that allow verification of these components. To make AI more trustworthy, optimisation procedures for AI systems must be analysed, and issues such as the manner in which specific data points can influence optimisation should be examined. With regard to the vulnerabilities of the AI systems, the report highlights that such risks can emerge when training data is not representative of the given environment. On the issue of engineering trustworthy AI augmented systems, the report submits that research is needed to develop theory, engineering principles and best practices when using AI as a component of a system. It also recommends researching ‘threat modelling, security tools, domain vulnerabilities, and securing human-machine teaming’. The report recognises the role of the existing cybersecurity network of the country and that this can be put to use once ‘overall system AI vulnerabilities are understood’ and can help in creating ‘robust system architectures that can withstand AI component failures and attacks’ as well as in exploring counter measures.

Notably, there were several attempts to introduce legislation that addresses cybersecurity. At least 38 states, Washington DC and Puerto Rico considered measures that included proposals for training government agencies, increasing penalties for cybercrime (specifically, ransomware), regulating cybersecurity in the insurance industry, encouraging further study into cybersecurity issues and supporting further education and training in cybersecurity. Other issues that were considered included cybersecurity in election processes and access to energy and other critical infrastructure.³⁴⁴

However, the most notable of these efforts was the signing into effect of the IoT Cybersecurity Improvement Act on 4

341. Executive Order on Maintaining American Leadership in Artificial Intelligence, February 2019, available at: <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>

342. NIST, “U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools”, August 2019, available at: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

343. NSTC, Networking & Information Technology Research & Development Subcommittee and Machine Learning & Artificial Intelligence Subcommittee, “Artificial Intelligence and Cybersecurity: Opportunities and Challenges Technical Workshop Summary Report”, March 2020, available at: <https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf>

344. National Conference of State Legislatures, “Cybersecurity Legislation 2020”, September 2020, available at <https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx>

December 2020.³⁴⁵ The law requires, among other things, that NIST develop and publish guidelines for the reporting and disclosure of security vulnerabilities, including for IoT based devices used by federal agencies.³⁴⁶

CHINA

Maturity Index – 3/5

The AIDP released in 2017, envisages an 'initial establishment' of AI security assessment and control capabilities. This would include the formation of AI algorithms and platform security test evaluation methods and establishment of smart robot standard systems and security norms. One of the important goals of the Plan is the creation of an intelligent network security infrastructure. It aims to strengthen AI cybersecurity technology R&D that will further fortify AI products and systems cybersecurity protection. The Plan focuses on network safety and security of AI systems. It aims at constructing a cross-domain AI test platform to promote AI security certification and assessment of AI products.

Further, the Artificial Intelligence Security White Paper³⁴⁷ (**White Paper**) was published in September 2018 by the China Academy of Information and Communications Technology, a research group under Ministry of Industry and Information Technology. The White Paper notes that the nascent nature of AI technology leads to security risks, because of algorithmic inexplicability and heavy dependence on data. The White Paper proposes an AI security architecture covering three dimensions of network security: risks, applications and management. As per the White Paper, AI security risks include cybersecurity risks, data security risks, algorithmic security risks, and information security risks. Cybersecurity risks primarily include exposures in network infrastructure, backdoor security issues, and systemic cybersecurity risks caused by mala fide applications of AI technologies. It recommends the use and application of AI systems in maintaining a secure network because of its 'outstanding data analysis, knowledge extraction, autonomous learning, intelligent decision-making, automatic control, and other capabilities'. In terms of next steps, it suggests further R&D into AI-based technologies and products for the detection of intrusion, malware detection, security situational awareness and early threat warning. The White Paper identified focus areas for further research, which include i) establishment of safety management laws, regulations, and policies for key application domains of AI and prominent security risks; ii) standards and specifications for AI security requirements and security assessments and evaluations; iii) building technological methods such as AI security risk monitoring and early warning, situational awareness, and emergency response; iv) increase the education and training of AI talent to form a stable talent supply; and v) guarantee the secure and controllable development of AI by strengthening research in the 'AI industrial ecology'. The White Paper also made the following recommendations:

1. Increase introduction and absorption of technology with indigenous innovation as the backbone, while augmenting research in AI security technology and improving AI security protection capabilities;
2. Build and enhance the legal architecture to address issues of privacy security risks and subject liability within the purview of AI;
3. Upgrade and amplify supervision and management through improving government's supervision system, optimising administrative framework, constraining enterprise behaviour, and strengthening corporate disciplinary responsibilities;
4. Improve the depth and extent of technology application and product maturity through promoting collaboration and cooperation between AI enterprises, cybersecurity enterprises, and public security enterprises; enhance social governance capabilities;

346. Ionut Arghire, "IoT Cybersecurity Improvement Act Signed into Law", December 2020, available at https://www.securityweek.com/iot-cybersecurity-improvement-act-signed-law?&web_view=true

347. China Academy of Information and Communications Technology, "Artificial Intelligence Security White Paper", 2019, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/>

5. Address both, the impact of AI on human workforce and need of talent in AI technology industry by strengthening the construction of talent corps, optimising personnel training systems, improving job skills of personnel, and reducing unemployment risk caused by AI; and
6. Strengthen technical research cooperation, resolve the current stage's bottlenecks in AI technology, and promote the mature development of AI and actively participate in the formulation of standards to jointly address the security issues.

CANADA

Maturity Index – 3/5

While there is no specific policy paper that addresses network security issues arising from AI, the National Cybersecurity Strategy, 2018³⁴⁸ states that Canada's cybersecurity framework is adaptive to emerging technologies. It mentions that by supporting advanced research, fostering digital innovation and developing cyber skills and knowledge, Canada proposes to position itself as a global leader in cybersecurity. The strategy refers to the Pan-Canadian Artificial Intelligence Strategy as one of the examples of the progress being made in this regard.

Further, the report³⁴⁹ of the Standing Senate Committee on Banking Trade and Commerce released in October 2018, highlights the issue of risks associated with IoT. It mentions that approximately 50% of households use IoT, which includes sensors on roads, autonomous vehicles and other devices with AI capabilities. As such, it recognises the urgency for the federal government to ensure that these devices are safe from intrusions before they are introduced in the market. It also highlights the need for increasing awareness among consumers of the security risks of using AI devices. The 2019 report³⁵⁰ of the Standing Committee on Public Safety and National Security also addressed the issue of cybersecurity in the financial sector. It recognises the dire threat of the malicious use of AI in the financial sector, and that AI for cybersecurity is a 'double-edged sword'. It notes that AI is an essential tool in maintaining a robust cybersecurity system, proposing the concept of a 'centralised AI' that could conduct semi or fully automated responses to cyber threats. Finally, as a matter of recommendation, the Committee suggests that Canadian government must recognise both the 'promise and the peril' of AI in cybersecurity, ensuring that this duality is addressed in its national cybersecurity framework. On the issue of emerging technologies, it also recommends that the 'Standing Committee on Public Safety and National Security should establish a sub-committee dedicated to studying the public safety and national security aspects of cybersecurity, with potential areas of inquiry including international approaches to critical infrastructure protection, impact of emerging technologies, and cyber supply chain security'.

In June 2019, the National Research Council of Canada established an 'innovation hub' in University of Waterloo to make discoveries and advances in AI, IoT and cybersecurity. While its primary focus would be to produce publications and patents, it will also offer various training opportunities to graduate and post-doctoral students to conduct research.³⁵¹

348. Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age", 2018, available at: <https://www.publicsafety.gc.ca/cnt/rsrccs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>

349. Standing Senate Committee on Banking, Trade and Commerce, "Cyber Assault, It Should Keep You Up At Night: Report of the Standing Senate Committee on Banking, Trade and Commerce", October 2018, available at: https://sencanada.ca/content/sen/committee/421/BANC/Reports/BANC_Report_FINAL_e.pdf

350. House of Commons, Standing Committee on Public Safety and National Security, "Cybersecurity in the Financial Sector as a National Security Issue", June 2019, available at: <https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf>

351. Canada.ai, "National Research Council Launches AI, Cybersecurity and IoT hub in Waterloo", June 2019, available at: <http://www.canada.ai/posts/national-research-council-launches-ai-cybersecurity-iot-hub-in-waterloo>

UK

Maturity Index – 4/5

In 2017, the All-Party Parliamentary Group on Artificial Intelligence³⁵² highlighted the need to invest in the physical and digital infrastructure to make it more secure and make the country 'AI-ready'. One of the key points of discussion related to the government's commitment towards providing universal access to reliable and safe physical and digital infrastructure as part of 'Universal Basic Infrastructure'. In this regard, to address the security threats that arise out of the deployment of AI systems, the report emphasised the need to update UK's National Cyber Security Strategy to ready the country for future experiments and experiences with AI.

The Interim Cyber Security Science and Technology Strategy (**CS Strategy**)³⁵³ released by the Cabinet Office in 2017 outlined the risks associated with the use of IoT, machine learning and AI. It specifically discussed the threat of illegitimate use of the vast amounts of data being generated through AI and wearable devices on an ongoing basis. The CS Strategy stressed that the security of such data is paramount and considered the ability of AI and machine learning techniques to analyse this data flow to spot anomalies or threats and further, quickly respond to protect networks before any damage occurs. Additionally, through an improved understanding of human-computer interaction, it notes that advances in cybersecurity using AI should allow cybersecurity experts monitoring the networks to receive the exact information required by them in the most effective way, enabling them to make the right decisions towards the security of data and networks. The CS Strategy further mentioned that to maintain UK's position as a world leader for cybersecurity, it was imperative that the support for growth, research and innovation in cybersecurity be focused in part on emerging technologies that represent the best opportunities, to not only keep the country ahead of all threats but also enable future growth of the cybersecurity sector. Further, the Department for Digital, Culture, Media and Sports (**DCMS**) is the lead government department responsible for the security of consumer internet-connected devices and services and for setting the UK Government's policy position on 'secure by default' products and services. The goal is to incentivise the industries to adopt 'secure by default' design in products and devices so that the chances of device hijacking, data breaches, data leaks and other events that destabilise networks are minimised. In this regard, the CS Strategy suggested that the DCMS undertake a review of the UK Government's role in ensuring the next generation of connected devices and services 'secure by default'.

However, the issue of adversarial users tainting the data sets to wrongly train the AI systems does not find mention in CS Strategy. The Select Committee on Artificial Intelligence in its report³⁵⁴ released in April 2018. The report highlighted the need to sanitise data sets that are used to train AI systems while ensuring that such data is sourced appropriately, to tackle the issue of AI systems being 'attacked' by tainted data. One suggestion from the Select Committee was mandatory third-party validation of AI systems to periodically check their effectiveness, especially in the case of cybersecurity systems which are safeguarding other systems. In this regard, the report recommended that such associated risks must be researched, mapped and incorporated in its final Cyber Security Science and Technology Strategy by the Cabinet and further the research should be translated into guidance. The government later accepted the recommendation in its response³⁵⁵ to the report.

In April 2019, the National Cyber Security Centre released guidance³⁵⁶ for individuals and organisations looking to use off-the-shelf security tools with AI as a core component. The guidance also addressed in-house AI security tools developers and AI deployed in non-security business functions. The guidance aims to help target stakeholders choose between various

352. All-Party Parliamentary Group on Artificial Intelligence Secretariat, "APPG AI Findings 2017", 2017, available at: http://www.appg-ai.org/wp-content/uploads/2017/12/appgai_2017_findings.pdf

353. Cabinet Office, "Interim Cyber Security Science & Technology Strategy: Future-Proofing Cyber Security", 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf

354. House of Lords, Select Committee on Artificial Intelligence, "AI in the UK: Ready, Willing and Able?", April 2018, available at: <https://publications.parliament.uk/pa/ld201719/ldselect/l dai/100/100.pdf>

355. Secretary of State for Business, Energy and Industrial Strategy, "Government Response to House of Lords Artificial Intelligence Select Committee's Report on AI in the UK: Ready, Willing and Able?", June 2018, available at: <https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response.pdf>

356. National Cyber Security Centre, "Intelligent Security Tools", April 2019, available at: <https://www.ncsc.gov.uk/collection/intelligent-security-tools>

AI systems for cybersecurity based on their needs and prescribes guiding principles to understand the data requirements of the tools, costs and risks involved in collecting data and handling data. The handling of data requires the stakeholder to answer questions such as 'will the processing be done within your existing system, in the vendor's system, or on a third-party platform? If your data is sent out, where will it be hosted? Is the processing secure?'; 'what security is applied to data in transit?'; 'will the data be stored by the vendor? How will it be stored?' and 'does this comply with all the data handling requirements for your sector and data type?'.

FRANCE

Maturity Index – 3/5

The report³⁵⁷ that formed the basis for France's AI strategy discusses cyber and network security, emphasising the primacy of integrating security and ethical concerns into AI systems from the start. It notes that integrating such crucial aspects after the fact would potentially require deconstructing the project to a large extent, which may not always be possible. It recommends that AI architects should be trained beforehand to ensure effective processes in the creation of well-rounded AI systems that address the problem at hand, while operating within the purview of what is ethically acceptable and secure. Further, the report suggests that standards, tests and measurement methods must be devised by public authorities to make AI technology more secure, reliable, usable and interoperable. Additionally, the report recognises the existing weakness of today's AI technologies and the subsequent risk attached to its deployment and use. To this end, it suggests that the French National Cybersecurity Agency could be tasked with 'monitoring, foresight and study on the subject of safety and security issues posed by AI', by facilitating a state-level skill network in the fields of cyber defense, defense, and critical systems.

In June 2019, the third Indo-French Bilateral Cyber Dialogue took place in which both countries presented the latest developments in their respective cyber policies, shared their threat analysis and discussed the roadmap for protection of critical national infrastructure.³⁵⁸ In terms of the way forward, the countries decided to work on developing and implementing AI policies/programs for citizen-centric services, data sovereignty from legal, regulatory and cybersecurity perspectives, by making the best use of their expertise and best practices.³⁵⁹

GERMANY

Maturity Index – 3/5

The Cybersecurity Strategy of Germany³⁶⁰ discusses the protection of infrastructure of information systems, while not explicitly highlighting AI systems. It is based on the premise that close coordination is required between various internal and external authorities to make the infrastructure effective and secure. The German National Strategy for AI (German National Strategy), however, addresses the importance of R&D into AI-based technology, to assist in civil security, particularly in inhospitable surroundings such as sites of chemical leaks or natural disasters, etc. Other priorities identified by the National Strategy include identifying manipulated and automatically generated content, buttressing the security of Germany's communications and information system networks (which are stated to be the "...central nervous system of [Germany's] digital economy and society"). The German National Strategy states the intention of the German government to conduct

357. Cedric Villani, "For a Meaningful Artificial Intelligence: Towards a French and European Strategy", March 2018, available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

358. France Diplomacy, "Indo-French Bilateral Cyber Dialogue", June 2019, available at: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19>

359. Ministry of External Affairs, "Indo-French Roadmap on Cybersecurity and Digital Technology", August 2019, available at: <https://mea.gov.in/bilateral-documents.htm?dtl/31757/IndoFrench+Roadmap+on+Cybersecurity+and+Digital+Technology+August+22+2019>

360. Federal Ministry of the Interior, "Cyber Security Strategy of Germany", November 2016, available at: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

further research into using AI-based security systems to spot anomalies and dangers in networks across industries and encourage private and public enterprises to consider security by design as a key element when moving to AI-based systems, especially in key sectors such as healthcare and energy.³⁶¹

ISRAEL

Maturity Index – 3/5

The issue of cybersecurity because of a surge in the usage of AI systems finds its mention in the 2017 report³⁶² published by the Israel Innovation Authority. While the mention is merely limited to the acknowledgement of cybersecurity threats, it reflects that Israeli authorities are not unaware of the associated threats. Moreover, subsequently, the report also mentions that such threats open opportunities for Israel to gain prominence in different markets. In July 2019, the Israel National Cyber Directorate (**INCD**) issued a warning about a cyberattack that can impersonate the high-level functionaries of the companies and commit fraud. Along with the warning, INCD also issues suggestion for taking precautions against such attacks such as – proper training of employees, verifying instructions, using means to prevent misuse of email and carefully observing deviations in the organisation processes.³⁶³ In January 2020, while speaking in a public address, the Director-General of INCD stated that 'artificial intelligence is the new battlefield that will accompany us in the near future', it was reported that he also said that the immediate challenge in front of us is the AI versus adversarial AI.³⁶⁴

RUSSIA

Maturity Index – 3/5

By June 2020, Russia plans to put in place national standards for information security in systems that implement AI technologies.³⁶⁵ One of the primary goals mentioned in the National Strategy of Russia³⁶⁶ on AI is to put together an integrated security system during the creation, development, introduction, and use of AI technologies hinting towards Russia's concern of securing the AI systems. The strategy also directs the development of software that employs AI towards the formulation of 'common standards in the field of security (including fault tolerance) and software compatibility, the development of computing system and software reference architectures, and the identification of software comparison criteria and reference open-source test environment (condition) criteria for the purpose of determining software quality and efficiency'. The strategy, that came in to force in the form of Presidential Decree also calls for the amendment of the national program called 'Digital Economy of Russian Federation' (**Digital Economy**)³⁶⁷ to include AI within its scope. Digital Economy is essentially aimed at creating a safe and powerful infrastructure for high-speed data transfer, processing, and storage which will be made available for all organisations and households of Russia. It is important to note that the even though there was no specific policy paper that could be found that directly addressed the interface of cybersecurity

361. (German) Federal Government, "National Strategy for AI", November 2018, available at www.ki-strategie-deutschland.de

362. Israel Innovation Authority, "Israel Innovation Authority Report 2017", October 2017, available at: <http://economy.gov.il/English/NewsRoom/PressReleases/Documents/2017/IsraellInnovationAuthorityReport.pdf>

363. Express Computer, "Israel Sees Cyberattacks by Voice Impersonating of Senior Staff", July 2019, available at: <https://www.expresscomputer.in/artificial-intelligence-ai/israel-sees-cyber-attacks-by-voice-impersonating-of-senior-staff/37689/>

364. Israel National Cyber Directorate, "Zero Successful Cyberattacks on Critical Nation Infrastructure", January 2020, available at: <https://www.gov.il/en/departments/news/cybertech2020>

365. Kingdom of The Netherlands, "Artificial Intelligence (AI) in Russia", available at: <https://www.rvo.nl/sites/default/files/2019/07/Artificial-intelligence-in-Russia.pdf>

366. Office of the President of the Russian Federation, Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation, October 2019, available at: https://cset.georgetown.edu/wp-content/uploads/t0060_Russia_AI_strategy_EN-1.pdf

367. Russian Federation, "Digital Economy 2024", May 2018, available at: <https://digital.ac.gov.ru/>

and AI, the government is definitely working to improve the information security infrastructure and has also developed a national program in this regard, targeting its implementation by 2024.³⁶⁸ A Technical Committee for Artificial Intelligence Standardisation was also formed in May 2019 to overlook the standardisation work execution of typical architectures of AI systems, data presentation formats in AI systems. The committee will develop indicators and quality criteria of AI systems in order to ensure people's faith in such technologies. It will also work to develop methods for identifying and countering the specific threats to information security of AI automated systems.³⁶⁹

DENMARK

Maturity Index – 3/5

The Danish National Strategy for AI³⁷⁰ states expressly that the government will supplement the principles mentioned in the strategy by carrying out initiatives to strengthen cybersecurity. It discusses various threats that emerge from the use of AI technologies. As per the strategy, AI systems could be manipulated or influenced for malicious use (for example, automating cyber-attacks), while also being crucial in the effort to safeguard critical digital infrastructure and other benefits (for example, developing advanced IT security solutions that can automatically detect new viruses and track novel digital incursion techniques). The strategy, therefore, lists both the limiting of malicious use of AI systems and encouraging the design of AI systems that benefit people and the economy as priorities.

Further, the strategy notes that the government will launch an initiative to support the secure development and deployment of AI, which is to track and analyse potential security risks to authorities and businesses borne out of increased use of artificial intelligence. It will also prepare guidelines to assign specific initiatives to buttress the efforts of authorities and businesses towards IT security and data protection technology. It explains that this initiative should be seen in the context of the government's 2018 National Strategy for Cyber and Information Security³⁷¹ (**Cybersecurity Strategy**). The Cybersecurity Strategy aims at enhancing Denmark's technological preparedness to protect critical IT systems and data. It also requires that public authorities ensure that they are geared to the current threat scenario and be able to coordinate with other agencies both in regard to prevention, and in the event of an actual attack.

EU

Maturity Index – 4/5

The White Paper on Artificial Intelligence³⁷² released by the EU in February 2020 offers some insights on the issue of network security. While it acknowledges that risks pertaining to cyber threats, personal security (on account of newer, wider applications of AI, for example in home appliances) and loss of connectivity exist and emerge due to the use of AI in products and services, it notes that current EU legislation does not explicitly address the matter. It suggests that the EU should employ all resources and tools at its disposal to explore the extent and character of such risks and enhance the

368. Russian Government, "The Passport of the National Program 'Digital Economy of the Russian Federation' is Published" (translated text), February 2019, available at: <http://government.ru/info/35568/>

369. Russian Venture Company, "Technical Committee on Artificial Intelligence Standardization will start its work on the basis of RVC", May 2019, available at: <https://www.rvc.ru/en/press-service/news/company/145233/>

370. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", March 2019, available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

371. Ministry of Finance, "Danish Cyber and Information Security Strategy", 2018, available at: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

372. EC, "White Paper on Artificial Intelligence - A European approach to Excellence and Trust", February 2020, available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

evidence base on potential risks linked to AI applications. For this, it suggested to also use the experience of the EU Agency for Cybersecurity (**ENISA**) in assessing the AI threat landscape.

In the context of AI and network security, ENISA has considered that on the one hand, one needs to consider that AI can be exploited to manipulate expected outcomes, but on the other hand AI techniques can conversely be utilised to support security operations and even to augment adversarial attacks. Before considering using AI as a tool to support cybersecurity, it notes that it is essential to understand what needs to be secured and to develop specific security measures to ensure that AI itself is secure and trustworthy.³⁷³ In June 2019, ENISA organised an event³⁷⁴ on AI and the EU cyber crisis management blueprint in Athens. The intent behind the event was to trigger a dialogue among stakeholders and experts about cyber-crisis cooperation and how AI and machine learning techniques can augment such efforts.

The key themes discussed were:

1. Potential of AI in tackling large-scale cross-border cybersecurity incidents at strategic and political level;
2. Role of AI in addressing challenges faced by global media – spread of misinformation and fake news, and the need to protect free speech;
3. Ability of AI assistance to supplement the capability decision-makers;
4. Role of AI in information fusion at the operation level; and
5. State of advancement and effectiveness of AI in Cyber Autonomous Response, Cyber Threat Detection and Security Automation – areas where AI is used extensively.

In October 2019, ENISA also organised its third annual ENISA-Europol IoT Security Conference,³⁷⁵ and AI was a key matter of discussion. The conference pointed out that 'trust' is one of the biggest concerns brought about by the use of AI and suggested that it was important to secure all future AI deployments in the best way possible. It further indicated that one means to achieve the same could be by establishing a dedicated platform to promote collaboration on the cybersecurity aspects of AI in the EU. In this regard, ENISA can explore its potential to enhance understanding of building blocks of AI and their interplay, engage stakeholders in AI cybersecurity dialogues, encourage collaboration and establish synergies among stakeholders, while raising awareness on AI cybersecurity among all relevant groups. Such efforts will need to be complemented by effective law enforcement in addressing criminal abuse of AI and adversarial AI (for example, data poisoning or algorithm manipulation).

The distinct and indisputable relationship between AI and data governance was also deliberated upon, in that for machine learning algorithms to be effective and unbiased, it is essential to have relevant training data and control over the learning process of the AI system. The conference came to the following conclusions and actionable suggestions:

1. Security concerns need to be integrated from the start in the design of all systems and products – and therefore should not be added as an afterthought in matters of IoT and AI;
2. Inclusion of law enforcement to enable a response beyond defence and incident response, thereby allowing investigation and prosecution of criminals that abuse connected devices;
3. Cooperation between law enforcement and cybersecurity community should be encouraged to address the criminal

373. ENISA, "Artificial Intelligence", available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence?tab=details

374. ENISA, "Artificial Intelligence: An Opportunity for the EU Cyber Crisis Management", June 2019, available at: <https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management>

375. EU Agency for Cybersecurity, Trustworthy AI requires solid cybersecurity, October 2019. Available at: <https://www.enisa.europa.eu/news/enisa-news/trustworthy-ai-requires-solid-cybersecurity>

- abuse and security of AI;
4. Considering the quantum of data collected by these algorithms and its susceptibility to manipulation, the discussion around digital forensics with regards to AI and IoT should be taken up keeping in mind the importance of data and privacy protection;
 5. In addition to horizontal guidelines regarding IoT and AI security, sectoral implementations such as autonomous cars, industrial automation, automation of cybersecurity operations among others, need to be explored. In this regard, guidelines on securing the software development process for IoT, as well as on cybersecurity of autonomous vehicles are expected to be published by ENISA; and
 6. In addressing cybersecurity, the interplay between all other emerging technologies like 5G and cloud computing with AI needs to be considered.

In March 2020, ENISA launched a call for an Ad Hoc Expert Group on AI cybersecurity to bring together a multi-disciplinary group of experts. The scope of this ad hoc working group is to advise ENISA on cybersecurity topics related to AI. The working group published its report on Artificial Intelligence Cybersecurity Challenges in December 2020,³⁷⁶ which has actively mapped the AI cybersecurity ecosystem and its “threat landscape”, which is meant to be a baseline for a common understanding on relevant AI cybersecurity threats. The ENISA AI Threat Landscape provides a framework for future cybersecurity policy initiatives and technical guidelines. It also highlights relevant challenges, such as complexity, technical issues, integrity, confidentiality and privacy. In particular, the report notes the significance of the supply chain related to AI. It highlights the need for an EU ecosystem for secure and trustworthy AI, including all elements of the AI supply chain. It emphasizes the need for the EU secure AI ecosystem to prioritize cybersecurity and data protection and foster relevant innovation, capacity-building, awareness raising and R&D initiatives.

On 16 December 2020, the EU also announced plans to revamp the Network Information System Regulations, 2008, and create an “EU-wide Cyber Shield”, which would link national security authorities and use AI / ML for early detection and defence. The new strategy is also expected to focus on public utilities and infrastructure, as well as the financial markets and the healthcare sector.³⁷⁷

AUSTRALIA

Maturity Index – 3/5

In June 2019, Standards Australia released a report³⁷⁸ following a public consultation on forming standards for AI in Australia. The report highlights that Australia’s e-Safety Commissioner has developed a ‘safety-by-design’ initiative which aims to protect citizens’ safety online. The initiative recognises the importance of considering the safety of AI systems in mind throughout the process of development rather than trying to defensively mitigate harm once an attack has taken place. It highlights that the Department of Home is also looking into the concept of ‘security-by-design’ in areas such as IoT, where AI-based technologies are involved. The report states that standard-setting to further enhance security in the AI industry will be necessary to maintain information security, privacy and safety and ensure that Australia’s systems and networks are secure and resilient. Consequently, Standards Australia envisages active industry participation to ensure the development of comprehensive AI security standards and considers it important that the Australian Government leverages industry best practices in developing its approach in this area.

376. ENISA, “Artificial Intelligence Cybersecurity Challenges”, 15 December 2020, available at https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/at_download/fullReport

377. Associated Press, “EU Unveils Revamp of Cybersecurity Rules Days After Hack”, 16 December 2020, available at https://www.securityweek.com/eu-unveils-revamp-cybersecurity-rules-days-after-hack?web_view=true

378. Standards Australia, “An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard”, February 2020, available at: <https://www.standards.org.au/getmedia/edc81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx>

Australia's policy roadmap for AI³⁷⁹ also identifies cybersecurity as a primary area of concern, noting the inevitability of the use of AI systems by cybercriminals to create new forms of risk and vulnerability. In this light, the roadmap acknowledges that achieving higher levels of cybersecurity, and developing entirely new systems of cybersecurity will be vital for achieving AI enablement of the Australian economy.

JAPAN

Maturity Index – 3/5

The Cybersecurity Strategy of Japan³⁸⁰ released in 2018, takes into account the development of new-age technologies such as AI and IoT. The strategy states that the advancement in technology and growing unification of cyberspace and real space brings as many favourable opportunities as it increases the likelihood of deployment of these very technologies to malicious and dangerous ends. It highlights that malicious actors have an asymmetrical advantage in two ways – that the existing frameworks and guidelines have loopholes and have not yet caught up with the speed at which the technology is developing, and that such malevolent groups have the flexibility to incorporate and make free use of developing technology (like AI and blockchain) to further develop destructive software and products with ease. This advantage is only expected to increase, especially since the formation of a defence depends on existing policies and technological systems. With new technology, it is difficult to precisely define the contours of risks that arise from their malicious use, and therefore it is necessary to develop high-quality products and services that eliminate such cybersecurity risks beforehand. The strategy paper also highlights the growing need to include cybersecurity measures in the process of creating these products and services (security by design). In this regard, the strategy mentions that cybersecurity businesses that provide specific solutions domestically need to be strengthened and extended government support for value creation using advanced technologies by both big companies and innovators.

In addition to this, the government has expressed its intention to work with the private sector to capture and analyse cybersecurity risks, prepare and disseminate guidelines, and promote research and development on risk analysis and threat countermeasures. It is important to note that the strategy emphasises that 'security by design' forms the foundation of all such initiatives. Further, to build a synergistic system where cybersecurity technologies keep pace with the advancement in technology, the government proposes to match enterprises that create novel value using advanced technologies with providers of cybersecurity technologies that support the use of said technologies.

To address the expansive issue of security and AI, the strategy identifies the following measures as being key:

1. Through international cooperation, work against measures inhibiting free trade in the name of cybersecurity and subsequently developing a business environment that facilitates international adoption;
2. Cultivate a shared understanding of the basic principles, objectives, methods, and time limits of measures, and clarify roles and functions of each sector or stakeholder to enable the realisation of the value created by secure IoT systems;
3. Promote stakeholder cooperation to allow synergies to develop in the advancement of technology while promoting autonomous cybersecurity measures;
4. Steadily improve systems to survey and identify vulnerable IoT devices on information and communication networks, and then expeditiously warn users thereof;

379. Hajkowicz SA, Karimi S, et al., "Artificial intelligence: Solving Problems, Growing the Economy and Improving our Quality of Life", CSIRO Data61, 2019, available at: <https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap>

380. Government of Japan, "Cybersecurity Strategy", 2018, available at: <https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf>

5. Work in cooperation with the private sector to promote international standardisation of the basic elements of cybersecurity to aid the development of secure IoT systems; and
6. With inputs from the private sector, list cybersecurity requirements for all categories and kinds of IoT device and then encourage the use of the devices that meet the stated requirements.

SINGAPORE

Maturity Index – 3/5

The Singapore Computer Emergency Response team recognises that from a cybersecurity perspective, AI can be a double-edged sword. It acknowledges that as the deployment of AI systems increase, cyber attackers are likely to use machine learning and AI technology to carry out attacks. On the other hand, it also notes that AI technology can be harnessed to improve their cyber defence capabilities by identifying the specific areas and times wherein the cybersecurity was compromised and to tackle such lapses.³⁸¹

While no further specific discussion appears to have taken place on the issue of cybersecurity or network security, there has been some discussion surrounding policy responses to protecting against vulnerabilities. A paper written by the Civil Service College of Singapore³⁸² discusses the vulnerabilities that the increased use of AI is exposed to, and the new age ‘thinking’ malware that can automatically target vulnerabilities with greater speed and accuracy. It suggests that the answer to these questions lies in harnessing the power of AI to strengthen the existing cybersecurity setups. On the issue of dissemination of fake news, it recommends that AI can help in identifying fake or misleading content as well.

Further, the Cybersecurity Strategy³⁸³ of Singapore also touches upon the intersection of the two and apprises about the government’s vision to invest in new-age technologies such as analytics and automation to bolster digital security infrastructure. This is expected to help maintain and enhance Cyber Watch Centre’s operational excellence and supplement its readiness in timely detection of and response to a cyber incident.

SOUTH KOREA

Maturity Index – 3/5

The Mid to Long Term Plan for AI³⁸⁴ briefly discusses the South Korean position on the intersection of AI and cybersecurity. The government proposes to expand the range of data (including data from AI-based devices such as surveillance cameras, cars, and robots as well as amorphous and irregular data) to be collected in the event of a cyber threat, and further use that data to establish a big-data-based cybersecurity centre. The government also plans to construct a cyber immunity system which would accumulate a wide range of information on different kinds of malicious code and cyber vulnerabilities to train and prepare for cybersecurity breaches. According to the plan, the government also plans to develop a ‘Personal AI Shield’

381. Singapore Computer Emergency Response Team, “Artificial Intelligence and Quantum Computing”, January 2020, available at: <https://www.csa.gov.sg/singcert/publications/jan-2020--artificial-intelligence-and-quantum-computing>

382. Jevon Tan and Rahul Daswani, “Artificial Intelligence: Impact on Public Safety and Security”, November 2019, available at: <https://www.csc.gov.sg/articles/artificial-intelligence-impact-on-public-safety-and-security#notes>

383. Cybersecurity Agency of Singapore, “Singapore’s Cybersecurity Strategy”, 2016, available at: <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>

384. Ministry of Science, ICT and Future Planning, “Mid to Long Term Master Plan in Preparation of the Intelligent Information Society”, July 2017, available at: https://english.mst.go.kr/cms/english/pl/policies2/_icsFiles/afieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

by 2025 that would automatically identify and troubleshoot security threats. The government through its AI plan also intends to develop security chips that can be inserted into devices, thereby ensuring its wide applicability, and may be modified and tailored to different user environments, such as homes and offices. Further, research is proposed to be conducted to ensure that AI systems are picking up the correct types of information to avoid AI systems receiving adversarial training. Finally, through the plan, the government aims to establish counter cyber-attack training facilities and provide machine-learning-based training to the AI developers.

SWEDEN

Maturity Index – 3/5

Sweden National Approach to AI³⁸⁵ touches upon the need to develop and enhance talent, skill and expertise of the workforce in cybersecurity. The report mentions that globally, there already exists stiff competition for qualified people with expertise in AI, and as AI technology gains ground in use and application, the shortage is likely to become more and more tangible. The report, therefore, highlights the importance of investing in training and education in the development and use of AI. The report further discusses that there exist opportunities in the interplay of civil and defence research, within the purview of cybersecurity and autonomous systems which must be explored and seized.

Further, the report³⁸⁶ by Swedish innovation agency, Vinnova states that with the increased deployment of AI across the globe, the risks associated with deliberate misuse and manipulation of data have increased and are expected to become more challenging going forward. It is, therefore, crucial to strategically develop adequate and competitive infrastructure that promotes research, development, and testing of AI applications to establish and maintain the security and integrity of AI systems across various value chains. In this regard, government control has been identified as an indispensable part of enabling value-creating AI development that balances innovation, privacy, ethics and digital security.

FINLAND

Maturity Index – 3/5

The Finnish Cyber Security Strategy³⁸⁷ released in 2019 mentions the importance of cybersecurity in the data economy and for applications that use AI. However, it does not explicitly discuss the application of cybersecurity standards on the AI systems.

Further, while the Ministry of Finance is responsible for the formulation and implementation of digital security policies, provisions and development programmes,³⁸⁸ it does not appear to have issued any specific literature that guides the resolution of various risks and concerns that arise out of the intersection of AI and cybersecurity.

The AI Finland steering group established under a programme by the Ministry of Economic Affairs released a report³⁸⁹ in

385. Government Offices of Sweden, "National Approach to Artificial Intelligence", 2018, available at: <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

386. Vinnova, "Artificial intelligence in Swedish Business and Society - Analysis of Development and Potential", May 2018, available at: https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf

387. The Security Committee, "Finland's Cyber Security Strategy", 2019, available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

388. Finland's Ministry of Finance, "Digital Security: Guidance of Services and Security", available at: <https://vm.fi/en/information-security-and-cybersecurity>

389. Ministry of Economic Affairs and Employment, "Leading the Way into the Age of Artificial Intelligence", June 2019, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf

June 2019 discussing various issues related to the deployment of AI in Finland. On the issue of cyber and network security, the report notes that the Security Committee of Finland is currently in the process of updating the National Cyber Security Strategy with an aim to develop a comprehensive state network security regime that includes the safe use of AI systems.

Further, it discusses the implementation of the Kyber 2020 programme, which is aimed at helping companies and public operators counter cyber threats and to recover from damage caused by cyberattacks. The report also recognises that AI can be used to better digital security infrastructure. However, the possibility of these systems being available to the 'hostile parties' makes it imperative that the misconduct must be prepared for at the design stages. It also divides the risks related to AI into three categories, i.e. (i) malicious use of AI, (ii) influencing AI systems with malicious intent and (iii) fallible AI. To minimise all three types of risks, it mentions the need to develop new tools for evaluation and audit of AI systems, and recommends the following:

1. augment foresight capacity and risk identification in cybersecurity;
2. track all opportunities and threats brought by AI technology and supplement security actions based on national cybersecurity strategy with such observations; and
3. support development of a digital security ecosystem, while aiming to join international networks.

SPAIN

Maturity Index – 3/5

The Spanish National Cybersecurity Institute (**INCIBE**) is responsible for the development of cybersecurity and digital trust in Spain.³⁹⁰ As per the RDI Strategy on AI³⁹¹ released by Spain, the threat of intrusions by cyber-attackers can be tackled by deploying AI. It also notes the necessity to review integrated AI in work elements or devices to increase the safety of operators in confined spaces to avoid collisions or security breaches. In today's globalised world where threats to network security are a major source of concern from a social, economic and political perspective, research and development in AI technologies dedicated to cybersecurity systems to detect and repel threats, through language technologies, image analysis and automatic learning, is considered key. It recognises that automated attacks and so-called "advanced and persistent threats" (**APT**) carried out by AI systems require developments provided by equally advanced defense systems in AI capabilities.

NORWAY

Maturity Index – 3/5

A report³⁹² published by Norwegian Board of Technology discusses the novel and unsolved vulnerabilities that exist in today's AI systems, which need to be addressed before AI systems can be relied on in any serious manner. The report recognises the ability of AI to exceed human performance in multiple ways and scenarios, but at the same time, it cautions against the fact that AI systems could make errors and draw conclusions that humans never would, and that manipulated data would be enough to train an AI system to act maliciously.

390. Spanish National Cyber Security Institute, "What is INCIBE", available at: <https://www.incibe.es/en/what-is-incibe>

391. Ministry of Science, Innovation and Universities, "Spanish RDI Strategy In Artificial Intelligence", 2019, available at: http://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_EN.PDF

392. The Norwegian Board of Technology, "Artificial Intelligence: Opportunities, Challenges and a Plan for Norway", September 2018, available at: <https://teknologiradet.no/wp-content/uploads/sites/105/2018/11/AI-and-machine-learning-1.pdf>

The Norwegian Strategy for AI³⁹³ recognises that establishing and maintaining a well-functioning digital society requires pre-emptively addressing potential cyber threats and minimising the risks that adverse cyber incidents may cause to the society. Considering this, the Norwegian government acknowledges cyber security as a priority area in its deliberations and discussions. The Norwegian Strategy also notes that in January 2019, the Government presented a National Strategy for Cyber Security that defined the following goals for its five priority areas:

1. digitisation by Norwegian companies should follow all protocols to ensure security and the organisations should continuously work towards safeguarding against cyber threats;
2. a robust and reliable digital infrastructure should be built to aid critical societal functions;
3. society's needs should remain the key consideration in developing the country's cybersecurity competence;
4. Norwegian society should collectively strive towards improving capacity and capability to both, detect and manage cyber-attacks; and
5. Norwegian police should build capacity to combat cyber-crime.

As per the National Strategy, the Ministry of Justice and Public Security and the Ministry of Defence have overarching responsibility for following up the National Cyber Security Strategy for Norway, while sector-specific ministries are responsible for ensuring that the strategy's priorities and measures are followed up in their respective sectors. The strategy notes that while the intersection of cybersecurity and AI has two aspects - security in solutions based on AI, and solutions based on AI for enhanced cybersecurity, the competence needs in both these areas largely overlap. At the same time, it highlights the need for 'in-depth specialisation in security architecture for protecting AI systems, and for specialisation in algorithms/big data for using AI to protect IT systems and society'. It further explains that AI systems not only inherit vulnerabilities of the conventional technology which is used as a base for the AI system (sensors, communication networks, big data et cetera) but also introduce new vulnerabilities as part of the new AI-based solution. In this respect, AI systems are quite like conventional IT systems and therefore, a structured and holistic approach to cybersecurity is needed before such systems are deployed and used.

ESTONIA

Maturity Index – 2/5

Estonia has been harnessing the importance of training its workforce to take care of the 'cyber hygiene'³⁹⁴ as businesses and public administration offices are required to undergo training and evaluate the extent of to which their systems were protected. The test was initiated by Estonian Ministry of Defence as a measure to improve cybersecurity.³⁹⁵ However, apart from this, there does not appear to be any specific guidance with respect to AI and cybersecurity.

393. Norwegian Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence", 2019, available at: https://www.regeringen.no/contentassets/1febbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

394. Cyber Hygiene refers to the discipline of using interconnected systems through internet in a way that is safe and avoid malicious content that is spread on internet.

395. Invest in Estonia, "How Estonia uses Cyber Hygiene as a Cornerstone of Cyber Security", June 2018, available at: <https://investinestonia.com/how-estonia-uses-cyber-hygiene-as-the-cornerstone-of-cyber-security/>

THE NETHERLANDS

Maturity Index – 2/5

The Netherlands' Strategic Plan for AI, 2019³⁹⁶ does recognise the perils of the use of AI systems with mala fide intent. It is, for this reason, it propounds that the 'cybersecurity by design' should be a guiding principle for the development of AI systems. Further, the Strategic Plan notes that in the Dutch Cyber Security Agenda, AI is mentioned as a 'technological and societal development' that can present opportunities as well as risks in the cyber world. It highlights that the existing measures for cybersecurity are inadequate and states that AI will play a major role in improving the cybersecurity. It also presents the example of automatic source code analysis that is used to detect errors, viruses and anomalies in networks. As a matter of action, the strategic plan notes that the Cyber Security Council has commissioned further research into the use of AI and other emerging technologies for cyber defence.

UAE

Maturity Index – 2/5

In November 2019, the Dubai Electronic Security Centre in collaboration with Institute of Electrical and Electronics Engineers organised a conference on 'AI and the Future of Cybersecurity'. The aim of the conference was to discuss the impact of AI on the cybersecurity.³⁹⁷ After the release of UAE's national strategy on AI, it was reported that at an initial level, cybersecurity would be one of the primary focus areas in the context of AI.³⁹⁸ Various important functionaries of UAE seem to be recognising the importance of cybersecurity for AI systems as is clear from the statement of Minister of State for AI in which he said 'disappointment by governments to take proactive measures to ensure the security of AI frameworks "is going to come back to bite us".³⁹⁹ No other specific guidance or policy documents appear to be available in respect of the UAE government's position on cybersecurity and AI.

HONG KONG

Maturity Index – 2/5

The Hong Kong Monetary Authority released guidelines in November 2019⁴⁰⁰ pertaining to the use of AI systems in the banking and finance sector that contains some guidance on cybersecurity. The guidelines acknowledge that the use of AI systems could expose banks to various cyber threats, such as data poisoning and adversarial attacks, which exploit AI models through data manipulation. The guidelines direct banks to ensure that their security controls can effectively deal with such attacks. Further, the guidelines require banks to stay aware of emerging threats and the defence measures that can be adopted to curtail such threats.

396. Government of The Netherlands, "Strategic Action Plan for Artificial Intelligence", October 2019, available at: <https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence>

397. Institute of Electrical and Electronic Engineers, United Arab Emirates, "IEEE UAE Cyber Intelligence Summit", 2019, available at: <https://ieee.ae/en/cybersecurity/>

398. Priya Dialani,"Artificial Intelligence Strategy of UAE", October 2019, available at: <https://www.analyticsinsight.net/artificial-intelligence-strategy-of-uae/>

399. ELE Times, "The Crucial Role of Cybersecurity and Artificial Intelligence", December 2019, available at: <https://www.eletimes.com/role-of-cyber-security-and-artificial-intelligence>

400. Hong Kong Monetary Authority, "High Level Principles of Artificial Intelligence", November 2019, available at: <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf>

In another white paper⁴⁰¹ published by the Hong Kong Monetary Authority, it is recommended that banks ensure that their AI systems are safe from cybersecurity lapses. To that end, it suggests that Intelligent Process Automation (**IPA**) be used to understand the user behaviour in order to discover security loopholes in an application, IT infrastructure or operational process. It further recommends that the banks must apply IPAs on the AI systems before rolling them out to prevent the possibility of a zero-day attack.⁴⁰²

401. Hong Kong Monetary Authority, "Reshaping Banking with Artificial Intelligence", available at: https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf

402. Zero-day attack is a cyberattack that is inflicted upon a system the moment it is operational and is most vulnerable, because of the absence of assistance applications that help prevent such attacks.



ETHICS & HUMAN RIGHTS

As AI systems continue to be deployed in a number of sectors that have an impact on the social, economic and political structure of society (prompting experts to declare a “Fourth Industrial Revolution”),⁴⁰³ the question of whether AI is “good” or “bad” for humankind continues to be debated. Some issues that arise for consideration are: will we face mass-scale unemployment due to AI systems replacing humans? how to avoid AI being used for inappropriate or dangerous purposes? the impact of AI on human dignity and personhood?⁴⁰⁴ and the implications of private and/or public ownership of AI systems on society’s structure⁴⁰⁵ Issues such as manipulating information in the run up to elections and potential hacking into the election process itself are now becoming realities that democracies have to contend with.⁴⁰⁶ According to the World Economic Forum, unemployment, inequality, racism, security and the rights of a robot are some of the ethical concerns raised by the existence of AI systems.⁴⁰⁷ Some of these questions are being considered by national and international organizations of late, as part of an examination of policy to govern AI systems. The private sector is also putting out its views, along with industry associations and non-profits.⁴⁰⁸ For instance, private companies like Microsoft⁴⁰⁹, Google⁴¹⁰, SAP⁴¹¹ and IBM⁴¹² have also formulated ethics guidelines to be considered while developing AI systems. Considering the scale and reach of these companies, and the fact that they are

at the forefront of the development of AI technology, the perspectives of private companies on the ethical principles governing the use of AI systems is valuable.

The calls for ethical principles to guide AI converge around the following principles, although the discussion around each of these principles may vary in terms of their exact constituents and the context in which each is prioritised:⁴¹³

1. Transparency - transparency is typically broken down into improving explainability and ensuring disclosure, and in the areas of data use, human-AI interaction, automated decision-making and understanding the purpose of AI systems, primarily with a view to increase trust in AI systems and as an important step to protect legal rights while using AI systems. There is a push to greater disclosure, in a manner that is understandable by non-experts, although the understanding of what may be disclosed is still uncertain, given the push to protect intellectual property rights of the developers of AI systems.⁴¹⁴
2. Justice and fairness – the focus in this category is typically fairness or prevention of bias or discrimination,⁴¹⁵ but in some cases, discussion has extended to the impact of AI on diversity,

403. World Economic Forum, “The Fourth Industrial Revolution”, 2016, available at: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

404. Stuart Russel and Peter Norvig, “Artificial Intelligence: A Modern Approach”, Pearson Education Limited, 2016.

405. Ian Bogost, “Why Zuckerberg and Musk are Fighting About the Robot Future”, The Atlantic, July 2017, available at <https://www.theatlantic.com/technology/archive/2017/07/musk-vs-zuck/535077/>

406. Kathleen Walch, “Ethical Concerns of AI”, Forbes, December 2019, available at: <https://www.forbes.com/sites/cognitiveworld/2020/12/29/ethical-concerns-of-ai/#40a9336123a8>

407. World Economic Forum, “Top 10 Ethical Issues in Artificial Intelligence”, available at: <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/>

408. Anna Jobin, Marcello Lenca, Effy Vayena, “Artificial Intelligence: The Global Landscape of Ethics Guidelines”, Health Ethics & Policy Lab, 2019, available at: <https://arxiv.org/ftp/arxiv/papers/1906/1906.11668.pdf>

409. Microsoft, “Responsible AI: Microsoft AI Principles”, available at <https://www.microsoft.com/en-us/ai/responsible-ai>

410. Google PAIR, “People + AI Guidebook”, May 2019, available at <https://pair.withgoogle.com/guidebook/>

411. SAP AI Ethics Steering Committee, “SAP’s Guiding Principles for Artificial Intelligence”, September 2018, available at <https://www.sap.com/products/intelligent-technologies/artificial-intelligence/ai-ethics.html?pdf-asset=940c6047-1c7d-0010-87a3-c30de2ffd8ff&page=1>

412. IBM, “Data Responsibility: IBM’s Principles for Trust and Transparency”, May 2018, available at <https://www.ibm.com/blogs/policy/trust-principles/>

413. Ibid.

414. Ibid, page 8-13.

415. For instance, see the Open Letter to ‘Springer Nature’ signed by close to 2500 researchers to prevent the publication of research on crime prediction software. Coalition for Critical Technology, “Abolish the #CrimeToPrison Pipeline”, Medium, June 2020, available at: <https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techttoprisonpipeline-9b5b14366b16>

the labour market, democratic governance, due process rights, etc. There have been suggestions to improve AI systems in these areas by incorporating these norms into technical standards and codes; increasing transparency; increasing public awareness and education about the possible influences of AI systems on rights; increased auditing or monitoring of AI systems' performance; strengthening existing legal systems to account for the issues that arise from AI systems, etc.

3. Non-malfeasance – the discussion around this principle has largely pertaining to the need for security and safety in the deployment of AI systems, i.e., that AI systems should not cause any foreseeable or unintentional harm. More specifically, these discussions have considered cybersecurity threats such as hacking, and the risk that technology advancements may outpace the ability to regulate. The various kinds of harm that have been considered are erosion of privacy, safety, negative impact on social well-being, and even physical harm. Proposed solutions include interventions in AI at the design stage, including privacy by design, multidisciplinary cooperation, establishing industry standards, increased oversight, etc.

4. Responsibility and accountability – the discussion relating to these principles have been quite varied, including recommendations on integrity, clarification on liability, and providing for remedies where AI systems could potentially cause harm. There is also lack of clarity on whether there is a difference in the way accountability is considered in the case of AI systems vis-à-vis humans.

5. Privacy – in the case of privacy, most jurisdictions connect the discussion to the right to privacy, which must be protected, and the issue is generally presented as a data protection or data security issue. In terms of potential solutions, stakeholders have considered privacy by design, differential privacy, data minimization and access control. There have been calls for privacy laws to adapt to AI.

6. Beneficence – this principle relates to the

promotion of wellbeing, peace and happiness, the creation of socio-economic opportunities and economic prosperity, for all people or all society.

7. Freedom and autonomy – the discussion around freedom and autonomy relates to measures ensuring that users are at the core of the system, protecting the freedom of expression, informational self-determination, freedom to use different platforms and other aspects of positive freedom. However, in some cases, freedom and autonomy has been interpreted to mean negative aspects of freedom as well, such as the freedom against technological experimentation, manipulation and surveillance. In most cases, freedom is believed to be served by ensuring that individuals have sufficient options and information about AI and its interactions with the world.
8. Trust – discussions around the principle of trust have typically involved ensuring trust in AI systems from users and society in general. This is ensured through other aspects mentioned above, such as accountability, explainability, transparency, etc. as a means to fulfil public expectations.
9. Dignity – dignity is discussed purely in the context of human beings, and that AI systems should be constructed such that they do not destroy, diminish or reduce human dignity in any way, and on the contrary, work to preserve and promote human dignity.
10. Sustainability – the idea of sustainability is referenced in the context of developing and using AI to protect the environment, contribute to fairer and more equal societies, and create systems that are sustainable and endure over time.
11. Solidarity – the principle of solidarity has been discussed as a fallout of AI systems on the labour market, and with the push for a strong safety net. The goal with this principle is to push for greater protections for vulnerable groups and ensure that AI does not destabilize social cohesion.

One of the most prominent AI ethics guidelines are the

OECD Principles on AI⁴¹⁶ in 2019 that formed the base for the human-centred principles⁴¹⁷ adopted in the G-20 Summit also in 2019. Both the instruments present a list of five principles that were adopted by the member nations, that included human-centred values and fairness, transparency and explainability, robustness, security and safety and accountability.

Similarly, the Global Partnership on AI (**GPAI**) was established in June 2020, with a view to support the responsible and human-centric development and use of AI in a manner consistent with human rights, fundamental freedoms, and our shared democratic values, as elaborated in the OECD Recommendations on AI. The GPAI proposes to involve multiple stakeholders across industry, civil society, governments and academia to collaborate across four Working Groups – (a) Responsible AI; (b) Data Governance; (c) the Future of Work; and (d) Innovation & Commercialisation. One of the first priorities of the GPAI is to consider how AI can be used to better respond to the COVID-19 pandemic. The GPAI is to comprise a Secretariat hosted by the OECD, along with two Centres of Expertise. The first GPAI

Multistakeholder Experts Group Plenary is proposed to be held in December 2020 and hosted in Canada.⁴¹⁸

As is evident from the above discussion, AI ethics initiatives have largely generated vague, high-level principles and value statements that do not translate to very specific recommendations. The next concrete step from a policy perspective would be for international and national bodies to

filter down these principles into concrete actionable form, that balances, to the extent possible, the business needs of private parties with the larger social good.⁴¹⁹ With greater scrutiny of big tech firms across major jurisdictions such as the EU, US and Australia, it is likely that these principles will filter down into specific mandates or guidelines in the digital services market in the near future.

This report maps the discussions or frameworks that have been adopted by the governments of various nations to address the ethical issues around the AI systems and technology.

416. OECD, "Recommendations of the Council on Artificial Intelligence", 2019, available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

417. G20 Ministerial Statement on Trade and Digital Economy, June 2019, available at: <https://www.mofa.go.jp/files/000486596.pdf>

418. GPAI, "Joint Announcement from the Founding Members of the Global Partnership on Artificial Intelligence", June 2020, available at <https://www.canada.ca/en/innovation-science-economic-development/news/2020/06/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence.html>

419. Brent Mittelstadt, "Principles Alone Cannot Guarantee Ethical AI", Nature Machine Intelligence, November 2019, available at: <https://ssrn.com/abstract=3391293>

MATURITY INDEX

ETHICS & HUMAN RIGHTS



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Spain

India, China, France, Germany,
Russia, Denmark, Australia, South Korea,
Sweden, Finland, Norway, Estonia, The Netherlands

Level 4

Policy
Recommendation

USA, Canada, UK, EU, Japan, Singapore,
UAE, Hong Kong

Level 5

Implementation into
Legislation



INDIA

Maturity Index – 3/5

The Ministry of Electronics and Information Technology report⁴²⁰ on cyber security, safety, legal and ethical issues provide a well-rounded analysis on the issues relating to social impact of AI. The report examines various ethical issues such as bias and observes that while the existence of bias in AI outcomes is a risk, this can be addressed through correcting for bias in non-algorithmic decisions that can be deployed appropriately. To this end, the report explains that understanding the decision-making process by examining the underlying factors that lead the AI systems to make biased decisions is important. It further recommends the establishment of a flexible framework for assessing the appropriate scope and technical feasibility of various accountability mechanisms.

An AI Task Force constituted by the Ministry of Commerce and Industry in 2017 looked at AI as a socio-economic problem solver at scale. In its report⁴²¹ the taskforce prescribes various principles that must be followed by the AI systems that are developed, which include transparency and explainability of AI systems, data protection, safety and security. It also makes the case for promoting interdisciplinary research for AI and human interactions and makes a crucial point about withholding the roll out of complete autonomy for weaponized platforms.

A National Strategy for Artificial Intelligence⁴²² was published in 2018 that examined AI as a lever for economic growth, social development, and considers India as a potential 'garage' for AI applications. The strategy also acknowledges the importance of transparency and explainability of AI and touches upon the elimination of bias and discrimination that may arise in the outcomes delivered by AI systems. The strategy notes the pitfalls of data selection bias, which could result in discrimination in the AI models. To that end, it also acknowledges that the issue of fairness is at the forefront of discussion in academic, research and policy fora, and requires a combined deliberation and sustained research to come to an acceptable resolution. It further suggests that one possible way to approach this would be to identify the in-built biases and assess their impact, and in turn find ways to reduce bias.

India is already moving towards deploying AI-assisted systems at the State or city level, that may affect the right to life and liberty as well as the freedom of expression. For instance, in 2013, Network Traffic Analysis⁴²³ developed by DRDO was launched as an internet monitoring system capable of scanning through internet data and detecting suspicious words. The intent as stated was to protect national security and to observe internet activities and trends of suspicious people, businesses and organization. Further, in 2015, the Delhi Police took a definitive step towards predictive policing by operationalizing Crime Mapping, Analytics and Predictive Systems (**CMAFS**), in partnership with Indian Space Research Organisation. CMAFS allows the identification and tracking of both reported and non-reported crimes for generating crime analytics, identifying hotspots, VIP target threat rating etc.⁴²⁴ In 2019, the Gujarat International Finance Tec-City deployed video analytics for indoor and outdoor security monitoring, which allows it to mark virtual 'restricted areas' and monitor trespass or suspicious activity across the boundaries.⁴²⁵ The Uttar Pradesh government has also deployed surveillance systems across 70 prisons to track security breaches and acts of violence among inmates.⁴²⁶ The Nenusaitham Project

420. Ministry of Electronics and Information Technology, "Report of Committee D on Cyber Security, Safety, Legal and Ethical Issues", available at: https://meity.gov.in/writereaddata/files/Committee_D-Cyber-n-Legal-and-Ethical.pdf

421. Ministry of Commerce and Industry, "Report of the Artificial Intelligence Task Force", 2018, available at: https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf

422. NITI Aayog, "National Strategy for Artificial Intelligence", 2018, available at: https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

423. Hemant Singh, "List of Top 5 Indigenously Developed Weapons/Systems of India", October 2019, available at: https://www.drdo.gov.in/sites/default/files/drdo-news-documents/DRDO_News_18_Oct_2019.pdf

424. Delhi Police, "Commissioner's Report 2015", available at: <http://delhipolice.nic.in/CP%20Forward2015.pdf>

425. AllGoVision, "Case Study: GIFT City", available at: <https://www.allgovision.com/case-study-gift-city.php>

426. "UP is using AI 'JARVIS' in prisons", Economic Times, November 2019, available at: <https://cio.economictimes.indiatimes.com/news/strategy-and-management/up-is-using-ai-jarvis-in-prisons/71969513>

by the Hyderabad Police is another example of deploying CCTV cameras and video analytics to aid in real time detection of crimes and traffic violations. Introduced in 2018, the software encourages communities to set up their own surveillance system which will be integrated with the nearest police station.⁴²⁷ Similar technologies have become increasingly pertinent as a result of COVID-19, from a public health perspective. Public places, such as Mumbai's Chhatrapati Shivaji Maharaj Terminus have introduced non-intrusive thermal scanners to detect passengers travelling with a high fever.⁴²⁸ However, it remains to be seen whether there will be any action to align action in these cases with the ethical principles outlined in respect of AI systems.

USA

Maturity Index – 4/5

The AI Executive Order⁴²⁹ creates an American AI Initiative guided by five high level principles and to be implemented by the NSTC Select Committee on Artificial Intelligence. These principles include the US driving development of appropriate technical standards and protecting 'civil liberties, privacy and American values' in AI applications to fully realize the potential for AI technologies for the American people.

Furthermore, executive departments and agencies that engage in AI related activities such as developing it, providing educational grants and regulating and providing guidance for applications of AI technologies must adhere to six strategic objectives including protection of 'American technology, economic and national security, civil liberties, privacy, and values' and ensuring that technical standards for AI 'minimize vulnerability to attacks from malicious actors and reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies; and develop international standards to promote and protect those priorities'. The AI Executive Order also acknowledges that the government plays an important role in training people for a changing workforce.

Post the constitution of Joint AI Center⁴³⁰ to explore the agency's use of AI, the Defense Innovation Board of the US Department of Defense (**US DoD**) released the AI Principles⁴³¹ to provide ethical recommendations to the US DoD in November 2019. The principles are again a guidance document and require that the Department's use of AI must align with the principles of responsibility, equitability, traceability, reliability and governability. It further lays out a list of twelve recommendations to put above mentioned principles into action.

The House of Representatives also adopted a resolution⁴³² to support the development of guidelines for ethical development of AI in consultation with diverse stakeholders with a ten-fold aim of engagement among industry, government, academia, and civil society; transparency and explainability of AI systems, processes, and implications; helping to empower women and underrepresented or marginalized populations; information privacy and the protection of one's personal data; career opportunity to find meaningful work and maintain a livelihood; accountability and oversight for all automated decision

427. Smart Cities Council, "See How Video Analytics Help Track Criminal Activities", November 2018, available at <https://india-smartcouncil.com/article/see-how-video-analytics-help-track-criminal-activities/>; and Express Computer, "Axis Communications Shares Implementation Details of Smart Cities at Axis Solutions Day 2018", August 2018, available at <https://www.expresscomputer.in/news/axis-communications-shares-implementation-details-of-smart-cities-at-axis-solutions-day-2018/27858/>

428. NDTV, "Artificial Intelligence-Based COVID-19 Screening Started at Mumbai Stations", June 2020, available at: <https://www.ndtv.com/mumbai-news/coronavirus-artificial-intelligence-based-covid-19-screening-started-at-mumbai-stations-2245910>

429. Executive order on Maintaining American Leadership in Artificial Intelligence, February 2019, available at: <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>

430. Chief Information Officer, Department of Defence, "Vision: Transform the DoD Through Artificial Intelligence", available at <https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/>

431. Defense Innovation Board, Department of Defense, "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense", November 2019, available at: https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF

432. 116th CONGRESS, H. RES. 153, February 2019, available at: <https://www.congress.gov/bill/116th-congress/house-resolution/153/text>

making; lifelong learning in STEM, social sciences, and humanities; access and fairness regarding technological services and benefits; interdisciplinary research about AI that is safe and beneficial and safety, security, and control of AI systems now and in the future.

In an example of implementation of ethical principles to the enforcement of AI, in 2017, New York City passed a law⁴³³ that aims to ensure that algorithms used by city agencies are transparent, fair, and valid by setting up a task force to make recommendations on algorithmic regulation, transparency, and bias. While these rules apply only to New York, this move to regulate AI may become a model for other cities or states in the US.

As mentioned earlier, private companies that are engaged in the development of AI-based technologies have also taken principled stands on the manner in which such technology is deployed. For instance, employees across Google, Microsoft⁴³⁴ and Amazon⁴³⁵ have protested on the weaponisation of AI technology and its use in warfare. Employee protests prompted Google to refuse the renewal of its contract with the Pentagon on Project Maven, aimed to improve accuracy of drone strikes.⁴³⁶ Similarly, IBM discontinued the development of its facial recognition software in the wake of rampant racial profiling.⁴³⁷ The impact of data collection and processing by digital platforms on the rights of individual users was also highlighted in the House Judiciary Committee report,⁴³⁸ issued in October 2020.

CHINA

Maturity Index – 3/5

In May 2019, the Beijing AI Principles⁴³⁹ were released by the Beijing Academy of Artificial Intelligence, which depicted the core of its AI development as the realization of beneficial AI for humankind and nature. In addition, the Principles considered that:

1. AI should be designed and developed to promote the progress of society and human civilization, avoiding the negative implications of 'malicious AI race' by promoting cooperation, also on a global level;
2. the R&D of AI should serve humanity and conform to human values as well as the overall interests of humankind. Human privacy, dignity, freedom, autonomy, and rights should be sufficiently respected;
3. researchers and developers of AI should have sufficient considerations for the potential ethical, legal, and social impacts and risks brought in by their products and take concrete actions to reduce and avoid them; and
4. the development of AI should reflect diversity and inclusiveness, and be designed to benefit as many people as possible, especially those who would otherwise be easily neglected or underrepresented in AI applications.

433. The New York City Council, "Automated Decision Systems Used by Agencies", 2018/049, available at: <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0>

434. Margi Murphy, "Microsoft Workers Protest Bid to Build Pentagon's \$10bn AI Warfare System", The Telegraph, June 2018, available at: <https://www.telegraph.co.uk/technology/2018/10/13/microsoft-workers-protest-bid-build-pentagons-10bn-ai-warfare/>

435. Anthony Cuthbertson, "Microsoft and Amazon Workers Protest Firms' Military AI Contract and 'Authoritarian Surveillance' Tech", The Independent, October 2018, available at: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-amazon-military-ai-protest-workers-jedi-rekognition-contract-pentagon-a8590016.html>

436. Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees", The New York Times, June 2018, available at: <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>

437. Hasan Chowdhury, "IBM scraps Facial Recognition Tool in Wake of Black Lives Matter protests", The Telegraph, June 2020, available at: <https://www.telegraph.co.uk/technology/2020/06/09/ibm-scrap-facial-recognition-tool-wake-black-lives-matter-protests/>

438. US House of Congress Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations", October 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

439. Beijing Academy of Artificial Intelligence, "Beijing AI Principles", May 2019, available at: <https://www.baai.ac.cn/blog/beijing-ai-principles>

Another group comprising top Chinese universities and companies and led by the Ministry of Industry and Information Technology's China Academy of Information and Communications Technology, the Artificial Intelligence Industry Alliance, released its Joint Pledge⁴⁴⁰ on Self Discipline in the Artificial Intelligence Industry. While the wording of the pledge is fairly generic, it points to the language of 'secure/safe and controllable' and 'self-discipline' as 'meshing with broader trends in Chinese digital governance'.

Finally, an expert group formed of researchers at Chinese universities and established by the Chinese Government Ministry of Science and Technology released its eight Governance Principles⁴⁴¹ for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence in June 2019. International co-operation is emphasised in the principles, including along with 'full respect' for AI development in other countries. A possibly novel inclusion is the idea of 'agile governance', so that problems arising from AI can be addressed and resolved in a timely manner. This principle reflects the challenge of rapid development in the field of AI that cannot be exactly resolved relying on the conventional governance structures. Other principles that deal with the ethical aspects of AI are harmony and friendliness; fairness and justice; inclusivity and sharing and respect for privacy; safety and controllability; shared responsibility and open collaboration.

CANADA

Maturity Index – 4/5

The Canadian government began looking into ethics in AI in 2018, by examining the integrity of data storage at the Department of National Defence.⁴⁴² A team was formed that was led by the Chief Information Officer of Canada and laid the groundwork for the Directive on Automated Decision Making.⁴⁴³ The objective of the directive was to ensure that automated decision systems are deployed in manner that leads to efficient, accurate, consistent and interpretable decisions made in line with Canadian law. This would require assessing the impact of algorithms on decision making so that the negative outcomes can be eliminated. However, the scope of the directive was restricted to the administrative decisions of the government only.

The directive also introduced the concept of Algorithmic Impact Assessment (**AIA**) wherein all the government and private players can assess the impact of the algorithms by answering a questionnaire with sixty questions that assess if the algorithms are delivering outcomes that are not counterproductive to the human ethics. The AIA looks into issues such as the extent of human intervention in the process of decision-making and whether there has been post facto analysis of processes to address data quality issues.⁴⁴⁴

While there does not appear to be any overarching policy discussion on how AI systems could interact with fundamental freedoms and rights, there have been local efforts in Canada that have begun to use AI in policing. For example, the Ottawa Police Strategic Operations Centre (**OPSOC**) was launched in 2018 with the aim of proactive community policing by leveraging data collected through multiple means including community inputs. The intent is to enable crime analysts at OPSOC to understand emerging trends and effectively and pre-emptively deploy resources while offering enhanced intelligence to road patrol for tactical and strategic coordination in reducing crime. While the goal with this initiative appears

440. China Academy of Information and Communications Technology, "The Artificial Intelligence Industry Alliance, Joint Pledge on Artificial Intelligence Industry Self Discipline", May 2019, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-ai-alliance-drafts-self-discipline-joint-pledge/>

441. National New Generation Artificial Intelligence Governance Expert Committee, "Governance Principles for New Generation Artificial Intelligence: Develop Responsible Artificial Intelligence", June 2019, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/>

442. Max Greenwood, "Canada's New Federal Directive Makes Ethical AI a National Issue", June 2019, available at <http://www.canada.ai/posts/canadas-new-federal-directive-makes-ethical-ai-a-national-issue>

443. Treasury Board of Canada Secretariat, "Directive on Automated Decision Making", 2019, available at: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>

444. Supra note 406.

to be sharing information that would help with quicker deployment of resources, it remains to be seen where the line is to be drawn between greater surveillance and promoting community safety.⁴⁴⁵

UK

Maturity Index – 4/5

In its 2017 Industrial Strategy⁴⁴⁶, the UK Government identified 'putting the UK at the forefront of the AI and data revolution' as one of four main challenges for the country. The UK government also proclaimed its vision that the UK 'will lead the world in safe and ethical use of data and AI giving confidence and clarity to citizens and business', including by setting up a Centre for Data Ethics and Innovation as an advisory body.

The UK Parliament has also been active in its consideration of AI governance and ethics issues. An All-Party Parliamentary Group on AI was set up in 2017, and one of its recommendations⁴⁴⁷ was to incentivise the corporate 'Ethics Boards' inside organisational structures to improve the transparency of innovations made by the organisations in the field of AI. The report also brought to light the need for an international forum on AI Global Governance to horizon scan the future of AI technologies and its effect of AI use, AI commerce and wider ethical and welfare implications.

A Select Committee on AI was also formed to look into emerging AI and ethics issues. The committee recommended that it was necessary to introduce AI-specific regulation at this point in time but advocated for further work to be done assessing how further additions can be made to existing legal and regulatory frameworks to deal with AI. The report recommended non-legally binding overarching principles that incorporated general ethical principles like common good of humanity, transparency and fairness, as the basis for a possible cross-sector AI code that it suggested being formulated and developed by the Centre for Data Ethics and Innovation.⁴⁴⁸

On the issue of bias and discrimination, the committee observed that the current generation of deep learning-based AI systems are trained by feeding data sets into them and these data sets can be myopic in their coverage of diverse and different demography that can lead to the problem of biased and discriminative outcomes. Therefore, the committee recommends that the Industrial Strategy Challenge Fund specifically work towards stimulating the creation of systems for testing and training datasets to ensure they represent diverse populations and prevent them from giving prejudicial outcomes.⁴⁴⁹

The UK government also appears to acknowledge the effect of deployment of AI and other automated systems on the labour market. To this end in 2017, the government announced the National Retraining Scheme⁴⁵⁰ to help adults retrain into better jobs, and be ready for future changes to the economy, including those brought about by automation.

On the question of use of AI in policing, a report by the Royal United Services Institute for Defence and Security Studies⁴⁵¹

445. Ottawa Police, "Annual Report, 2016", available at: <https://www.ottawapolice.ca/en/annual-report-2016/OPSOC.aspx>

446. Government of UK, "Industrial Strategy: Building a Britain fit for the Future", November 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730048/industrial-strategy-white-paper-web-ready-a4-version.pdf

447. All-Party Parliamentary Group on Artificial Intelligence, "APPG AI Findings 2017", available at: http://www.appg-ai.org/wp-content/uploads/2017/12/appgai_2017_findings.pdf

448. Select Committee on Artificial Intelligence, "AI in the UK: Ready, Willing and Able?", April 2018, available at: <https://publications.parliament.uk/pa/ld201719/ldselect/l dai/100/100.pdf>

449. Ibid.

450. Department of Education, "Policy Paper: National Retraining Scheme", 2017 available at: <https://www.gov.uk/government/publications/national-retraining-scheme/national-retraining-scheme>

451. Alexander Babuta and Marion Oswald, "Data Analytics and Algorithmic Bias in Policing", 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

discussed data analytics and algorithmic bias in policing throws light on the increased use of machine learning software in policing across the UK primarily for the purposes of ‘facial recognition and video analysis; mobile phone data extraction; social media intelligence analysis; predictive crime mapping; and individual risk assessment’. The report also discusses how the algorithmic fairness cannot be understood solely as a matter of data bias, but requires careful consideration of the wider operational, organisational and legal context, as well as the overall decision-making process informed by the analytics.

FRANCE

Maturity Index – 3/5

In March 2018, the French President released the National AI Strategy based on recommendations made in the report⁴⁵² prepared under the supervision of French mathematician and National Assembly member Cédric Villani. There are seven key proposals, which include the recommendation that AI should be made more open, to reduce the possibility of bias. The French strategy proposes developing transparent algorithms that can be tested and verified, determining the ethical liability of persons working in AI, establishing consulting ethics committee and administrative auditing of the algorithms. It advances the idea that the potential to evaluate and audit AI should not be confined to government agencies; it should also be provided by civil society.

It also introduces a mechanism for Discrimination Impact Assessment (**DIA**) that postulates that the AI systems responsible for decisions that are required to be non-discriminatory, must be subjected to a DIA before being deployed. The DIA is along the same lines as the Privacy Impact Assessment that is recommended by the regulatory authority responsible for data privacy, CNIL.

The CNIL also issued a report,⁴⁵³ which extensively discusses the ethical concerns that need to be addressed in the deployment of AI systems. It delves into the concepts of algorithmic profiling and filter bubbles and their effect on society. While the report raises some serious ethical concerns, it does not specifically lay out a solution but provides some guidance and scaffolding for the discussion of ethics by policy makers.

GERMANY

Maturity Index – 3/5

As a consequence of the significant push in Germany is giving to AI research, a national ‘AI Strategy’ was published in 2018.⁴⁵⁴ The aims of the initiative are to strengthen Germany as a research hub and to support the domestic economy, while being at the forefront of AI.

In keeping with its liberal democratic principles, Germany has stated its intention to base its AI policy on the founding ideas of data protection – friendly, trustworthy, and human-centred AI systems, which are to be used for the common good; such as application in the fields of climate and environment protection. At the centre of these claims is the establishment of the ‘AI Made in Germany’ brand,⁴⁵⁵ which is proposed to become a globally acknowledged label of quality. Part of this ‘brand’ is

452. Cédric Villani, “For a Meaningful Artificial Intelligence: Towards a French and European Strategy”, March 2018, available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

453. National Commission for Information and Liberty, “How Can Humans Keep the Upper Hand? The Ethical Matters raised by Algorithms and Artificial Intelligence”, December 2017, available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

454. Alumniportal Deutschland, “AI Made in Germany’: Overview of Artificial Intelligence (AI) in Germany”, December 2019, available at <https://www.alumniportal-deutschland.org/en/science-research/news-from-science/ai-made-in-germany/>

455. German Federal Government, “Artificial Intelligence Strategy”, November 2018, available at <https://www.ki-strategie-deutschland.de/home.html>

the idea that AI applications made in Germany, or to be more precise, the datasets these AI applications use, stand under the umbrella of data sovereignty, informational self-determination and data safety.

Moreover, to ensure that AI research and innovation is in line with ethical and legal standards a Data Ethics Commission was founded, with the aim to assist the Federal Government and to give advice on how to use AI in an ethically sound manner. The National Strategy envisages a total of twelve agglomerations for research and innovation to be established by the Federal government. It is hoped that this will attract research talent to work in the area of ethics-based AI models and systems. Further fields of action include the promotion of procedures to facilitate the auditing and interpretability of algorithmic prediction and decision-making systems as well as AI safety. The report essentially supplements the recommendations⁴⁵⁶ of the Federal Data Ethics Commission of the country on incorporation of ethics as a necessity throughout the AI development and design process.

RUSSIA

Maturity Index – 4/5

The National Strategy of Russia⁴⁵⁷ is the key guiding document on Russia's approach towards AI. While the strategy does touch upon the need for the technology to be socially and ethically viable, it does not explicitly present a roadmap for the inclusion of same in the regulatory process. In fact, the strategy notes that excessive regulation in this sphere might significantly slow the pace of development of technological solutions and therefore focuses heavily on promoting research and investment. Notably, Russia has been at the forefront in development lethal autonomous weapon systems.

However, the strategy does prescribe a list of principles that are obligatory in its implementation. These include the protection of human rights guaranteed by Russian and international law; the impermissibility of the use of AI for the purpose of intentionally inflicting harm on individuals and legal entities; intelligibility of AI as well as non-discriminatory access by the users of products that have been created on the basis of such technologies; assurance of the necessary level of Russian Federation self-sufficiency in the field of AI; the assurance of the close collaboration of research and development in the field of AI with an actual sector of the economy and finally the support of the government to increase the quality and competition in the field.

DENMARK

Maturity Index – 3/5

The Danish government presented its National Strategy for AI in 2019⁴⁵⁸ The strategy aims to ensure that Denmark will have a human-centric and common ethical foundation for AI, in line with the principles set out by the OECD and EU. Furthermore, it strives to partner with Danish companies to develop and use AI to offer world-class services for the benefit of citizens and organisations in Denmark. It also includes ethical principles for the use of AI that focus on ensuring that privacy, security, transparency and justice are not being undermined by AI systems. The strategy endorses the responsible use of AI; it not only provides general principles that must be followed to make AI more ethical, but also rolls out a host of initiatives to bolster its ethical principles. For example, it recommends the establishment of Data Ethics Council to monitor

456. Data Ethics Commission, "Recommendations of the Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence", October 2018, available at: https://www.bmjjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen_englisch.pdf?__blob=publicationFile&v=3

457. Office of the President of the Russian Federation, Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation, October 2019, available at: https://cset.georgetown.edu/wp-content/uploads/t0060_Russia_AI_strategy_EN-1.pdf

458. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", March 2019, available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

technological development and help to ensure that ethical issues are taken up so that the many advantages of using data can be supported in an ethically appropriate manner. It also sets up an inter-ministerial working group to examine whether the issues in using AI can be managed within the existing legislative framework. This working group will identify the need for guidelines on the regulations that apply in relation to the use of AI.

EU

Maturity Index – 3/5

The European Parliament Resolution of 2017 on the Civil Law Rules on Robotics⁴⁵⁹ marked the first step towards the regulation of AI in the EU. The resolution is not binding, but it offers the EC a series of recommendations on possible actions in the area of artificial intelligence, not only with regard to civil law, but also to the ethical aspects of robotics.

As per the resolution, a comprehensive EU system of registration of advanced robots should be introduced, which would be managed by a designated EU Agency for Robotics and Artificial Intelligence. The same agency would provide technical, ethical and regulatory robotics assessment.

The resolution proposes two codes of conduct for dealing with ethical issues: a Code of Ethical Conduct for Robotics Engineers and a Code of Conduct for Research Ethics Commissions. The first code proposes four ethical principles:

1. Beneficence – robots should act in the best interests of humans;
2. Non-maleficence – the doctrine of “first, do no harm,” whereby robots should not harm a human;
3. Autonomy – the capacity to make an informed, un-coerced decision about the terms of interaction with robots; and
4. Justice – fair distribution of the benefits associated with robotics and affordability of homecare and healthcare robots in particular.

The EU is one of the leaders in the global debate on AI governance and ethics. Among other prominent developments in the EU is the Communication on Artificial Intelligence⁴⁶⁰ for Europe, issued by EC in March 2018 which is tasked with ensuring that AI is governed by an appropriate ethical and legal framework that are in line with the Charter of Fundamental Rights of the EU. Also, in March 2018, the European Group on Ethics in Science and New Technologies, an independent advisory body to the President of the EC comprising interdisciplinary experts, released its Statement on Artificial Intelligence, Robotics and Autonomous Systems.⁴⁶¹ The Statement proposed a set of basic principles and democratic prerequisites, based on the fundamental values laid down in the EU Charter of Fundamental Rights.

Another prominent EU initiative with respect to ethics has been the EU High-Level Expert Group on Artificial Intelligence releasing the Ethics Guidelines for Trustworthy AI⁴⁶² in April 2019. The guidelines include seven keys, but non-exhaustive, requirements that AI systems should meet in order to be trustworthy. These requirements are human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness;

459. European Parliament, “Recommendations to the Commission on Civil Law Rules on Robotics”, 16 February 2017, available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

460. EC, “Communication on Artificial Intelligence”, March 2018, available at: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>

461. European Group on Ethics in Science and New Technologies, “Statement on Artificial Intelligence, Robotics and ‘Autonomous Systems’”, available at: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

462. High-Level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, April 2019, available at: <https://ec.europa.eu/futurum/en/ai-alliance-consultation/guidelines#Top>

societal and environmental wellbeing and accountability. These principles are to be accompanied by a framework to assess the trustworthiness of AI systems, which was to be prepared in discussion with the stakeholders and then pilot tested.

The High-Level Expert Group also issued Policy and Investment Recommendations for Trustworthy AI⁴⁶³ in June 2019. The document contains 33 recommendations in an attempt to guide Trustworthy AI towards sustainability, growth and competitiveness, as well as inclusion – while empowering, benefiting and protecting human beings. Among the recommendations is strong criticism of both state and corporate surveillance using AI, including that governments should commit not to engage in mass surveillance and that commercial surveillance of individuals including via free services should be countered. Another specific recommendation is that AI-enabled mass scoring of individuals be banned. The panel also recommends that sustainability be taken account of, including the enactment of a circular economy plan for digital technologies and AI.

The most recent EC proposals⁴⁶⁴ of the Digital Services Act⁴⁶⁵ and the Digital Markets Act⁴⁶⁶ also specifically notes the goal of regulating digital platforms through these new draft frameworks is to protect consumers and their fundamental rights better in the online space.

AUSTRALIA

Maturity Index – 3/5

There has been increasing attention in Australia on the human rights impacts of technology, and the development of an ethics framework for AI. The Australian Human Rights Commission⁴⁶⁷ has commenced a Technology and Human Rights project. The proposals given in the discussion paper range from a moratorium on potentially harmful use of facial recognition technology in Australia, and more accessible technology for people with disability. It also brings to light the importance of transparency so that the decision made by the automated systems can also be reviewed and challenged, where they impinge upon fundamental rights or result in bias. There is considerable discussion in the paper on the issue of biased profiling and outcomes and discrimination. Stakeholders have also called for the enactment of a national legislation to solve the problem of bias and discrimination in AI outcomes. The discussion paper proposes a principle-based regulation that must include principles like transparency, trust, fairness, mitigation of risk and responsibility as its foundation. The Human Rights Commission of Australia also emphasises that the discussion on the issue of impact of automation of jobs and social inequality would also benefit from further research and discussion on the same.

Further, the Australian Government Department of Industry, Innovation and Science has released a discussion paper to track the development of Australia's ethics framework for Artificial Intelligence. The most prominent of these developments is the proposed Australian Ethics Framework currently under development. The advancement of the Australian AI ethical framework⁴⁶⁸ sets out eight core or key principles to form an ethical framework for AI, namely: generates net-benefits; do no harm; regulatory and legal compliance; privacy protection; fairness; transparency and explainability and contestability.

463. High-Level Expert Group on Artificial Intelligence, "Policy and Investment Recommendations for Trustworthy AI", June 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>

464. EC, "Europe fit for the Digital Age: Commission Proposes New Rules for Digital Platform", 15 December 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

465. EC, "The Digital Services Act: Ensuring a Safe and Accountable Online Environment", December 2020, available at https://ec.europa.eu/info-strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

466. EC, "The Digital Markets Act: Ensuring Fair and Open Digital Markets", December 2020, available at <https://europa.eu/!Rd39Mp>

467. Australian Human Rights Commission, "Human Rights and Technology: A Discussion Paper", December 2019, available at: https://tech-humanrights.gov.au/sites/default/files/2019-12/TechRights_2019_DiscussionPaper.pdf

468. Dawson D, Schleiger E, et al., (2019) "Artificial Intelligence: Australia's Ethics Framework", Data61 CSIRO, Australia, 2019, available at: <https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting-documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf>

The proposed Australian AI ethical framework is accompanied by a toolkit of strategies, which attempts to operationalise the high-level ethical principles in practice. The toolkit indicates how the high-level ethical principles are intended to translate into practice. These include impact assessments; internal/external review; risk assessments; best practice guidelines; industry standards; collaboration; mechanisms for monitoring and improvement; recourse mechanisms, and consultation.

JAPAN

Maturity Index – 4/5

Japan is one of the first in Asia to initiate policy discourse on the ethical aspects of AI. In 2016, the Ministry of Internal Affairs and Communication (**MIC**) of Japan released a report⁴⁶⁹ that dealt with the ethical issues in the use of AI technology. It raised concerns about manipulating emotion, faith, behaviour and ranking or selecting AI technologies without awareness in the wake of automated decision-making systems without any human intervention. It also argued that cooperation between humans and AI technologies can lead to the augmentation of human ability, which could form a new sense of values and advocated the need for discussion about these newfound values, if any. The report also brings forth the economic impact of the use of AI systems and its impact on 'job style' and suggests that at the government level, combining educational and employment policies is an effective procedure for mobilizing labour, revitalizing the economy and preventing economic disparities.

Importantly, in 2017, the MIC conducted a conference toward AI network society that released Draft AI Research and Development Guidelines (**R&D Guidelines**).⁴⁷⁰ The basic philosophy of the R&D Guidelines was to achieve a human-centred society where all human beings enjoy the benefits from living in harmony with AI networks, while human dignity and individual autonomy are respected. It also set out seven principles concerning the sound development of AI networking, promotion of the benefits of AI systems and mitigating the risks associated with such systems. These included collaboration, transparency, controllability, safety, security, privacy and ethics. Finally, two more principles were prescribed to bolster the acceptability of AI systems among people, i.e., user assistance and accountability.

Basis the R&D Guidelines, the MIC developed the AI Utilization Guidelines⁴⁷¹ in July 2018. These guidelines also adopted the principles given by the R&D Guidelines and added the principles of fairness and data quality to finally present ten principles to be followed in the utilization of AI. It also classified various kinds of users of such technology for the convenience of understanding their role in the network (and market) possibly for the purpose of fixing responsibility.

Finally, in June 2019, the Integrated Innovation Strategy Promotion Council released the AI Strategy⁴⁷² that made social principles for human-centric AI as its base. While the strategy largely focused on the use of AI in the social sectors like health, education etc. it did discuss the question of ethics to some extent. It stated that in order to minimize the negative ramifications of AI, a high ethical perspective that reflects the cultural background is important, and so-called AI social principles are needed in order to promote the use of AI in a way that respects human beings. One important and novel initiative that the strategy proposed was the establishment of a multilateral framework on the social principles of AI, including consideration for the prevention of ethics dumping.⁴⁷³

469. Advisory Board on Artificial Intelligence and Human Society, "Report on Artificial Intelligence and Human Society" (unofficial translation), June 2016, available at: https://www8.cao.go.jp/cstp/tyousakai/ai/summary/aisociety_en.pdf

470. Director-General, Institute for Information and Communications Policy (IICP), Ministry of Internal Affairs and Communications, the Government of Japan, "Draft AI R&D Guidelines", 2017, available at: https://www.soumu.go.jp/main_content/000507517.pdf

471. Director-General, Institute for Information and Communications Policy (IICP), Ministry of Internal Affairs and Communications, the Government of Japan, "AI Utilization Guidelines", 2018, available at: https://www.soumu.go.jp/main_content/000581310.pdf

472. Integrated Innovation Strategy Promotion Council, "AI Strategy 2019", June 2019, available at: <https://www8.cao.go.jp/cstp/english/humancentricai.pdf>

473. Ethics dumping refers to conducting unethical research in countries/regions where ethics rules are loose.

SINGAPORE

Maturity Index – 4/5

Singapore considered the ethical aspects of AI in 2018, when the government announced the establishment of an Advisory Council for the Ethical Use of AI and Data (**Advisory Council**).⁴⁷⁴ The Advisory Council was mandated to advise and work with the Infocomm Media Development Authority on the responsible development and deployment of AI.

A second initiative by the government was the release of a discussion paper⁴⁷⁵ by the PDPC that set forth two sets of principles. The first set was based on the premise that the decisions made by or with the assistance of AI should be explainable, transparent and fair so that affected individuals will have trust and confidence in these decisions and therefore included principles such as explainability, transparency and fairness. The other set of principles dealt with the ethical aspect of the decisions made by these systems and that they should be human centric and included the principle of beneficence. The discussion paper also proposed a governance framework, which included a recommendation that organisations adopt an internal review system along with practices to mitigate risk and bias by conducting assessment of the impact of an AI system deployed by them. The next step proposed in the governance model was the management of communications with affected individuals and providing measures for recourse, which are important for building consumer trust and confidence. This involves constant engagement of the consumers in the form of installing a mechanism for feedback and grievance redressal. The proposal also considered the incorporation of risk assessment structures in the governance model but did not present a cogent structure to that effect.

The third initiative was to set up a Research Programme on Governance of AI and Data use to be run by Singapore Management University to advance and inform scholarly research on AI governance issues.⁴⁷⁶

Finally, the IMDA and PDPC together came up with a Model AI Governance Framework⁴⁷⁷ in January 2019, which contains guidance on measures promoting the responsible use of AI that organisations should adopt in the following key areas:

1. Internal governance structures and measures Adapting existing or setting up internal governance structure and measures to incorporate values, risks, and responsibilities relating to algorithmic decision-making.
2. Determining the level of human involvement in AI-augmented decision-making A methodology to aid organisations in setting its risk appetite for use of AI, i.e., determining acceptable risks and identifying an appropriate level of human involvement in AI-augmented decision-making.
3. Operations management Issues to be considered when developing, selecting and maintaining AI models, including data management.
4. Stakeholder interaction and communication strategies for communicating with an organisation's stakeholders, and the management of relationships with them.

The framework also included a system to audit of the algorithms by as a forensic investigation to be conducted by the designated regulator which in this case, as proposed by the framework, would be the PDPC.

474. Infocomm Media Development Authority, "Composition of the Advisory Council on the Ethical Use of Artificial Intelligence and Data", August 2018, available at <https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2018/composition-of-the-advisory-council-on-the-ethical-use-of-ai-and-data#01>

475. Personal Data Protection Authority Singapore, "Discussion Paper on Artificial Intelligence (AI) And Personal Data – Fostering Responsible Development and Adoption of AI", June 2018, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI-Discussion-Paper-on-AI-and-PD--050618.pdf>

476. Supra note 434.

477. Infocomm and Media Development Authority, "Personal Data Protection Authority. Model AI Governance Framework (Second Edition)", January 2019, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

Apart from this, Monetary Authority of Singapore also came up with the Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector⁴⁷⁸ in 2018 laying out the principles to be observed while deploying the AI systems in the financial sector. The principles were general principles like fairness, ethics, accountability and transparency. However, the same was not guided by a framework as such for putting these principles into practice.

The implementation of these principles is emphasised in the National Artificial Intelligence Strategy formulated as part of the 'Smart Nation' initiative in 2019. Adopting a human-centric approach is one of the four stated objectives of the strategy, and while the emphasis is on deployment, the strategy also notes that AI would be deployed to serve human needs, rather than technology for technology's sake, the strategy is also conscious of the need to proactively address risks and governance issues as well as the importance of educating society on the changes and benefits of AI-based systems.⁴⁷⁹

SOUTH KOREA

Maturity Index – 3/5

The National Information Society Agency of South Korea released its Ethics Guideline for the Intelligent Information Society⁴⁸⁰ in April 2018. The guideline envisages various principles to be kept in mind while developing and deploying the AI systems and further provides general guidelines that must be adhered to for each set of principles like elimination of social discriminatory elements in technology development; prohibition of use with malicious intention; compliance with consumer behaviour principles at all times; defining conditions and scope of machine-based decision-making in intelligent information services etc. The guideline extensively covers all the ethical aspects of AI and attempts and aims at making the use and development of AI human centric.

The Mid to Long term Government Investment Strategy⁴⁸¹ rolled out by the South Korean government in 2019 also covers reforms that enable individuals and businesses alike to use Intelligent IT freely and safely. It proposes framework legislation to present a vision and aims for the intelligent information society; establish human-centred ethics to govern data-collection processes and AI algorithms; amend the Software Industry Promotion Act and update other legal provisions to ensure better reliability and security tests for Intelligent IT applied to various industries and introduce proactive legal reforms and changes to better prepare for social changes in the future.

In January 2019, the government also announced⁴⁸² a 'Regulatory Sandbox'⁴⁸³ for some sectors that needed the protection for the benefit of their growth. The sectors included AI and big data.

478. Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", 2018, available at: <https://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf>

479. Smart Nation and Digital Governance Office, "National Artificial Intelligence Strategy", November 2019, available at: https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4

480. National Information Society Agency, "Ethics Guidelines for the Intelligent Information Society", April 2018, available at: <https://eng.nia.or.kr/>

481. Government of Republic of Korea, "Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society", 2019, available at: https://english.msit.go.kr/cms/english/pl/policies2/_icsFiles/afifieldfile/2017/07/20/Master%20Plan%20for%20the%20intelligent%20information%20society.pdf

482. Kim Minji, "Trade Minister pledges Stronger Support for Regulatory Sandbox", January 2020, available at <http://www.korea.net/NewsFocus/policies/view?articleId=181992>

483. A regulatory sandbox is a mechanism for exempting or suspending regulations on goods and services that were formerly unavailable due to such rules

SWEDEN

Maturity Index – 3/5

In 2018, the Government of Sweden released its National Approach for AI⁴⁸⁴ as per which the government assessed the ethical concerns that the use and development of AI comes with. Pursuant to this assessment the government's observations as mentioned in the national approach were:

1. Sweden needs to develop rules, standards, norms and ethical principles to guide ethical and sustainable AI and the use of AI.
2. Sweden needs to push for Swedish and international standards and regulations that promote the use of AI and prevent risks.

Apart from this the country has also established a Committee for Technological Innovation and Ethics in 2018;⁴⁸⁵ however, the committee does not appear to have released any literature on this issue.

FINLAND

Maturity Index – 3/5

The first guidance paper on AI⁴⁸⁶ published by the Ministry of Economic Affairs and Employment in 2017, very briefly touched upon the ethical questions that may come up in the context of AI. This marked the beginning of the discussion process on various aspects related to AI to be culminated into a final report that was published in 2019.

The final report⁴⁸⁷ highlighted the need to face the ethical challenges related to AI and proposed human-centric design of AI and the implementation of ethical principles in the public sector through the Aurora AI project. The report sought to draw the focus in the AI debate in Finland on ethical issues such as: protection of privacy, accountability for the errors made by AI systems and the traceability and transparency of algorithm-based decision-making. It urged the members of the expert panel consider these issues and that they can only be solved through international cooperation.

Meanwhile in December 2018, Ministry of Finance submitted its Information Policy Report⁴⁸⁸ on ethical information policy in the age of AI to the Finnish parliament. The specific measures deal with information security, data protection, the gathering and combining of information, and information disclosure and storage. Other areas examined include ethical issues, securing expertise, regulatory issues, new focus areas and policy-level participation in the EU and international forums.

484. Government Offices of Sweden, "National Approach to Artificial Intelligence", 2018, available at: <https://www.regeringen.se/4aa638/contentassets/a6488ccebc6f418e9ada18bae40bb71f/national-approach-to-artificial-intelligence.pdf>

485. OECD.AI Policy Observatory, "Sweden: Committee for Technical Innovation and Ethics (KOMET)", available at <https://oecd.ai/dashboards/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F24978>

486. Steering Group of the Artificial Intelligence Programme, "Finland's Age of Artificial Intelligence: Turning Finland into a Leading Country in the Application of Artificial Intelligence. Objective and recommendations for measures", December 2017, available at: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf

487. Steering Group and Secretariat of the Artificial Intelligence Programme, "Leading The Way Into the Era of Artificial Intelligence: Final report of Finland's Artificial Intelligence Programme", 2019, available at: [http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed="](http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=)

488. Ministry of Finance, "Ethical Information Policy in the Age of Artificial Intelligence", 2018, available at: https://vm.fi/documents/10623/7768305/VM_Tiepo_selonteko_070219_ENG_WEB.pdf/89b99a8e-01a3-91e3-6ada-38056451ad3f/VM_Tiepo_selonteko_070219_ENG_WEB.pdf/VM_Tiepo_selonteko_070219_ENG_WEB.pdf

The Ministry of Finance also set a preliminary study project⁴⁸⁹ on the Aurora national AI programme for the period of five months in September 2018. The aim of the study was to identify what kind of changes a human-centric and life-events-based approach would entail in terms of, inter alia, the provision and management of services. The study seeks to provide a holistic set of personalised AI-driven services for citizens and businesses in a way that is human-centric and works towards their well-being as its ultimate goal. The study proposes development of a management-by-information model based on users' needs provided by AI, and to formulate a playbook and guidelines implementing the change. The overall aim of the Aurora national AI programme is to implement an operations model based on people's needs, where AI helps citizens and companies to utilise services in a timely and ethically sustainable manner.

An important report⁴⁹⁰ on the effect of AI deployment in employment was released by the Ministry of Economic Affairs and Employment of Finland in 2018. The report observes that the use of AI will affect the labour market in a profound way, that new job roles will emerge, and conventional clerical jobs may be on the decline owing to the deployment of AI systems. To this end the report makes various policy recommendations like focus on innovations that complement human work, a significant share of which are social and socio-technical, introduction of a combined curriculum that focuses on putting the technological and interaction skills together for better employability and improve in labour mobility to move workers on to tasks that are a better match with their skills.

SPAIN

Maturity Index – 3/5

The RDI Strategy on AI⁴⁹¹ released by Spain in 2019 acknowledges that it is necessary to make an additional effort through research to determine how to design better AI systems that incorporate ethical reasoning. The strategy notes that the Spanish Ethics in Research Committee as an independent and consultative body on materials related to professional ethics in scientific and technical research, must be active in ethical aspects of definition and identification of AI at national level. It further recommends that the development of new applications must be guided by the ethical, legal and social principles of Spain and Europe. To this end it envisages the creation of an AI Code of Ethics to be co-developed at the inter-ministerial level.

NORWAY

Maturity Index – 3/5

In 2018, the Norwegian Board of Technology published a report⁴⁹² that addressed and discussed the problem of biased algorithms, black box challenge, explainability of AI systems and the possibility of malicious use of such systems. The discussion highlighted the pitfalls posed by the technology and the need to prepare for the same rather than taking a technical direction of explaining the way forward. It noted that the government has declared that it will develop guidelines and ethical principles for the use of AI; it presents six guiding principles for the government to use as a framework, which include: autonomy of humans, democracy, justice, equality, solidarity and responsibility.

489. Government of Finland, "Development and Implementation Plan 2019–2023 Based on the Preliminary Study on the Aurora National Artificial Intelligence Programme", 2019, available at: <https://vm.fi/documents/10623/13292513/AuroraAI+development+and+implementation+plan+2019%20%932023.pdf/7c96ee87-2b0e-dadd-07cd-0235352fc6f9/AuroraAI+development+and+implementation+plan+2019%20%932023.pdf>

490. Ministry of Economic Affairs and Employment, "Work in the Age of Artificial Intelligence: Four Perspectives on the Economy, Employment, Skills and Ethics", 2018, available at: <https://julkaisut.valtioneuvosto.fi/handle/10024/160980>

491. Ministry of Science, Innovation and Universities, "RDI Strategy on Artificial Intelligence", 2019, available at: http://www.ciencia.gob.es/stifs/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_EN.PDF

492. Norwegian Board of Technology, "Artificial Intelligence – Opportunities, Challenges and a Plan for Norway", 2018, available at: <https://teknologiradet.no/wp-content/uploads/sites/105/2018/11/Al-and-machine-learning-1.pdf>

The approach of the Norwegian Government towards the ethical aspects of the technology can be more properly seen in the country's National Strategy for AI⁴⁹³ released in January 2020. At the very outset the strategy unequivocally expresses the government's commitment towards ethical use of the technology in the country and the desire of the government to lead the way in developing and using AI with respect for individual rights and freedoms. The principles set forth by the strategy were same as mentioned above. However, it takes a step forward and advocates that ethical considerations should be built into algorithms during the development of the technology. It stated that among other things, it will be important to assess whether an algorithm may lead to discrimination and whether it is sufficiently robust to withstand manipulation.

ESTONIA

Maturity Index – 3/5

While Estonia's AI Strategy released in July 2019⁴⁹⁴ does not provide much of a roadmap to tackle the ethical challenges raised by the technology, the country is guided by the report of Estonia's Task Force on AI released in May 2019⁴⁹⁵ which briefly explains the general connections and principles resulting from EU law.

As per the report there are various areas of fundamental rights should be considered above all with regard to artificial intelligence. These fundamental rights are right to human dignity; right to freedom; respect of the principles of democracy and the state, based on the rule of law; right to equality, non-discrimination, and acknowledgement of minorities and civil rights.

It further proposes the following five principles that must be kept in mind while developing AI:

1. The principle of usefulness (beneficence)
2. The principle of refraining from causing harm
3. The principle of autonomy
4. The principle of fairness
5. The principle of clarity

THE NETHERLANDS

Maturity Index – 3/5

The Dutch AI Manifesto, 2018,⁴⁹⁶ created by the Special Interest Group on AI of Netherlands identifies certain multidisciplinary challenges for sustainable next-generation AI systems to which the Dutch AI community can make strong contributions in the coming decade. These are: designing of socially aware AI systems are to allow for an effective social interface with

493. Government of Norway, "National Strategy for AI", January 2020, available at: https://www.regjeringen.no/contentassets/1feb8bb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

494. Government of the Republic of Estonia, "Estonia's National Artificial Intelligence Strategy – 2019–2021", July 2019, available at https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf

495. (Estonian) Ministry of Economic Affairs and Communication, "Report of Estonia's AI Taskforce", 2019, available at https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_486454c9f32340b28206e140350159cf.pdf

496. Special Interest Group on AI of Netherlands, "The Dutch Artificial Intelligence Manifesto", 2019, available at: <http://ii.tudelft.nl/bnvki/wp-content/uploads/2018/09/Dutch-AI-Manifesto.pdf>

humans; to interpret, reason about, and influence human behaviour and to collaborate and coordinate their behaviour with human beings. Apart from these, the challenges identified by the manifesto to build a responsible structure of AI systems are to design AI systems which allow integrating our moral standards for responsible data processing and integrate our moral, societal and legal values.

As per the Strategic Action Plan for Artificial Intelligence, 2019,⁴⁹⁷ the government of The Netherlands plans to stimulate the participation of Dutch companies as well as public organisations in the pilot phase of the ethical guidelines for AI from the High-Level Expert Group of the EC. The Ministry of Economic Affairs and Climate Policy is investigating which algorithms are used for different sectors, the risks this entails, how companies manage these risks and what safeguards are in place. The NEN Standards Committee on AI is to share good practices, develop frameworks for reliable and ethically responsible AI applications and contribute to the development of global AI standards by the International Organization for Standardization. Finally, the report proposes the use of instruments such as the AI Impact Assessment and quality marks/ audits and encourage collaboration between supervisory authorities with the aim of building up expertise, sharing it and discussing the division of tasks with regard to the supervision of algorithms and of AI in general.

UAE

Maturity Index – 3/5

The Minister of State for AI announced that the UAE government adopted an integrated and dynamic model for the utilisation of AI that supports industry growth, development of new sectors as well as strengthening governance and ethics frameworks, ultimately anticipating future challenges and creating a positive change for humanity in April 2019.⁴⁹⁸

However, the administration of city of Dubai launched its own approach to help businesses and governments create fair, interpretable, explainable, accountable, and ultimately trusted AI systems that manage the tension between innovation potential, societal values and the downside risks. This ethical toolkit⁴⁹⁹ supports industry, academia and individuals in understanding how AI systems can be used responsibly. It consists of principles and guidelines, and a self-assessment tool for developers to assess their platforms. The self-assessment tool⁵⁰⁰ is built to enable AI developer organisations or AI operator organisations to evaluate the ethics level of an AI system, using Dubai's AI Ethics Guidelines in the toolkit. It contains a four-level impact assessment system to adjudge the fairness, accountability, transparency and explainability of the AI system.

HONG KONG

Maturity Index – 3/5

The Privacy Commissioner for Personal Data, Hong Kong, issued an Ethical Accountability Framework (**Framework**) in 2018,⁵⁰¹ following industry consultation. The discussion in the Framework explicitly links the issue of data ethics to AI and acknowledges how an ethical approach can offer additional guidance to the principles-based and technology-neutral

497. Government of The Netherlands, "Strategic Action Plan for Artificial Intelligence", October 2019, available at: <https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence>

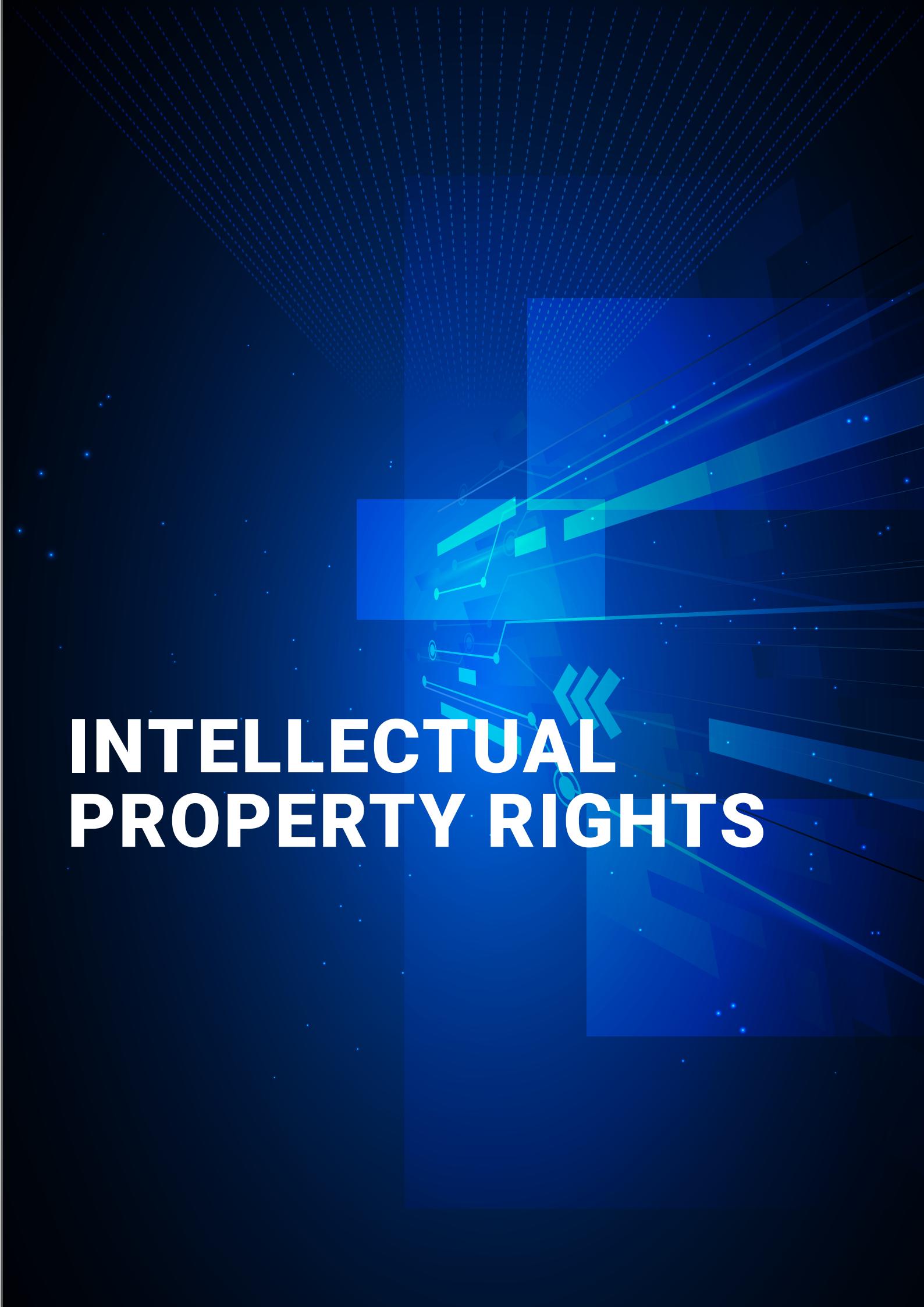
498. Staff Report, "UAE government adopts dynamic model of AI governance", Gulf News, 10 April 2019, available at <https://gulfnews.com/business/uae-government-adopts-dynamic-model-of-ai-governance-ethics-1.63247873>

499. City Government of Dubai, "Smart Dubai AI Ethics Principles & Guidelines", January 2019, available at: https://www.smartdubai.ae/pdfviewer/web/viewer.html?file=https://www.smartdubai.ae/docs/default-source/ai-principles-resources/ai-ethics.pdf?sfvrsn=d4184f8d_6

500. Smart Dubai, "AI System Ethics Self-Assessment Tool", 2019 available at: <https://www.smartdubai.ae/self-assessment>

501. Chartered Secretaries Journal, "Data Ethics – New Guidance", December 2018, available at <http://csj.hkics.org.hk/site/2018/12/12/data-ethics-new-guidance/>

legislations. The Framework includes a series of 'Enhanced Elements' and three 'recommended' Hong Kong Data Stewardship Values of respectful, beneficial and fair which were developed with the industry consultees, along with two assessment models for use by stakeholders. The assessment models are the Ethical Data Impact Assessment (**EDIA**) and the Process Oversight Model (**POM**). While the EDIA assesses the impact to all stakeholders' interests in data collection, use and disclosure, and in data-driven activities, the POM looks at how an organisation translates organisational ethical values into principles and policies and into an 'ethics by design' programme through internal review processes.



INTELLECTUAL PROPERTY RIGHTS

The World Intellectual Property Organisation (**WIPO**) in 2019 published a report⁵⁰² discussing trends in patent applications and grants, noting that of late, there has been a rise in AI-related applications in the fields of telecommunications, transportation, and life and medical sciences. These patents have involved technology relating to NLP, speech processing and computer vision. In 2017, an AI system named DABUS was named as the inventor in the patent applications filed in UK, USA and Europe. However, the same was rejected in all three jurisdictions on the account of it not being a legal person as required by most Intellectual Property Rights (**IPR**) regimes.⁵⁰³ Similarly, Google's Digital News Initiative has funded the creation by the UK's Press Association and Urbs Media of Reporters and Data and Robots, an AI system which will help create local news content based on templates created by real journalists across various genres.⁵⁰⁴ This surge in patent filings claiming authorship or ownership by AI over a period of years ,have raised interesting questions and discourse in the world of IPRs , as to whether AI can be treated as the author or creator of innovations.

A separate issue that is considered in the context of AI and IPRs is the practical difficulty of the patentability of AI systems in the context of the subject-matter eligibility standard. In most jurisdictions, algorithms by themselves qualify as a vague system lacking technical character, and hence cannot be protected under the IP laws, unless it has been given a technical character in

the form of effective software.⁵⁰⁵ However, in response to the changes in technology and rising applications, IP regulators in different countries have also come up with guidelines regarding examination, and initiatives to encourage patent protection in these areas of technology. They provide clarity over the eligibility of algorithms that can come under the purview of patentability, for them to then be tested on merits such as novelty and enablement.⁵⁰⁶

Another important debate is on issues related to ownership/user/authorship rights of content, and inventions that are autonomously generated by AI systems.⁵⁰⁷ At the present stage of development, though, examples of content generated by absolutely autonomous AI systems are few and far between; we are still quite a way from 'independent acting' computers being more ubiquitous in society.⁵⁰⁸ Nevertheless, this gives rise to a debate about the patentability/copyrightability of the inventions and content that is created using AI systems as a tool. The current IPR laws accord rights to entities accorded a legal personhood (whether natural or corporate); it is for this reason that in most jurisdictions, at present, an AI system is precluded from the grant of such protection.⁵⁰⁹ However, since AI technology is still very nascent, and there is ambiguity around the definitions of AI and "autonomy", there appears to be some difficulty around legislating on this point.⁵¹⁰

502. World Intellectual Property Organisation, "WIPO Technology Trends 2019", Artificial Intelligence, 2019, available at: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

503. James Nurton, "EPO and UKIPO Refuse AI Invented Patent Application", IP Watchdog, January 2020, available at: <https://www.ipwatchdog.com/2020/01/07/epo-ukipo-refuse-ai-invented-patent-applications/id=117648/>
Also see, Rebecca Tapscott, "USPTO Shoots Down DABUS Bid for Inventorship", IP Watchdog, May 2020. Available at: <https://www.ipwatchdog.com/2020/05/04/uspto-shoots-dabus-bid-inventorship/id=121284/>

504. Julia Gregory, "Press Association wins Google grant to run news service written by computers", The Guardian, July 2017, available at: <https://www.theguardian.com/technology/2017/jul/06/press-association-wins-google-grant-to-run-news-service-written-by-computers>

505. World Economic Forum, "Artificial Intelligence Collides with Patent Law", April 2018, available at: http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf

506. Danny Yap and Judia Kok, "Artificial Intelligence: Disruption in Progress", Singapore Academy of "aw, 2019. Available at: <https://journalsonline.academypublishing.org.sg/Journals/SAL-Practitioner/Fintech/ctl/eFirstSALPDFJournalView/mid/595/ArticleId/1483/Citation/JournalsOnlinePDF>

507. Daryl Lim, "AI & IP: Innovation & Creativity in an Age of Accelerated Change", Akron Law Review, Volume 52 Issue 813, 2019, available at: <https://ssrn.com/abstract=3369200>

508. Reto Hilty, Jörg Hoffmann, et al, "Intellectual Property Justification for Artificial Intelligence" (draft chapter), February 2020, forthcoming in: Artificial Intelligence & Intellectual Property, Oxford University Press, 2020, available at: <https://ssrn.com/abstract=3539406>

509. Swapnil Tripathi and Chandni Ghatak, "Artificial Intelligence and Intellectual Property Law", Christ University Law Journal, 2018, available at: <https://core.ac.uk/download/pdf/236436865.pdf>

510. Ramalho, Ana, "Patentability of AI-Generated Inventions: Is a Reform of the Patent System Needed?", Institute of Intellectual Property, Foundation for Intellectual Property of Japan, February 2018, available at: <https://ssrn.com/abstract=3168703>

This further makes it difficult to ascertain the standards associated with IPR laws such as duration of protection, identification of beneficiary for licensing remuneration, differentiating between human and AI creations etc. While there are many challenges, one argument for allowing computers to be classified as inventors/authors and afforded with IP protection is the 'incentive theory'. While this may not be any motivation for computers themselves, it will continue to incentivize humans to produce such technologies as they understand the benefits emerging due to IPR protection.⁵¹¹

In September 2019, WIPO organised a conference⁵¹² to discuss the impact of AI on IP policy of various countries and the relevant questions to set the foundation for better informed policymaking by member states. Pursuant to the conference, WIPO published a Draft Discussion Paper⁵¹³ on IP and AI in December 2019 (**WIPO Discussion Paper**) inviting member states and other interested parties to provide comments and suggestions. The WIPO Discussion Paper identifies thirteen issues that relate to the issue of AI and IP policy:

1. Issue 1 pertains to ownership and inventorship. It deals with issues such as whether the law should permit or require that the AI application be named as the inventor or whether this should necessarily be a human. Further, it considers the practical challenges of whether there should be any indicators of which human ownership or authorship should be attributed to, if AI systems cannot be given ownership, i.e., whether this decision should be left to private arrangements, such as corporate policy, with the possibility of judicial review by appeal in accordance with existing laws concerning disputes over inventorship. Finally, under issue 1 the WIPO Discussion Paper asks comments of the member states on the question –'Should the law exclude from the availability of patent protection any invention that has been generated autonomously by an AI application?'.
2. Issue 2 of the WIPO Discussion Paper is about patentable subject matter and patentability

guidelines. Here, it considers the issues of whether inventions autonomously generated by an AI application ought to be excluded from IPR laws, whether specific provisions should be introduced for inventions assisted by AI (or if they should be treated in the same way as other computer-assisted inventions), whether patent examination guidelines need to be amended for AI assisted inventions, etc.

3. Under issue 3, the WIPO Discussion Paper explores the issue of understanding the inventive step test that needs to be met for the invention to be granted a patent in the context of AI inventions.
4. Issue 4 deals with disclosure of the technology, and whether AI-assisted or AI-generated inventions present any challenges in the disclosure requirement; further, it considers whether the initial disclosure requirement would be sufficient where the algorithm continually changes over time through machine learning; how to treat data used to train an algorithm; and whether human expertise used to select data and to train the algorithm be required to be disclosed.
5. Issue 5 relates to general policy considerations such as whether a *sui generis* IPR system should be considered for AI generated inventions, and whether the interface between AI and IPRs should be considered at a later stage once AI technology itself is more advanced or better understood.
6. Issue 6 relates to copyright and discusses authorship and ownership issues, such as whether copyright be attributed to original literary and artistic works that are autonomously generated by AI; in whom should copyright in an AI-generated work vest; whether the issue of according legal personality to an AI application should be considered, where it creates original works autonomously; and whether a separate *sui generis* system of protection ought to be envisaged for original literary and artistic works autonomously generated by AI.

511. Id. at 8.

512. World Intellectual Property Organisation, "WIPO Conversation on Intellectual Property and Artificial Intelligence", September 2019, available at: https://www.wipo.int/about-ip/en/artificial_intelligence/news/2019/news_0007.html

513. World Intellectual Property Organisation, "Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence", December 2019, available at: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053

7. Issue 7 pertains to IPR infringements and seeks to understand whether the use of the data subsisting in copyright works without authorization for machine learning would constitute an infringement of copyright and what impact that would have on the development of AI and on the free flow of data to improve innovation in AI; whether an exception should be made for limited types of use of such data in machine learning, such as the use in non-commercial user-generated works or the use for research; how would existing exceptions for text and data mining interact with such infringement; whether a licensing system would be useful as an alternate to copyright infringement and whether the unauthorized use of data subsisting in copyright works for machine learning can be detected and enforced, in particular when a large number of copyright works are created by AI.
8. Issue 8 considers the issue of 'deep fakes' or 'the generation of simulated likenesses of persons and their attributes, such as voice and appearance', and whether copyright can subsist in deep fakes themselves; whether there should be a system of equitable remuneration for persons whose likenesses and "performances" are used in a deep fake;
9. Issue 9 relates to whether there are seen or unforeseen consequences of copyright on bias in AI applications; whether the dignity of human creation should be prized as a right over and above innovation in AI;
10. Issue 10 considers whether there should be a new set of IPRs in data or whether the existing regime of IPR laws are sufficient; what kinds of data would be protected under such new rights, if created; whether certain qualities in the data such as commercial value, or protection against certain kinds of activities should be the defining characteristic for these new rights; how would such rights interact with existing rights and how would they be enforced.

11. Issue 11 considers industrial designs and looks into questions such as whether design protection should be accorded to an original design that has been produced autonomously by an AI application, or whether a human designer is required;
12. Issue 12 addresses capacity building, to address the containment or the reduction in the technology gap in AI capacity and whether any policy measures are required in this regard.
13. Issue 13 of the WIPO Discussion Paper pertains to accountability for the decisions in IP administration.

Various member jurisdictions of the WIPO and individuals submitted their comments on each of these issues, as a part of the ongoing discussion on the interface of IPRs and AI.

On 4 November 2020, the WIPO held its third "Conversation on Intellectual Property and Artificial Intelligence",⁵¹⁴ which was focused on the following issues:

1. Defining AI and future-proofing its definition as the technology evolves, exploring the distinction between "AI inputted" and "AI generated";
2. The impact of AI on trademarks and the implications of human perception to determine registration and infringement of trademarks;
3. The role of IP policy in bridging the capacity gap; and
4. The policy implications of using AI in IP administration.

Although it was noted that there is flexibility in the current law on these and other issues relating to IP and AI, there do not appear to be any policy or legislative solutions on the table as yet. The WIPO is expected to publish a White Paper in 2021 that proposes a definition of AI for the purposes of IP policy, which could be the first step towards international comity in AI regulation.⁵¹⁵

514. WIPO, "WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI): Third Session", 4 November 2020, available at https://www.wipo.int/meetings/en/details.jsp?meeting_id=59168

515. Morgan Lewis & Bockius LLP, "Artificial Intelligence and Intellectual Property: Transatlantic Approaches", November 2020, available at <https://www.lexology.com/library/detail.aspx?g=da7ffc2d-e1b7-46ef-9eb5-5865cbd69e83>

In light of the above, the current chapter maps IPR policy vis-à-vis AI of various countries, and their views on these issues in their respective jurisdictions. In most cases, the legislative framework treats AI systems as equivalent to software, and therefore offers limited protection; further, in most jurisdictions, the issue of granting AI itself authorship status is a novel one and is not something that is accounted for in the existing IPR system.

MATURITY INDEX INTELLECTUAL PROPERTY RIGHTS



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation

Denmark, Hong Kong

India, China, Canada, Israel, Russia, Australia,
South Korea, Finland, Spain, Norway, Estonia,
The Netherlands, UAE

USA, UK, France, Germany, EU, Japan,
Singapore, Sweden



INDIA

Maturity Index – 3/5

The National Strategy for AI (**NSAI**)⁵¹⁶ released in 2018 notes that the current IP law regime in India could pose a challenge for adoption and innovation of AI. As per the NSAI, it is imperative that the IP regime be robust and enforceable for innovators to have the confidence that they will be able to retain credit for their work, recoup their investment and earn rewards for their efforts. To this end, the NSAI recommends the formation of a taskforce comprising jointly of Ministry of Corporate Affairs and Department for Promotion of Industry and Internal Trade to examine and issue appropriate modifications to the IP regulatory regime pertaining to AI. Further, NSAI also notes that various challenges remain in application of 'stringent and narrowly focused patent laws to AI application'. One example of such challenges given is the importance of data for the development of models that are useful. In this light, the NSAI suggests that IP facilitation centres should be established to help bring the AI and developers and IP practitioners in close contact. It also suggests adequate training of the IP granting authorities, judiciary and tribunals for a better understanding of the AI systems.

In a report⁵¹⁷ released by TATA Consultancy Services and Confederation of Indian Industries, it was suggested that India needs to bring in guidelines and policies for the enforcement of IPR and IP management with respect to AI. The report also informs that currently as per the Computer Related Inventions (**CRI**), computer applications and software can be the basis of the patents given that a human being is a true and original inventor. However, when an invention is created by an AI system the rule does not apply.

USA

Maturity Index – 3/5

In 2018, the head of the US Patent and Trademark Office (**USPTO**) expressed in a Senate hearing that the US needs to make sure that its IP rules adequately protect and incentivize innovation in AI⁵¹⁸. In January 2019, USPTO held a public discussion conference⁵¹⁹ with six panels featuring IP specialists from around the world to consider the topics such as economic frameworks and impacts, how AI related inventions can be protected and international perspectives in this regard.

Pursuant to this the USPTO published two notices in the Federal Register in August 2019⁵²⁰ and October 2019⁵²¹ seeking comments on patenting AI innovations and IP protection (other than patents) for AI innovations respectively. The notices list various questions relating to IP policy, AI inventions (inventions that utilize AI as well as inventions that are developed by AI) and works created by AI. The questions asked in the notices are summarised as follows:

1. Why or why not should a work created by an AI system without the involvement of a natural person be qualified as a work of authorship as per US Copyright law.

516. NITI Aayog, "National Strategy for Artificial Intelligence", June 2018, available at: https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

517. Confederation of Indian Industries and TATA Consultancy Services, "Understanding the Dynamics of Artificial Intelligence in Intellectual Property", 2019, available at: <https://www.mycii.in/KmResourceApplication/64715.CIITCSReportUnderstandingtheDynamicsofAIinIP.pdf>

518. Nathan Calvin and Jade Leung, "Who Owns Artificial Intelligence? A Preliminary Analysis of Corporate Intellectual Property Strategies and Why They Matter", Centre for the Governance of AI Future of Humanity Institute, University of Oxford, January 2020, available at: https://www.fhi.ox.ac.uk/wp-content/uploads/Patents_-FHI-Working-Paper-Final-.pdf

519. USPTO, "Artificial Intelligence: Intellectual Property Policy Considerations", January 2019, available at: <https://www.uspto.gov/about-us/events/artificial-intelligence-intellectual-property-policy-considerations>

520. USPTO, "Request for Comments on Patenting Artificial Intelligence Innovations", August 2019. Available at: <https://www.federalregister.gov/documents/2019/08/27/2019-18443/request-for-comments-on-patenting-artificial-intelligence-inventions>

521. USPTO, "Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation", October 2019, available at: <https://www.federalregister.gov/documents/2019/10/30/2019-23638/request-for-comments-on-intellectual-property-protection-for-artificial-intelligence-innovation>

2. What level of human involvement (in the preparation of the algorithm and the work) should be considered as sufficient for the work to be copyrightable or an invention to be patentable?
3. If current laws regarding inventorship need a revision to take into account the inventions in which entities other than a natural person have contributed?
4. Are there any disclosure related questions that are unique to AI inventions and must be considered while devising the IP policy for AI inventions?
5. How can patent applications best comply with the enablement requirement given the unpredictability of certain AI systems?
6. Are there any patent eligibility considerations unique to AI systems?
7. Is the 'ingestion' of copyrighted material by the AI systems be considered legal as per the current US Copyright law?
8. Are current laws for assigning copyright infringement adequate to address a situation in which an AI process infringes an already copyrighted work?
9. Should an entity other than the natural person (to which the natural person assigns the copyrighted work) be allowed to own the copyright or patent on the AI work?
10. Does AI impact the level of person of ordinary skill in art? If it does then how?
11. Other copyright and patent issues that need to be addressed with respect to artificial intelligence.
12. Would the use of AI in trademark searching impact the registrability of trademarks and how?
13. How does AI impact the trademark law? If the current language of the law adequate to address these issues?
14. How does the use of AI affect the need to protect data and if the current laws are adequate to address the issue of use of AI in marketplace?
15. How does the use of AI impact trade secret law?
16. Does law need a change to create a balance between IPR protection and maintenance of trade secrets with respect to AI?
17. Any other issue related to IP rights and AI that USPTO should examine?
18. Are there any IP policies related to AI in other jurisdictions to help inform USPTO's policy decisions?

Apart from this, there is some basic guidance in the Compendium of US Copyright Office Practices,⁵²² which says that works produced by a machine with no creative input or intervention from a human cannot be given authorship. In January 2019, the USPTO published the 'Revised Patent Subject Matter Eligibility Guidelines'⁵²³ that identified mathematical concepts (algorithms), certain methods of organising human activity and mental processes per se as an abstract idea that fall

522. USCO, "Compendium of US Copyright Office Practices", September 2017, available at: <https://copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf>

523. USPTO, "2019 Revised Subject Matter Eligibility Guidance", January 2019, available at: <https://www.federalregister.gov/documents/2019/01/07/2018-28282/2019-revised-patent-subject-matter-eligibility-guidance>

outside the purview of patent eligibility unless the same has been put to practical applicability. This means that it will have to be shown to the patent examiners that an algorithm has been put to 'practical application' for it to be eligible as a patent. Example 37 from various examples⁵²⁴ released by USPTO clarifies this, by noting that the claim of a system that rearranges the icons on a Graphical User Interface of a computer system based on their usage relates to the 'mental process' of using a processor to give effect of a technical nature i.e., the change in the position of icons as per usage. Therefore, the claim is not excluded from the patentability purview because the per se excluded 'mental process' has a practical applicability.

In addition to this, the response⁵²⁵ of the US Copyright Office (USCO) to the WIPO Discussion Paper also brings to light various policy discussions undertaken by the USCO including the 1965 Annual Report that noted that the line between the human and machine authorship will be a crucial consideration in establishing the copyrightable authorship. It also brought to light various conferences that were held in close co-ordination with the WIPO including the event titled 'Conversation on Intellectual Property and Artificial Intelligence' held in September 2019 and 'Copyright in the Age of Artificial Intelligence' held in February 2020 in which issues related to AI and IPR were discussed. The response appreciated the complexity in the registration of copyrights that has been created by machine-created works and expressed the USCO's intention to closely work with WIPO in this regard and participate in the process.

Further, a response⁵²⁶ to the WIPO Discussion Paper was also submitted by the USPTO. The response discussed the two federal notices (discussed above) for public discussion on various issues related to AI and IPR and expressed that it will release a report later in 2020 mapping the discussion. This report was published in October 2020⁵²⁷ and indicated that a majority of respondents to its call for comments believed that existing IP laws are equipped to deal with emerging AI related issues. However, there was no consensus as to whether it would be beneficial to introduce new types of IP rights. The lack of a universally recognized definition of AI was also highlighted as a difficulty with creating cogent IP and AI policy. It was also agreed that the USPTO should stay abreast of technological developments to be able to create policy that is relevant and effective. The report is expected to be a springboard to examine further measures to bolster understanding of Alnand ensure that US IP policy is sufficiently equipped to handle the requirements of new innovations.

CHINA

Maturity Index – 3/5

In January 2020, it was reported⁵²⁸ that a court in China ruled that work generated by AI qualified for copyright protection. The court observed that the article generated by an AI system called 'Dreamwriter' met the legal requirements to be a written work and therefore was ruled to be a legal person's work created by Shenzhen Tencent Computer System Pvt. Ltd. (the plaintiff) and was therefore entitled to compensation. In a state council plan, which declared the nation's intention to be the world leader in AI by 2030, one section advised that policy makers in China must strengthen the protection of IPR in the field of AI.⁵²⁹

524. USPTO, "Subject Matter Eligibility Examples: Abstract Ideas", January 2019, available at: https://www.uspto.gov/sites/default/files/documents/101_examples_37to42_20190107.pdf

525. USCO, "Comments to the World Intellectual Property Organisation", February 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_usa_usco.pdf

526. USPTO, "Response to the World Intellectual Property Organisation", February 2020. Available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_usa.pdf

527. USPTO, "Public Views on Artificial Intelligence and Intellectual Property Policy", October 2020, available at https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-05.pdf

528. Aaron Wininger, "Shenzhen Court Rules AI-Generated Articles are Entitled to Copyright Protection", National Law Review, Volume 10 Issue 3, January 2020, available at: <https://www.natlawreview.com/article/shenzhen-court-rules-ai-generated-articles-are-entitled-to-copyright-protection>

529. Id.

Further, the country in its National Development Plan on AI, 2017⁵³⁰ lists establishment of AI technology standards and IPR system as one of the measures to bolster the governance and enforcement of AI systems. As per the National Development Plan, China will strengthen the protection of IPR in the field of AI, improve the field of AI technology innovation, patent protection, and standardization of interactive support mechanisms to promote the innovation of IPR in AI. Moreover, the plan also suggests the establishment of AI public patent pools to promote the use of AI and the spread of new technologies.

In its response⁵³¹ to the WIPO Discussion Paper, the Copyright Department of China suggested that more research must be conducted to get clarity over three main points. Firstly, if the autonomous generation of artistic or literary work by AI should be considered as an act of creation. Secondly, how to differentiate between the ideas and expression of the literary or artistic works autonomously generated by AI and finally, whether the literary or artistic works autonomously generated by AI meet the requirements for originality. The response also suggested a comparative study between various regimes on the issue of content created in the course of employment and the protection regimes based on related rights.

CANADA

Maturity Index – 3/5

Practice notices released by Canadian Intellectual Property Office as early as 2013 considered the examination of computer-implemented inventions. These notices consider the question of whether the problem of innovating is a computer problem or a problem whose solution is merely implemented on a computer.⁵³² Apart from this, the CIPO has not released any guidance documents that refer specifically to AI technologies.⁵³³

Canada also responded⁵³⁴ to the WIPO Discussion Paper on IPR and AI. In its response it critically commented on the formulation of the questions as premature and suggested that WIPO at this stage should focus on collection of evidence with respect to member states having evidence that inventions/works/designs can be autonomously generated by AI, the criteria that was used to define autonomy in these cases and the level of human intervention was involved. The response further suggests that certain questions can be reformulated to build further evidence, such as 'how many applications for patent protection 3 has your IPO received in which the applicant has named an AI application as the inventor? Has any patent been granted pursuant to such application? If not, what were the grounds for refusal?' It further suggests that 'more generic questions on how the IP systems in Member States are evolving may also help us gain valuable insights and thereby move the conversation forward'. In its response Canada also opined that the discussion should include examination of issues such as use of AI in IP administration and the accountability of IP Offices using such systems. The questions suggested by Canada in this regard were 'What best practices have you identified or adopted to monitor and audit algorithmic decision-making to ensure a trustworthy, fair and accountable approach? Have you adopted specific measures to provide for appeal or other recourse options to challenge decisions taken via algorithmic decision-making? Given the importance of public trust in algorithmic decision-making in the public sector, what are some best practices to effectively engage with and educate the public and stakeholders on algorithmic decision-making?'.

530. State Council of China, "A New Generation Artificial Intelligence Development Plan", July 2017, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>

531. The Copyright Department, "National Copyright Administration of China, Response to the World Intellectual Property Organisation Discussion Paper", February 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_china_ncac.pdf

532. Laurence MacPhie, "Canada: 2019 Artificial Intelligence Year in Review", March 2020, available at: <https://www.mondaq.com/canada/patent/898914/2019-artificial-intelligence-year-in-review>

533. Id.

534. Submission from the Government of Canada, "WIPO Consultation on Artificial Intelligence and Intellectual Property", February 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_canada.pdf

UK

Maturity Index – 3/5

The Copyright, Designs and Patents Act 1998 (**CDPA**) is the primary legislation governing the protection of IPRs in the UK. The CDPA makes special provision for Computer Generated Works (**CGW**) with different rules for authorship and copyright duration. Under section 178 of CDPA, CGW are defined as those generated by a computer in circumstances such that there is no human author of the works. For these works, the CDPA under section 9(3) provides that, in the case of a literary, dramatic, musical or artistic work which is computer generated, the author shall be taken to be the person by whom the arrangement necessary for the creation of the work are undertaken. This, however, does not in itself grant the copyright to the AI but it does make such works copyrightable. By contrast to copyright, there is no statutory provision governing patents for CGWs, and there appear to have been no cases on the subject⁵³⁵.

The report published by the Select Committee on AI also discusses the issue of IPR in AI. However, the same pertains to the issue of patenting of AI systems. To this end it recommends that universities should use clear, accessible and where possible common policies and practices for licensing IPRs and forming spin-out companies. To supplement this, it also recommended the Alan Turing Institute should develop the abovementioned concept into concrete policy advice for universities in the UK, looking at examples from other fields and from other nations, to help start to address this long-standing problem.

Much like other countries, UK also responded⁵³⁶ to the WIPO Discussion Paper in February 2020. The IP Office of UK in the aforementioned response expressed that it is interested in exploring the importance of IP framework in ‘harnessing’ the power of AI. It further informed that most of the questions included in the WIPO Discussion Paper were also discussed in the 2019 London AI conference. On the issue of patents, UK submitted that there are some important questions that need to be answered including AI’s capability to generate inventions without any human intervention and the rationale for granting IPR protection to such inventions. It also highlighted the need for discussing the standard of inventive test when AI is used as tool for inventing something and wanted the same to be included. Further, on the issue of copyrights it submitted that currently the AI systems require some level of human intervention and the scope of the discussion should be broad enough to include such systems that require human intervention and are not entirely autonomous to understand the issue of ownership and standard for granting protection. It also asked the issues of designs and trademarks to be included in the questionnaire so as to include them in the scope of discussion.

On 7 September 2020, the UKIPO issued a call for views to consider how the IP framework currently relates to AI and future directions for AI and IP policy. It sought comments on six sections, covering patents, copyrights, designs, trademarks, trade secrets and general questions across IPRs. It is expected to publish a report in early 2021, on the basis of the comments received.⁵³⁷

FRANCE

Maturity Index – 3/5

The report⁵³⁸ commissioned by French Government and prepared by Member of Parliament Cedric Villani, that forms the basis for the French National Strategy on AI addresses the issue of IPR from a different perspective. It discusses that

535. Ryan Benjamin Abbott, “Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the UK”, Research Handbook on Intellectual Property and Digital Technologies (Tanya Aplin, ed.), 2017, available at: <https://ssrn.com/abstract=3064213>

536. UK Intellectual Property Office, “Response to the World Intellectual Property Organisation Draft Discussion on AI and IPR”, February 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_united_kingdom.pdf

537. Morgan Lewis & Bockius LLP, “Artificial Intelligence and Intellectual Property: Transatlantic Approaches”, November 2020, available at <https://www.lexology.com/library/detail.aspx?g=da7ffc2d-e1b7-46ef-9eb5-5865cbd69e83>

538. Cedric Villani, “For a Meaningful Artificial Intelligence: Towards a French and European Strategy”, 2018, available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

there is need to balance the disclosure for the purpose of maintaining transparency on the one hand and falling foul of the provisions relating to IPR rights on the other hand. In that regard, the report recognises the need of the government to formulate guidance for a better functioning of the same. The same issue has been touched upon in a report⁵³⁹ by the French Data Protection Authority, CNIL to the extent that it says that disclosure of the working of an AI system clashes with the right to protect IPR and both need to be balanced to keep the private sector motivated for innovation in the AI sector.

In its response⁵⁴⁰ to the WIPO Discussion Paper, the National Institute of Industrial Property submitted crucial inputs on various issues relating to copyright, patent, design etc. In relation to patents, various crucial questions were posed by the country in its response, such as how the moral right of an inventor can be applied to an AI system; Is it necessary to establish a specific legal link between the AI and a potential rightful claimant; If the patent eligibility to the autonomously generated inventions should be denied, then on what basis is this to be done; do amendments need to be introduced in patent examination guidelines for AI assisted inventions; etc. It also submitted various questions that it believes should be added on the issue of ownership and authorship like 'Should copyright be attributed to original literary and artistic works that are autonomously generated by AI or should a human creator be required?', 'In the event copyright can be attributed to AI-generated works, in whom should the copyright vest? Should consideration be given to according a legal personality to an AI application where it creates original works autonomously, so that the copyright would vest in the personality and the personality could be governed and sold in a manner similar to a corporation?' and 'Should a separate sui generis system of protection (for example, one offering a reduced term of protection and other limitations, or one treating AI-generated works as performances) be envisaged for original literary and artistic works autonomously generated by AI?'. On the issue of infringement of copyright, the questions suggested were 'Should the use of the data subsisting in copyright works without authorization for machine learning constitute an infringement of copyright? If not, should an explicit exception be made under copyright law or other relevant laws for the use of such data to train AI applications?', 'If the use of the data subsisting in copyright works without authorization for machine learning is considered to constitute an infringement of copyright, what would be the impact on the development of AI and on the free flow of data to improve innovation in AI?', 'If the use of the data subsisting in copyright works without authorization for machine learning is considered to constitute an infringement of copyright, should an exception be made for at least certain acts for limited purposes, such as the use in non-commercial user-generated works or the use for research?', 'If the use of the data subsisting of copyright works without authorization for machine learning is considered to constitute an infringement of copyright, how would existing exceptions for text and data mining interact with such infringement?', 'Would any policy intervention be necessary to facilitate licensing if the unauthorized use of data subsisting in copyright works for machine learning were to be considered an infringement of copyright?' and 'How would the unauthorized use of data subsisting in copyright works for machine learning be detected and enforced, in particular when a large number of copyright works are created by AI?'.

GERMANY

Maturity Index – 3/5

The extent to which AI is patentable was one of the main topics of the AI conference at the German Patent and Trademark Office (**DPMA**)⁵⁴¹ The three-step approach of the DPMA in examining patentability was discussed, in the context of patentability of AI applications: Is the subject of the invention at least partly technical? Does the patent claim contain instructions which serve to solve a concrete technical problem by technical means at least in partial aspects? And: Is the claimed subject matter considered new and inventive in relation to the state of the art? It further noted that as per

539. CNIL, "How Can Humans Keep the Upper Hand", December 2017, available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

540. National Institute of Industrial Property (France), "INPI's Contribution to the Public Consultation on the Draft Position Paper on Artificial Intelligence And Intellectual Property Policies prepared by the WIPO Secretariat", February 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_france_inpi.pdf

541. German Patent and Trade Mark Office, "AI and Future of Intellectual Property Rights: How Can Future Technology be Protected", available at: https://www.dpma.de/english/our_office/publications/background/ai/aiconferenceatdpma/index.html

the jurisdictional case law that considered Computer Implemented Innovations (**CII**) guidelines,⁵⁴² for a CII to become patentable, the claimed teaching must contain instructions which serve to solve a practical technical problem by technical means. It further added that however, it is sufficient for a partial aspect of the protected teaching to overcome a technical problem.

In the response submitted by Germany to the WIPO Discussion Paper the country asked for a common understanding of terms such as 'AI-assisted inventions' and 'AI Application'. It also submitted that 'a more detailed characterization of problems would allow a better understanding of the questions with regard to specific challenges addressed'. On the issue of inventions autonomously generated by AI, Germany commented that a sound understanding as to how AI can generate inventions, is needed before going further into the policy questions. It further suggested the addition of the question – 'How can the authorities identify an autonomously AI generated, or AI assisted invention without (mandatory or voluntary) information by the applicant?'. It also submitted that the categories such as 'AI generated inventions (where AI acts autonomously without human intervention)'; 'AI-assisted inventions (where humans use AI as a tool to invent)' and 'AI implemented inventions (where AI is implemented as part of the invention)' should be properly distinguished. On the issue of amending the patent examination guidelines the country comments that it is too early to ask this question as of now. On the question related to 'person skilled in art' the country suggests that more general questions should be asked as they have been asked under the head of 'Disclosure' in the draft. The questions under the 'Disclosure' head relate to the functioning of the AI systems to understand the level of disclosure that can be possible in an AI system. On the issue of copyrights, Germany suggests that a factual basis should be considered before delving into the specific questions related to copyright. It further observes that the issue of right of the author's protection of copyright doesn't suit the context since AI does not have a legal personality and therefore, as such cannot be granted authorship rights. It also submitted that one rationale behind giving authors the copyright is to incentivise them to produce more work. However, now that the AI has developed at a fast pace without any protection then 'this could indicate that a protection system is not necessary'. The submission also pointed out that if a protection system for the AI is to be considered, then the same must consider the requirement of a 'sector wise differentiation'.

Finally, on the issue of infringement, Germany responded by noting that the questions mentioned thereby have been answered in Article 3 and 4 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. While article 3 talks about the need to 'adapt and supplement' the existing copyright framework owing to the development in technology, article 4 says that the Directive complements rules laid down in the directives currently in force in EU.

ISRAEL

Maturity Index – 3/5

Currently there are no specific regulations/laws that address either the issue of patentability of AI systems or that of protection of AI generated works. The Israel Patent office has adopted a similar approach to the European Patent Office that the AI system will be treated as software that has been used to implement a particular invention. Therefore, the cornerstone of examination would be the technical effect that has been brought about by the invention as a whole.⁵⁴³

Unlike the requirement of legal personhood as required for inventorship in US, the Israel IPR regime considers the applicant to be the first owner of the patent. Therefore, in effect, the process does not raise issues with regards to the presumption of ownership. This peculiar situation may be conducive for obtaining the patent protection for the machine-made invention by a person who is the owner/designer of the AI system that created the invention.⁵⁴⁴

542. German Patent and Trademark Office, "Computer Implemented Innovations", October 2020, available at: https://www.dpma.de/english/patents/patent_protection/protection_requirements/computerimplemented_inventions/index.html

543. Asia Kling, Golan Kaneti, et al, "Machine and Big Data in 2019: Israel", Global Legal Insights, available at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/israel>

544. Ibid.

RUSSIA

Maturity Index – 3/5

As per the Russian IPR law regime, algorithms are excluded from copyright protection. However, many AI systems including the underlying AI code can be protected as knowhow. But to avail such a protection the AI system must have an actual or potential commercial value. It is important to note that as per the Russian laws a company can be considered as an exclusive right holder of a software provided that the same is created by the employees of the company working on a work-for-hire basis.⁵⁴⁵

Russia in its response⁵⁴⁶ to the WIPO Discussion Paper suggested the addition of various questions pertinent to the issues related to patents and copyrights. It suggested that the question that must be asked is if AI can manage IPR including the payment of fee, enter into licensing agreements, represent itself in court etc.) and what mechanisms are or should be put in place in order to make it possible. Further on the issue of patents it asked the discussion to focus on differentiating between the inventions autonomous generated by AI, inventions created jointly by AI and humans and computer-assisted inventions created by humans. It also raised the question if a 'quasi-separate' structure is to be created for AI and humans. In relation to copyright, it raised questions such as what would be the incentive for the AI systems to license their IPR and should an AI request permission to use the results created by another AI and what can be the conditions of such arrangement?

DENMARK

Maturity Index – 3/5

There does not appear to be any specific discussion around the impact of AI on IPRs both in terms of affording IPR protection to AI systems and AI itself being granted authorship or ownership under IPR laws. The protection of AI algorithms falls under the same legal framework as the traditional software. Algorithms, like many IPR law regimes, cannot be patented or copyrighted per se and can be normally protected as a part of the computer program.⁵⁴⁷

EU

Maturity Index – 3/5

In June 2019, the High-Level Expert Group on Artificial Intelligence (**AIHLEG**) in its Policy and Investment Recommendations report⁵⁴⁸

examined the importance of IPR law regimes for the smooth development and deployment of AI systems. The report recommends that guidance should be issued to ensure the participation of industry in research collaborations and R&D-based innovation so that the IPRs are also not undermined. It also mentions that the collaboration with industry and other stakeholders should be based on an appropriate model for IPRs.

545. Maria Ostashenko and Arman Galoyan, "AI, Machine Learning and Big Data, 2019: Russia", available at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/russia>

546. Russia State Space Corporation, "Response to the WIPO Draft Discussion Paper on AI and IPR", 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_russian_federation.pdf

547. Timo Minssen, et al, "AI, Machine Learning and Big Data 2019: Denmark", Global Legal Insights, available at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/denmark>

548. EC High Level Expert Group on AI, Policy and Investment, "Recommendation for Trustworthy Artificial Intelligence", June 2019, available at: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>

Further, the report⁵⁴⁹ by European Parliament on Civil Liability rules for Robots noted that currently there are no legal provisions that specifically apply to robotics, but the existing legal regimes and doctrines can be readily applied. At the same time, it calls on the EC to support a horizontal and technologically neutral approach to IPRs applicable to the various sectors in which robotics could be employed. The motion for resolution with the report calls on the EC to elaborate upon the criteria for 'own intellectual creation' for copyrightable works produced by computers or robots is pertinent. Along the same lines, the Communication⁵⁵⁰ by the EC to the European Parliament on AI released in 2018 also comments that a reflection is needed on the interaction of AI and IPRs, from the perspective of IPR offices as well as the users, and developers with a view to fostering innovation and legal certainty in a balanced way.

Further, the patentability of the AI systems and algorithms is also guided by the Guidelines for Examination⁵⁵¹ issued by the European Patent Office (**EPO**). As per the guidelines, the algorithms and computational methods form the basis of AI and machine learning and are of abstract nature *per se* and for them to be patented they must have a technical character. This means that if a claim is directed either to a method involving the use of technical means (for example, a computer) or to a device, its subject matter has a technical character as a whole and is thus not excluded from patentability. The release of new Examination Guidelines by EPO also means that while earlier it was the applicant of the patent who had to prove the technical character of the algorithm, now the EPO experts will have to prove the lack of it to exclude algorithms from patentability.⁵⁵²

The EU also submitted a response⁵⁵³ to the public consultation on the WIPO Discussion Paper. As per the submission, the EU notes that the WIPO should focus on specific issues such as identification of AI-generated or AI-assisted inventions by the IP Offices, the possibility of naming a legal person as inventor and the possible consequences to society of giving inventorship rights to AI, in the context of patents. In the case of copyrights, it considered that the focus should be on questions such as whether the content created by the AI systems is copyrightable, and also on the content created with the assistance of AI.

In October 2020, the EU Parliament Committee on Legal Affairs published a report on IPRs for the development of AI technologies,⁵⁵⁴ which considers a more defined approach to IP and AI than the US and other countries. It considers that any future approach to govern IP and AI systems should take the form of a regulation, rather than a directive, in order to harmonize laws across the EU region. Moreover, it emphasizes that the role of IP is to protect the interests of human creators and encourage innovation. Nevertheless, it recognizes that AI-generated works may be copyrightable, with the right being vested in the ultimate human creator. It is expected to publish a draft legislative proposal on this issue by early 2021.⁵⁵⁵

549. European Parliament, Committee on Legal Affairs, "Report with Recommendations to the Commission on Civil Law Rules for Robots", January 2017, available at: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf

550. EC, "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic And Social Committee and the Committee of the Regions: Artificial Intelligence for Europe", April 2018, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

551. European Patent Office, "Guidelines for Examination in the European Patent Office", Chapter II, 3.3.1, November 2018, available at: https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1.htm

552. Grzegorz Wesela-Bauman, "New EPO Guidelines – Easier Procedures For Patenting AI-Based Inventions", November 2019, available at: <https://www.mondaq.com/patent/865922/new-epo-guidelines-easier-procedures-for-patenting-ai-based-inventions>

553. EU, "Response of the EU and its Member States to the Public Consultation on the WIPO Draft Issues Paper on Intellectual Property and Artificial Intelligence", December 2019, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/org_european_union.pdf

554. European Parliament Committee on Legal Affairs, "Report on Intellectual Property Rights for the Development of Artificial Intelligence Technologies", 2 October 2020, available at https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.pdf

555. Morgan Lewis & Bockius LLP, "Artificial Intelligence and Intellectual Property: Transatlantic Approaches", November 2020, available at <https://www.lexology.com/library/detail.aspx?g=da7ffc2d-e1b7-46ef-9eb5-5865cbd69e83>

AUSTRALIA

Maturity Index – 3/5

IP Australia (Office for IPR for Australia) in December 2019 prepared a report⁵⁵⁶ for the Australian Computer Society. The report does not comment on the patentability of the algorithms or the inventions made by the AI systems as much as it analyses emerging technologies in machine learning relating to AI in various sectors and maps the patent applications trends of the same. As per the report, a total of 36,740 patents filed since 2012 in the world involved machine learning. The report also points out that China is both the largest patent filing destination with 73 per cent (26,758) of machine learning inventions filed here, and the largest source of innovation in machine learning, with 69 per cent (25,319) of patent families having a Chinese applicant. The report also makes it clear that United States, South Korea and Japan follow China to be the second, third and fourth top patent destinations and countries of origin, respectively, for patent applications relating to machine learning. Further, the report also found that the greatest number of patents related to machine learning were filed in the technology that engaged in image recognition, followed by analytics/processing, speech/ text analysis, control and automation and finally signal analysis.

In its submission⁵⁵⁷ on the WIPO Discussion Paper, Australia acknowledged the need for discussion on the underlying issues. It further suggested various questions that warrant discussion such as 'should the law on inventorship/ownership by AI be codified or allowed to develop judicially?', 'can AI at most be a co-inventor, in conjunction with either the creator of the machine or the person who put the invention into practice (or both)?' et cetera. The submission also raises some important policy questions on the duration of the protection granted to the AI generated content/technologies, who would be the beneficiary in case such and how much of the functioning of the AI warrants disclosure. Finally, it raised the question of ethical concerns that need to be considered in the use of AI in IP administration and what skills will the examiners need in order to use AI assistance in their decision making.

JAPAN

Maturity Index – 3/5

In 2018, the EPO and the Japan Patent Office (**JPO**) released a comparative study⁵⁵⁸ on CII / Software Related Inventions (**SRI**) in order to reveal the similarities and differences of examination practices specific to software related inventions. As stated in the report JPO follows two steps to make the assessment as to inclusion of SRI under the purview of inventions. First, if the claimed SRI is 'creation of a technical idea utilizing a law of nature', and second, if 'the idea is based on standpoint of software'. As per this analysis in Japan, if a computer software causes a computer to execute a method which is the creation of a technical idea utilizing a law of nature then the same can be called an invention.

The JPO in 2019 released a guidance document⁵⁵⁹ on the examination of AI related patents. The guidance document claimed that the AI related patents can easily be examined as per the current Examination Guidelines of the JPO. It further pointed out the specific provisions that need to be adhered to for examination of AI related patents and also presents case examples for better clarity. The same was later supplemented by more case examples⁵⁶⁰ and a lucid explanation of description requirements such as enablement and written description and also expounds upon the inventive step requirement as given in the examination guidelines.

556. IP Australia, "Machine Learning Innovation: A Patent Analytics Report", December 2019, available at: https://www.ipaustralia.gov.au/sites/default/files/reports_publications/patent_analytics_report_on_machine_learning_innovation.pdf

558. EPO & Japan Patent Office, "Comparative Study on Computer Implemented Inventions/Software Related Inventions", 2018, available at: https://www.jpo.go.jp/e/system/laws/rule/guideline/patent/document/ai_jirei_e/01_en.pdf

559. Japan Patent Office, "Case Example Related to AI Technologies, 2019", available at: https://www.jpo.go.jp/e/system/laws/rule/guideline/patent/document/ai_jirei_e/jirei_e.pdf

560. Japan Patent Office, "Newly Added Case Examples Related to AI Technologies", 2019, available at: https://www.jpo.go.jp/e/system/laws/rule/guideline/patent/document/ai_jirei_e/jirei_tsuika_e.pdf

Further, the AI Research and Development Guidelines⁵⁶¹ for International Discussion released by Japan in 2017 guide the developers to 'make efforts to promote open and fair treatment of license agreements for and their conditions of IPRs, such as standard essential patents, contributing to ensuring the interconnectivity and interoperability between AI systems and other AI systems, etc., while taking into consideration the balance between the protection and the utilization with respect to IPR related to the development of AI'.

SINGAPORE

Maturity Index – 3/5

In April 2019, the Intellectual Property Office of Singapore (**IPOS**) released the revised set of Examination Guidelines⁵⁶² for patents clarifying that the mathematical methods such as AI algorithms per se cannot be considered as inventions as per the Singapore Patents Act. However, a patent claim may be considered more than a mere mathematical method if it is functionally limited to solve a specific problem as opposed to a generic one. The revised guidelines also note the potential breadth of AI applications and that care should be taken when the contribution of claims falls within other subject matter not considered as inventions, such as an AI algorithm that streamlines business methods.

In the same month, IPOS launched the Accelerated Initiative for AI.⁵⁶³ The initiative offers applicants filing an AI-related invention a significantly reduced timeline to grant patents, potentially as short as six months or less, without any additional fees.

IPOS also submitted its response⁵⁶⁴ to the WIPO Discussion Paper. In the response IPOS acknowledged the surge in AI related patent based on WIPO data and posed critical questions for discussion such as unauthorised use of data (which may potentially include copyright protected works) for machine learning and if the same constitutes breach of IP rights; capacity building using AI systems in IP administration and IP offices and accountability of decisions made by AI systems in IP administration (examination). Further, the response also sheds light on the economic incentive for innovation and comments that the discussion on copyrights being granted to AI must not be restricted to human creativity. With regards to patents, the response of IPOS invited consideration on the joint ownership framework to ascertain (joint) ownership on the AI generated inventions.

SOUTH KOREA

Maturity Index – 3/5

In 2017, the Korean Ministry of Justice published the 27th Volume of the magazine titled Recent Trends of Law and Regulation in Korea.⁵⁶⁵ The magazine featured an expert column on the convergence of IPRs and Fourth Industrial Revolution era. The column expounded upon various ways the issues regarding IPR and AI converge in patents and copyrights. The column

561. (Japanese) Ministry of Internal Affairs and Communication, "Draft AI R&D Guidelines for International Discussions", July 2017, available at: https://www.soumu.go.jp/main_content/000507517.pdf

562. Intellectual Property Office of Singapore, Para 8.22-8.27, "Examination Guidelines for Patent Applications at IPOS", April 2019, available at: https://www.ipos.gov.sg/docs/default-source/resources-library/patents/guidelines-and-useful-information/examination-guidelines-for-patent-applications-at-ipos_2019-apr.pdf

563. Intellectual Property Office of Singapore, "Circular No. 2/2019: Launch of AI2 - Accelerated Initiative for Artificial Intelligence: An Accelerated Application-to-Grant Service for Patent Applications in Artificial Intelligence", April 2019, available at: [https://www.ipos.gov.sg/docs/default-source/resources-library/patents/circulars/\(2019\)-circular-no-2--ai2-initiative_final.pdf](https://www.ipos.gov.sg/docs/default-source/resources-library/patents/circulars/(2019)-circular-no-2--ai2-initiative_final.pdf)

564. Intellectual Property Office Singapore, "Response to Public Consultation on Artificial Intelligence and Intellectual Property Policy", 2019, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_singapore.pdf

565. Ministry of Justice, "Recent Trends of Law and Regulation in Korea", Volume 27, 2017, available at: <http://www.moj.go.kr/bbs/moj/168/319098/download.do>

further divides the issue of patents into three categories, with the first category relating to the patentability of the AI system itself, and category two and category three of inventions pertaining to the instances wherein the AI assists and generates the invention respectively, which can be patented. The column also addressed the issue of artistic content generated by the AI systems and if the same can be copyrightable or not. The column without giving any concrete suggestion merely discusses the issue of ownership and granting of IP rights in case the invention/content is generated by AI.

In 2018, Korean Intellectual Property Office (**KIPO**) rolled out a program for accelerated examination of the patents application with AI being one of the seven technologies identified to get the benefit of prioritised examination.⁵⁶⁶

KIPO also submitted its comments on the WIPO Discussion Paper.⁵⁶⁷ In its submission KIPO recognised the need for discussion on whether AI generated IP should be given protection or not. But specifically, it suggested that the issue should be looked from the angle of its impact on industrial development and that such protections incentivise innovation. It also suggested a discussion on the duration of such a protection and commented that providing these systems the protection for the same amount of time is unnecessary. Further, the submission also brings to light the issue of effect of AI on trademark law. According to the KIPO submission there is an increase in AI-assisted consumer product selection can lead to a decrease in the reliance on consumer recognition of brands and less possibility of brand confusion over products when selected by AI. This in turn may affect appropriate methods of observation to determine the similarity of the trademark and that the same can be a starting point for the discussion of convergence between AI and trademark law.

SWEDEN

Maturity Index – 3/5

Sweden's Innovation Agency, Vinnova, in its report⁵⁶⁸ released in May 2018 categorised the issue of IPR as one of the threats in its SWOT analysis. Further the report brings to light the surge in AI related patent applications. This goes to show that Sweden has had some experience in respect of the convergence of IPR with AI. In the absence of any specific guidance for the patentability of the AI systems it is important to note that AI related patent applications continue to be governed as per the existing framework.

It is important to note that like other jurisdictions, Swedish patent law also includes an algorithm under the purview of patentability if it has been given a technical nature by allowing it to be run by device that solves a technical problem or performs a technical function, in which case the whole system is patentable.⁵⁶⁹

FINLAND

Maturity Index – 3/5

The Finnish Patent and Registration Office (**PRH**) organised a seminar⁵⁷⁰ on AI and its relationship to IPRs on 5 February

566. Danny Yap and Judia Kok, "Artificial Intelligence: Disruption in Progress", SAL Practitioner, December 2019, available at: <https://journalsonline.academypublishing.org.sg/Journals/SAL-Practitioner/Fintech/ctl/eFirstSALPDFJournalView/mid/595/ArticleId/1483/Citation/JournalsOnlinePDF>

567. Korean Intellectual Property Office, "Comments on the Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence", available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_korea.pdf

568. Vinnova, "Artificial Intelligence in Swedish Business and Society: Analysis of Development and Potential", May 2018, available at: https://www.vinnova.se/contentassets/29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf

569. Marcus Swensson, Lisa Hellewig, Hakan Nordling, "AI, Machine Learning and Big Data 2019: Sweden", Global Legal Insights, June 2019, available at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/sweden>

570. Finnish Patent and Registration Office, "IP Rights as Key Success Factors for AI Driven Businesses", February 2019, available at https://www.prh.fi/fi/tietoa_prhsta/tapahdumat/M0MqZ2Mqc.html

2019. The seminar saw some key speakers from the PRH deliver guidance presentations on various aspects of AI and IPR. The presentation⁵⁷¹ delivered by the Principal Patent Examiner of PRH shed some light on the patentability of the Computer Implemented Inventions. It highlighted that much like the approach followed by most of the European countries Finland also follows the two-hurdle approach for the examination of such patents. Firstly, the CII must have a technical nature and secondly there must be an involvement of inventive step over the prior art and such an inventive step cannot be based on non-technical features. Similarly, another presentation⁵⁷² delivered by the Government Counsellor examined the benefits and challenges with AI driven technologies for copyrights. The presentation largely discussed the use of AI in streamlining the licensing process and did not talk about issues like copyright of the AI generated content.

Apart from this, Finland is also in the process of preparing a nationwide IP Strategy keeping in mind the development and deployment of AI systems in the country.⁵⁷³ In February 2020, Government of Finland also submitted its response⁵⁷⁴ to the WIPO Discussion Paper. The submission suggested some important questions to be considered in the discussion such as the level of autonomy to distinguish the AI system as a mere tool of assistance from the AI system as an inventor; how would the society benefit by rewarding autonomous inventors with patents and if identical AI systems operated by separate corporations then be given different identities? Further, the submissions pose similar question with respect to copyright and then goes on to explain the reasons for the inclusion of such question in the scope for discussion. The Finnish IP Office, through the submission makes it abundantly clear that it does not support copyrights to be granted to the AI generated content since the very basis for the social and legal justification of the copyright system lie on the human creative spirit and respect and reward for the expression of human creativity. As per the submission, the content generated by AI does not involve 'human creativity'. It further suggests that the term 'AI creations' must be replaced with the term 'AI output' for a better understanding of the concepts and terms. The submission also brings to light the issue of identification of works so that only the work of original human creativity is accorded with the copyright and suggests the formation and application of unique identification codes for each author, or producer, and as well as piece of work at a global level. Comments also include certain questions raised by the Ministry of Education and Culture pertaining to the identification of the different works by humans and AI systems and levels of disclosure.

SPAIN

Maturity Index – 3/5

Spain does not have a specific policy either with respect to the protection of AI systems or protection being given to the works and inventions generated by AI. However, protection can be granted to complex algorithms for the 'simple existence of a substantial investment at an economic level'. Also, there is some insight with respect to ownership that Spain has jurisprudence for. As per the Spanish law, if the algorithm has been prepared by a worker under specific instructions of the employer then the employer can claim the ownership of the protection granted to that particular algorithm.⁵⁷⁵ Spain also submitted its response to the WIPO Discussion Paper.⁵⁷⁶

571. Mika Inki, "Some Principles for Successful Protection of AI", February 2019, available at: https://www.prh.fi/stc/attachments/info/kurssitjaseminaarit/Principles_05-02-2019_Mika_Inki.pdf

572. Anna Vuopala, "Benefits and Challenges with AI Driven Technologies for Copyrights", February 2019, available at: https://www.prh.fi/stc/attachments/info/kurssitjaseminaarit/AI_seminar_Vuopala_LS.pdf

573. Government of Finland, "Government Report on Information Policy and Artificial Intelligence", 2018, available at https://vm.fi/documents/10623/7768305/VM_Tiepo_selonteko_070219_ENG_WEB.pdf/89b99a8e-01a3-91e3-6ada-38056451ad3f/VM_Tiepo_selonteko_070219_ENG_WEB.pdf.pdf/VM_Tiepo_selonteko_070219_ENG_WEB.pdf

574. Government of Finland, "Comments by Finland on WIPO Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence", May 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/submissions_march2020/ms_finland.pdf

575. Sonke Lund, "AI, Machine Learning and Big Data 2019: Spain", Global Legal Insights, June 2019, available at: <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/spain>

576. The Spanish response to the WIPO discussion paper (available at https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/submissions_march2020/ms_spain_e_s.pdf) could not be reviewed as there was no English translation.

NORWAY

Maturity Index – 3/5

Norway's National Strategy on AI⁵⁷⁷ released in January 2020 acknowledges the importance of reviewing the IPR regime in the country in the wake of advancement in AI systems. The strategy notes that the Ministry of Trade, Industry and Fisheries has already begun mapping the needs in the area of IPR rights in Norwegian industry and will assess whether the guidance offered on the system of policy instruments is adequate. The strategy also mentions the issue of ascertainment of ownership and user rights when development of an AI-based solution is conducted through cooperation between the public sector and a private company. It also brings forth the need to balance the level of disclosure (for transparency) and IPR but does not specifically present a solution.

ESTONIA

Maturity Index – 3/5

The National AI strategy⁵⁷⁸ of Estonia does not propose any specific strategy regarding IP. The only reference to IP concerns the suggestion that one of the measures in developing AI research and development in Estonia should be ensuring support in IP matters to companies involved in such research. In its submission⁵⁷⁹ to WIPO, Estonia answered that currently there are no specific provisions that have been enacted in the IP law in the country related to AI. However, it confirmed there exists a text and data mining exemption in the Estonian Copyright Act since 2017 which, among else, enables training of AI algorithms in the academic and research sphere using copyrighted content. It also informed that the Estonian Copyright Act allows the mining of data without the permission of the author if it not for the commercial purpose.

In its response⁵⁸⁰ to the WIPO Discussion Paper, Estonia endorsed the view taken by the submission of EU and further called upon the member states to discuss the regulatory procedures in order to understand and tackle the impact of AI on IP regime.

THE NETHERLANDS

Maturity Index – 3/5

The Strategic Action Plan for AI,⁵⁸¹ released by the government in October 2019 addresses the issue of AI and IPR in more detail than most of the national strategies on AI. The document recognises the two-fold question that related to AI and IPR. The grant of IP protection to the AI system as a creation and grant of IP protection to the AI generated content or invention. It raises important questions like what kind of rights apply to the AI systems and what is the nature of these rights, who is to be considered as the owner the creative content generated by AI and should the bar for obtaining copyrights or patents

577. Norwegian Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence", 2019, available at: https://www.regjeringen.no/contentassets/1febbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

578. Government of Republic of Estonia, "Estonia's National Artificial Intelligence Strategy 2019-2021", July 2019, available at: <https://www.kratid.ee/in-english>

579. Republic of Estonia, "Comments on the WIPO Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence", March 2020, available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/submissions_march2020/ms_estonia.pdf

580. (Estonian) Ministry of Justice, "Comments by the Ministry of Justice of the Republic of Estonia on the WIPO Draft Issues Paper on Intellectual Property and Artificial Intelligence", available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_estonia.pdf

581. Government of The Netherlands, "Strategic Action Plan for Artificial Intelligence", October 2019, available at: <https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence>

be raised when AI becomes a tool for authors or inventors. It further informs that currently there exists no specific IPR protection for AI and also touches upon the need to balance the level of disclosure and revelation of trade secrets.

As a matter of action, the Netherlands informs that it is keeping a close on developments in IPR laws at a European and International level and welcomes the new guidelines regarding the patentability of inventions based on AI, published by the European Patent Office in October 2018.

UAE

Maturity Index – 3/5

In October 2019, the UAE Ministry of Economy signed a Memorandum of Understanding with the KIPO to utilise AI technologies in IPR titles such as patents, trademarks, industrial designs, and copyright.⁵⁸² The Under-Secretary for Ministry of Economy of UAE mentioned the importance of IPR in stimulating the creativity and innovation and 'creating an environment conducive to research'. This goes to show that the government is aware of the convergence of IPR and AI and it can be expected that more policy discussion in this regard can be expected. Specific regulations or provisions with respect to AI and IPR could not be found.

HONG KONG

Maturity Index – 3/5

No regulation or policy discussion could be found with respect to IPR and AI in Hong Kong. Therefore, it is safe to say that the applications for patent and copyright are being examined as per the existing IP laws of the country. Further, there do not appear to be any government submissions in response to the WIPO Discussion Paper.⁵⁸³

^{582.} Esra Ismael, et al, "UAE, South Korea to Harness AI in Intellectual Property", Emirates News Agency, October 2019, available at: <https://www.wam.ae/en/details/1395302791496>

^{583.} See, https://www.wipo.int/about-ip/en/artificial_intelligence/submissions-search.jsp?type_id=&territory_id=302&issue_id=

CIVIL LIABILITY



AI systems have now advanced so much that they are on the cusp of becoming an integral and inextricable part of our lives, both as individuals and as a society. In several countries, AI systems are involved in handling crucial private and public functions such as counting of votes, approving loans, online advertising, autonomous transportation, etc.⁵⁸⁴ The development and the subsequent commercialization of AI systems raise the question of how liability risks will play out in real life. Since even the best technology is not error-free and as the interaction between humans and robots increases, domestic robots, self-driving cars, and other autonomous systems will inevitably cause harm to people and property. In light of the same, the question of how accountability for decision-making by AI systems should be allocated, has rightfully drawn attention. ‘However, as technical advancements are starting to outpace legal actions, it is not entirely clear how the law will treat AI systems.

As a preliminary step, several countries have considered whether the existing legal framework is enough to handle these questions of liability and accountability. Legal systems contain a well-defined (not necessarily codified) system of laws that ascertain civil, criminal and contractual liability of persons that have inflicted civil harm to the other person (or property). Researchers working to understand the interplay of law and technology opine that the traditional approaches to handling liability are inadequate for dealing with autonomous artificial agents due to a combination of two factors—unpredictability, and causal agency without legal agency.⁵⁸⁵ The unpredictability and inability to clearly explain the functioning of AI systems makes it

difficult to measure the extent of human intervention and control.⁵⁸⁶

Much of the discussion surrounding liability boils down to determining legal status of AI systems. Some researchers have argued in favour of granting a separate legal status to AI systems (similar to that given to companies), but that such status should be determined by the level of autonomous decision making and “intelligence” of the AI system.⁵⁸⁷ On the other hand, there are several arguments that disregard the idea of bestowing AI systems with a separate identity, as the issue of liability can be dealt with under a strict product liability regime;⁵⁸⁸ it is argued that treating AI systems as legally fictitious persons (like corporations) does not actually solve the problem and could give rise to several new problems.⁵⁸⁹

In terms of practical solutions, there appear to be multiple models; one of these is to upgrade or modify existing law to suit or accommodate technological advancements related to AI;⁵⁹⁰ Others have considered enacting a separate legislation that specifically addresses legal aspects of the development and deployment of AI systems.⁵⁹¹ In some cases, there have also been calls for the prior regulation of AI, i.e. that certain classes of new algorithms should not be permitted to be distributed or sold without approval from a government agency designed along the lines of the Food and Drug Administration of the USA that develops standards and ensures consequent compliance.⁵⁹²

The current chapter maps the approach that has been adopted by various jurisdictions to address the issue.

584. Joshua A. Kroll, et al, “Accountable Algorithms”, University of Pennsylvania Law Review, 2018, available at: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review

585. J.K.C. Kingston, “Artificial Intelligence and Legal Liability”, 2018, available at: <https://arxiv.org/ftp/arxiv/papers/1802/1802.07782.pdf>

586. Id at 2.

587. Matthew U. Scherer, “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies”, Harvard Journal of Law & Technology Volume 29 Number 2, Spring 2016, available at: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>

588. Paul Opitz, “Civil Liability and Autonomous Robotic Machines: Approaches in the EU and US”, Stanford-Vienna TTLF Working Paper No. 43, 2019, available at: https://law.stanford.edu/wp-content/uploads/2019/02/opitz_wp43.pdf

589. Peter M. Asaro, “The Liability Problem for Autonomous Artificial Agents”, AAAI Spring Symposia 2016, available at: <https://www.aaai.org/ocs/index.php/SSS/SSS16/paper/download/12699/11949>

590. Id at 2.

591. Id at 4.

592. Andrew Tutt, “An FDA for Algorithms”, Administrative Law Review, Volume 69 Issue 83, 2017, available at <http://dx.doi.org/10.2139/ssrn.2747994>

MATURITY INDEX CIVIL LIABILITY



Level 1

No Discussion

Level 2

Preliminary
Discussions

India, USA, China, Canada, UK, France,
Israel, Denmark, South Korea, Sweden, Finland, Spain,
Norway, The Netherlands, UAE, Hong Kong

Level 3

Established Policy
Position

Germany, Australia, Singapore, Estonia

Level 4

Policy
Recommendation

Russia, EU, Japan

Level 5

Implementation into
Legislation



INDIA

Maturity Index – 2/5

The National Strategy on AI⁵⁹³ released in 2018 addresses the issue of liability by drawing parallels with the airline industry wherein every accident is meticulously investigated to eliminate loopholes in security thereby making the industry safer and service providers more accountable. The Strategy proposes a framework that may include the following components:

1. Negligence test for damages caused by AI software, as opposed to strict liability. This involves self-regulatory damage impact assessment, by the stakeholders, at every stage of development of an AI model.
2. As an extension of the negligence test, safe harbours need to be formulated, to insulate or limit liability so long as appropriate steps to design, test, monitor, and improve the AI product have been taken.
3. Framework for apportionment of damages needs to be developed so that the involved parties bear proportionate liability, rather than joint and several liability (for harm caused by products in which Discussion Paper National Strategy for Artificial Intelligence 89 the AI is embedded) especially where the use of AI was unexpected, prohibited, or inconsistent with permitted use cases.
4. Actual harm requirements policy may be followed, so that a lawsuit cannot proceed only on the basis of speculative damage or a fear of future damages.

Additionally, it proposes the establishment of an Ethics Council at every Centre of Excellence (i.e., the organisation proposed to be established by the Strategy to advance research in AI), to set standards to understand liability and fix accountability on the developers and users of AI.

USA

Maturity Index – 2/5

In 2016, the US NSTC's Committee on Technology published a report⁵⁹⁴ which addresses the issue of accountability of AI systems. It In 2016, the US NSTC's Committee on Technology published a report⁵⁹⁴ which addresses the issue of accountability of AI systems. It

In 2019, the US House of Representatives adopted a resolution⁵⁹⁵ in support of developing guidelines in consonance with various AI principles, one being accountability. NIST's response,⁵⁹⁶ to the AI Executive Order acts as a guide for the development of standards for AI. It states that the developers contributing to these standards must work on accountability and auditing tools to enable examination of an AI system's output (e.g., decision-making or prediction). As per this document, these tools can improve traceability, by providing a record of events and information regarding technologies' implementation and testing. In doing so, they can enhance assessment and documentation of gaps between predicted and achieved AI systems' outcomes.

593. NITI Aayog, "National Strategy for AI #AIforAll", June 2018, available at: https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

594. NSTC, Committee on Technology, "Preparing for the Future of Artificial Intelligence", October 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

595. 116th Congress, H. Res. 153, February 2019, available at: <https://www.congress.gov/bill/116th-congress/house-resolution/153/text>

596. NIST, "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools", August 2019, available at: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

CHINA

Maturity Index – 2/5

The AIDP of China⁵⁹⁷, released in 2017, briefly discusses ascribing liability to the actions of AI systems. As one of the guarantee measures, the plan seeks to strengthen research on legal, ethical, and social issues related to AI, and establish laws, regulations and ethical framework to ensure healthy development of AI. In tandem, it also envisages conduction of research, on civil and criminal liability issues and development of laws on the same.

CANADA

Maturity Index – 2/5

There does not appear to be any specific regulation or policy approach that has been released by the Government of Canada to ascertain civil liability of AI systems. Hence, the performance of AI and any breach of their duty will be examined under the product and tort liability laws of the country. This would give rise to the difficulty of fulfilling the standards of "negligence", "intent", "foreseeability" or "defect" as relevant in tort, contract or consumer law, which are even more difficult to pin-point in the case of autonomously operating AI systems. While the issue of transparency and accountability are being considered from an ethics perspective and are required to be addressed in the design stage itself, it is unclear how any errors or harm caused by AI systems despite these measures could be addressed by traditional liability principles.⁵⁹⁸

UK

Maturity Index – 2/5

The UK currently does not possess a liability framework specifically applicable, to harm or loss resulting from the use of emerging technologies such as AI.⁵⁹⁹ However, a Select Committee for AI constituted by the House of Lords⁶⁰⁰ discusses the issue of liability of AI systems and recommends considering the adequacy of existing legislation to address the legal liability issues of AI and, where appropriate, recommend to Government remedies to ensure that the law is clear in this area.

The recommendation was welcomed by the Government of UK in its response⁶⁰¹ to the House of Lords report. It noted that the Government will involve the Office for Artificial Intelligence, Centre for Data Ethics and Innovation, and the AI Council to look into these aspects and will seek the guidance of the Law Commission wherever necessary.

597. State Council of China, "New Generation Artificial Intelligence Development Plan", 2017, available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>

598. Lisa Lifshitz, "It's hard to sue a robot: product liability considerations and AI in Canada", Canadian Lawyer, September 2018, available at <https://www.canadianlawyermag.com/news/opinion/its-hard-to-sue-a-robot-product-liability-considerations-and-ai-in-canada/275459>

599. Helen Scott-Lawler, "Artificial Intelligence: Legal Liability Implications", January 2020, available at <https://www.burges-salmon.com/news-and-insight/legal-updates/commercial/artificial-intelligence/legal-liability-implications/>

600. Select Committee on Artificial Intelligence, "AI in the UK: Ready, Willing and Able?", April 2018, available at: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10012.htm>

601. Secretary of State for Business, Energy and Industrial Strategy by Command of Her Majesty, "Government Response to House of Lords Artificial Intelligence Select Committee's Report on AI in the UK: Ready, Willing and Able?", June 2018, available at: <https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response2.pdf>

FRANCE

Maturity Index – 2/5

Currently there is no legal regime tailored to specifically govern AI and any liability arising from the same.⁶⁰² Thus it is governed under the existing civil liability laws of France. However, the 2018 report⁶⁰³ released by Member of Parliament Cedric Villani briefly touches upon the issue of accountability and acknowledges that at this stage, the accountability of AI systems based on machine learning, constitutes a real scientific challenge and recommends the establishment of a body of experts with the skills essential for the documentary auditing of algorithms and databases.

GERMANY

Maturity Index – 2/5

As with other countries, Germany currently does not have an AI specific legal regime to govern its liability issues. However, as a response, to the review of the National Strategy on AI, the Data Ethics Commission of Germany released its recommendations⁶⁰⁴ on the same in 2018. In the document, the Commission has suggested the inclusion of an additional objective of 'upholding ethical and legal principles based on Germany's liberal democracy, through the entire process of developing and applying artificial intelligence'. This was followed by a detailed opinion⁶⁰⁵ released by the Commission in October 2019 wherein it expressly advised the government against the idea of granting a separate legal personality to AI systems, with the intention of making the systems liable themselves. It notes that harm caused by autonomous systems should be attributed to those operating the systems in accordance with rules of vicarious liability, as in the case of human auxiliaries. It also discusses the existing law of the country governing liability and acknowledges that it may not be possible to solve complex technical legal questions that arise, and hence fail to pinpoint accurate solutions in terms of liability, at this stage. It concludes that the current liability regime needs to be re-assessed considering the range of usage, autonomy and control of AI systems.

RUSSIA

Maturity Index – 2/5

In Russia, the rules of the Civil Code of the Russian Federation are applied to ascertain the civil liability of a person; article 1064 of the Civil Code mentions that 'injury inflicted on the personality or property of an individual shall be subject to full compensation by the person who inflicted the damage'.⁶⁰⁶ It is also relevant to consider 'Grishin Law' that entered into force on 1 March 2018,⁶⁰⁷ which introduces a legal definition of robots as autonomous intellectual systems, i.e. autonomous from humans, and states that 'a robot is a device capable of acting, determining its actions and evaluating their consequences

602. Claudia Weber et al., "AI, Machine Learning and Big Data 2020: France", Global Legal Insights, May 2020, available at <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/france>

603. Cedric Villani, "For a Meaningful Artificial Intelligence: Towards a French and European Strategy", 2018, available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

604. Data Ethics Commission, "Recommendations of the Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence", October 2018, available at https://www.bmjjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen_englisch.pdf?__blob=publicationFile&v=3

605. Data Ethics Commission, "Opinion of the Data Ethics Commission", October 2019, available at: https://www.bmjjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

606. Maksim Karliuk, "The Ethical and Legal Issues of Artificial Intelligence", April 2018, available at: <https://russiancouncil.ru/en/analytics-and-comments/analytics/the-ethical-and-legal-issues-of-artificial-intelligence/>

607. Victor Naumov and Vladislav Arkhipov, "Dentons develops first robotics draft law in Russia", January 2017, available at <https://www.dentons.com/en/insights/alerts/2017/january/27/dentons-develops-first-robotics-draft-law-in-russia>

based on information coming from the external environment, without full human control'.⁶⁰⁸ Further, according to the law the owner and possessor of a robot agent shall bear responsibility for the actions of the robot agent to the extent of their owned property transferred into the possession and/or use of the robot agent. It also mentions that the 'in cases where the responsibility of the robot agent is connected with its legal nature as property (including if harm is caused by activity creating an increased danger to the public), responsibility for the action of the robot agent shall be borne by its possessor'.⁶⁰⁹

ISRAEL

Maturity Index – 2/5

Currently, there are no laws that specifically govern the liability of AI systems. General civil law is expected to address the issue along with legal precedents as and when they are passed in the Israeli courts.

DENMARK

Maturity Index – 2/5

Denmark's National Strategy for AI⁶¹⁰ emphasizes that the use of AI systems is governed under the relevant existing legislative provisions of the country. This implies that AI systems will be governed by existing liability laws as well. The strategy also proclaims that the government will monitor developments closely and regularly assess the need for guidelines on the interpretation of the current legal framework as well as the need for new legislation, as more experience is obtained with the technology and its possibilities. To this effect, the strategy envisages the establishment of an inter-ministerial working group to examine whether the issues in using AI can be managed within the existing legislative framework. The said working group will identify the need for guidelines on the regulations that apply in relation to the use of AI.

EU

Maturity Index – 4/5

One of the first documents published on the issue of civil liability of AI systems was the European Parliament commissioned study⁶¹¹ on European Civil Law Rules for Robotics in 2016. The study assessed the main challenges posed by emerging technologies and addressed the issue in two ways: Firstly, it noted that a machine cannot be equated to a human on a 'de facto' level and disregarded the idea of autonomous robots having a legal personality, as this would give rise to new legal conundrums. Secondly, with regards to liability, it noted that the damage caused by autonomous robots may also be traced back to user error and in such a situation, either strict or fault-based liability may be imposed on a case-by-case basis. However, the study asserts that there is a need to engage in more 'techno-legal' research to formulate an airtight liability regime.

608. A A Vasilyev, et al, "The Russian Draft Bill of "The Grishin Law" in terms of Improving the Legal Regulation of Relations in the Field Of Robotics: Critical Analysis", Journal of Physics Conference Series, Volume 1333 Number 5, October 2019, available at: <https://ui.adsabs.harvard.edu/abs/2019JPhCS1333e2027V/abstract>

609. Ibid at 14.

610. Ministry of Finance and Ministry of Industry, Business and Financial Affairs, "National Strategy for Artificial Intelligence", March 2019, available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf

611. European Parliament, Director General for Internal Policy, "European Civil Law Rules in Robotics", 2016, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

The aforementioned study was followed by the adoption of a 2017 resolution⁶¹² by the European Parliament with recommendations to the Commission on Civil Law Rules on Robotics. The resolution called on the EC to:

1. Adopt a proposal for a legislative instrument providing civil law rules on the liability of robots and AI;
2. Propose common definitions of cyber physical systems, autonomous systems, smart autonomous robots and their subcategories;
3. Establish criteria for the classification of robots that would need to be registered;
4. Establish a designated EU Agency for Robotics and Artificial Intelligence; and
5. Propose a charter consisting of a code of conduct for robotics engineers, a code for research ethics committees when reviewing robotics protocols, and model licenses for designers.

In a follow-up⁶¹³ to the resolution, it was found necessary to “examine whether and how to adapt civil law liability rules to the needs of the digital economy”. The EC stated that it intended to work with the European Parliament and the EU Member States on a collective EU response, as well as evaluate the product liability laws and explore risk-based liability regimes.

In March 2018, the EC set up an expert group on liability and new technologies⁶¹⁴, which was divided into two formations. The first sub-group, i.e., the Product Liability Directive Formation (**PLDF**), was tasked with assessing the product liability directive while the second sub-group, the ‘New Technologies Formation’ (**NTF**) was created to explore the main liability challenges raised by these new technologies. At the end of November 2019, the EC published NTFs main findings,⁶¹⁵ which looked at issues such as the complexity and opacity of AI systems and liability in the event of a breach of duty. It also provided a basis of liability, stating that comparable risks should be addressed by similar liability regimes, to better determine what losses are recoverable and to what extent. It further proposed that fault liability and strict liability should be able to co-exist for the victim to have more than one basis to seek compensation against more than one person, based on the circumstances.

On 19 February 2020, the EC presented its proposal for comprehensive regulation of AI at the EU level in the form of a white paper,⁶¹⁶ accompanied by a report⁶¹⁷ on safety and liability. While the white paper adopted a holistic approach towards the development of regulations at the EU level, the report on safety and liability analysed existing product safety and liability legislations in EU member countries. The report noted that the existing horizontal and sector-specific legislative framework was robust and reliable, owing to the fact that their current definition of product safety already includes an extended concept of safety, and that liability issues are generally covered by the existing liability concept. With regards to safety and liability, the report addressed issues like complexity of products, services, and the value chain; burden of proof in complex environments, level of autonomy and opacity.

612. European Parliament Resolution of 16 February 2017 with “Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))”, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&from=EN>

613. Follow up to the European Parliament Resolution of 16 February 2017 on civil law rules on robotics2015/2103 (INL), available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2017/11-20/A8-0005-2017_EN.pdf

614. EC, “Call for Experts for Group on Liability and New Technologies”, March 2018, available https://ec.europa.eu/growth/content/call-experts-group-liability-and-new-technologies_en

615. EC, “Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence”, 2019, available at: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>

616. EC, “White Paper on Artificial Intelligence - A European Approach to Excellence and Trust”, February 2020, available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

617. EC, “Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics”, February 2020, available at: https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf

In July 2020, the European Parliament published a report on Artificial Intelligence and Civil Liability,⁶¹⁸ which considers how technology regulation should be technology-specific and advocates a risk management approach. It notes the lack of a common notion of AI, even from a technological perspective and that most conceptions of AI are considered from the perspective of its application and end-use. This imposes strict liability (rather than fault-based) on the party who is best capable of controlling and managing a technology-related risk, for the purposes of litigation. It also includes various case studies and recommendations on this basis, including that the Product Liability Directive be reformed to be more claimant-friendly, given the opacity of AI systems is likely to give rise to difficulties in apportioning liability among multiple potential responsible parties. It also considers that ad-hoc legislation may be necessary to regulate AI given the complexity of the products and systems involved, and the difficulty of seeking relief through the Product Liability Directive.

AUSTRALIA

Maturity Index – 3/5

Currently, the issue of liability is assessed using the traditional duty of care concepts as they prevail in Australia. However, the discourse suggests that the 'owner' of an AI system should be subject to more stringent and strict liability for its actions, either through the development of the law of tort or statutory intervention.⁶¹⁹ Apart from this, a discussion paper⁶²⁰ released by the Australian Government provides an ethics framework that briefly discusses the issue of liability. It recommends that human-in-the-loop principles should be considered during the design phase of automated decision systems, and to ensure that sufficient human resources are available to handle the inquiries in this regard.

JAPAN

Maturity Index – 3/5

Due to lack of sufficient experience in contract practices and the gaps in understanding the scope of AI systems and their impact, the Japanese Ministry of Economy, Trade and Industry formulated the Contract Guidance on Utilization of AI and Data in 2018⁶²¹ to summarize issues and factors to be considered when drafting a contract on the utilization of AI or data. The guidance describes types of contracts and factors to be considered in contract preparation, with sample clauses provided. It also proposes that the assessment of the AI system or program, that is the subject matter of the contract, be followed by a reasonable description of the development process.

SINGAPORE

Maturity Index – 3/5

Even though the Model Framework for Governance of AI⁶²² prepared by the PDPC, does not establish a separate civil liability

618. European Parliament Committee on Legal Affairs, "Artificial Intelligence and Civil Liability", July 2020, available at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf)

619. Gavin Smith and Richard Cumbley, "Practical Guidance for AI Projects", 2019, available at https://www.allens.com.au/globalassets/pdfs/campaigns/report-ai-toolkit_may19.pdf

620. Dawson D et al, "Artificial Intelligence: Australia's Ethics Framework", Data61 CSIRO, 2019, available at: https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

621. (Japanese) Ministry of Economy, Trade and Industry, "METI Formulates "Contract Guidance on Utilization of AI and Data", June 2019, available at https://www.meti.go.jp/english/press/2018/0615_002.html

622. Infocomm and Media Development Authority and Personal Data Protection Authority, "Model AI Governance Framework (Second Edition)", January 2019, available at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

regime, it explicitly assumes that they will not absolve organisations from compliance with current laws and regulations. It also mentions that framework is an accountability-based framework, and therefore adopting it will assist organisations in demonstrating that the organizations have implemented accountability-based practices. The framework also provides for a system of audit of algorithms at the request of a regulator or any other authority having the jurisdiction to do so. This is expected to help in understanding the responsibility and the level of control exercised by the possessor, to allocate liability.

SOUTH KOREA

Maturity Index – 3/5

As with most jurisdictions, there are no civil liability laws specific to AI. This means that the issue regarding liability would continue to be governed as per the Korean Civil Act, which provides for fault liability, negligence (based on foreseeability of the injury caused), supervisor's liability, etc. In all these cases, the legislation imputes liability only on "persons", which does not cover AI systems. Even if a separate legal entity were created to include AI systems, it would be difficult to establish relationships such as that of a supervisor or employer with respect to the AI system. Moreover, if the responsibility of the manufacturer or developer (or any person that deploys the AI system) extends only to exercising due care, they would be exempt from liability where the AI system is able to operate autonomously and takes decisions that cause harm. As such, it would seem that further consideration is required to understand what adjustments are necessary to examine AI systems and the liability issues that arise therefrom.⁶²³

SWEDEN

Maturity Index – 3/5

Sweden does not have any legislation that pertains specifically to AI systems. This means that the liability issues continue to be governed by the existing laws and regulations of the country. Again, these legislations do not recognise AI as having a separate legal entity, and therefore, liability is more likely to be borne by individuals or companies related to the AI system, whether in the case of contracts, torts or product liability cases. These issues have not yet been discussed in detail, and therefore, it remains to be seen if a test case emerges to consider the way in which existing legal principles can be applied to AI systems.

FINLAND

Maturity Index – 3/5

Finland has published several reports on its priorities with respect to the incorporation of AI into society and governance.⁶²⁴ While each of these reports examine the latest developments in various sectors – e.g., the labour market, the automotive sector, governance, etc., they do not yet have a detailed investigation into the question of civil liability, aside from a solitary mention of the EU's efforts to develop a framework for considering this question at the Europe wide level.⁶²⁵

623. Won H Cho and Hye In Lee, "AI, Machine Learning and Big Data 2020: Korea", Global Legal Insights, available at <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/korea#chaptercontent7>

624. Ministry of Economic Affairs and Employment, "Finland's Age of Artificial Intelligence: Turning Finland into a Leading Country in the Application of Artificial Intelligence", 18 December 2017, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y; Ministry of Economic Affairs and Employment, "Work in the Age of Artificial Intelligence", 2018, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160980/TEMJul_21_2018_Work_in_the_age.pdf and Ministry of Economic Affairs and Employment, "Leading the Way into the Age of Artificial Intelligence", 2019, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf.

625. Ministry of Economic Affairs and Employment, "Leading the Way into the Age of Artificial Intelligence", 2019, available at, http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf.

SPAIN

Maturity Index – 2/5

Spain does not currently have any laws that specifically pertain to the activities of AI based systems. Its Digital Agenda (2013) was created with the purpose of giving effect to and building on the European initiatives with respect to AI based systems, with specific plans on digital inclusion, e-governance, smart cities and advancement of language technologies.⁶²⁶ While the focus of these plans are to invest further and create a suitable framework for R&D in AI systems in Spain, these discussions do not appear to have considered the question of liability, apart from reiterating the principles of accountability, avoiding bias and improving trustworthiness in AI based systems.⁶²⁷ As such, it is likely that any questions of liability arising from damage caused by AI is likely to be dealt with under Spain's existing strict liability standard under its product liability laws. This question remains yet to be tested.⁶²⁸

NORWAY

Maturity Index – 2/5

The Norwegian Strategy on Artificial Intelligence does not expressly consider the issue of civil or contractual liability in the use of AI systems. However, when considering the ethical principles on which AI based technology is to be developed, it states the importance of maintaining human control and autonomy, and emphasises the need to design for accountability in the creation process itself.⁶²⁹ Apart from this, there does not yet appear to be any specific discussion on the question of civil liability in AI in Norway.

ESTONIA

Maturity Index – 2/5

In the report⁶³⁰ released by Estonia's Task Force on AI, the issue of creating a new law to address the liability of the AI systems was discussed. The report mentions that even though legal clarity on the issue of liability is necessary, a new law addressing the same is not required. As per the report granting AI a separate legal status would only create illusionary legal certainty and would not solve issues of liability. It further explains that in private relationships, for both natural and legal persons, the actions of an AI system should be considered as the actions of the user. Despite rejecting the idea of a new legislation, the report supported the review of outdated laws to adjust to a society that widely uses AI systems. In a more recent article⁶³¹ written by National Digital Advisor the Government Office of Estonia, it was argued that after a year into the public debate over algorithmic-liability law, opinion leans toward avoiding sector-based regulation, opting for general algorithmic liability instead.

626. Ministry of Energy, Tourism and the Digital Agenda and Ministry of Finance and Public Function, "Digital Agenda for Spain", 2013, available at <https://www.planit.gob.es/digital-agenda/Paginas/digital-agenda-spain.aspx>

627. Sonke Lund, "AI, Machine Learning and Big Data 2020: Spain", Global Legal Insights, May 2020, available at <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/spain>

628. Xavier Moliner and Juan Martinez, "Spain: Product Liability Laws and Regulations 2020", International Comparative Legal Guides, June 2020, available at <https://iclg.com/practice-areas/product-liability-laws-and-regulations/spain>

629. Norwegian Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence", 2019, available at: https://www.regeringen.no/contentassets/1febbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf

630. (Estonian) Ministry of Economic Affairs and Communication, "Report of Estonia's AI Taskforce", 2019, available at https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_486454c9f32340b28206e140350159cf.pdf

631. Marten Kaevats, "Estonia considers a 'kratt law' to legalize AI", Medium, September 2017, available at <https://medium.com/e-residency-blog/estonia-starts-public-discussion-legalising-ai-166cb8e34596>

THE NETHERLANDS

Maturity Index – 2/5

The Netherlands, in its position paper⁶³² on the EC proposal, for legislation for a coordinated European approach on the human and ethical implications of AI, supported the effort of the EC to investigate the lacunae that exist in relevant legislation and whether future legislation for a coordinated European approach to AI should include extra provisions related to liability. In this paper, the Netherlands also considers whether a new approach, if required, should be application specific or generic, keeping in mind issues such as the timeliness of introducing relevant reforms to existing legal systems and ensuring the principles of trust in AI, accountability and safety are not compromised. The Netherlands identified the following sectors as being areas of priority for regulation: self-driving cars, P2P energy markets, judges, self-efficacy and content moderation on platforms.

UAE

Maturity Index – 2/5

The laws pertaining to civil liability in UAE regulate the conduct of a natural person, which do not, at present, account for AI systems. It is for this reason that the issue of liability continues to be governed by the existing liability laws. However, various judicial experts have started pondering over the challenges raised by the advancement of technology and considered the question of whether a legal identity should be created/granted to AI systems similar to that of corporations. However, the discussion did not offer any concrete positions and instead noted that this issue is still subject to worldwide deliberation.⁶³³

HONG KONG

Maturity Index – 2/5

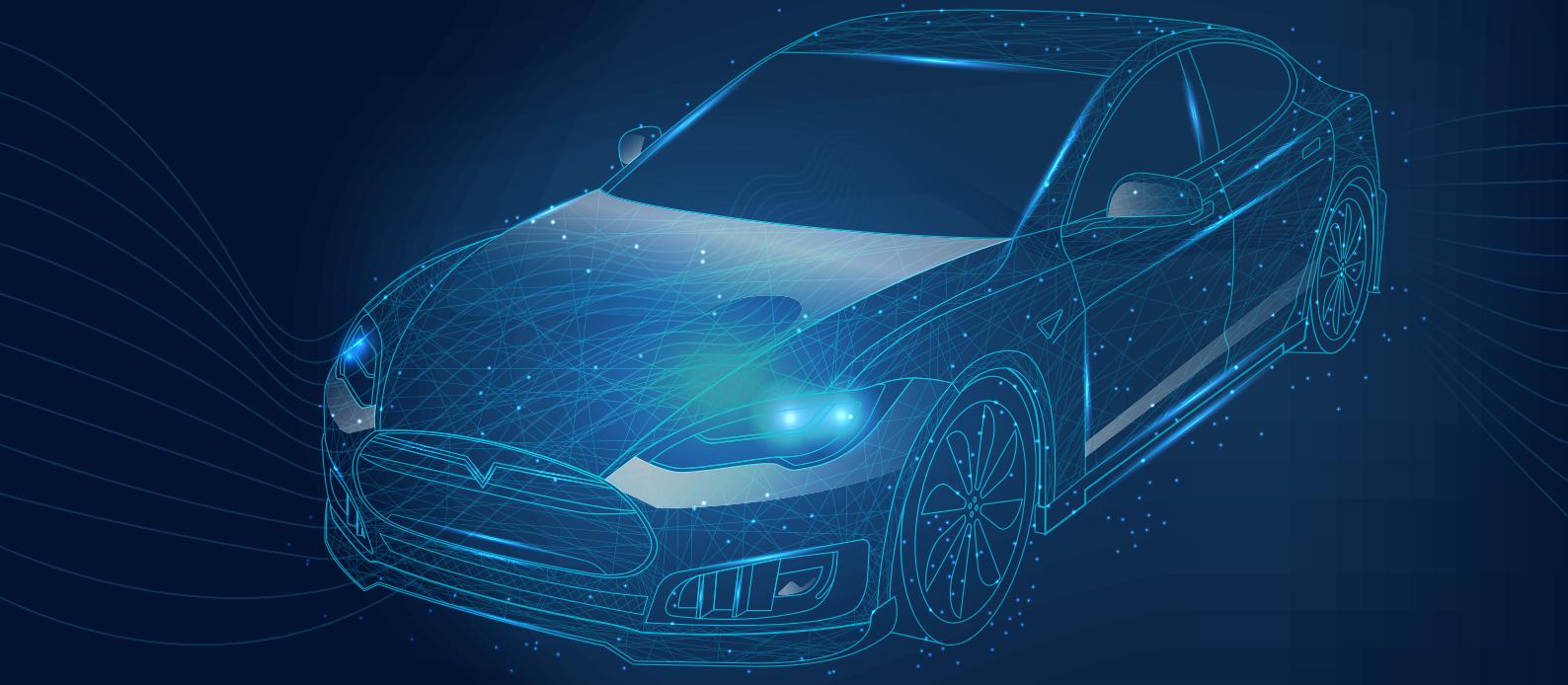
While Hong Kong has been at the forefront of the financial sector in Asia, it has been slower to adopt AI based processes in comparison to mainland China. As such, there do not appear to be any specific legislations that govern the use of AI-based systems, apart from data privacy ordinances that govern the use of data collected and used, potentially by AI based systems. In the context of attributing liability, however, it appears existing law in Hong Kong would govern civil, contractual or consumer liability for actions taken by AI based systems; as with other jurisdictions. It remains unclear how ownership or the responsibility of foreseeability could be distributed between the user, the manufacturer/designer and even the AI system itself.⁶³⁴

632. Government of the Netherlands, "Position Paper of the Netherlands on the EC Proposal regarding legislation for a Coordinated European Approach on the Human and Ethical Implications of Artificial Intelligence (AI) 18 December 2019", December 2019, available at: https://www.permanentrepresentations.nl/binaries/nlatio/documents/publications/2019/12/19/position-paper-legislation-ai/Position+paper+legislation+AI+20191218_.pdf

633. Marie Nammour, "Experts discuss Legal Liability of Artificial Intelligence Actions", Khaleej Times, October 2019, available at <https://www.khaleejtimes.com/technology/experts-discuss-legal-liability-of-artificial-intelligence-actions>

634. Alan Chiu et al., "AI, Machine Learning and Big Data Laws and Regulations 2020: Hong Kong", May 2020, available at <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/hong-kong>

AUTONOMOUS VEHICLES



Even though self-driving car technology has been an area of interest since 1984,⁶³⁵ it has only recently come close to a commercial reality when Tesla announced its commercially available autopilot software update for its electric cars in 2014, that allows its vehicles to be parked without human intervention.⁶³⁶ Since then, other private enterprises have also invested significant resources into developing autonomous vehicles.⁶³⁷ Given autonomous vehicles have arrived at the testing stage, the inevitable legal issues arise, especially as examples of accidents involving self-driving vehicles come to the fore in the media.⁶³⁸ Such instances have given rise to a global discussion over the regulation of deployment of autonomous vehicles.

Many researchers and international composite bodies are now grappling with the question of what to regulate and how to regulate. For instance, in 2015, the International Transport Forum at the OECD presented its report⁶³⁹ on the challenges that are faced by the governments in regulating the deployment of autonomous vehicles. A few of the key challenges mentioned in the report were identifying the respective obligations and liabilities of manufacturers, technology developers, vehicle operators and their responsibilities in case of an accident. Since decisions and tasks that were once entirely the remit of human drivers are now carried out by the vehicle itself, there arises a need for regulations around licencing as well.⁶⁴⁰ The regulatory challenges would depend on the level of automation of the vehicle and the level of human

involvement in the vehicle, e.g. whether it requires a human operator, human driver or if the vehicles are so autonomous that there is requirement of coding the law into algorithms for the vehicle to make its choices keeping the laws of liability in 'mind'.⁶⁴¹

In this regard, Society of Automotive Engineering International (a professional association and standards organization for engineering professionals in various industries across the world) announced a visual chart for use with its "Levels of Driving Automation" standard⁶⁴² in 2018 that defines the six levels of driving automation, from no automation to full automation. These standards revised its 2016 report⁶⁴³ that focused on creating an initial regulatory framework and best practices to guide manufacturers and other entities in the safe design, development, testing, and deployment of automated vehicles.

Another important challenge is the problem of standardization of AI systems across vehicles. Differently programmed algorithms across vehicles would give rise to difficulties in uniform liability attribution standards. However, increased standardization of autonomous behaviour could help make self-driving cars more predictable, easing some regulatory difficulties as well.⁶⁴⁴

Another challenge around which there has been some debate is the infusion of the 'greater good' principle in

635. Carnegie Mellon University: The Robotics Lab, "Navlab: The Carnegie Mellon University Navigation Lab", available at <https://www.cs.cmu.edu/afs/cs/project/alv/www/index.html>

636. The Tesla Team, "Your Autopilot has Arrived", October 2015, available at <https://www.tesla.com/blog/your-autopilot-has-arrived>

637. Keith Naughton, "Here's Where the Self-Driving Car Stands Right Now", Bloomberg, December 2016, available at <https://www.bloomberg.com/news/articles/2016-12-14/heres-where-the-self-driving-car-stands-right-now>

638. Daisuke Wakabayashi, "Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam", The New York Times, March 2018, available at <https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatalty.html>

639. International Transport Forum, "Automated and Autonomous Driving: Regulation under Uncertainty", 2015, available at: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf

640. Alex John London and David Danks, "Regulating Autonomous Vehicles: A Policy Proposal", In Proceedings of the 2018 AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society, 2018 available at: <https://www.cmu.edu/dietrich/philosophy/docs/london/London%20Danks%20Regulating%20Autonomous%20Systems%20-%20flattened.pdf>

641. Antje Von Ungern-Sternberg, "Autonomous Driving: Regulatory Challenges Raised by Artificial Decision-Making and Tragic Choices", Woodrow, Barfield and Ugo Pagallo (Eds), Research Handbook on the Law of Artificial Intelligence, September 2017, available at: <https://ssrn.com/abstract=3049653>

642. SAE International, "Taxonomy and Definitions for Terms Related To Driving Automation Systems for On Road Motor Vehicles", June 2018, available at: https://www.sae.org/standards/content/j3016_201806/

643. Jennifer Shuttleworth, "SAE Standards News: J3016 Automated Driving Graphic Update", January 2019, available at <https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic>

644. Harry Surden and Mary-Anne Williams, "Technological Opacity, Predictability, and Self-Driving Cars", Cardozo Law Review, Volume 38, March 2016, available at <http://dx.doi.org/10.2139/ssrn.2747491>.

the algorithms that run the autonomous vehicles,⁶⁴⁵ i.e., whether the vehicle will be able to make decisions after duly considering the relevant ethical concerns in an accident. Broadly, academics have reached “the shared conclusion” that the elimination of a human driver will shift responsibility onto manufacturers as a matter of product liability law, with most tort litigation in this regard involving claims for design or warning defects.⁶⁴⁶

At the international level, the Vienna Convention on Road Traffic, 1968 sets out a legal framework for national road traffic legislation, which was amended in 2016⁶⁴⁷ to remove legal obstacles for contracting parties to allow the transfer of driving tasks to the vehicle itself, provided that the technologies used are in conformity with UN Vehicle Regulations or can be overridden by the driver. This amendment still requires that every vehicle must have a driver, who may remove their hands from the steering wheel but who must be ready at all times to take back control of the vehicle and override the autonomous system. This is a requirement that is incompatible with high or full automation. A similar attempt was made to amend the Geneva Convention on Road Traffic 1949, by the Working Party on Road Traffic Safety of the Inland Transport Committee (which leads international endeavours for the adaptation of these treaties to new

technologies). The proposal, however, was rejected by contracting parties due to procedural and administrative difficulties.⁶⁴⁸

Given how quickly autonomous vehicle technology is advancing, it is important that the relevant stakeholders proactively engage with one another in further research, studies and discussions to adapt current legal frameworks to automation from both technical and non-technical aspects. As with many aspects of AI, private companies are taking the lead in terms of developing the technology, and there is imminent danger in legislation and policy not reacting appropriately or in a timely manner. In most cases, however, there appears to be an acknowledgment that autonomous vehicles are shortly going to be a reality, and that special dispensations are required to permit at least the testing and trials of such vehicles in defined areas or sectors. However, there are very few instances of actual implementation of autonomous vehicles at level 3 or above in particular sectors or in the general public, or legislation that accounts for this development. Moreover, few countries have thought through the implications from the perspective of insurance or liability at levels 4 and 5 of automation, with the responsibility being borne by the driver in the case of level 3 automation.

645. John Markoff, “Should Your Driverless Car Hit a Pedestrian to Save Your Life?”, New York Times, June 2016, available at <https://www.nytimes.com/2016/06/24/technology/should-your-driverless-car-hit-a-pedestrian-to-save-your-life.html>

646. Dorothy J. Glancy, “A Look at the Legal Environment for Driverless Vehicles”, The National Academies Press, 2017, available at: <http://www.trb.org/Publications/Blurbs/173557.aspx>

647. United Nations Economic Commission for Europe, “UNECE Paves the Way for Automated Driving by Updating UN International Convention” March 2016, available at <https://www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html>

648. United Nations Economic Commission for Europe, “Report of the Seventy-Second Session of the Working Party on Road Traffic Safety”, April 2016, available at: <https://www.unece.org/fileadmin/DAM/trans/doc/2016/wp1/ECE-TRANS-WP1-153e.pdf>

MATURITY INDEX AUTONOMOUS VEHICLES



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation



INDIA

Maturity Index – 2/5

The Motor Vehicles Amendment Act, 2019⁶⁴⁹ introduces section 2B in the existing Motor Vehicles Act that allows the Central Government to exempt certain types of mechanically propelled vehicles from the provisions of the Act, in the interest of promoting innovation and R&D in the autonomous vehicles space.

However, the Union Minister for Road Transport & Highways speaking in a public event announced that he was opposed to driverless cars as it would adversely affect the employment of one crore people of the country.⁶⁵⁰ Another prospective legislation that deserves a mention here is the Draft Geospatial Information Regulation Bill, 2016 which seeks to regulate the acquisition, dissemination, publication and distribution of geospatial information of India which would lay the cornerstone of intelligent mapping to enable driverless vehicles to find the ways. However, as yet, there has not been much progress in terms of introducing the technology or in legislation or policy in respect of autonomous vehicles in India.

USA

Maturity Index – 4/5

In September 2016, the U.S. Department of Transportation through its National Highway Traffic Safety Administration (**NHTSA**) published non-binding performance guidance to facilitate the development of autonomous vehicles, with the intent to establish a consistent regulatory regime for carmakers and technology companies that are looking to bring self-driving cars to market.⁶⁵¹ The aforementioned guidelines have been revised⁶⁵² since 2016 and include:

1. best practices that states should consider in driver regulation;
2. a set of voluntary, publicly available self-assessments by automakers showing how they are building safety into their vehicles; and
3. proposal to modify the current system of granting exemptions from federal safety standards

In 2017, the U.S. House of Representatives passed the Self-Drive Act,⁶⁵³ a legislation that aims to set the standards and further promote innovation in autonomous vehicles. A separate bill, called the AV START Act, was reported from the Senate Committee on Commerce, Science and Transportation in late 2017. While both prospective legislations could have consolidated the federal stance on the regulation of self-driving vehicles, neither of them was passed to become formal legislation.⁶⁵⁴ Owing to this the US does not have a federal regulatory framework currently in place (apart from the non-binding guidance reports by the NHTSA discussed above) to address autonomous vehicle testing and deployment. Instead, testing and deployment is regulated by state laws.

649. Text of the Motor Vehicles Amendment Act, 2019, available at: <http://egazette.nic.in/WriteReadData/2019/210413.pdf>

650. Press Trust of India, "Won't Allow Driverless Cars in India: Gadkari", Economic Times, September 2019, available at https://economictimes.indiatimes.com/industry/auto/auto-news/wont-allow-driverless-cars-in-india-gadkari/articleshow/71282488.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

651. U.S. Department of Transportation, "Federal Automated Vehicles Policy – September 2016", September 2016, available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016>

652. US Department of Transportation, "USDOT Automated Vehicles Activities", April 2020, available at <https://www.transportation.gov/AV>

653. H.R. 3388 The Self Drive Act, available at: <https://www.congress.gov/115/bills/hr3388/BILLS-115hr3388eh.pdf>

654. Congressional Research Service, "Issues in Autonomous Vehicle Testing and Deployment", February 2020, available at: <https://fas.org/sgp/crs/misc/R45985.pdf>

Between 2013 and October 2019, at least 41 states and the District of Columbia considered legislation related to autonomous vehicles. In the same time period, 29 states and the District of Columbia enacted legislation, while Governors in 11 states issued executive orders and 5 states issued both an executive order and enacted legislation on the regulation of autonomous vehicles.⁶⁵⁵

There are three main state-level strategies to facilitate autonomous vehicle testing:

1. Non-regulatory approach, as adopted in Arizona and Colorado;
2. Supervisory approach towards autonomous vehicles, as in California - at the outset, the state passed legislation directing the California Department of Motor Vehicles to create pilot programs. The resulting set of regulations established three different application and oversight processes, one for testing with a back-up driver, one for testing without a back-up driver and one for deployment; and
3. No action on autonomous vehicles at all.⁶⁵⁶

In February 2020, NHTSA announced⁶⁵⁷ its approval of the first autonomous vehicle exemption—from three federal motor vehicle standards—to Nuro, a California-based company that plans to deliver packages with a robotic vehicle smaller than a typical car.

CHINA

Maturity Index – 2/5

China has considered the promotion and regulatory aspects of autonomous vehicles for several years now. In 2015, the State Council published a document entitled “Made in China 2025,” in which it detailed not only the reasoning behind the stated goal, but also the specific time frame in which the country hopes to achieve it. In this document, the State Council named 10 specific industries in which China intends to take the lead. Three of these—robotics, new-generation information technology and new-energy vehicles—are associated with the autonomous vehicle industry.⁶⁵⁸ Similarly, in April 2017, Ministry of Industry and Information Technology, National Development and Reform Commission, and the Ministry of Science and Technology issued the Medium- and Long-term Development Plan for the Automobile Industry, highlighting autonomous vehicles as a transformational breakthrough and an opportunity to upgrade the domestic automobile industry.⁶⁵⁹

On 15 December 2017, Beijing Municipal Commission of Transport, Beijing Traffic Management Bureau and Beijing Municipal Commission of Economy and Information Technology jointly issued the Beijing Guidance on Accelerating Road Testing for Self-Driving Vehicles (Trial) and Beijing Implementing Rules for Managing Road Testing for Self-Driving Vehicles (Trial)⁶⁶⁰ (collectively, the Regulations) with the aim of advancing transformation, upgradation and innovation of transport

655. National Conference of State Legislatures, “Autonomous Vehicles: Self Driving Vehicles Enacted Legislation”, February 2020, available at: <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>

656. In this category, while there are autonomous vehicles in operation in those states, they are not explicitly authorized, although there are also no regulations that declare operating such vehicles illegal. In such cases, autonomous vehicles may operate as long as they adhere to all existing state and federal laws.

657. US National Highway Traffic Safety Administration, “NHTSA Grants Nuro Exemption Petition for Low-Speed Driverless Vehicles”, February 2020, available at <https://www.nhtsa.gov/press-releases/nuro-exemption-low-speed-driverless-vehicle>

658. Institute for Security and Development Policy, “Made in China 2025 Backgrounder”, June 2018, available at: <https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf>

659. Lan Suying, “NewsTurbo Special: China Issues Mid- and Long-Term Development Plan for Car Industry”, National Business Daily, April 2017, available at <http://www.nbdpress.com/articles/2017-04-26/2397.html>

660. Mark Schaub et al., “Beijing Regulation on Self-Driving Cars Road Testing”, China Law Insight, December 2017, available at <https://www.chinalawinsight.com/2017/12/articles/corporate-ma/beijing-regulations-on-self-driving-cars-road-testing/>

while also regulating the administration of road testing of autonomous vehicles. As per the **Regulations**, a test vehicle including passenger vehicles and vehicles for commercial uses (but excluding low-speed automobiles and motorcycles) are required to meet the following conditions:

1. It has not undergone registration for motor vehicles;
2. It satisfies all statutory testing requirements, except endurance, for the corresponding type of vehicles. If a particular statutory testing requirement is not met due to the self-driving function, the testing subject has to prove that the safety performance of the vehicle has not been jeopardized;
3. It can be steered manually and automatically and can switch between the self-driving mode and the manual driving mode in a safe, rapid and easy manner, accompanied with a warning sound, in order to ensure the vehicle could be switched to the manual driving mode immediately under any circumstance;
4. The test vehicle shall be used to conduct actual tests in certain areas, such as a closed road or venue, in compliance with the applicable industry standards of the State, testing requirements issued by provincial and municipal governments and testing evaluation rules of the testing subject, and fulfil conditions for road testing; and
5. The self-driving function of the test vehicle shall be tested and verified by a third-party testing institute recognized by the State or local province or municipality to engage in automobile-related business.

In February 2020, 11 departments including the National Development and Reform Commission jointly issued the Innovative Development Strategy for Intelligent Vehicles.⁶⁶¹ This Development Strategy envisions the development of a thorough framework for Chinese-standard intelligent vehicles by 2025, which would consider aspects like technical innovation, industry ecology, infrastructure, regulations and standards, product regulation and network safety. To this end, the Development Strategy outlines six key tasks, one of which is building an intelligent vehicle industry ecology that integrates various sectors. The strategy further outlines the need and importance of creating new market players to ensure a rounded development of the sector. It further calls for strengthened management of vehicle products and vehicle use. This entails improvement in the administrative provisions regarding production, entry, sale, inspection, registration and recall of intelligent vehicles; enactment of the administrative provisions in respect of upgrading of intelligent vehicles' software and hardware, after-sales services, quality guarantee, financial insurance and other related fields will be enacted, while also propelling vigorously the commercial application of intelligent vehicles.

CANADA

Maturity Index – 2/5

The Canadian Federal Government has not yet introduced a specific policy governing autonomous vehicles. However, the Senate has provided guidance to federal agencies to take a policy leadership role in this regard and to guide provinces in facilitating trials of autonomous vehicles. In January 2018, the Standing Senate Committee on Transport and Communications provided guidance⁶⁶² through 16 recommendations to Transport Canada to build a coordinated national strategy on automated and connected vehicles. The recommendations included, among other things, that a separate spectrum be allocated for use of connected vehicles by national licensing and registration authorities for Canadian vehicles, and the creation of a policy unit to coordinate federal efforts on automated and connected vehicles in cooperation with Transport Canada. It is also recommended that Transport Canada engage with provincial governments through the Canadian Council

661. National Development and Reform Commission, "Notice on the issuance of Smart Car Innovation Development Strategy", February 2020, available at: https://www.ndrc.gov.cn/xxgk/zcfb/tz/202002/t20200224_1221077.html

662. Standing Senate Committee on Transport and Communications, "Driving Change: Technology and the Future of the Automated Vehicle", January 2018, available at: https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf

of Motor Transport Administrators (**CCMTAs**) to develop a model provincial policy for the use of automated and connected vehicles.

At present, Transport Canada and the CCMTA have developed Testing Guidelines⁶⁶³ for the provinces for levels 3, 4 and 5 driving automation systems, setting out licensing requirements and certifications for wireless technologies and highly automated vehicles. The guidelines look into the safe deployment of automated and connected vehicles on public roads and set out a flexible approach by utilizing non-regulatory tools to support safe testing of Automated Driving System. Additionally, any organization considering a trial of an automated vehicle also needs to comply with provincial regulations. The CCMTA's Canadian Jurisdictional Guidelines⁶⁶⁴ for the Safe Testing and Deployment of Highly Automated Vehicles further supplements the Testing Guidelines and elaborates on additional guidance regarding preparation and rolling out of AVs while maintaining road safety.

In January 2019, Transport Canada provided policy guidance on safety in its report,⁶⁶⁵ Safety Assessment for Automated Driving Systems in Canada. The report looks into three aspects of safety:

1. The design and validation of the vehicle;
2. Safety systems within the vehicle for driver accessibility; and
3. Cybersecurity and data management.

UK

Maturity Index – 2/5

The UK has also been an early adopter in the field of autonomous vehicles. To enable the trials of driverless vehicles on UK roads, which was seen as a preliminary step to ensuring industry and wider public benefit, the government pledged a review of legislative and regulatory framework as part of the 2013 National Infrastructure Plan. These plans were also announced in the 2013 Autumn Statement.⁶⁶⁶

In February 2015, following the conclusion of a review of the Autonomous Vehicle Technology regulation, the Department for Transport published a further detailed review of regulations for automated vehicle technology.⁶⁶⁷ The review identifies issues that need to be addressed to enable testing automated vehicle technology on UK roads without compromising on the highest levels of road safety. It also covers the best and safest ways to conduct automated vehicle trials, which entails the presence of a qualified individual that can assume control of the car in times of need. The review also looks into the implications of potential use of fully autonomous vehicles.

Following this, in July 2015, the Department of Transport published a Code of Practice for testing,⁶⁶⁸ to provide non-statutory

663. Transport Canada, "Guidelines for Trial Organisation", April 2019, available at: <https://www.tc.gc.ca/en/services/road/safety-standards-vehicles-tires-child-car-seats/testing-highly-automated-vehicles-canada.html>

664. Canadian Council for Motor Transport Administrators, "Canadian Jurisdictional Guidelines for the Safe Testing and Deployment of Highly Automated Vehicles", June 2018, available at: <https://www.ccmta.ca/images/publications/pdf/CCMTA-AVGGuidelines-sm.pdf>

665. Transport Canada, "Safety Assessment for Automated Driving Systems in Canada", January 2019, available at: https://www.tc.gc.ca/en/services/road/documents/tc_safety_assessment_for_ads-s.pdf

666. HM Treasury, "Autumn Statement", December 2013, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/263942/35062_Autumn_Statement_2013.pdf

667. Department of Transport, "The Pathway to Driverless Cars: A Detailed Review of Regulations for Automated Vehicles Technology", February 2015, available at: <https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review>

668. Department of Transport, "The Pathway to Driverless Cars: A Code of Practice for Testing", July 2015, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf

guidelines regarding testing of automated vehicles on public roads, designed specifically for manufacturers and trialing organizations.

In the same year, the Department of Transport and the Department for Business, Energy & Industrial Strategy together established the Centre for Connected and Autonomous Vehicles (**CCAV**) which is dedicated to working across government verticals to support the market for connected and automated vehicles. CCAV replaced the earlier code of practice⁶⁶⁹ by a new code of practice for automated vehicle trialing.⁶⁷⁰ As per the new code, the trialing organizations will need to ensure additional safety parameters such as ensuring that the vehicle is roadworthy, ensuring appropriate vehicular insurance, and ensuring that a suitably licensed and trained test driver or operator is supervising the vehicle at all times and can override automated operation if required. Expanding the breadth of regulation to keep up with technology, in August 2017, the CCAV introduced the key principles of vehicle cyber security for connected and automated vehicles,⁶⁷¹ a set of non-statutory principles for use throughout the sector.

Further in 2018, the government passed the Automated and Electronic Vehicles Act 2018 (**AEVA**) which brings 'intelligence led' vehicles into the ambit of insurance law and provides a framework that permits the accelerated growth of electric vehicles or ultralow emission vehicles. AEVA introduced a statutory insurance regime for autonomous vehicles which provides that, where an accident is caused by an insured autonomous vehicle, the insurer is liable for damage suffered by a person (covering death, personal injury and property, with limited exceptions). It prohibits exclusions and limitations from the policy, except where the accident is caused directly by software alterations made by or with the knowledge of the insured person or where the insured person failed to install safety-critical software updates they ought reasonably to have been aware of. The insurer is entitled under the AEVA 2018 to recover amounts it has paid out as a result from that person.

FRANCE

Maturity Index – 2/5

In 2014, the French Government announced the adoption of a necessary legal framework to enable the testing of driverless cars on public roads under strict conditions by 2015.⁶⁷² In May 2018, the government released the strategy⁶⁷³ for development of autonomous vehicles. It traces the development of regulation of autonomous vehicles and mentions the government's strategic framework for public action for the development of autonomous vehicles along with the transport orientation strategy bill, both of which were published in 2018.

The strategy envisages the deployment of highly automated vehicles by 2022, and maps 10 priority actions from the government for such deployment. The priority actions include the construction of a national framework, updating technical regulations, implementing a system for monitoring and designing a national programme for implementation.

In April 2019, France adopted⁶⁷⁴ the Pacte Bill that seeks to provide a complete regulatory framework to allow for broad open road testing of autonomous level 3 to 5 vehicles, to facilitate the possibility of conducting experiments. Additionally,

669. Ibid at 29.

670. Department of Transport, "Guidance on Code of Practice: Automated Vehicle Trialling", February 2019, available at: <https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public>

671. Centre for Connected and Autonomous Vehicles, "The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles", August 2017, available at: <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles>

672. Benoit Hamon, et al., "Six New Plans for New France Industrial Policy Rolled Out", July 2014, available at <http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/17720.pdf>.

673. Government of France, "The French Strategy for Development of Autonomous Vehicles", May 2018, available at: https://www.ecologique-solaire.gouv.fr/sites/default/files/18029_D%C3%A9veloppement-VA_8p_EN_Pour%20BAT-3.pdf

674. SAMMAN, "Adoption of the PACTE Bill – New Steps in the Government's Economic Policy", April 2019, available at <https://www.cabinet-samman.com/en/our-news/334>

the Pacte Bill aims to attract researchers and create an international centre of excellence with shared tools, which would further trigger the development of autonomous technology in a more holistic and all-encompassing manner.

GERMANY

Maturity Index – 2/5

Germany has been at the forefront of automobile manufacture in the 20th century and has also been quick to develop policy in respect of automated vehicles. In 2015, the German government devised the Strategy for Automated and Connected Driving,⁶⁷⁵ with the aim that Germany remain a leading innovator in the automotive industry and at the same time become a leading market in the digital era, which necessitated the creation of a robust legal framework. On 21 June 2017, Germany enacted a law legalizing automated vehicles. The legislation modifies the already existing Road Traffic Act and defines the requirements for highly and fully automated vehicles to use public roads. In addition to this, it also elaborates on the rights and duties of the driver when activating the automated driving mode. As per this law, the general liability concept under German law holds even in cases of autonomous vehicles, implying that the liability in case of a mishap even if the vehicle is in automated driving mode lies on both, the owner and the driver, with the driver escaping such liability if they lawfully used the automated driving mode. The new legislation also requires a black box (an event data recorder) for autonomous vehicles, which would record system data and actions for review in the case of accidents.⁶⁷⁶ The amendment also sets the maximum amount that a victim is allowed to recover for driving accidents involving such automated driving systems to €10 million for personal injury or death and to €2 million for property damage.

To deal with the legal and ethical issues in autonomous driving, the federal government set up an Ethics Committee in 2016, consisting of a panel of 14 scientists and experts. The Committee adopted a final report⁶⁷⁷ in 2017 which consisted of a total of 20 ethical rules, and stated among other things, that protection of man always has priority. The report also made high demands in respect of data protection. These are being used today in the development of automated and autonomous systems. In total, three clear principles apply: transparency, self-determination and data security.

ISRAEL

Maturity Index – 2/5

In 2017, the Ministry of Transport of Israel passed a directive that regulates the licensing of experiments in vehicles systems and features to be installed in vehicles that may interfere or influence vehicle systems and their performance with respect to control, safety, fuel consumption and air pollution, including any form of connection to communication interfaces of the vehicles.⁶⁷⁸ The directive also expressed its support for advancing new technologies and development of vehicle systems based on strategic vision for advancement of the Israeli industry.

In May 2018, Israel's Ministry of Transport issued the Transportation (Amendment No. 12) Regulations, which authorize the National Traffic Controller to exempt vehicle operators conducting experiments in new technologies from requirements

675. Die Bundesregierung, "Strategy for Automated and Connected Driving: Remain a Lead Provider, Become a Lead Market, Introduce Regular Operations", September 2015, available at: https://www.bmvi.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.pdf?__blob=publicationFile

676. Dr Mark Ruttloff, "New Legal Rules on Automated Driving", September 2017, available at <https://www.gleisslutz.com/en/automated%20driving.html-0>

677. Federal Ministry of Transport and Digital Infrastructure, "Ethics Commission: Automated and Connected Driving", June 2017, available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile

678. Ministry of Transportation, "Approval of Experiments in Vehicles for Research and Development", Automated Technological Systems § 1(1) (Directive No. H-02-2017, Nov. 1, 2017), <http://rishuy.mot.gov.il/he/vehicle/maintenance/rules-gv> (click on H-02-2017), archived at <https://perma.cc/RFQ2-8ZJF>. As quoted in https://www.loc.gov/law/help/artificial-intelligence/middleeast-northafrica.php#_ftn12

under the Transportation Regulations. Such exemptions may be obtained following consultation with the licensing authority and a police officer, and an evaluation of the experiment's possible impact on traffic safety, traffic flow, and the ability of authorities to respond to emergencies.⁶⁷⁹

RUSSIA

Maturity Index – 2/5

In March 2018, the government of Russia adopted an action plan⁶⁸⁰ to improve legislation and remove administrative barriers in order to ensure the implementation of Autonet. Autonet is a national technology initiative aimed at developing and promoting unmanned transport technologies, service telematics platforms, navigation technologies, driver assistance systems, cybersecurity technologies, new generation wireless communication systems, technologies in the field of electric transport and related services.

In November 2018, the government of the Russian Federation issued a regulation⁶⁸¹ that permitted the testing of driverless cars on regular roads, subject to fulfilment of several conditions. The regulation allows the use of highly automated vehicles on public roads in two select regions of Russia between 1 December 2018 and 1 March 2022.

Further, the government has designated a national research laboratory that would review all applications for testing from owners of driverless cars and coordinate testing. The regulation also mandates the presence of a pilot in the car, and a mechanism allowing the pilot to activate and deactivate the autonomous driving system, along with a data recording system, and equipment for recording traffic and the pilot's actions. Such video recordings are required to be preserved for at least 10 years and can be given to the government agencies upon their request.

DENMARK

Maturity Index – 2/5

In May 2017, the Danish parliament passed an amendment to the Danish Road Traffic Act⁶⁸² allowing testing of self-driving cars. Per this law, a permit from the Ministry of Transportation is required by any company carrying out testing with self-driving cars. The amendment makes it clear that only projects with vehicles up to SAE level 4 (high automation) are to be approved and will be permitted to operate only in specific areas and during a certain time span. The amendment also covers new rules regarding liability for damages for cars. According to the amendment the liability for damages rests with the holder of the permit and is a strict liability.

679. "Israel: Ministry of Transport Issues Regulations on Autonomous Vehicle Testing", January 2019, available at, <https://bitrss.com/news/121467/israel-ministry-of-transport-issues-regulations-on-autonomous-vehicle-testing>

680. Order of Government of March 29, 2018. No. 535-r, available at: <http://government.ru/docs/31810/>

681. Decree of November 26, 2018 No. 1415, available at: <http://government.ru/docs/34831/>

682. Danish Road Traffic Amendment Act, 2017, available at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=191638>.

EU

Maturity Index – 2/5

In November 2016, the EC adopted the Co-operative Intelligent Transport Systems (**C-ITS**) initiative⁶⁸³ which presents a strategy for the coordinated deployment of co-operative intelligent transport systems within the European internal market. It addresses critical issues, including cyber-security, data protection and interoperability. It mandates that the C-ITS service providers should offer transparent terms and conditions to end-users, using clear and plain language in an intelligible way and in easily accessible forms, enabling them to consent to the processing of their personal data. Further, it expresses the EC will work together with all relevant stakeholders in the C-ITS domain to develop a common security and certificate policy for deployment and operation of C-ITS in Europe.

On 17 May 2018, the EC published the EU strategy on connected and automated mobility,⁶⁸⁴ which proposes to revise the minimum standards for motor vehicle safety, update the rules on road infrastructure safety management, and introduces new rules on the sharing of vehicle data. It further highlights that there is a need to update the research and innovation roadmap for driverless mobility including a concrete action plan for short, medium and long-term research and innovation actions. This roadmap will be developed with the help of representatives from Member States with the input from experts and stakeholders. The EC noted the importance of adopting a harmonised approach to the guidelines for national ad-hoc vehicle safety assessments of automated vehicles and to adopt a new approach for safety certifications for automated vehicles.

In February 2018, the European Added Value Unit of the European Parliament Research Service published a study⁶⁸⁵ assessing the common EU approach to liability rules and insurance for connected and autonomous vehicles. The findings of the study suggest that it is necessary to revise the current legislative EU framework for liability rules and insurance for connected and autonomous vehicles. As per the report, the revised liability and insurance framework would ensure legal coherence, better safeguarding of consumers rights and also generate economic added value. It is argued that accelerating the adoption curve of driverless or autonomous vehicles by five years has the economic potential to generate European added value worth approximately €148 billion.

On 9 April 2019 the Technical Committee - Motor Vehicles of the EC published guidelines on the exemption procedure for the EU approval of automated vehicles.⁶⁸⁶ These guidelines aim to harmonize the practice of Member States for the national ad-hoc assessment of automated vehicles and to streamline the mutual recognition of such assessment, as well as to ensure fair competition and transparency. The guidelines focus on automated vehicles that can operate in a limited number of driving situations and require the manufacturer to declare the scope of the automated driving mode where and when the automated driving system is designed to operate. This would include specifying road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.); geographical area (urban and mountainous areas, etc.); environmental conditions (weather, night-time limitations, etc.); speed range; other conditions that must be fulfilled for the safe operation in the driving mode.

683. EC, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy on Cooperative Intelligent Transport Systems, A Milestone Towards Cooperative, Connected And Automated Mobility", 2016, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A766%3AFIN>

684. EC, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the Road to Automated Mobility: An EU Strategy for Mobility of the Future", 2018, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0283&from=EN>

685. European Parliament Research Service, "A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles", 2018, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU\(2018\)615635_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf)

686. EC, "Guidelines on the Exemption Procedure for the EU Approval of Automated Vehicles", April 2019, available at: https://ec.europa.eu/growth/content/guidelines-exemption-procedure-eu-approval-automated-vehicles_en

AUSTRALIA

Maturity Index – 4/5

The National Transport Commission (**NTC**) is an intergovernmental agency charged with improving the productivity, safety and environmental performance of Australia's road, rail and intermodal transport systems. In November 2016, the NTC released a policy paper⁶⁸⁷ introducing regulatory reforms for automated road vehicles. The policy paper recommended that governments at the federal and local level support on-road trials, remove unnecessary legal barriers and provide for the safe operation of automated vehicles. It suggested that the reforms include near-term, medium-term and long-term priorities, based on an assessment of when different levels of automated vehicles are likely to be commercially available.

In May 2017, the guidelines⁶⁸⁸ for trials of automated vehicles in Australia were released. The guidelines set out the criteria for automated vehicle trials and note that trials would differ in technology, scale and risk. The guidelines mandate that the trialing organisations must set out how they have addressed each criterion such as liability, safety management systems, insurance and management of trials or explain why that criterion is not relevant for their trial.

In August 2017, the Standing Committee on Industry, Innovation, Science and Resources issued a report⁶⁸⁹ that examined the social issues arising from the introduction of automated vehicles in Australia. The report identifies the benefits of automated vehicles such as reduction in road accidents, as well as greater mobility for people. On the other hand, the report raises concerns about the apportionment of liability where an accident or incident takes place, as well as loss of employment for drivers.

In November 2017, the National Enforcement Guidelines for Automated Vehicles⁶⁹⁰ were released by the NTC. These national enforcement guidelines provide guidance about how the requirement of proper control in Australian road law should apply to vehicles with automated functions. The guidelines also confirm that the human driver is responsible for compliance with road traffic laws when a vehicle has conditional automation engaged at a point in time.

With regards to the issue of liability, the NTC released a discussion paper titled "Changing driving laws to support automated vehicles" in 2017.⁶⁹¹ The Discussion Paper provides in-depth analysis of the need to legally recognize an Automatic Driving System (**ADS**) in Australia. It explains that an ADS is a system - not a person - so it cannot be held responsible for its actions. An entity needs to be responsible for the actions of an ADS to ensure they can operate safely.

In October 2019, the NTC released its Automated Vehicle Program,⁶⁹² which included information on further planned reform and interaction with other agencies. In the program report, the NTC also confirmed it will consider data from insurers to assess and manage liability for road traffic law breaches and crashes.

687. National Transport Commission, "Regulatory Reforms for Automated Road Vehicles", November 2016, available at: <https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Policy%20Paper%20-%20Regulatory%20reforms%20for%20automated%20road%20vehicles.pdf>

688. National Transport Commission, "Guidelines for Trials of Automated Vehicles", May 2017, available at: https://www.ntc.gov.au/sites/default/files/assets/files/AV_trial_guidelines.pdf

689. Standing Committee on Industry, Innovation, Science and Resources, "Social Issues Relating to Land-Based Automated Vehicles in Australia", August 2017, available at: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024056/toc_pdf/Socialissuesrelatingtoland-basedautomatedvehiclesinAustralia.pdf?fileType=application%2Fpdf

690. National Transport Commission, "National Enforcement Guidelines for Automated Vehicles", November 2017, available at: https://www.ntc.gov.au/sites/default/files/assets/files/AV_enforcement_guidelines.pdf

691. National Transport Commission, "Changing Driving Laws to Support Automated Vehicles", October 2017, available at: <https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Policy%20Paper%20-%20Changing%20driving%20laws%20to%20support%20automated%20vehicles.pdf>

692. National Transport Commission, "Automated Vehicle Program", October 2019, available at: <https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Automated%20Vehicle%20Reform%20Program%20Approach%20%28October%202019%29%20-%20Public%20version.pdf>

JAPAN

Maturity Index – 3/5

In November 2015, the Japanese Prime Minister Abe announced that Japan sought to ensure that driverless mobility services and automated driving were able to be offered in time for the 2020 Olympic and Paralympic Games, and that the government was prepared to invest in the necessary infrastructure and frameworks, including the human resources to carry out final testing.⁶⁹³ In the same year, the Ministry of Economy, Trade and Industry and the Ministry of Land, Infrastructure, Transport and Tourism jointly established the Panel on Business Strategies for Automated Driving, which aimed to ensure competitiveness of the Japanese automobile industry in automated driving while also attempting to reduce the amount of traffic accidents worldwide, for which it has been collaboratively holding discussions with government, industry and academia.⁶⁹⁴ In March 2018, the Panel released “Action Plan for Realizing Automated Driving”⁶⁹⁵ which identifies 10 key co-operative areas for developing automated driving policies such as the development of geospatial technologies for better navigation, development of infrastructure, research and investment in recognition technology etc.

The National Strategic Special Zones Law also went into effect in 2017 as a part of the concerted efforts to support commercial activities focused on demonstrating the viability of automated driving systems. In addition to this, the National Police Agency has also published guidelines concerning the testing of automated vehicles on public roads.⁶⁹⁶

On May 17, 2019, the Road Transport Vehicle Act was amended to include the term “automatic operating device” to the list of devices which must satisfy safety standards if incorporated into a vehicle. The new law mandates equipping all vehicles having an automatic operating device with a drive recording device.⁶⁹⁷

SINGAPORE

Maturity Index – 2/5

In 2014, the government of Singapore constituted the Committee on Autonomous Road Transport for Singapore⁶⁹⁸ to facilitate expert discussion for development of a roadmap and making informed policy choices with respect to deployment of autonomous vehicles.

Singapore’s Parliament also amended the Road Traffic Act⁶⁹⁹ (**RTA**) in February 2017, incorporating different standards for autonomous vehicles. This included allowing for trials to be conducted on public roads and exempting autonomous vehicles, their operators, and those in charge of said trials from existing standards of the RTA. The key provision of the RTA that no longer applies to autonomous vehicles is that making the human driver of the vehicle responsible for its safe use. Along with the amendment in the main legislation, the Road Traffic (Autonomous Motor Vehicles) Rules⁷⁰⁰ were also enacted to effectuate the guidelines regarding the testing of autonomous vehicles.

693. Government of Japan, “Open Innovation for Fully Automated Driving”, 2017, available at https://www.japan.go.jp/tomodachi/2018/winter2018/open_innovation.html

694. Ministry of Economy, Trade and Industry, “Automated Driving and Mobility Service”, August 2020, available at https://www.meti.go.jp/english/policy/mono_info_service/automobile_industry/adms/index.html

695. Panel on Business Strategies for Automated Driving, “Action Plan for Realizing Automated Driving”, March 2018, available at: https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/pdf/ad_v2.0_hokusho.pdf

696. Ibid at 53

697. Dan Matsuda et al., “Legalization of Self Driving Vehicles in Japan: Progress Made But Obstacles Remain”, July 2019, available at: <https://www.mondaq.com/Transport/819992/Legalization-Of-Self-Driving-Vehicles-In-Japan-Progress-Made-But-Obstacles-Remain>

698. Ministry of Transport, “Committee on Autonomous Road Transport for Singapore”, August 2014, available at <https://www.mot.gov.sg/news-centre/news/Detail/Committee-on-Autonomous-Road-Transport-for-Singapore>

699. Singapore’s Road Traffic Act, 1961, available at: <https://sso.agc.gov.sg/Act/RTA1961>

700. Road Traffic (Autonomous Motor Vehicles) Rules, 2017, available at: <https://sso.agc.gov.sg/SL/RTA1961-S464-2017?DocDate=20170823>

In January 2019, Enterprise Singapore and the Land and Transport Agency jointly developed a set of provisional national standards⁷⁰¹ to promote the safe deployment of autonomous vehicles in Singapore. The standards cover 4 key areas of autonomous vehicle deployment: vehicle behaviour, vehicle functional safety, cybersecurity, and data formats. Examples of these standards include the speeds at which such vehicles should travel and the space between them on the road. Currently, this is only a non-binding provisional standard which will be subsequently refined and expanded to cover other aspects of autonomous vehicles development and deployment.

Singapore has recently expanded AV testing to cover all public roads in western Singapore and aims to serve 3 areas with driverless buses from 2022. It is also investing in digital infrastructure to introduce more charging points for EVs. The government of Singapore is considering introducing a usage tax for these charging points to replace lost fuel excise duties.⁷⁰²

SOUTH KOREA

Maturity Index – 2/5

South Korean companies have had a strong presence in the automobile sector for the past few decades. The President of South Korea, in a speech in 2019, unveiled their plans to continue to maintain this strength by pushing for the adoption of electric cars, self-driving vehicles and even flying automobiles. The plan proposes to invest 2.2 trillion won to help develop the relevant technology and infrastructure, with the hope that fully autonomous vehicles can be commercialised by 2024-2027.⁷⁰³ In keeping with this plan, the Hyundai Motor Group has also planned to invest 40 trillion won and the government has pledged to extend support through deregulation, tax benefits, engineer training and automotive electronic component development.⁷⁰⁴

The South Korean government proposes to bring self-driving to commercial use along this timeline by working on developing level 3 and level 4 autonomous vehicles at the same time along with the related infrastructure and other systems such as vehicle performance evaluation, insurance systems, telecommunications, traffic control and road infrastructures.⁷⁰⁵

In keeping with this vision, in early 2020, the Ministry of Land, Infrastructure and Transport of South Korea released safety standards to operate Level 3 (partially autonomous) self-driving vehicles, where drivers must be present behind the wheel to take over in case of dangerous situations. The regulations require that the car has to indicate to the driver to take over in 15 seconds prior to exiting a 'safe zone' such as an expressway. Reports indicate that South Korea proposes to make level 3 autonomous vehicles available for purchase by July 2020.⁷⁰⁶

701. Land Transport Authority, "Joint Media Release by the Land Transport Authority, Enterprise Singapore, Standards Development Organization and Singapore Standards Council – Singapore Develops Provisional National Standards to Guide Development of Fully Autonomous Vehicles", January 2019, available at <https://www.lta.gov.sg/content/ltagov/en/newsroom/2019/1/2/joint-media-release-by-the-land-transport-authority-lta-enterprise-singapore-standards-development-organisation-singapo.html>

702. KPMG International, "2020 Autonomous Vehicles Readiness Index", June 2020, available at https://assets.kpmg/content/dam/kpmg/es/pdf/2020/07/2020_KPMG_Autonomous_Vehicles_Readiness_Index.pdf

703. Kyunghee Park, "South Korea Speeds Up Plans for Autonomous, Electric and Flying Cars", Bloomberg, October 2019, available at <https://www.bloomberg.com/news/articles/2019-10-15/south-korea-speeds-up-plans-for-robocars-electric-vehicles>

704. Jung Min-hee, "South Korea Aiming to Complete Infrastructure for Level 4 Autonomous Driving in 5 Years", Business Korea, October 2019, available at <http://www.businesskorea.co.kr/news/articleView.html?idxno=37002>

705. Id.

706. Yonhap, "Level 3 Autonomous Car to be sold in South Korea from July", The Korea Herald, January 2020, available at <http://www.koreaherald.com/view.php?ud=20200105000078>

SWEDEN

Maturity Index – 2/5

In 2014, the Swedish Government launched the project called 'Drive Me', a joint initiative between Volvo Car Group, the Swedish Transport Administration and the Swedish Transport Agency. The project involved self-driving cars using approximately 50 kilometres of selected roads in and around Gothenburg city and demonstrating the capability of such vehicles.⁷⁰⁷ In the same year, the Swedish Transport Agency, released a report⁷⁰⁸ on autonomous vehicles that outlined various challenges and a plan for the safe and judicious deployment of autonomous vehicles in the country. The report analysed the then prevailing regulatory framework with respect road traffic and presented the issues that the government must address through its policies.

Pursuant to the discussion in the aforementioned report, the government of Sweden initiated the Drive Sweden, a program that gathers leading experts from across various sectors to work together across organisational boundaries, with the aim of positioning Sweden as a leader in automated transportation systems. The program is being jointly run by the Swedish Innovation Agency, Vinnova; Swedish Research Council Formas and Swedish Energy Agency.⁷⁰⁹

In 2017, the Swedish government passed an ordinance on trials of self-driving vehicles. This introduced the requirement of a permit to conduct trials of self-driving vehicles, with the Swedish Transport Agency as the nodal authority to examine matters concerning permits. The ordinance required the presence of a physical driver in or outside the vehicle and provides for fines for those who conduct trials without a permit.⁷¹⁰ Apart from this, multiple projects have been launched under the Drive Sweden programme addressing issues such as intelligent and self-learning traffic control, use of self-driving vehicles in countryside, development of Automated Vehicle Traffic Control Tower etc.⁷¹¹

FINLAND

Maturity Index – 2/5

In a press release of 21 May 2014, Finland announced that the Ministry of Transport and Communications is preparing an amendment to the Road Traffic Act that would allow for driverless robotic cars to drive within a restricted area on public roads. This would be an experimental legislation that would be in force for five years starting at the beginning of 2015, allowing for robotic cars to be tested, subject to a permit, in areas defined by the Finnish Transport Safety Agency.⁷¹²

In 2016, a road map and action plan⁷¹³ for road transport automatization were drawn up by representatives of the Ministry of Transport and Communications, the Finnish Transport Safety Agency, the Finnish Transport Agency, and the Technical Research Centre of Finland. The aim of the report was to create a plan to promote and facilitate automated driving in Finland by 2020. The report examines various aspects of automated driving like the technology that will be used, ethical

707. Lindholmen Science Park, "Drive Me – Self-driving Cars at Lindholmen", April 2014, available at <https://www.lindholmen.se/en/news/drive-me-self-driving-cars-lindholmen>

708. Swedish Transport Agency, "Autonomous Driving" (Summary), August 2014, available at: https://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/Autonomous_driving_eng_short.pdf

709. Drive Sweden, "About Drive Sweden", available at <https://www.drivesweden.net/en/about-drive-sweden>

710. Ministry of Enterprise and Innovation, "Government paves the way for Self-Driving Vehicles", May 2017, available at <https://www.govt.se/articles/2017/05/government-paves-the-way-for-self-driving-vehicles/>

711. Drive Sweden, "Projects", available at <https://www.drivesweden.net/en/projects-5>

712. Ministry of Transport and Communications, "MINTC to launch an experiment that would allow for robotic cars", May 2014, available at <https://www.lvm.fi/en/-/mintc-to-launch-an-experiment-that-would-allow-for-robotic-cars-795399>

713. Finnish Transport Agency, "Road Transport Automation Road Map and Action Plan 2016–2020", 2016, available at: https://julkaisut.vayla.fi/pdf8/its_2016-19eng_road_transport_web.pdf

concerns and environmental impact of using AI based driving technology. It further presents the steps that can be taken by the government to improve the infrastructure and bridge the legislative gaps to bolster the development and deployment of the technology.

In November 2017, the Finnish Government submitted to Parliament its proposal on a new Road Traffic Act. The purpose of the new act is to improve the smooth running and safety of transport and create preconditions for the digitalisation and safe automation of traffic while making progress with deregulation.⁷¹⁴ The Road Safety Act entered into force on 1 June 2020, after a series of modifications.⁷¹⁵ It proposes integrate detailed location data on roads, signs, traffic lights and other control mechanisms for autonomous vehicle operators to use, and is set to repaint the continuous yellow lines on Finnish roads in white, partly as these are easier for machines to detect.

SPAIN

Maturity Index – 2/5

Despite the automotive industry being an important one in Spain, autonomous vehicles continue to remain unregulated and are not authorized for the public in general. However, in 2015, the Spanish Directorate General of Traffic (**DGT**) issued an instruction⁷¹⁶ which authorizes testing or research trials with automated vehicles which incorporate technology functions associated with automation levels 3, 4 and 5. The Spanish government indicated in 2018 that it is developing programs to support companies in terms of facing digitization and globalization, including autonomous vehicles; and also work towards developing international regulations.⁷¹⁷

The Spanish DGT has been working with private companies to trial various aspects of autonomous vehicles, which include road safety, traffic management, interconnectivity and accessibility.⁷¹⁸ In January 2019, Mobileye entered into a collaboration with the DGT to reduce road accidents and work to develop the infrastructure and policy for autonomous vehicles. This project was piloted in Barcelona, with a 5,000-vehicle fleet being introduced in the city, that were equipped with the Mobileye 8 Connect technology.⁷¹⁹

NORWAY

Maturity Index – 3/5

In 2017, the Ministry of Transport and Communication presented the National Transport Plan 2018-2029.⁷²⁰ The plan mentions many reforms undertaken by the government to better the transport system of Norway. One of the reforms mentioned in the document is that the new technology based on Intelligent Transport System is proposed to be implemented

714. International Transport Forum, "Road Safety Annual Report-Finland", 2019, available at: <https://www.itf-oecd.org/sites/default/files/finland-road-safety.pdf>

715. Finnish Ministry of Transport and Communications, "Revisions to Road Safety Act, 2018", available at: https://valtioneuvosto.fi/en/article/-/asset_publisher/tielikennelaki-uudistuu

716. Instruction 15/V-113 of 13 November 2015. Jon Aurrecoechea and Alex Dolmans, "Automotive in Spain", Lexology: Getting the Deal Through, June 2019, available at <https://www.lexology.com/library/detail.aspx?g=82ef102c-b4eb-4a6c-b055-222dc07c0b65>

717. Bird and Bird, LLP, "Spain", At a Glance: Autonomous Vehicles, available at <https://www.lexology.com/library/detail.aspx?g=5490fad1-493e-4170-a01e-94b1df59d0d4>

718. Directorate General for Traffic, "Spanish Approach on Automated Driving", Presentation at the Workshop on Automation Pilots on Public Roads, December 2016, available at <https://connectedautomateddriving.eu/wp-content/uploads/2017/02/ES-Presentation-Workshop-16-12-16.pdf>

719. Autovista, "The State of Autonomous Legislation in Europe", February 2019, available at <https://autovistagroup.com/news-and-insights/state-autonomous-legislation-europe>

720. Ministry of Transport and Communication, "National Transport Plan 2018-2029", 2017, available at: <https://www.regjeringen.no/en/dokumenter/meld.-st.-33-20162017/id2546287/?ch=4>

on priority.

Apart from this, a report⁷²¹ released by the Norwegian Technology Board in May 2018 noted that the government has allowed the testing of automated vehicles on public roads by passing the Testing of Autonomous Vehicles Act. The was passed pursuant to a proposal presented by the government for consultation in 2016.⁷²² As per the report, the law requires that a person assuming responsibility for the test must be appointed. It further recommends that ethical guidelines for how automated vehicles should act in traffic should be established. It further recommends the development of infrastructure for testing of autonomous vehicles in the extreme temperatures faced by the countries for the ease of usage by the public.

ESTONIA

Maturity Index – 2/5

In August 2016, the government of Estonia created an expert group on self-driving vehicles aiming at developing policies, studies, and a legal framework for autonomous vehicles. In February 2017 the group recommended test driving of autonomous vehicles on Estonian roads. As per the report 90% of the kilometres covered in Estonia could be self-driven by 2030 and what such a radical change would mean to the public sector, business and society⁷²³.

The Estonian Ministry of Economic Affairs and Communications announced in March 2017 that the test driving of autonomous cars is allowed on the streets and roads of Estonia, however, the car must have a driver who is able to take control of the car any time needed, additionally the driver can sit within the vehicle or act remotely but is still responsible for the vehicle and must take control of the vehicle if it is necessary.⁷²⁴

THE NETHERLANDS

Maturity Index – 2/5

The Netherlands has looked to adopt technology facilitating self-driving vehicles from fairly early on.⁷²⁵ Since June 2015, it has been possible to test self-driving cars on public roads but only with a driver in the vehicle. At the end of 2017, the House of Representatives received the Experimenteerwetzelfrijdende Auto, a draft bill governing the experimental use of autonomous cars. In April 2018, the bill was rejected, which means that it is still not possible to issue permits for conducting tests on public roads using remote drivers.⁷²⁶ Subsequently, the government of Netherlands allowed the testing of autonomous vehicles on public roads under strict conditions from July 2019. Even though testing of autonomous vehicles on public roads has been allowed since 2015, it required the presence of a driver at all times. The change effected in July 2019 also enables remote driver tests.⁷²⁷

721. Norwegian Technology Board, "Self-Driving Cars – The Technology Behind and The Way Forward", 2018, available at: https://teknologiradet.no/wp-content/uploads/sites/105/2018/11/Self-driving-cars_WEB.pdf

722. Ministry of Transport, "Self-Driving Vehicles – Testing by the Public in Norway", December 2016, available at <https://www.regjeringen.no/en/aktuelt/selfdrivingtesting/id2523654/>

723. Republic of Estonia Government Office, "Final Report: Self-Driving Vehicles on Estonian Roads may Signal the End of Traffic Deaths", February 2018, available at <https://www.riigikantselei.ee/en/news/final-report-self-driving-vehicles-estonian-roads-may-signal-end-traffic-deaths>

724. Republic of Estonia, Ministry of Economic Affairs and Communications, "Estonia Allowing a Number of Self-Driving Cars on the Streets Starting Today", 2017, available at: <https://mkm.ee/en/news/estonia-allowing-number-self-driving-carsstreets-starting-today>

725. The Netherlands is ranked no. 1 in the KPMG report titled 'Autonomous Readiness Index 2019'. Available at: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf>

726. Iris Ruysch, "Paving the Way for Autonomous Cars: Current Projects and Challenges in the Netherlands", June 2019, available at: <https://repository.tudelft.nl/islandora/object/uuid:fd77349a-2f9b-467f-8b97-ed4598dea4d4/datastream/OBJ/download>

727. Ministry of Infrastructure and Water Management, "Green Light for Experimental Law for Testing Self-Driving Vehicles on Public Roads", July 2019, available at <https://www.government.nl/latest/news/2019/07/02/green-light-for-experimental-law-for-testing-self-driving-vehicles-on-public-roads>

UAE

Maturity Index – 2/5

The UAE drafted a series of rules and regulations for self-driving vehicles. The rules which were laid out by the Emirates Authority for Standardisation and Metrology include certain criteria for autonomous vehicles, infrastructure, communication systems and testing.⁷²⁸

In addition to national laws or policy relating to autonomous vehicles, individual cities in the UAE have taken the lead with respect to AI systems, especially Dubai. For instance, Dubai has set a target of 25 per cent of all journeys to be self-driving by 2030.⁷²⁹ This goal was set after Sheikh Mohammed launched the Dubai Smart Self-Driving vision in 2016.⁷³⁰ Dubai's Self Driving Transport Strategy and Roadmap⁷³¹ is the guidance instrument adopted by the government to further its ambitions mentioned in the Dubai Smart Self Driving Vision. The strategy is focused on the provision of comprehensive, multi-modal Self Driving Technology services and addresses the issues such as changes needed in the legislation to allow testing and operation; setting standards for driver behaviour and acceptance; preparing a code for the licencing and registration requirements and infrastructure that needs to be developed for the deployment of such vehicles. Further, the Dubai Roads and Transport Authority is seeking to introduce the two-seater autonomous vehicle (Autonomous Air Taxi) which is capable of transporting people without human intervention or a pilot. The trial operation of the air taxi began in the fourth quarter of 2017 and is being tested.⁷³² In addition, the Dubai Electronic Security Centre announced in July 2018 that it will launch the 'Cyber Security Standard' for autonomous vehicles which will cover aspects such as the autonomous vehicle's communication security, software security, hardware security and supply chain security.⁷³³

HONG KONG

Maturity Index – 2/5

The initiatives for autonomous vehicles in Hong Kong form part of the Smart City Blueprint which was published in 2017. The Hong Kong Transport Department has facilitated trials of autonomous vehicles at various locations in the city, as a part of its Smart Mobility initiative. Since 2017, the Transport Department has permitted 25 trials of 8 different models of autonomous vehicles and has also issued a guidance document on how to apply for movement permits for testing and demonstrations to facilitate further endeavours by private companies in this space.

The Transport Department has also set up the Technical Advisory Committee on the Application of Autonomous Vehicle Technologies which comprises representatives and experts from relevant fields and is working towards developing an appropriate regulatory framework for autonomous vehicles.

In terms of regulation, the Transport Department is also currently drafting new guidance notes for autonomous vehicle

728. Emirates Authority for Standardization and Metrology, "ESMA Develops Federal Requirement for Safety in Self-Driving Vehicles", December 2017, available at <https://www.esma.gov.ae/en-us/Media-Center/news/%E2%80%9CESMA%E2%80%9D-develops-federal-requirements-for-safety-in-self-driving-vehicles.aspx>

729. Roads and Transport Authority, "Self-Driving Transport", available at <https://www.rta.ae/links/sdt/en/index.html>

730. The National News, "A Peek at Dubai's Self Driving Future", September 2017, available at <https://www.thenational.ae/uae/watch-a-peek-at-dubai-s-self-driving-future-1.625791>

731. Dubai Road Transport Authority, "Self Driving Transport Strategy and Roadmap", 2017, available at: <https://www.rta.ae/links/sdt/sdt-final.pdf>

732. Roads and Transport Authority, "Agreement with German Volocopter to Operate the Autonomous Air Taxi", June 2017, available at <https://www.rta.ae/links/sdt/en/news2.html>

733. Mark Sutton, "Dubai Develops Cybersecurity Standards for Autonomous Vehicles", July 2018, available at <https://www.itp.net/617465-dubai-develops-cybersecurity-standards-for-autonomous-vehicles>

trials,⁷³⁴ to allow for trials of more sophisticated vehicles under current legislation. It proposes to use a regulatory sandbox approach to encourage private players to continue to innovate and contribute to the legislative framework that would govern autonomous transportation, while maintaining the objectives of safety and efficient transport management.⁷³⁵

734. Transport Department, "Guidance Notes on the Trials of Autonomous Vehicles", December 2019, available at https://www.td.gov.hk/filemanager/en/content_4808/guidance%20notes%20on%20the%20trials%20of%20autonomous%20vehicles%20eng.pdf

735. Government of the Hong Kong Special Administrative Region, "Press Release - LCQ8: Development and Application of Autonomous Vehicles", November 2019, available at <https://www.info.gov.hk/gia/general/201911/27/P2019112700311.htm>



AUTONOMOUS WEAPONS

The discourse on the conception and deployment of AI is incomplete without addressing the use of the technology in respect to weapons. With most countries allocating a major portion of their budgets to maintaining and strengthening their defence systems, it is inevitable that AI systems would be deployed to bring about ‘improvements’ in weaponry. Potentially even more dangerous than this, is the fact that weapons are increasingly available to private individuals in various countries, with differing levels of regulation and/or licensing. A discussion on regulatory limits placed on weaponry using AI systems is increasingly crucial.

At the individual level, the discourse tends to deal with the use of ‘security robots’ and the culpability of the person deploying such systems if such robots are unable to distinguish between threats and innocent passers-by. The courts in these cases are likely to face the challenge of identifying the level of control that the person deploying such systems has over the technology. The greater the autonomy, the complex the problem becomes.⁷³⁶

However, the debate over the regulations of Lethal Autonomous Weapon Systems (**LAWS**) is dominated by research, induction and usage in national defence systems. The development of self-guided weapons can be traced back to World War I,⁷³⁷ but advancement in technology has given a greater level of autonomy and lethality to LAWS that are now capable of selecting and engaging targets without any human intervention. For example, armed quadcopters today can search for and eliminate people meeting certain pre-defined criteria.⁷³⁸

A prime deployment issue is whether an autonomous weapons system is capable of adequate target discrimination. International law requires combatants to

observe the principle of “distinction” (i.e., discrimination) which prohibits 1) the use of weapon systems that indiscriminately strike both lawful and unlawful targets, and 2) the indiscriminate use of a weapon regardless of its accuracy.⁷³⁹ In the case of a conventional weapon system, this responsibility is discharged by placing the burden on the operator to use it with discretion. An autonomous weapon system, on the other hand, must comply with both facets since the system itself selects and strikes a target. For example, in traditional automated weapon systems such as land mines, discretion is exercised by the military commander through the placement of mines in either marked locations or locations where they were unlikely to be triggered by civilians.⁷⁴⁰ In contrast, those deploying a system such as the Harpy⁷⁴¹, which patrols a broad geographic area, cannot rely on the absence of civilians from its targeting area as a means of discrimination. Therefore, to meet the distinction requirement, the new LAWS must have an effective means of distinguishing civilian from military targets. This diminishing level of human control will continue to raise increasingly difficult questions about both state and individual accountability for the actions of autonomous weapon systems.

Owing to this, in 2013, the Convention on Certain Conventional Weapons (**CCW**) Meeting of State Parties decided to convene an informal Meeting of Experts to discuss the questions related to emerging technologies in the area LAWS. At the 2016 Fifth CCW Review Conference, the High Contracting Parties decided to establish a Group of Governmental Experts (**GGE**) on LAWS to meet in 2017 with a mandate to assess questions related to emerging technologies in the area of lethal autonomous weapons systems.⁷⁴² Since then, the GGE meeting has been convened five times and the latest meeting took place in August 2019.⁷⁴³ In 2019,

736. Elizabeth E Joh, “Private Security Robots, Artificial Intelligence, and Deadly Force”, UC Davis Law Review, Volume 51 Issue 569, 2017, available at: https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Joh.pdf

737. “Definition of Autonomous Weapons”, available at <https://cs.stanford.edu/people/eroberts/cs181/projects/autonomous-weapons/html/history.html> 738 Ryan Joseph Vogel, “Drone Warfare and the Law of Armed Conflict”, Denver Journal of International Law and Policy, Volume 39 Issue 1, 2011, available at: <https://ssrn.com/abstract=1759562>

739. Evan Wallach & Erik Thomas, “The Economic Calculus of Fielding Autonomous Fighting Vehicles Compliant With the Laws of Armed Conflict”, Yale Journal of Law and Technology, Volume 18 Issue 1, 2017, available at: <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/1/>

740. IAI, “HARPY: Autonomous Weapon for All Weather”, available at <https://www.iai.co.il/p/harpy>

741. United Nations Office for Disarmament Affairs, “Background on LAWS in the CCW”, available at <https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/>

742. Reaching Critical Will, “2019 CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems”, available at <https://reachingcriticalwill.org/disarmament-fora/ccw/2019/laws>

the GGE met and adopted a set of 11 principles⁷⁴³ that would guide the future discussion of the group. The principles incorporated the tenets of International Humanitarian Law and declared that they will continue to be applied to all weapons, including LAWS. They highlight the consideration of risk assessment and mitigation, accountability and the risk of acquisition of such weapons by the terrorist outfits. One of the principles stated that the discussions and any potential policy measures taken within the context of the CCW should not hamper progress in or access to peaceful uses of AI technologies. Finally, it noted that CCW offers an appropriate framework for dealing with the issue of emerging technologies in the area of LAWS within the context of the objectives and purposes of the Convention, which seeks to strike a balance between military necessity and humanitarian considerations.

The response of the independent international NGOs also deserves a mention. Human Rights Watch, along with various other independent organisations is steering an international campaign called the 'Campaign to Stop Killer Robots' that aims for an international ban over the development and deployment of LAWS.⁷⁴⁴ In March 2019, the UN Secretary General Antonio Guterres advocated the ban of LAWS in international law.⁷⁴⁵

While the major opposition comes from ethical concerns raised by the use of such weapons, the issue deserves to be considered from the angle of economic viability as

well. Given the development and deployment of LAWS requires considerable financial resources,⁷⁴⁶ it leaves a disparity between developing nations and developed nations. It is relevant to note that 28 countries have called for a ban on these weapons.⁷⁴⁷

Amidst the growing discourse over the opposition of the autonomous weapons there are various countries⁷⁴⁸ and independent researchers that have shown support for the development of such systems arguing better precision and therefore, less collateral damage.⁷⁴⁹ In the case of most liberal democracies, the policy position appears to be to discourage and outlaw the development of LAWS as being violative of international humanitarian rights, while regulating existing weaponry to ensure that the decision-making power lies under human control. There appears to be a growing recognition under these countries that the ability to de-escalate warfare would be severely limited if development and production of LAWS continues unchecked. In combination with such a ban, the goal has also been to arrive at a globally accepted definition for LAWS, to facilitate an informed discussion and draw a line between what is permissible and what actions fall outside the boundaries of acceptable conduct in modern warfare.

In the light of this the instant chapter maps the regulatory discussion (domestic and international) of various countries to help better inform the discussion on the issue.

743. Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, "Draft Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems", August 2019, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/5497DF9B01E5D9CFC125845E00308E44/\\$file/CCW_GGE.1_2019_CRP1_Rev2.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/5497DF9B01E5D9CFC125845E00308E44/$file/CCW_GGE.1_2019_CRP1_Rev2.pdf)

744. Campaign to Stop Killer Robots, "The Threat of Fully Autonomous Weapons", available at <https://www.stopkillerrobots.org/learn/>

745. UN News, "Autonomous Weapons that Kill must be Banned, insists UN Chief", March 2019, available at <https://news.un.org/en/story/2019/03/1035381>

746. Ibid.

747. Campaign to Stop Killer Robots, "Country View on Killer Robots", November 2018, available at https://www.stopkillerrobots.org/wp-content/uploads/2018/11/KRC_CountryViews22Nov2018.pdf

748. Mattha Busby and Anthony Cuthbertson, "Killer Robots' Ban Blocked by US and Russia at UN Meeting", The Independent, September 2018, available at <https://www.independent.co.uk/life-style/gadgets-and-tech/news/killer-robots-un-meeting-autonomous-weapons-systems-campaigners-dismayed-a8519511.html>

749. Paul Scharre, "Why You Shouldn't Fear 'Slaughterbots'", IEEE Spectrum, December 2017, available at <https://spectrum.ieee.org/automaton/robotics/military-robots/why-you-shouldnt-fear-slaughterbots>

MATURITY INDEX AUTONOMOUS WEAPONS



Level 1

No Discussion

Level 2

Preliminary
Discussions

Level 3

Established Policy
Position

Level 4

Policy
Recommendation

Level 5

Implementation into
Legislation



INDIA

Maturity index – 2/5

There does not appear to be a specific policy paper or discussion on the guiding approach towards the proper regulation of the LAWS in the country. However, in February 2018, Ms. Nirmala Sitharaman, the Defence Minister created a task force to formulate a roadmap, establish tactical deterrence, visualising potential transformative weaponry and developing intelligent autonomous weapons systems.⁷⁵⁰ In May 2018, the taskforce met in Stakeholders Workshop on Artificial Intelligence in National Security and Defence, Listing of Use Cases. One of the use-case was with regards to the military use of the technology, in which development of LAWS was discussed.⁷⁵¹ The task force submitted its report to the Defence Minister on 30 June 2018, and includes recommendations relating to making India a significant power of AI in defence, specifically in the area of aviation, naval, land systems, cyber, nuclear and biological warfare including both defensive and offensive needs including counter AI needs; recommendations for policy and institutional interventions required to regulate and encourage robust AI based technologies for defence sector; working with start-ups/commercial industry and recommendations for appropriate strategies of working with start-ups.⁷⁵²

Apart from this, India's position in the CCW informal meeting on LAWS is relevant. India has stated that there is a need for "increased systemic controls on international armed conflict in a manner that does not widen the technology gap amongst states or encourage the increased resort to military force in the expectation of lesser casualties or that use of force can be shielded from the dictates of public conscience." It has also highlighted the issue of international security in case of proliferation of such weapon systems, including to non-state actors. India has noted that there continue to be "wide divergences" on the key issues of definition and "mapping autonomy" and that there is a need to resolve these issues for any substantial framework to evolve. It has emphasized the fact that such technology has both peaceful and military uses, and that the CCW remains the "relevant and acceptable framework" for addressing any issues of concern.⁷⁵³

In the November 2017 meeting of the GGE, Commodore Nishant Kumar, representing India, acknowledged that CCW is the appropriate podium to discuss the issue and that 'it may not be prudent to jump to definitive conclusions' without proper discussion.⁷⁵⁴ Further in 2019, in a statement made by him in the GGE meet, he underlined four main factors that need consideration in the discussion. The four factors are intelligibility, human role and responsibility, not stigmatizing technology and not prejudicing the regulatory response.⁷⁵⁵

750. Rajat Pandit, "India Now Wants Artificial Intelligence-Based Weapons Systems", The Times of India, May 2018, available at <https://timesofindia.indiatimes.com/india/india-moves-to-develop-ai-based-military-systems/articleshow/64250232.cms>

751. Press Information Bureau, "Raksha Mantri Inaugurates Workshop on AI in National Security and Defence", May 2018, available at <https://pib.gov.in/newsite/PrintRelease.aspx?relid=179445>

752. Press Information Bureau, "AI Task Force Hands Over Final Report to RM", June 2018, available at: <https://pib.gov.in/newsite/PrintRelease.aspx?relid=180322>

753. R. Shashank Reddy, "India and the Challenge of Autonomous Weapons", Carnegie India, June 2016, available at: https://carnegieendowment.org/files/CEIP_CP275_Reddy_final.pdf

754. Statement by Commodore Nishant Kumar, Director (Military Affairs), Ministry of External Affairs, Government of India During the First Session of the Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) Held in Geneva on April 9, 2018, Permanent Mission Of India To Conference On Disarmament, available at: <http://meaindia.nic.in/cdgeneva/?6490?000>

755. Statement by Commodore Nishant Kumar, Director (Military Affairs), Ministry of External Affairs, Government of India on Agenda item 5(e): Possible Options for addressing the humanitarian and international security challenges posed by emerging technologies in the area of LAWS, available at: <http://meaindia.nic.in/cdgeneva/?7925?000>

USA

Maturity index – 2/5

The US government explored the subject of autonomous weapons as early as 2012, when it passed a directive⁷⁵⁶ regarding autonomy in weapons systems that essentially established the U.S. policy on autonomy in weapons systems. The directive is significant in that it defines different categories of autonomous weapons systems for the purposes of the U.S. military, creating a framework for further discourse. Although these definitions have not been established with the technological sophistication of the weapons system as the pivotal consideration, they consider the role of the human operator with regard to target selection and engagement decisions. The directive requires the design of all systems, including LAWS, be such that commanders and operators can exercise appropriate levels of human judgement in the working of these systems, over the use of force.

To ensure robustness in terms of safety of such systems against engagement with unintended targets or potential loss of control, the directive further requires the fulfilment of the following as precursory conditions for deployment of any autonomous weapons systems:

1. software and hardware of all systems, including LAWS, be tested and evaluated to ensure that they function as anticipated in realistic operational environments against adaptive adversaries;
2. complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement;
3. systems are sufficiently robust to minimize failures that could lead to unintended engagements or to loss of control of the system to unauthorized parties

Additionally, to ensure that the system has retained the ability to operate as intended post any change to the system's operating state, it is required to go through the weapons review process all over again after any modification or alteration.

Apart from this, Section 238 of the John S. McCain National Defence Authorization Act for Fiscal Year 2019 directs the Department of Defence to undertake several activities regarding AI systems. It directs the Secretary of Defence to appoint a coordinator responsible for overseeing and directing all activities of the Department relating to Artificial Intelligence and Machine Learning, with respect to their development to their application. Within this Act however, development or deployment of autonomous weapons or LAWS finds no explicit mention.

At the 2018 meeting of the GGE, the representatives of the USA argued⁷⁵⁷ that it would be premature to ban LAWS under the Convention at that time, and instead of stigmatizing such systems, their use should be viewed within the framework of the current laws of war. They further stated that while it was pertinent for all parties involved to develop a common understanding of the concept involved, it was not necessary to create a definition of LAWS as yet.

756. US Department of Defence, Directive 3000.09, 2012, available at: https://fas.org/irp/doddir/dod/d3000_09.pdf

757. United States Mission to International Organizations in Geneva, "Statement by Shawn Steene to Meeting of the Group of Governmental Experts to the CCW on Lethal Autonomous Weapons Systems", August 2018, available at: <https://geneva.usmission.gov/2018/08/27/meeting-of-the-group-of-governmental-experts-of-the-high-contracting-parties-to-the-ccw-on-lethal-autonomous-weapons-systems/>

CHINA

Maturity index – 2/5

In December 2016, China called for a new international law on autonomous weapons and a legally binding protocol on LAWS. As per China's position paper⁷⁵⁸ to the 5th Review Council of CCW, the country expressed concerns that weapons like LAWS may not be capable of effective target distinction or deducing a proportionate response and cited the 1995 CCW protocol that banned blinding lasers to support its position.

In 2017, at the First Committee meeting of the 72nd Session of the United Nations General Assembly, China⁷⁵⁹ reiterated the need for responsible use of LAWS which should be in accordance with the laws of armed conflict and the UN Charter. It further stated that in the deployment of such weapons, the sovereignty and territorial integrity of all associated parties should be respected. Interestingly, at the 2018 CCW GGE meeting, the Chinese delegation stated that while it supported a ban on the use of LAWS, it supported the development of such weapon systems. To understand the support for a ban on use, it is relevant to note that the delegation defines LAWS to be 'indiscriminate, lethal systems that do not have any human oversight and cannot be terminated', which implies an inherent violation of the Law of Armed Conflict by such systems. At the same time, the dual-use benefits of the enabling technologies behind LAWS⁷⁶⁰ need to be valued on merit and developments in this regard should be facilitated. The position paper⁷⁶¹ also states that it is necessary to have full consideration of the applicability of general legal norms to LAWS.

Concerning emerging technologies such as AI, China "believes that the impact of emerging technologies deserves objective, impartial and full discussion". It states that "until such discussions have been done, there should not be any pre-set premises or prejudged outcome which may impede the development of AI technology."

CANADA

Maturity index – 2/5

In September 2017, Canada supported the formation of the GGE and expressed its willingness to participate in deliberations. It also highlighted that the disproportionate effect of even conventional weapons lingers after the armed conflict has come to end and that the issue must prioritised in deliberations surrounding LAWS as it is likely to be felt manifold.⁷⁶²

In April 2018 meeting of the GGE, Canada emphasised on the need to comply with International Humanitarian Law including the obligation for all states to ensure the lawfulness of their weapons, means and methods of warfare. It also expressed its support for the development of key 'Transparency and Confidence Building Measures'.⁷⁶³ In December 2019 Prime Minister

758. Chinese Delegation to the CCW 5th Review Conference, "Position Paper" available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/DD1551E60648CEBBC125808A005954FA/\\$file/China's+Position+Paper.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/DD1551E60648CEBBC125808A005954FA/$file/China's+Position+Paper.pdf)

759. Statement by the Chinese Delegation at the Thematic Discussion on Conventional Weapons at the First Committee of the 72 nd Session of the UNGA, available at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com17/statements/20Oct_China.pdf

760. Congressional Research Service, "International Discussions Concerning Lethal Autonomous Weapon Systems", August 2019, available at: <https://fas.org/sgp/crs/weapons/IF11294.pdf>

761. Position Paper submitted by China to the Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, April 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/E42AE83BDB3525D0C125826C0040B262/%24file/CCW_GGE.1_2018_WP.7.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/E42AE83BDB3525D0C125826C0040B262/%24file/CCW_GGE.1_2018_WP.7.pdf)

762. Canada – Thematic Debate Statement on Conventional Weapons – First Committee on 72nd session of UN General Assembly, February 2019, available at: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2017-10-22-weapons-armes.aspx?lang=eng

763. CCW States Parties, Group Of Governmental Experts On Lethal Autonomous Weapons Systems (LAWS), Opening Statement- Canada, April 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/86612887B010EB33C12582720056F0C6/\\$file/2018_LAWSGeneralExchange_Canada.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/86612887B010EB33C12582720056F0C6/$file/2018_LAWSGeneralExchange_Canada.pdf)

Justin Trudeau released the mandate letter⁷⁶⁴ of the Canadian Minister for Foreign Affairs Francois-Philippe Champagne and instructed him to 'advance international efforts to ban the development and use of fully autonomous weapons systems', indicating that the Canadian position would not likely be in the direction of regulating the further development of LAWS.

UK

Maturity index – 2/5

In 2016, the government of UK⁷⁶⁵ declared its commitment to maintaining human control over all weapon systems, and explicitly mentioned that there is "no intention of ever developing systems that could operate without any human control". To facilitate an effective and constructive discussion, the representatives encouraged other countries to share their national policies and approach on LAWS and expressed the intention to discuss the experience of different nations on the process of LAWS Review to thoroughly assess the legality of new weapons.

In 2017, UK's policy on LAWS was updated by means of a revised doctrine⁷⁶⁶ published by the Ministry of Defence on the best practices for Unmanned Aerial Vehicles. The doctrine acknowledged that its definition of LAWS differed from those of other states and further clarified such systems as those 'capable of understanding higher-level intent and direction and that it is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control'. This reiterated its position in not intending to develop such weapon systems in the future, while also clarifying that fully autonomous weapon systems do not exist within UK's defence arrangements. The government's policy position is clear that 'the operation of UK weapons will always be under human control as an absolute guarantee of human oversight, authority and accountability'.

A House of Lords report⁷⁶⁷ on AI, published in 2018, noted the need to establish an agreed definition of LAWS to allow for constructive dialogue and discussion in this regard, stating that the definition used by the military as one where it "is capable of understanding higher-level intent and direction" is not in tandem with the definitions adopted by most other nations. It noted that this acts as a roadblock in UK's participation in international discourse/debate on autonomous weapons and limits its ability to emerge as a moral and ethical leader on the global stage in this area. More importantly, this impedes the efforts to come up with an internationally agreed definition, which is of critical significance given the rapid advancements in AI and the increasing influence that defence holds in shaping global geopolitics. The committee recommended that the government realign the definition of autonomous weapons to a similar form as used by the rest of the world.

FRANCE

Maturity index – 2/5

In 2013, France took the initiative to propose a debate on this issue within the framework of the meetings of the CCW.⁷⁶⁸

764. Minister of Foreign Affairs Mandate Letter, December 2019, available at: <https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-foreign-affairs-mandate-letter>

765. United Kingdom of Great Britain and Northern Ireland Statement to the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, April 2016, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/49456EB7B5AC3769C1257F920057D1FE/\\$file/2016_LAWS+MX-GeneralExchange_Statements_United+Kingdom.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/49456EB7B5AC3769C1257F920057D1FE/$file/2016_LAWS+MX-GeneralExchange_Statements_United+Kingdom.pdf)

766. Ministry of Defence, Joint Doctrine Note 2/11, the UK Approach to Unmanned Aircraft Systems, 2017, available at: <https://www.law.upenn.edu/live/files/3890-uk-ministry-of-defense-joint-doctrine-note-211-the>

767. House of Lords Select Committee On Artificial Intelligence, "AI in the UK: Ready, Willing And Able?" April 2018, available at: <https://publications.parliament.uk/pa/l201719/lselect/l dai/100/100.pdf>

768. Permanent Representation of France to the Conference on Disarmament, "Meeting of Experts on Lethal Autonomous Weapons Systems", August 2016, available at <https://cd-geneve.delefrance.org/Meeting-of-experts-on-lethal-autonomous-weapons-systems-Geneva-13-16-May-2014>

Further, in 2016, France intervened in the CCW Informal meeting to present a definitional condition for a weapon to be identified as LAWS, which was that 'no form of human supervision is possible, the weapon must be autonomously mobile within a terrestrial, aerial or marine area, it must be able to select a target and launch the shoot of a lethal munition autonomously, it must be able to adapt to its environment and the behaviour of agents around it'.⁷⁶⁹

In the GGE meeting that took place on 7 November 2017 France and Germany submitted a working paper⁷⁷⁰ that called upon countries to develop a transparency and confidence building mechanism, before permitting the development of LAWS. It also acknowledged the prematurity of defining the LAWS, but nonetheless proposed a working definition for smooth discussion within the committee. It also proposed that the countries should declare that they share the conviction that humans should continue to be able to make ultimate decisions with regard to the use of lethal force and should continue to exert sufficient control over lethal weapons systems they use. It endorsed the proposal to develop a politically binding code of conduct.

In March 2018, French Prime Minister Emmanuel Macron expressed his disagreement with the deployment of LAWS and mentioned that the automated weapons give rise to 'absence of responsibility'.⁷⁷¹ In the same year in March, France and Germany re-iterated the proposals given in the working paper submitted in 2017 through a joint statement.⁷⁷²

GERMANY

Maturity index – 2/5

Apart from Germany's joint initiatives and statements with France (as stated above),⁷⁷³ a Coalition Agreement was signed by the Federal Government in 2013, in which the coalition partners express their intention 'to work for an international ban on fully automated weapon systems that exclude humans from the decision to the use of force' but also to regulate unmanned systems below this threshold internationally.⁷⁷⁴ The coalition agreement of 2018 has also expressed the similar intentions.⁷⁷⁵

In its campaign for a worldwide ban on fully autonomous weapons systems and LAWS, the first goal in the German approach is to reach agreement on a political declaration that states that all weapon systems must be controlled by humans.⁷⁷⁶ Corresponding to this outreach effort, Germany recognized the need to first establish broadly accepted definition of autonomous weapons, and in this respect the German Federal Foreign Office funds the International Panel on Regulation of Autonomous Weapons⁷⁷⁷, a network of international experts that is drawing up recommendations for international

769. Permanent Representation of France to the Conference on Disarmament in Geneva, "Presentation and Position of France", August 2016, available at: <https://cd-geneve.delegfrance.org/Presentation-and-position-of-France-1160>

770. Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, For consideration by the Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS) – Submitted by France and Germany, November 2017, available at: <https://undocs.org/ccw/gge.1/2017/WP.4>

771. Nicholas Thompson, "Emmanuel Macron talks to WIRED about France's AI Strategy", WIRED, March 2018, available at <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/>

772. Meeting of the Group of Governmental Experts on Lethal Autonomous Weapons Systems Geneva, Statement by France and Germany, April 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/895931D082ECE219C12582720056F12F/\\$file/2018_LAWSGeneralExchange_Germany-France.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/895931D082ECE219C12582720056F12F/$file/2018_LAWSGeneralExchange_Germany-France.pdf)

773. Ibid at 28 and 30.

774. Anja Dahlmann and Marcel Dickow, "Preventive Regulation of Autonomous Weapon Systems", German Institute for International and Security Affairs, March 2019, available at: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP03_dnn_dkw.pdf

775. Ibid at 32.

776. Federal Foreign Office, "A Worldwide Ban on Killer Robots", August 2018, available at: <https://www.auswaertiges-amt.de/en/aussenpolitik/themen/abrustung/autonomous-weapons-systems/2131672>

777. Federal Foreign Office, "Regulating Killer Robots", November 2019, available at: <https://www.auswaertiges-amt.de/en/aussenpolitik/themen/abrustung/killer-robots/2277026>

standards for weapons with autonomous functions.

In the 2019 meeting of GGE, the German representative contributed to the debate by providing various issues to be considered in the characterisation of LAWS in order to promote a common understanding on concepts and characteristics relevant to the objective and purpose of the Convention. As per Germany following can be considered to understand the autonomy in weapons:⁷⁷⁸

1. the capacity to perceive (sense and interpret) an environment,
2. evaluate the circumstances of a changing situation without reference to a set of pre-defined goals,
3. reason and decide on the most suited approach towards their realization,
4. initiate actions based on these conclusions, and
5. all of the above being executed without any human involvement once the system has been operationalized.

ISRAEL

Maturity index – 2/5

As per the statement submitted by the Israeli mission to the GGE on LAWS in August 2018, Israel supports further discussions in consideration of any possible regulation of LAWS. However, much like the Russian stance on the issue (discussed below), it advocated the preservation of research mandate for the civilian use of the AI technology. It further acknowledges that there are differences of opinion on the definition or characterization of LAWS and the appropriate type and level of human judgment throughout the various phases of the weapon's life cycle, as well as the suitable terminology. It suggests that such differences may stem from the fact the technology itself is in a preliminary stage of development and that a prudent approach is necessary. The statement calls for recognizing the potential military and humanitarian advantages of LAWS, including better precision of targeting which would minimize collateral damage and reduce risk to combatants and non-combatants. The statement further clarified the Israeli position that human judgment will always be an integral part of any process regarding LAWS throughout their life cycle; the statement also referenced Israel's domestic process for legal review of new weapons.⁷⁷⁹

RUSSIA

Maturity index – 2/5

In November 2017 GGE meet, Russia clarified that even though the discussion on the LAWS is welcome, the same is bereft of any specific definition and characterisation for the world community to assume as the base for an elaborate dialogue same and asked to 'preserve the research mandate' in this regard. The delegation further argued that development of AI

778. Group Of Governmental Experts On Emerging Technologies In The Area Of Lethal Autonomous Weapons Systems Of The Convention On Prohibitions Or Restrictions On The Use Of Certain Conventional Weapons Which May Be Deemed To Be Excessively Injurious Or To Have Indiscriminate Effects, Statement by Germany – On Agenda Item 5(d) Characterization of the systems under consideration in order to promote a common understanding on concepts and characteristics relevant to the objective and purpose of the Convention, March 2019, available at: <https://genf.diplo.de/blob/2203636/405f5b8fad59b21f17c553289296aa57/statement2-germany-gge-laws-data.pdf>

779. Group of Experts meeting on Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons, Statement by Mr. Ofer Moreno Director, Arms Control Department, Strategic Affairs Division, Ministry of Foreign Affairs, Israel; August 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/7A0E18215E16382DC125830400334DF6/%24file/2018_GGE%2BLAWS%2B2_6d_Israel.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/7A0E18215E16382DC125830400334DF6/%24file/2018_GGE%2BLAWS%2B2_6d_Israel.pdf)

systems to the level of ‘singularity or ‘superintelligence’⁷⁸⁰ will take a significant amount of time and therefore did not agree with the alarmist sentiments that predict inevitable emergence of fully autonomous systems in the near future.

In March 2018, the Head of General Staff of the Russian Army stated⁷⁸¹ that, ‘certainly, every military conflict has its own distinctive features. The main features of future conflicts will be the widespread use of high-precision and other types of weapons, including robotic ones. The objects of the economy and the government system of the enemy will be destroyed first’.

DENMARK

Maturity index – 2/5

In 2015, Denmark made its statement⁷⁸² in the Informal Meeting of Experts on CCW emphasizing the country’s stance that the use of autonomous weapons must be in compliance with the fundamental humanitarian law rules of distinction, proportionality and precautions in attack. It further said that all use of force must remain under ‘meaningful human control’

Apart from this the Danish Defence Ministry has published a report that addresses the issues connected to autonomous weapons and international law. It concluded that current developments have increased the demand for lawyers within the military, to establish the boundaries of legality of LAWS.⁷⁸³

EU

Maturity index – 2/5

In the April 2018 meeting of the GGE on LAWS, the EU stated that it considers it worthwhile to review more regularly and systematically the fast-paced developments in the area of emerging technologies, including AI, providing an opportunity to technical experts to share information on autonomous technologies relevant for our work. It emphasized that it is necessary that humans remain in control of the development, deployment and use with regard to possible military applications of emerging technologies, including AI, and prevent the creation and use of harmful applications.⁷⁸⁴ Pursuant to this the European Parliament passed a resolution⁷⁸⁵ in September 2018, stressing the fundamental importance of preventing the development and production of any lethal autonomous weapon system lacking human control in critical functions such as target selection and engagement. The resolution also underlined the fact that none of the weapons or weapon systems currently operated by EU forces are LAWS. It also highlighted that weapon systems specifically designed to defend own

780. Statement by the Russian Delegation on Agenda Item 8 of the Meeting of the States Parties to the Convention on Certain Conventional Weapons Consideration of the Report of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, November 2017, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/37365361B9432DC2C125823B00418F0C/\\$file/2017_GGE+LAWS_Statement_Russia.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/37365361B9432DC2C125823B00418F0C/$file/2017_GGE+LAWS_Statement_Russia.pdf)

781. Interfax News Agency, “The Use of Robots and the Widespread Use of High-Precision Weapons Will Become the Main Features of the Wars of the Future: Chief of the General Staff Of The Russian Army” (translated), March 2018, available at <https://www.militarynews.ru/story.asp?rid=1&nid=476975&lang=RU>

782. The Convention on Certain Conventional Weapons: Informal Meeting of Experts on LAWS, Statement of Denmark, April 2015, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/C5B8B0A4AD379822C1257E26005D7D20/\\$file/2015_LAWS_MX_Denmark.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/C5B8B0A4AD379822C1257E26005D7D20/$file/2015_LAWS_MX_Denmark.pdf)

783. Library of Congress (Law Library), “Regulation of Artificial Intelligence in Selected Jurisdictions”, January 2019, available at: <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf>

784. European External Action Service (EEAS), Convention on Certain Conventional Weapons – Group of Governmental Experts – Lethal Autonomous Weapons Systems, “EU Statement Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons Geneva”, April 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/00E636906F2DB883C12582720056F109/\\$file/2018_LAWSGeneralExchange_EU.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/00E636906F2DB883C12582720056F109/$file/2018_LAWSGeneralExchange_EU.pdf)

785. European Parliament Resolution on Autonomous Weapon Systems (2018/2752(RSP), September 2018, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IP0341&from=EN>

platforms, forces and populations against highly dynamic threats such as hostile missiles, munitions and aircraft are not considered LAWS.

In the March 2019 meeting of the GGE on LAWS, the EU's statement⁷⁸⁶ emphasised that countries have a responsibility to ensure that the development, deployment and use of emerging technologies in the area of LAWS comply with international law. It further recalled that national legal weapons reviews must be conducted, pursuant to Article 36 of Additional Protocol I to the Geneva Conventions, in the study, development, acquisition or adoption of a new weapon, means or method of warfare, in order to determine whether its employment would, in some or all circumstances, be prohibited by applicable international law. This, as per the EU delegation, would contribute to transparency and confidence-building between countries and help countries to respond to emerging challenges in this space. On the issue of assessment of potential military application of AI, it stated⁷⁸⁷ that it is important to holistically review the development of AI at a global level.

AUSTRALIA

Maturity index – 2/5

The 2015 inquiry⁷⁸⁸ by the Senate Foreign Affairs, Defence and Trade Committee on the potential use of unmanned air, maritime, and land platforms by the Australian Defence Force recommended that given the existence of capability requirement, such armed unmanned platforms should be acquired by the Australian Defence Force and further advised the Australian Government to make a policy statement regarding their use. The report maintained the primacy of law of armed conflict and international humanitarian law in that the introduction of armed unmanned platforms should be checked for compliance with the stated international laws and recommended the Australian Defence Force to notify the Australian Government of measures taken to address any relevant identified gaps training and dissemination programs when these platforms are acquired.

In the 2017 GGE meeting on LAWS, Australia again emphasized the primacy of international laws by which it is bound, and fully supported and assured adherence to the obligation to undertake a review of any new weapon, means or method of warfare to determine whether its employment would, in some or all circumstances, be prohibited by relevant international laws.⁷⁸⁹ Recognising the potential complexity of reviewing weapons systems with increasingly automated functions, and acknowledging that the level of complexity bound to increase with further development in AI and machine learning, Australia stated that it looked forward to further discussions on the same while it stayed committed to the existing legal framework for reviewing new weapons.

In 2019, Australia presented⁷⁹⁰ its nine-stage approach towards the deployment of LAWS beginning from developing a legal and policy framework followed by design and development till the after-use evaluations. It also includes the evaluation, training and certification that is necessary for the deployment of LAWS. Further, it brought to light how Australia's system

786. EU Statement Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons, March 2019, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/EA84B3C2340F877DC12583CB003727F3/\\$file/ALIGNED+-+LAWS+GGE+EU+statement+IHL.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/EA84B3C2340F877DC12583CB003727F3/$file/ALIGNED+-+LAWS+GGE+EU+statement+IHL.pdf)

787. EU Statement Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons, "Review of Potential Military Applications of Related Technologies in the Context Of The Group's Work", March 2019, available at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/statements/25March_EuropeanUnion5d.pdf

788. State Standing Committees on Foreign Affairs Defence and Trade, "The Potential Use by the Australian Defence Force of Unmanned Air, Maritime and Land Platforms", 2015, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Defence_Unmanned_Platform/Report

789. Australian Statement - General Exchange of Views, GGE on LAWS, November 2017, available at: <https://geneva.mission.gov.au/gene/Statement783.html>

790. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Australia's System of Control and applications for Autonomous Weapon Systems, March 2019, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/16C9F75124654510C12583C9003A4EBF/\\$file/CCWGGE.12019WP.2Rev.1.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/16C9F75124654510C12583C9003A4EBF/$file/CCWGGE.12019WP.2Rev.1.pdf)

of control provides comprehensive control over any weapon system, and how and under what circumstances it can be deployed, ensuring, at its core, the weapon system is driven by human direction and is compliant with international and domestic law.

JAPAN

Maturity index – 2/5

Japan's submitted its position paper⁷⁹¹ in the third Informal meeting of Experts on LAWS in 2016 wherein it emphasised the need to decide upon a definition or common understanding of LAWS. It considered concepts of 'autonomy' and 'meaningful human control' to be instrumental to the discussion. The report accorded particular importance to recognizing the dual-use nature of robotic technology - working with the assumption that 'technologies of autonomous systems usable for LAWS have a high affinity with those technologies that have been under research and development in civil use', and advocated that deliberations on LAWS should not inhibit the promotion, research and development of peaceful and sound use of robots.

In 2019, Japan focused its statement⁷⁹² on the lethality aspect of the LAWS and stated that it is appropriate to limit the discussion only to autonomous weapons systems with lethality. It suggested that weapons systems designed to directly kill human beings be made subject to rules on lethality. The statement highlighted the indispensability of meaningful human control over a lethal weapon system, which entails proper operation of such systems and requires persons with sufficient information on such weapons systems to be engaged in their operation. It would be necessary to deepen discussion on where and how much meaningful human control is necessary in the life cycle of weapons systems. Further it also supported the standard measures to be developed for transparency.

SOUTH KOREA

Maturity index – 2/5

In 2013, at the Meeting of the High Contracting Parties on CCW, South Korea supported the efforts to respond to concerns over weapons technology and warfare. It commended that the chair invited them to a discussion on lethal autonomous weapon systems in the future and the challenges such weapons would pose to future armed conflicts and international humanitarian law.⁷⁹³

SWEDEN

Maturity index – 2/5

In its statement⁷⁹⁴ in the 2016 meeting of Experts on LAWS by CCW, Sweden emphasised that that humans should always bear the ultimate responsibility when dealing with questions of life and death. It further assured the international community

791. CCW 3rd Informal Meeting on LAWS, "Japan's Views on Issues Relating to LAWS, 2016, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/4E8371EAD5E34263C1257F8C00289B5E/\\$file/2016_LAWS+MX_CountryPaper+Japan.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/4E8371EAD5E34263C1257F8C00289B5E/$file/2016_LAWS+MX_CountryPaper+Japan.pdf)

792. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Possible outcome of 2019 Group of Governmental Experts and future actions of international community on Lethal Autonomous Weapons Systems –Submitted by Japan, March 2019, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/B0F30B3F69F5F2EEC12583C8003F3145/\\$file/CCW+_GGE+.1._+2019_+WP3+JAPAN.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/B0F30B3F69F5F2EEC12583C8003F3145/$file/CCW+_GGE+.1._+2019_+WP3+JAPAN.pdf)

793. Statement of South Korea, Convention on Conventional Weapons Meeting of High Contracting Parties, Geneva, November 2013, available at: https://www.stopkillerrobots.org/wp-content/uploads/2013/03/KRC_CountryStatus_14Mar2014.pdf

794. General Statement by Sweden at the 2016 CCW Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/1E243D02F4D06BEEC1257F9400420DA0/\\$file/2016_LAWS+MX_GeneralExchange_Statements_Sweden.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/1E243D02F4D06BEEC1257F9400420DA0/$file/2016_LAWS+MX_GeneralExchange_Statements_Sweden.pdf)

about Sweden's compliance to International Humanitarian Law and supported the compliance-based framework for the regulation of LAWS.

In the 2018 GGE meeting on LAWS, Sweden recommended the need for all countries to review new weapons, means or methods of warfare, on the usefulness of voluntary exchange of their national experiences with review procedures. It further encouraged information exchange between countries, including on best practices, all in the interest of greater transparency.⁷⁹⁵

In 2017, the Swedish Riksdag saw a motion being raised for the prohibition of lethal autonomous weapons system and joined the group of 19 countries supporting the ban of such weapons.⁷⁹⁶ In a 2019 speech⁷⁹⁷ by the Swedish Foreign Minister in Berlin, it was stated that Sweden supported the approach jointly adopted by France and Germany of political declaration and that it would 'allow us to state, and commit to, the points and principles on lethal autonomous weapons systems on which we have common understanding'.⁷⁹⁸

FINLAND

Maturity index – 2/5

Finland took part in the 2015 UNOG expert panel on LAWS, where they welcomed more work on whether LAWS is compatible with the CCW framework. In its statement the delegation of Finland highlighted that countries have the obligation of assessing the legality of their weapons and welcomed more discussion on LAWS.⁷⁹⁸

NORWAY

Maturity index – 2/5

A statement on the Norwegian position on LAWS can be found in the Norwegian Council on Ethics' (for the Norwegian Government Pension Fund Global) annual report, 2017,⁷⁹⁹ which refers to the ethical guidelines made by the Government Pension Fund. These state that the fund shall invest in companies which produce weapons that violate fundamental humanitarian principles through their normal use. The report emphasises the importance of observing the International Humanitarian Law principles of distinction and proportionality and that combatants must take the necessary precautions to comply with these principles. It highlights that decision of life and death if left up to the machines poses intrinsic humanitarian problem at the outset and that it is important to understand the functioning of autonomous weapons to reach a proper conclusion.

In 2017, Norway highlighted the importance of accountability in the GGE Meeting on LAWS and stated that without accountability, deterring and preventing international crimes becomes more difficult. It brought to light that a robot or an

795. General Statement by Sweden at the CCW GGE on Lethal Autonomous Weapons Systems (LAWS), 9-13 April 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/12706C2B73502F13C125827400536FA9/\\$file/2018_LAWSGeneralExchange_Sweden.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/12706C2B73502F13C125827400536FA9/$file/2018_LAWSGeneralExchange_Sweden.pdf)

796. Statement by Carl Schlyter (MP), "Prohibit Autonomous Lethal Weapons Systems and Regulate the Development of Artificial Intelligence" (translated), October 2017m available at https://www.riksdagen.se/sv/dokument-lagar/dokument/motion/forbjud-autonoma-dodliga-vapensystem-och-reglera_H5022655

797. Speech by the Minister for Foreign Affairs, "Capturing Technology: Rethinking Arms Control" (translated), March 2019, available at <https://www.govt.se/speeches/2019/03/uttalande-av-um-i-berlin-den-15-mars/>

798. Statement by Delegate of Finland at the High Contracting Parties to the CCW, November 2015, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/43811AA71321CDF9C1257F0F00383E96/%24file/finland.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/43811AA71321CDF9C1257F0F00383E96/%24file/finland.pdf)

799. Council on Ethics for the Norwegian Government Pension Fund Global, "Annual Report 2015", available at: https://nettsteder.regjeringen.no/etikkraadet3/files/2017/02/Etikkraadet_AR_2015_web-1.pdf

algorithm is obviously precluded from any moral and legal accountability. Considering the limited role that humans may have in operating these systems, it is easy to foresee situations in which no one can be held responsible if fully autonomous weapons are used in violation of international law. Norway emphasised the importance of bridging this accountability gap so that culpability can be analysed.⁸⁰⁰

ESTONIA

Maturity index – 2/5

In the 2018 Meeting of GGE on LAWS, on the agenda of possible options for addressing the humanitarian and international security challenges, Estonia unequivocally stated that it is not convinced of the need for a new legally binding instrument on weapon systems with autonomous functions. It however, reiterated that any weapon system, irrespective of its autonomous functionality, must only be used in strict compliance with the principles and rules of international law, in particular international humanitarian law and human rights law. Further, it noted that weapons systems with autonomous functions need to be assessed for their lawfulness on a case-by-case basis, taking into account their technical capabilities and intended uses and cannot be called inherently illegal.⁸⁰¹ Additionally, on the agenda of consideration of the human element in the use of lethal force, Estonia acknowledged the fundamental role played by commanders and operators in ensuring compliance with international humanitarian law. Therefore, it stated that weapon systems with autonomous functions can be lawfully relied on, conditional upon absolute confidence in the weapon system to not lead to unintended consequences and breaches of the law, given its fixed and programmable features, and the operational situation prevailing at the time. As per the statement, this assessment must form a part of the commander's and operator's duty to take precautionary measures under international humanitarian law.⁸⁰²

THE NETHERLANDS

Maturity index – 2/5

In April 2015, the Dutch Ministers of Foreign Affairs and Defence requested an advisory report on legal, ethical, and policy issues with regard to LAWS from the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law. The report, which was published in October 2015, concluded that meaningful human control is required in the deployment of autonomous weapon systems. The Dutch government concurs with this view. It therefore proposed, among other things, to establish a GGE at the 2015 annual meeting of the CCW to study this issue.⁸⁰³ The Netherlands in its address⁸⁰⁴ in the General Debate at the 5th Review Conference of the CCW, highlighted the importance of discussion on LAWS and more importantly addressed the issue of tight financing of the Convention hampering its proper functioning.

800. CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), General Statement by Norway, November 2017, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/DF861D82B90F3BF4C125823B00413F73/\\$file/2017_GGE+LAWS_Statement_Norway.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/DF861D82B90F3BF4C125823B00413F73/$file/2017_GGE+LAWS_Statement_Norway.pdf)

801. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Statement by Estonia, Agenda Item 6(d) - Possible options for addressing the humanitarian and international security challenges, August 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/051E90835D7D6135C1258316002BB414/\\$file/2018_GGE+LAWS+2_6d_Estonia.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/051E90835D7D6135C1258316002BB414/$file/2018_GGE+LAWS+2_6d_Estonia.pdf)

802. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Statement By Estonia, Agenda Item 6(b) - Further consideration of the human element in the use of lethal force, August 2018, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/721FACB291BFF5CCC1258316002B6071/\\$file/2018_GGE+LAWS+2_6b_Estonia.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/721FACB291BFF5CCC1258316002B6071/$file/2018_GGE+LAWS+2_6b_Estonia.pdf)

803. Library of Congress (Law Library), "Regulation of Artificial Intelligence in Selected Jurisdictions", January 2019, available at: <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf>

804. General Debate, 5th Review Conference of the CCW, Netherlands Opening Statement, 2016, available at: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/F5C3B4035ADBD01DC125808A005BC201/\\$file/Netherlands+Statement+General+RevCon+CCW+\(final\).pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/F5C3B4035ADBD01DC125808A005BC201/$file/Netherlands+Statement+General+RevCon+CCW+(final).pdf)

The Dutch Parliament also adopted a resolution in May 2019 that calls for binding international rules on new weapons technologies, including autonomous weapons or killer robots. The resolution was supported by all but one party in the parliament and calls on the Dutch government to boost a treaty on these types of weapons.⁸⁰⁵

The Netherlands proactively participated in the 2019 deliberation in the GGE meeting on LAWS, on the issue of review of review of the potential military applications of related technologies. In the context of the Group's work, it stated that the Netherlands' armed forces have been using systems that can, to a large extent, operate automatically and possess a certain degree of autonomy; although all of them under a meaningful human control. The Netherlands stated that it considers weapons reviews mandatory under international law and crucial for all weapon systems, including weapon systems with some degree of autonomy.⁸⁰⁶

805. PAX, "Breakthrough: Dutch Parliament Calls for International Rules on Killer Robots", May 2019, available at <https://www.paxforpeace.nl/stay-informed/news/breakthrough-dutch-parliament-calls-for-international-rules-on-killer-robots>

806. Group of Governmental Experts on LAWS, Statement of the Netherlands, April 2019, available at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/statements/25March_NL5c.pdf



INDIAI

A MEITY, NEGD & NASSCOM INITIATIVE