KONRAD ADENAUER STIFTUNG

Law & Innovation

This page is intentionally left blank.

ABOUT KONRAD-ADENAUER STIFTUNG

Freedom, justice, and solidarity are the basic principles underlying the work of the Konrad-Adenauer-Stiftung (KAS). KAS is a political foundation, closely associated with the Christian Democratic Union of Germany (CDU). As co-founder of the CDU and the first Chancellor of the Federal Republic of Germany, Konrad Adenauer (1876-1967) united Christian-social, conservative and liberal traditions. His name is synonymous with the democratic reconstruction of Germany, the firm alignment of foreign policy with the trans-Atlantic community of values, the vision of a unified Europe, and an orientation towards the social market economy. His intellectual heritage continues to serve both as our aim as well as our obligation today. In our European and international cooperation efforts, we work for people to be able to live self-determined lives with freedom and dignity. We make a contribution underpinned by values to help Germany meet its growing responsibilities throughout the world.

KAS has been working in Cambodia since 1994, striving to support the Cambodian people in fostering dialogue, building networks, and enhancing scientific projects. Thereby, the foundation works towards creating an environment conducive to social and economic development. All programs are conceived and implemented in close cooperation with the Cambodian partners on central and sub-national levels.

Learn more through: KAS Cambodia Website.

Publisher Information
The Legal Len: Law & Innovation

Editor:
Thomas Honnet

Proofreading By
Koeut Sokunkosoma
Touch Rattanakraingsey
Moeung Cheery

Cover Design
Nai Monyoudom

Layout Design
Tann Sopheavy

FOREWORD

In an era defined by rapid technological advancement and shifting global dynamics, the relationship between law and innovation has grown both vital and increasingly complex. As Cambodia moves toward a more knowledge-based and digitally driven economy, it is essential that legal and regulatory frameworks evolve in parallel with innovation. Achieving this balance, however, is no simple task. Too often, the law is seen not as a facilitator, but as a constraint to innovation.

Through this publication, Konrad-Adenauer-Stiftung Cambodia is proud to present the forward-thinking ideas of our contributors—ideas that aim to support and inform this complex and necessary evolution.

Law does not merely respond to innovation; it also has the power to shape the environment in which innovation can flourish. At the same time, when poorly designed or implemented, legal frameworks can inadvertently stifle creativity and progress. Whether in areas such as digital governance, intellectual property, data protection, or emerging technologies like artificial intelligence, the legal system must serve a dual role: safeguarding fundamental rights while enabling societal and technological advancement.

Fulfilling this dual function demands foresight, adaptability, and inclusive dialogue—among lawmakers, practitioners, innovators, and the public alike. It is only through collaboration across these communities that truly responsive and future-ready legal systems can emerge.

KAS Cambodia is honoured to support this timely and important work, which brings together diverse perspectives from legal scholars, policymakers, and thought leaders. The aim is to contribute to informed debate, offer practical insights, and inspire concrete steps that align legal development with the aspirations of a modern, innovative society.

We firmly believe that fostering a legal environment that promotes innovation—while upholding ethical standards, truth and social justice—is not only possible, but necessary. Through knowledge-sharing and critical engagement, we hope this publication serves as a foundation for continued legal innovation in Cambodia and beyond.

I extend my sincere thanks to all contributors, and warmly invite readers to explore the ideas presented here with curiosity and an open mind. At KAS Cambodia, we are confident that the reflections and proposals in the following pages will help advance the dynamic interplay between law and innovation. Let us work together toward an innovative, just, and prosperous future.

Daniela Braun
Country Director
KAS Cambodia

INTRODUCTION

The law is often seen as an obstacle to innovation. This curious approach only sees the regulation as something prohibits, hinders, prevents, and slows down. However, it is not so surprising when we consider its origins: the libertarianism that has shaped digital technologies since Silicon Valley, which views the government as an unnecessary and even illegitimate obstacle. “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather…”

This position has since been widely criticized and contradicted (we now know, for instance, how the development of the internet and GAFAM has often benefited from government support), and its main goal is the development of a new form of capitalism, one based on knowledge, with the least amount of intervention and external control.

The relationship between law and innovation is actually more complicated: regulation can also be supportive or protective, it can be an incentive to innovate differently, and of course, it can also sometimes be a hindrance to innovation. The law can enable and stimulate research, establish specific conditions for innovators by simplifying certain administrative procedures, authorizing practices that would otherwise be prohibited, creating advantageous financial conditions, etc. It can be more “flexible” within a temporary framework for innovation within a defined time frame and scope, for example through experimental legislation that may or may not subsequently be generalized.

Also, innovation can be a new way to inspire the law and the way rules are created. Digital technology, for example, enables new ways of consulting the public and co-constructing the law, with online public consultations open to all citizens.

This publication aims to show, through various concrete examples from different legal and technical fields, that the interaction between law and innovation is complex. Our brilliant authors, who come from all over the world, share their views on this interaction: this could give to the Kingdom of Cambodia some ideas and inspire it in the current process of drafting all its legal framework in digital law.

Thomas Honnet

CONTENT

PART I

ECOSYSTEM OF LEGAL INNOVATION

Photo: How Cambodia's Students Are Thriving Through Digital Literacy
Source: Swisscontact

INNOVATIVE TECHNOLOGIES IN CAMBODIA LAW/ LEGALCURRICULUM AND EDUCATION: TO FIT WITH THE HIGHER EDUCATION FRAMEWORK

Sok Chea Am

I. Introduction

The traditional educational program and teacher-centered learning do not ultimately produce graduates with all the skill sets required by the current and future work environment.[1] Currently, many companies and institutions seek candidates who have the technical skills (technology, digitalization, and artificial intelligence – AI skills) and soft skills (21st-century skills, lifelong learning, system thinking, and resilience) to complete the given complicated tasks effectively.[2] For the context of legal/law education, such a graduate is also needed for current and future legal work. In response to those requirements, law institutions have to improve the curriculum and apply effective innovative pedagogy approaches to produce graduates who have the important interdisciplinary skills, innovation skills, and technology and entrepreneurship mindset essential in a modern market or workplace environment.

Innovation, technology, and social changes are moving legal education towards a crossroads of curriculum design, disrupting traditional modes of delivery, pedagogy, and educational business models. Stakeholders such as law schools, law societies, accreditation bodies, quality assurance regulatory offices, the higher education sector, relevant ministries, and the judiciary face challenges presented by the new structure of curriculum and its modes of delivery of legal education, and the effectiveness of assessment methodology.

For a nation like Cambodia, integrating digital literacy at the core of its higher education framework becomes pivotal to ensure the acquisition of the required skills for the relevant industry. This encompasses not just the ability to use digital tools but also the understanding and leveraging of them for innovation, problem-solving, and knowledge creation.[3] In addition, rapid advancements in artificial intelligence, known as AI, have led to the creation of powerful AI tools that have been proven to assist in various aspects of learning, from personalized tutoring to real-time feedback. With the emergence of AI-driven tools, Cambodia's higher education system has the opportunity to revolutionize teaching methods and equip students with the knowledge, skills, and attitude necessary to excel in an increasingly technology-driven future. Integrating AI-driven tools in Cambodia's higher education could bridge the gap between traditional teaching methods and the dynamic demands of a digital future.

There are some questions regarding the integration of innovation and technology in legal education: Are law schools equipping graduates with the skills required for 21st-century legal practice? Should an understanding of the impact of artificial intelligence, innovation, and machine learning on legal services now be a prerequisite for the contemporary law degree in Cambodia? Will an innovation mindset and professional ethic be integrated into a legal educational program? This article will discuss how the digital age requires a commitment to developing the capacity of law students to respond to technological innovation.[4]

1 S. C. Am et al., "Engineering Curriculum Development Toward Innovation and Entrepreneurship for Sustainable Education: Outcome-Based Education (OBE)," Digital Insights – Future of Education, Kingdom of Cambodia, Konrad-Adenauer-Stiftung (KAS), 2023, pp. 117-132.

2 L. Memmert et al., "Learning by Doing: Educators' Perspective on an Illustrative Tool for AI-Generated Scaffolding for Students in Conceptualizing Design Science Research Studies," JISE vol.34, no.3, 2023, pp. 279-292.

3 S. Heng and S. Seng, "Revolution and Readiness through AI-Driven Learning in Cambodia's Higher Education," Digital Insights – Future of Education, Phnom-Penh, Konrad-Adenauer-Stiftung (KAS), 2023, pp. 117-132.

4 F. Ryan and H. McFaul, "Innovative Technologies in U.K. Legal Education," 1st Edition Key Directions in Legal Education, U.K., Routledge, 2020, pp. 1-13.

This article is organized as follows. Section 2 elaborates on the big picture framework for curriculum design and implementation in the higher education sector. Section 3 discusses the current practice of law education and benchmarking. Section 4 discusses the potential of legal/law education in Cambodia to align with the higher education framework. Finally, the conclusion is given in section 5.

II. A Big Picture about the Curriculum Design in the Higher Education Sector

In the effort to modernize academic programs in Cambodia, a framework was developed as a guide to integrate all the policies, enablers, and drivers that are aligned to the Cambodian Sustainable Development Goals (CSDG), Pentagonal Strategy,[5] Industrial Development Policy,[6] Education Strategic Plan,[7] market needs, Plan-Do-Check-Act (PDCA) approach, Continuous Quality Improvement (CQI) concept, and Conceive-Design-Implement-Operate (CDIO) approach. Furthermore, the Cambodian Qualifications Framework (CQF),[8] released in 2012, is the instrument for the development and classification of qualifications for specific learning levels, based on a set of criteria that is agreed upon nationally. They are classified into ten learning domains for graduates to equip them with during their learning experiences within the program. Those ten learning domains are knowledge, cognitive skills, psychomotor skills, interpersonal skills, responsibility, entrepreneurial skills, ethics and professionalism, communication, IT or digital skills, and numerical skills. At its core, the framework requires academic programs to adopt the following initiatives; *i)* Transformative Curriculum Design, *ii)* Innovative and Effective Pedagogy and *iii)* Holistic Assessment, together with program generic design – mode of program operation, to produce graduates who possess attributes of Lifelong Learners, Systems Thinking, Resilience, 21st-Century Skills, Holistic and Entrepreneurial Skills, and Technology – Digitalization – AI Skills (Figure 1).

5 Royal Government of Cambodia, "Pentagonal Strategy-Phase I for Growth, Employment, Equity, Efficiency and Sustainability: Building the Foundation Towards Realizing the Cambodia Vision 2050," The Royal Government of Cambodia of the Seventh Legislature of the National Assembly, Kingdom of Cambodia, 2023, pp. 1-85.

6 Royal Government of Cambodia, "Cambodia Industrial Development Policy 2015-2025: Market Orientation and Enabling Environment for Industrial Development" Council of Ministers at Its Plenary Meeting, Kingdom of Cambodia, 2015, pp. 1-36.

7 "Education Strategic Plan 2024-2028," Ministry of Education, Youth and Sport - MoEYS, Kingdom of Cambodia, 2024, pp. 1-168.

8 "Cambodia Qualifications Framework - CQF," National Training Board (NTB), Kingdom of Cambodia, 2012, pp. 1-70.

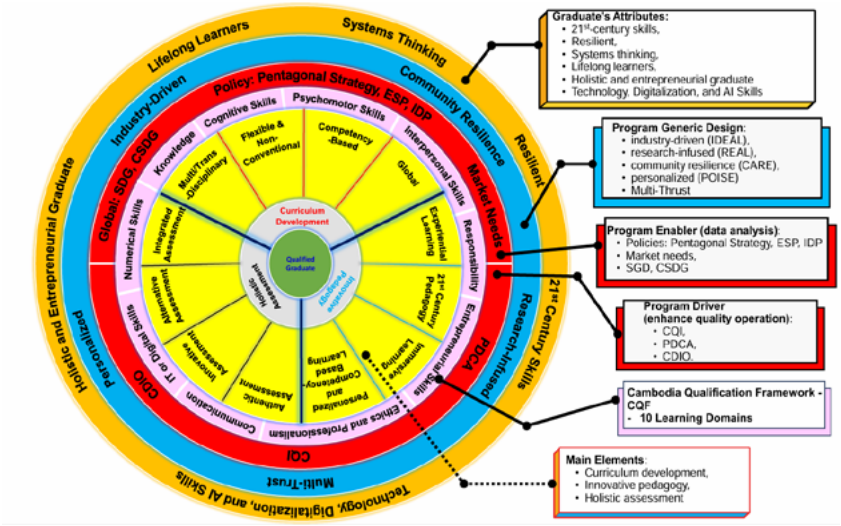


Figure 1. Proposed Framework for Holistic Academic Program Development and Implementation (this figure is redesigned from the original framework of the Directorate General of Higher Education – DGHE)[9]

Transformative Curriculum Design

Transformative curriculum design is an approach to designing education programs that aims to create meaningful and impactful learning experiences for students. It goes beyond traditional curriculum design by focusing on fostering critical thinking, creativity, and social change. This type of curriculum design often incorporates real-world problems, multi/inter transdisciplinary learning, flexible and non-conventional learning, competency-based learning, and opportunities for students to engage in hands-on experiential learning. The goal of transformative curriculum design is to empower students to become active and engaged learners who are prepared to address complex challenges in the world.

As illustrated in Figure 2, for an educational program to be multi/trans-disciplinary, its structure and model of operation must provide choices to achieve a few majors that are the foundation for their future workplace and equip them with lifelong learning ability. Besides a single major program, a program should consider majors with minors, double majors, or double degrees to expand the opportunities of graduates for upcoming and complex working environments. Moreover, the program should be designed in a model that can equip students with real-world experiences through engagement with industry projects, research activities, and the community's projects. Flexibility is to offer choices for learners to select from elective courses or interdisciplinary options. At a higher level of program development, learners have the competency to accumulate different courses for their degree program, which is sometimes called a "*Personalized Degree Program*". This is a clear example of a program with high flexibility options or majors. An academic program must specify clearly the program-specific and generic competencies that learners should acquire during and after the completion of the study. The global context of curriculum development refers to international programs and benchmarking

9 Directorate General of Higher Education – DGHE, "FutureFit Educational Framework for Outcome-Based Education in Cambodian Higher Education," Ministry of Education, Youth and Sport – MoEYS, 2025.

with similar programs in the region and overseas. Innovation, technology, AI skills, area-specific skills, and soft skills are pivotal competencies for current and future workplaces in any major.

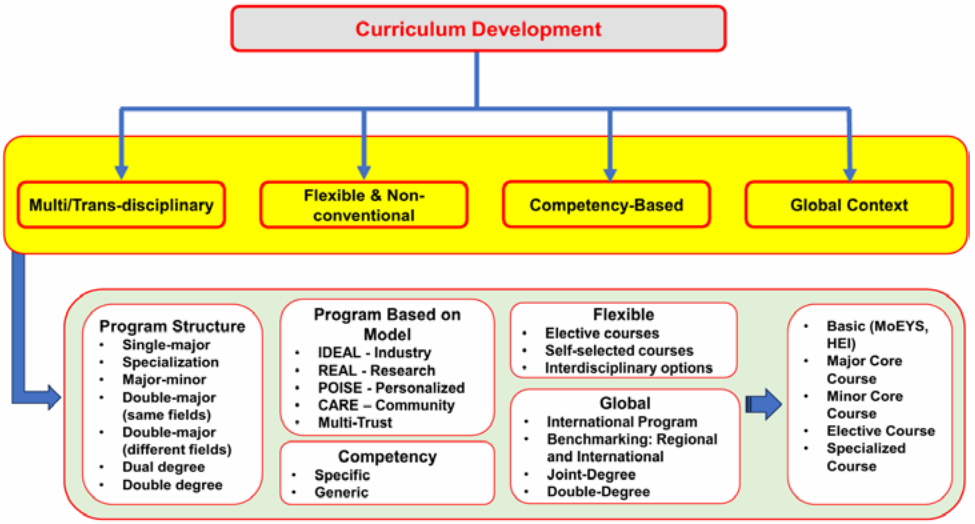


Figure 2. Curriculum Development (this figure is redesigned from the original framework of the Directorate General of Higher Education – DGHE)

Innovative Pedagogy

Innovative pedagogy plays a crucial role in implementing a transformative curriculum based on the above design concept. It refers to the use of creative and cutting-edge teaching methods and strategies to enhance student learning, engagement, and achievement. Figure 3 lists four main elements of innovative pedagogy:

1) experiential learning,
2) 21st-century pedagogy,
3) immersive learning, and
4) personalized and competency-based learning.

Innovative pedagogy aims to foster critical thinking, creativity, collaboration, communication, technology, digital, AI skills, 21st-century skills, and other skills in students by providing them with dynamic and interactive learning experiences. Some examples of innovative pedagogies include project-based learning, problem-based learning, immersive learning – digital/virtual reality, experiential learning, inquiry-based learning, gamification, personalized learning, experiential learning, collaborative learning, and technology integration. A combination of mixed teaching and learning modalities, such as in-person learning, blended learning, online learning, hybrid learning, and hyflex learning, is very useful to cultivate the required specific and generic competencies of graduates. By embracing innovative pedagogical approaches, educators can create more effective and impactful learning environments that prepare students for success in a rapidly changing world.

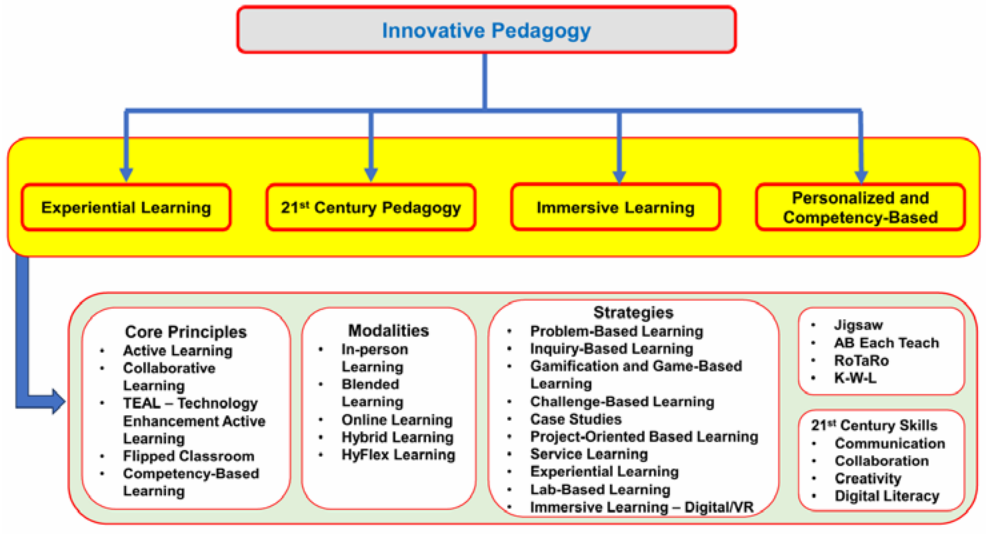


Figure 3. Innovative/effective Pedagogy approach for driving students to achieve knowledge, skills, and attitude (this figure is redesigned from the original framework of the Directorate General of Higher Education – DGHE)

Holistic Assessment

Holistic assessment is an approach to evaluating student learning that takes into account various aspects of a student's performance and development, rather than focusing solely on traditional measures such as tests and exams. It involves assessing students' knowledge, skills, attitudes, behaviors, and values in a comprehensive and integrated manner. Holistic assessment considers the whole student and seeks to provide a complete picture of their abilities and progress. The assessment, for assessing students' performances, must be authentic, innovative, alternative, and integrated (Figure 4).

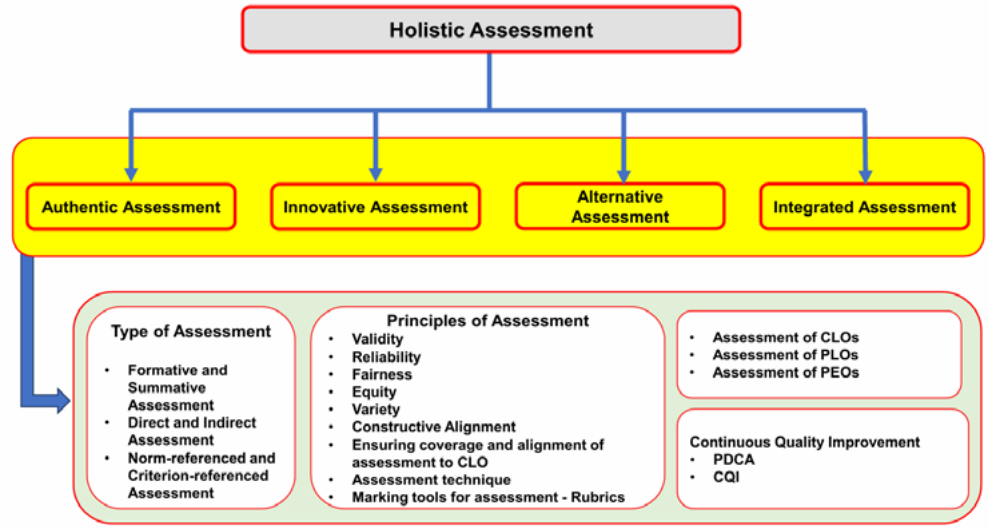


Figure 4. Holistic assessment to assess each student's knowledge, skills, and attitude (this figure is redesigned from the original framework of the Directorate General of Higher Education – DGHE)

In holistic assessment, educators use a variety of assessment methods, such as observations, portfolios, projects, presentations, self-assessments, peer assessments, and reflective journals, to gather information about students' learning and growth. To do so, each assessment task of one course learning outcome (CLO) must ensure content validity, reliability, fairness, equity, and variety. This approach allows for a more nuanced understanding of students' strengths, weaknesses, and areas for improvement.

Overall, holistic assessment aims to promote a more comprehensive and meaningful evaluation of student learning that goes beyond traditional academic measures and supports students in achieving success in all aspects of their education and personal growth.

Inception Process for Curriculum Development – Aligning to Sectoral Framework

The inception process for curriculum development, two other fundamental concepts, constructive alignment, and backward design, should be demonstrated. Figure 5 presents the concept of constructive alignment (CA) that demonstrates *1)* how to set the objective and learning outcomes, *2)* how to use appropriate teaching and learning approaches to achieving the early set learning outcomes (different outcomes require different pedagogy approaches), and *3)* how to formulate quality assessment with specific rubric to assessing the achievement of learning outcomes (different learning outcomes require different assessment and evaluation methods). Figure 6 shows a backward design concept for developing a curriculum. It describes several stages required before the curriculum is completely set up. On the top level, vision and missions, program educational objectives (PEOs), and program learning outcomes (PLOs) must be well-established and followed by courses set up. As a result, Figure 7 details the inception process for curriculum development under the new framework in the higher education sector.

This process is thoroughly designed to cover the essential stakeholders and activities required for the effective implementation of the framework and curriculum setup. It outlines four main steps that must be followed sequentially to develop an academic curriculum successfully:

1) Realize the vision and mission statements of the university/institution based on all relevant stakeholders' inputs.
2) Develop the PEOs' statements, and these statements must be mapped to the vision and mission statements.
3) Formulate the PLOs' statements, which must be mapped to PEOs' statements.
4) Determine the program structure where the program developer should decide on the structure (e.g., single major, major-minor), identify courses, contents, and implement teaching and learning activities.

Assessment must be conducted in every step, and data collected needs to be analyzed to identify strengths, weaknesses, and areas for improvement. This data-driven approach helps instructors make informed decisions on the curriculum design, teaching approaches, assessment methods, and resources as part of the CQI process.

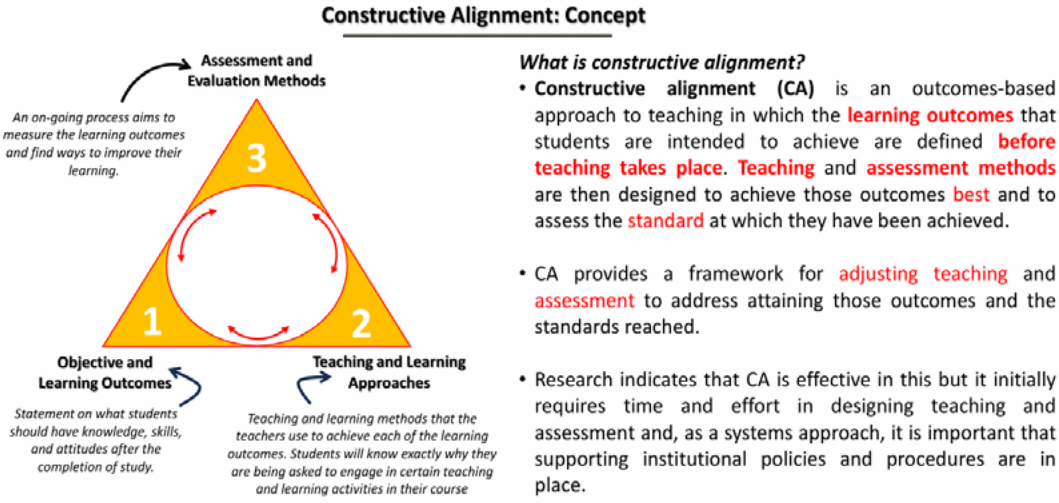


Figure 5. Constructive Alignment

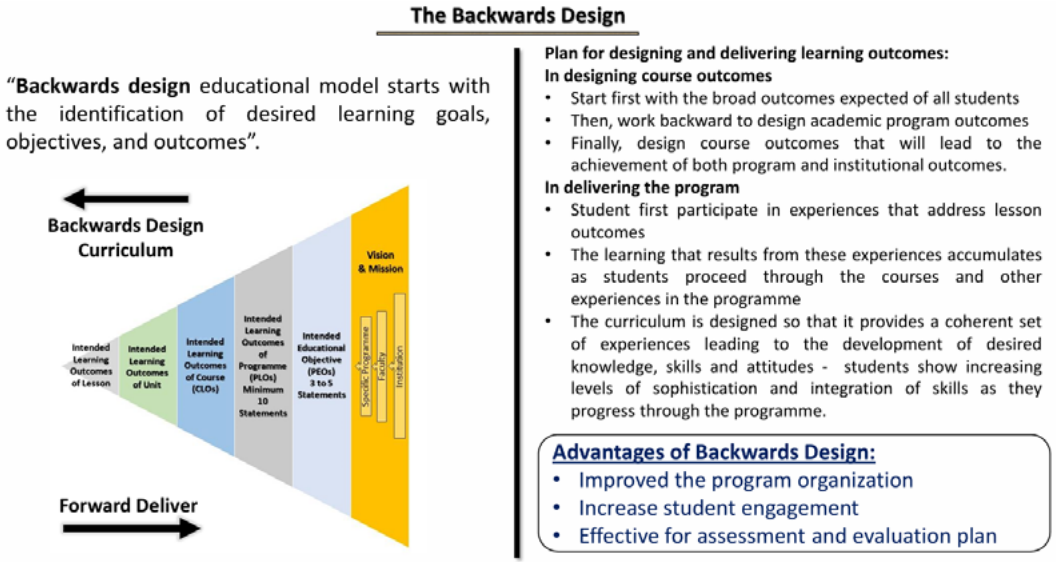


Figure 6. Backward Design

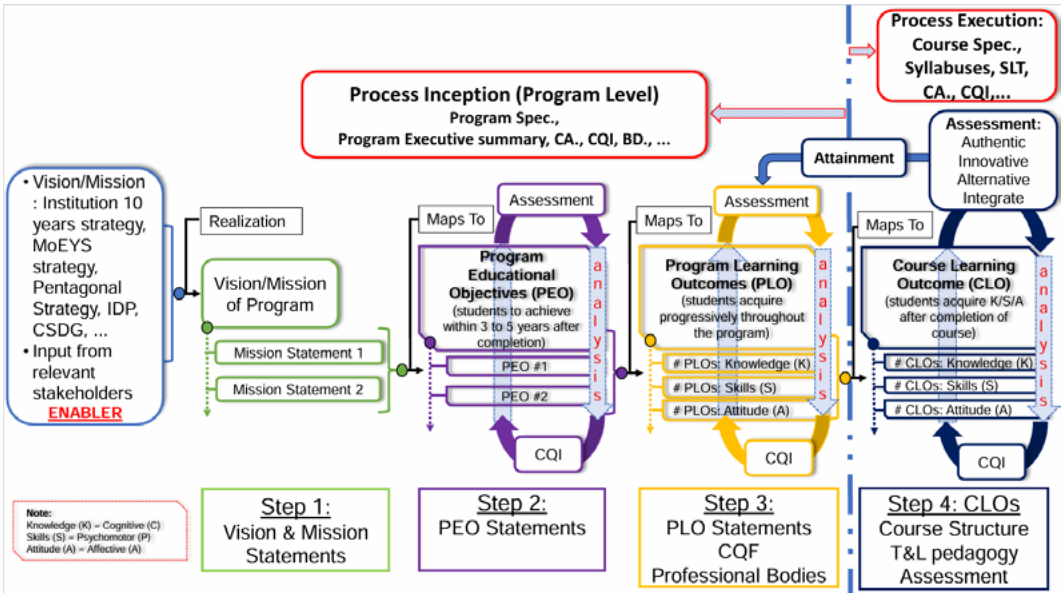


Figure 7. Inception Process for Curriculum Development

III. Current Practice of Law/Legal Education and Benchmarking

For analysis of the current implementation of the Bachelor of Laws program, we investigated three curricula from three different universities in Cambodia, namely "*University A, University B, and University C*". They are all a four-year (eight semesters) program. As illustrated in Table 1, University A provides courses that cover nearly 100% of the technical skills for law, with fewer courses on soft skills and no courses for research innovation/digitalization/AI skills. The same situation is found in courses at the university C. However, University B set up some interesting courses that can train students to achieve the expected graduates' attributes of the above framework. However, some aspects of AI technology, innovation, digitalization, and 21st-century skills are still left over. For regionally benchmarking, the author investigated the curriculum of the Bachelor of Laws in Thailand and Malaysia.

Table 1: Law Curriculum

Description	Cambodia			Benchmarking: Regional	
	University A	University B	University C	Bangkok University	University of Malaya
Duration	*4 years (8 semesters)*	*4 years (8 semesters)*	*4 years (8 semesters)*	*4 years (8 semesters)*	*4 years (8 semesters)*
Courses	**Year 1:** • Introduction to Law • Constitutional Law • College English • English Composition • Cambodian History • Cambodian Culture • Introduction to Statistics • Introduction to Political Science **Year 2: Major Core** • Civil Law • Labor Law • Contract Law • Family Law • Civil Procedure • Set of Elective courses (no courses on innovation, technology, AI skills)	**Year 1:** • English for Law • Intro. to Political Science • ICT Skills for Legal Studies • Environmental Science • Gender Studies • History of Cambodia and State Institutions • Basic Skills for Legal Studies • Academic Research • Intro. to Law • Cambodian Constitution **Year 2:** • Personal Growth and Development • Civil Law • Legal Research and Writing Skills I • Intro. to Economics and Entrepreneurship • Intro. to Political Economy • Criminal Law • Intro. to Public Policy and Administration • Civil Law II • ASEAN Governments, Politics and Economics • Business Law • Administrative Law	**Year 1:** • Introduction to Political Science • Legal Principles & Institutions • Introduction to Law • Khmer Culture & History • English for Law I • ASEAN Legal System • Environmental Law • Criminology • Administrative Law • English for Law II **Year 2:** • Constitutional Law • Criminal Law I • Civil Law • Commercial Law I • Legal Writing • Human Rights Law • Criminal Law II • Civil Law II • Commercial Law II • Alternative Dispute Resolution	• Everyday English • Social English • Global English • Thinking skills for lifelong learning • Citizenship in Society and International Community • Technology and Innovation for Future • Aesthetics and Well-being for Life • Entrepreneurial Spirit and Financial Literacy • Fundamental Legal Study Skills • Civil and Commercial Law • Juristic Acts and Contracts Law • General Principes of Public Law • Law of Obligations • Law of Tort, Management of Affairs without Mandate and Undue Enrichment • Law of Property and Land • Criminal Law • Fundamental English for Lawyers • Administrative Law • Law of Business • Law of Secured Transactions • Law of Insurance	• Legal Method • The Malaysian Legal System • Islamic Law • Tort • Law of Contract • English Language • Malaysian Constitutional Law • Criminal Law • Administrative Law • Land Law • Family Law • Equity and Trusts • Jurispridence • Company Law • Introduction to International Law • Set of elective courses

	Year 3: Major Core • Business Law • Criminal Law • Public International Law • Taxation Law • Criminal Procedure • International Institutions and Global Governance Set of Elective courses (no courses on innovation, technology, AI skills) **Year 4: Major Core** • Administrative Law • International Trade Law and Policy • Land Management and Urbanization Law • Human Rights Law • Legal Research and Writing • Set of Elective courses (no courses on innovation, technology, AI skills)	**Year 3: Major Core** • Intro. to International Law • Criminal Procedures • Alternative Dispute Resolution • Civil Law III • Labor Law • Court Advocacy Skills • IP Law • Fiscal Legislation and Taxation • International Human Rights Law • Civil Procedures • Legal Research and Writing Skills II • Set of Elective courses **Year 4: Major Core** • Civil Law IV • Client Counselling and Practice • Legal Ethics and Professional Responsibility • Clinical Legal Education • Information Technology and E-Commerce Law • Contract Writing and Practice • Law Seminar • Graduation Path	**Year 3:** • Advanced/Special Contract Law • Company & Bankruptcy Law • Criminal Procedure • Civil Procedure • Land Law • Private International Law • Trial Advocacy Skills • Family Law and Succession • Commercial Transactions • Critical Legal Thinking and Writing **Year 4:** • Labor Law • Banking Law & Securities Market • Public Finance • Public International Law • Legal Research Methods • Comparative Constitutional Law • Comparative Administrative Law & Procedure • Comparative Criminal Law & Procedure • Comparative Civil Law & Procedure • Public Policy Analysis	• Law of Negotiable Instruments • Law of Business Organizations and Mergers and Acquisitions • Law of Family • Court Systems and Principles of Procedural Law • Law of Civil Procedure • Constitutional Law and Political Institutions • IP Law • Law of Succession • Law of Criminal Procedures • Law of Evidence • English for Legal Works • Law of Bankruptcy and Insolvency • Private International Law • Public International Law • Labor Law • Legal Profession • Tax Law • Legal Philosophy	

Digitalization	Fewer courses on digitalization • Fundamentals of Computing and Information	• Information Technology and E-Commerce Law • ICT Skills for Legal Studies	No course on digitalization	From 2025, the new courses are: • AI and Robotic Laws • Laws and Regulations for Influencers • FinTech Laws • Data Protection and Cybersecurity Laws • Digital Marketing Laws and Regulations • Creators Assistance Clinic • Information Technology Law • Digital Asset Law • Energy Law • Industrial Law • Other research and innovation subjects on legal	Fewer courses on digitalization
AI Tech and Innovation	No courses dedicated to AI tech and Innovation	No courses dedicated to AI tech and Innovation	No courses dedicated to AI tech and Innovation		No courses dedicated to AI tech and Innovation

Based on the observation, the Bachelor of Laws at Bangkok University is structured with interesting courses that align well with our framework. From the provided courses, their program responded to all the required graduates' attributes, including equipping law professionals with technology, innovation, and AI. A list of these courses should be considered to include for curriculum modernization:

- Artificial Intelligence and Robotic Laws;
- Laws and Regulations for Influencers;
- FinTech Laws;
- Data Protection and Cybersecurity Laws;
- Digital Marketing Laws and Regulations;
- Creators Assistance Clinic;
- Information Technology Law;
- Digital Asset Law;
- Energy Law;
- Industrial Law;
- Other research and innovation subjects on legal.

IV. Law/Legal Education in Cambodia Aligns with Higher Education Framework and Technology/Digital Integration

Propose Law/Legal Curriculum Aligning to the Framework

As elaborated in sections 2 and 3, achieving graduate attributes is defined as the educational goal of the study curriculum. To reach that target, the program developer team should establish vision and mission statements, three to five PEOs statements, a minimum of ten PLOs-CQF statements, and a set of courses for students to conduct their studies.

In the context of innovative technologies in law/legal education, the proposed vision and mission statements are:

- "*The vision is to become a prominent Law/Legal Education Program that produces graduates with 21st-century skills, technology integration, and innovation who will contribute to the vision of the country in legal and emerging globalization."*
- *"Mission #1: Produce graduates with high skills (both technical skills and soft skills) for innovative technology in law for the country's vision 2030/2050, as well as for the emergence of globalization in the related field.*
- *Mission #2: Produce graduates who are lifelong learners and entrepreneurs through research and internship projects."*

The proposed PEOs' statements for laws and technology programs are:

- *"Statement #1:* To produce graduates with strong foundational knowledge in legal principles, uphold ethical standards, and effectively navigate the evolving demands of the legal profession in both traditional and digital environments.
- *Statement #2:* To produce graduates who will be equipped to leverage digital tools, legal technologies, and artificial intelligence to enhance legal research, litigation, compliance, and decision-making in diverse legal contexts.
- *Statement #3:* To produce graduates who will engage in continuous learning and innovative thinking by integrating law with emerging technologies such as AI, blockchain, data privacy, and cybersecurity to solve complex legal challenges.
- *Statement #4:* To produce graduates who will develop a global outlook on legal systems and demonstrate responsible digital citizenship, contributing to policy development and legal reforms in a digitally interconnected world.
- *Statement #5*: To produce graduates who will take initiative in legal entrepreneurship, public policy, and legal innovation, using technology to expand access to justice and create scalable legal solutions with social impact."

The expressions below are the proposed PLOs' statements for the laws and technology program. After completion of the program, students are able to:

- *"Statement #1:* Efficiently use digital legal databases, AI-powered tools, and online platforms to conduct advanced legal research and case analysis.
- *Statement #2:* Analyze complex legal and technological issues using logical reasoning, creative thinking, and informed judgment in real-world contexts.
- *Statement #3:* Effectively communicate legal arguments and opinions through written, oral, and digital formats, including presentations, virtual moot courts, and AI-assisted legal drafting.
- *Statement #4:* Demonstrate a comprehensive understanding of legal doctrines, statutes, and judicial decisions across various fields of law.
- *Statement #5:* Apply legal technology tools (e.g., e-discovery, contract automation, and case management software) to streamline legal tasks and improve efficiency.
- *Statement #6:* Evaluate the ethical implications of legal practice in digital and AI-driven environments, upholding professional integrity and client confidentiality.

- *Statement #7:* Collaborate across disciplines (e.g., law, computer science, data privacy) to address emerging legal challenges in technology-driven sectors.
- *Statement #8:* Demonstrate a commitment to continuous learning and adaptability, keeping pace with legal developments, tech innovations, and policy reforms.
- *Statement #9:* Analyze legal issues in global, digital, and socio-political contexts and contribute to technology-driven legal solutions that promote access to justice and societal well-being."

Then, as presented in Figure 8, a group of courses is recommended for building a complete and well-structured law/legal program with innovation and technology integrations. The mapping from one layer to another is necessary for ensuring the correctness and effectiveness of curriculum implementation.[10]

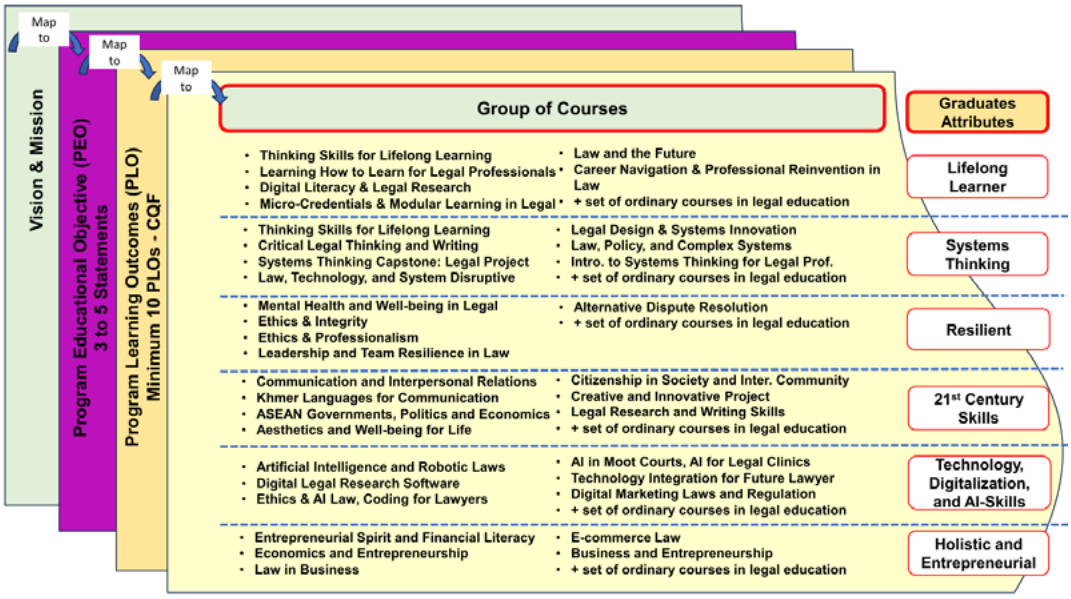


Figure 8. Propose Courses for Law Education

Applying Active Learning Systems with Technology

Active learning combined with supporting technologies and digital tools can transform how law is taught, shifting from passive lectures to hands-on, tech-enabled experiences that develop real-world skills:[11]

10 Mm Mahbubul, S. et al., "Outcome-Based Education (OBE): Defining the process and practice for Engineering Education," In IEEE Open Access, vol. 10, 2022, pp. 119170-119192. https://doi.org/10.1109/ACCESS.2022.3219477.

11 W. Hashim Abdulalsalam, Z. H. Majeed, H. TH.Salim Alrikabi. "Utilizing Machine Learning Techniques to Predict University Students' Digital Competence." In iJEP, vol. 15, No.3, 2025, pp. 75-91. https://doi.org/10.3991/ijep.v15i3.54943.

- *Flipped Classroom:* The instructor provides the learning material for students to learn theory at home (via videos/readings) and do problem-solving, debates, or drafting in class. Learning management systems (LMS: Moodle, Canvas, etc.) with digital tools (Kahoot, Edpuzzle, Padlet, etc.) should be used to support teaching and learning activities where teachers and students can interact effectively to enhance the learning outcomes.
- *Project-Based Learning/ Design Thinking Project:* Students co-create legal tech solutions or policy interventions to solve legal access or compliance issues. Some real projects from private stakeholders should be considered for engaging learners in the loop of real experiential learning. Some digital platforms, such as Trello, Mindmap, and Canva, are useful for collaborative learning in the case of a joint project among students.
- *Technology Enhancement Active Learning*: Technology such as Augmented Reality (AR), Virtual Reality (VR), and Streaming Services can be used to enhance students' learning experiences to achieve maximum learning outcomes.[12]
- *Gamified Legal Learning*: Use of quizzes, puzzles, and games to reinforce legal reasoning and memorization.
- *Reflective Practice & Self-Assessment*: Students reflect on their learning through journals, blogs, or vlogs.

Some other active learning systems can be implemented and found in recent articles or journal publications.

V. Conclusion

This article indicates a comprehensive and concrete academic framework that produces graduates with 21st-century skills, lifelong learning skills, resilience, entrepreneurship mindset, systems thinking, technology, digitalization, and AI skills. The complete set of curriculum design for a legal education is demonstrated by providing the leading statements from vision/mission to PLOs, and followed by some recommended group courses for each graduate's attribute in the national framework. All statements (vision/mission, PEOs, PLOs), expectations from the program to produce quality graduates, are elaborated within the context of modern technology, digitalization, and AI skills that drive the proposal of some new courses for program developers to consider adding in their future curriculum modernization. To conclude the study, some active learning systems (innovative and effective pedagogy approach) together with digital platforms are highlighted for ensuring the effectiveness of course delivery. For future work, we will study on how to develop a digital assessment platform for each course in the curriculum and issue the outcome-based education certification under the format of a spiderweb.

12 E. Pineda-Torres, W. Rodriguez-Lopez, O. Iparraguirre-Villanueva. "Role of Augmented Reality, Virtual Reality, and Streaming Services in the Field of Education (2020-2023) – A Systematic Review." In iJEP, vol. 15, No.3, 2025, pp. 134-151. https://doi.org/10.3991/ijep.v15i3.51595.

ABOUT THE AUTHOR

Sok Chea Am

Department of Electrical and Energy Engineering, Institute of Technology of Cambodia, P.O. Box 86, Rus-4 sian Conf. Blvd., Phnom Penh, Cambodia

Sok Chea was born in Kompong Cham, Cambodia, in 1988. He received his Eng. degree in Electrical and Energy Engineering from the Institute of Technology of Cambodia (ITC), Cambodia, in 2012. Then, he received a Master's degree in electrical and energy engineering from "Institut National Polytechnique de Grenoble (INP-G)", France, in 2013, and his Ph.D. degree in Power Electronics from University of Grenoble Alpes (UGA), G2ELab Laboratory, Grenoble, France, in 2016. In 2021, Sok Chea was awarded a Fulbright Visiting Scholar to research at the Colorado School of Mines (CSM), USA.

ONE SIZE DOES NOT FIT ALL: A LEGAL FRAMEWORK FOR DATA CLASSIFICATION IN CAMBODIA'S OPEN DATA GOVERNANCE

Sereivathna Bunny **Sreykun Bunthoeun**

I. Introduction

Cambodia's Digital Government Policy 2022-2035 outlines an ambitious vision for a digital future, one where data is leveraged as a strategic asset to fuel innovation, drive economic growth, and deliver improved public services.[1] However, while data itself consists of raw facts, the context and content of that data create vastly different implications.[2] Data containing a citizen's private health information, for example, carries inherent risks that aggregated economic statistics do not.[3] The way this data is handled and processed is therefore critical. This creates a challenge for policymakers: "*how to unlock the immense value of data while simultaneously protecting citizens from potential harm.*"[4]

To examine this challenge, a legal mechanism is needed to apply different rules based on the level of risk associated with the data.[5] This mechanism is "*data classification*", a process of categorizing data to assign specific, legally enforceable rules for its protection, handling, and use.[6] Currently, Cambodia's legal framework lacks such a formal data classification system. This absence creates a critical policy gap.[7] In this context, the recent introduction of the Draft Law on Personal Data Protection (LPDP) showcases the possibilities that government agencies and private companies may face legal liability for issues in relation to privacy breaches.[8] And without clear rules to distinguish which data can be shared and which must be protected, these organizations will likely default to over-restricting all data. This will lead to a policy gridlock, stifling the very innovation that the Digital Government Policy aims to foster. This article situates Cambodia as a central case study to argue that integrating a formal data classification framework into the nation's legal architecture is the essential step to resolve this gridlock. By analyzing Cambodia's emerging legal frameworks and drawing lessons from established international standards. This article provides recommendations for the forthcoming Data Governance Framework.

Why Data Classification is Important for Cambodia's Innovation

While progress has been made toward the LPDP and other digital transformation initiatives, there remains a systematic way to manage data across the public and private sectors. This deficiency hinders the effective use of data, which is the most essential ingredient, a fundamental point for innovation advancement. As of mid-2025, a comprehensive LPDP is in its draft stages, aiming to establish rules for the collection, use, and disclosure of personal data, drawing parallels

1 Royal Government of Cambodia, "Cambodia digital Government Policy 2022-2035.", https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf.
2 John MM Rumbold and Barbara K Pierscionek, "What are data? A categorization of the data sensitivity spectrum" *School of Science and Technology*, Nottingham Trent University, https://irep.ntu.ac.uk/id/eprint/32178/1/9685_Rumbold.pdf.
3 Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006), https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/.
4 Rumbold and Pierscionek, "What are data?"
5 OECD Legal Instruments, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" OECD, (2023), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
6 Rumbold and Pierscionek, "What are data?"
7 M. Janssen, Y. Charalabidis, and A. Zuiderwijk, "Benefits, Adoption Barriers and Myths of Open Data and Open Government," *Information Systems Management (ISM) 29*, no. 4 (2012), https://pad.undp.org.mx/files/g/820dcf0c1242364677545293.44594fd/banco/archivo/107/0/benefits-adoption-barriers-and-myths-of-open-data-and-open-government.pdf.
8 Open Development Cambodia, *Draft Law on Personal Data Protection* (final version June 23, 2025), https://data.opendevelopmentcambodia.net/en/dataset/792fc94d-1a84-49cc-bad3-9b420f99b70f/resource/03e9c060-9bc8-42d5-80a6-8db777f61d1c/download/20250623_final-draft-pdp-law_eng.pdf.

with the European Union's General Data Protection Regulation (GDPR).[9] However, the absence of a fully enacted and enforced data classification policy means that organizations often lack standardized guidelines for categorizing data based on its sensitivity, value, and regulatory requirements. This results in inconsistent data handling practices, making it challenging to implement appropriate security controls, manage access, and ensure compliance. Furthermore, limited digital literacy and a fragmented regulatory environment pose significant barriers to equitable digital transformation.[10]

The importance of robust data classification for fostering innovation cannot be overstated. Firstly, it enables effective data governance and security. Without clear classification, identifying and protecting sensitive information becomes a daunting task. For instance, without proper categorization of Personal Identifiable Information (PII) or proprietary business data, organizations cannot apply encryption, access controls, or data loss prevention measures effectively. This exposes data to higher risks of breaches and misuse, eroding trust, which are critical components for any digital innovation that relies on user data. A case in point is the risk of inaccurate or unclassified data leading to significant financial losses and reputational damage for businesses, as demonstrated by global incidents where "*bad data*" resulted in substantial revenue loss and operational disruptions.[11] In Cambodia, where digital trust is still building, data breaches stemming from poor classification could severely impede the adoption of new digital services and technologies.

Secondly, data classification streamlines data accessibility and utility for analytical purposes. Innovation often stems from the ability to analyze vast datasets to identify patterns, gain insights, and develop new products or services. When data is unclassified or poorly organized, it becomes a chaotic "*data swamp*" rather than a valuable "*data lake*." This makes it difficult for developers, researchers, and entrepreneurs to locate, access, and integrate relevant information. For example, a Cambodian Fintech startup aiming to develop personalized financial products would struggle to leverage disparate customer data if it lacks consistent categorization, making it impossible to identify key demographics, spending habits, or risk profiles efficiently. This significantly slows down the innovation cycle, as valuable time is spent on data cleansing and organization rather than on developing solutions.[12]

Thirdly, it ensures regulatory compliance and facilitates cross-border data flows. As Cambodia integrates further into the global digital economy, adherence to international data protection standards becomes increasingly important. While the LPDP is a step in the right direction, effective data classification is the operational backbone for meeting such requirements. Without it, organizations face increased risks of non-compliance, leading to potential penalties and restrictions on international collaboration. For innovative Cambodian businesses seeking

9 Hogan Lovells, "Cambodia moves to enact comprehensive data privacy law," Hogan Lovells, last modified July 28, 2025, https://www.hoganlovells.com/en/publications/cambodia-moves-to-enact-comprehensive-data-privacy-law.

10 ResearchGate, "Digital Government in Cambodia: Challenges and Solutions," ResearchGate, last modified February 16, 2024, https://www.researchgate.net/publication/376686542_Digital_Government_in_Cambodia_Challenges_and_Solutions.

11 DATAVERSITY, "Understanding the Impact of Bad Data," DATAVERSITY, last modified January 19, 2024, https://www.dataversity.net/putting-a-number-on-bad-data/.

12 UNCTAD, "Data for development," United Nations Conference on Trade and Development, last modified March 27, 2024, https://unctad.org/system/files/official-document/ecn162024d2_en.pdf.

to expand regionally or globally, the inability to demonstrate clear data classification and protection protocols can become a significant barrier to partnerships and market entry, thus stifling growth and innovation that could benefit from international data sharing for research and development.[13]

Identifiability, Sensitivity, and Access

A. Identifiability

Identifiability is defined as a piece of information that can identify a person both directly and indirectly. Although identifiability is a continuous process, law is binary. Information is either identifiable or non-identifiable. The question under this point is: *Can this piece of data be used to identify a specific living person?* If the answer is *yes*, the data is classified as personal data, and it immediately falls under the protection of privacy laws.[14] Once data is determined to be personal, the next analytical step is to assess its sensitivity. The law recognizes that some personal information, if exposed, could cause more harm than other types.[15] Information about a person's health, genetics, political opinions, or religious beliefs is inherently more sensitive than their name or contact information.[16] This is because its misuse could lead to discrimination, social stigma, or other severe infringements on an individual's rights and freedoms.[17]

There are two broad categories of non-identification: *pseudonymization* and *anonymisation*. Pseudonymization will minimize the risk of identification through removing and altering direct identifiers (e.g, name or address) and other unique characteristics while still allowing for re-identification under certain circumstances. Pseudonymization is not a method of anonymisation. It merely reduces the likelihood of a dataset with the original identity of the data subject. It is the additional technique required to obscure, remove, aggregate, and protect data that is no longer about an identifiable individual. There is no correct way to do pseudonymization. It depends on risk assessment to ensure that data is being protected and that the information is still useful for the intended purpose.

On the other hand, anonymisation is the process of ensuring that no data can be tracked back to an individual, even by a data holder or a third party. There are two approaches to do this. First is removing PII. All direct identification should be either removed or limited to the remaining information as far as practical. Those data contain PII such as name, IP address, social security number, phone number, financial information, medical records, and biometric data.[18] Second is modifying PII. Instead of complete removal, it is possible to manipulate the dataset in a way that makes it impossible to track a particular subject with certainty. The techniques include data masking (*Ex, replacing names with alien characters*) and generalisation (*Ex, expanding the specific*

13 APCICT, "Cambodia National Training on Data Governance for Digital Transformation," Asian and Pacific Training Centre for ICT for Development, last modified January 28, 2025, https://www.unapcict.org/sites/default/files/202501/Cambodia%20DDG%20and%20OD%20concept%20note%20v28Jan2025.pdf.

14 European Commission. 2023. "Data Protection Explained." European Commission. 2023. https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

15 "Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models." 2024. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

16 Ibid.

17 Ibid.

18 GeeksforGeeks. 2024. "Data Anonymization Definition, Meaning, Techniques." GeeksforGeeks. March 25, 2024. https://www.geeksforgeeks.org/data-analysis/what-is-data-anonymization/.

into a category by age group or postal code). Anonymisation allows organisations to utilize valuable data for analytics, research, and other purposes without compromising individual rights. It also facilitates data sharing in terms of collaboration, giving more room for creativity and less privacy invasion. In addition to that, managing and storing anonymous data costs relatively less than raw data. Raw data would require higher safeguards for its high risk, which is not favorable for the organisation.[19] Data that is truly anonymous, with no reasonable possibility of re-identifying an individual, can be classified for broader use, forming the foundation of Open Data initiatives.[20] For example, aggregated statistics about nationwide crop yields are not identifiable.

In contrast, a list of farmers in a specific village, even without names, could become identifiable when combined with other information. The process of making data genuinely non-identifiable is deceptively complex. As legal scholar Paul Ohm has argued, the belief that we can easily anonymize data is a "*broken promise*".[21] Studies have repeatedly shown that re-identification is a very real and persistent risk. Adversaries can take a dataset that has been scrubbed of obvious identifiers like names and ID numbers and cross-reference it with publicly available information. Such as movie ratings, voter lists, or social media profiles, to re-identify individuals with alarming accuracy.[22] This technical reality demonstrates that meeting the legal standard where re-identification is "*reasonably impossible*" is an extremely high bar.[23] It also counters that data, regardless of whether *pseudonymised* or *anonymised*, should be treated as personal data because of the possibility of re-identification.[24] A legal framework for data governance must acknowledge these technical challenges and incorporate robust safeguards, recognising that any data that is useful for analysis likely retains some risk of being traced back to an individual.

B. Sensitivity

At its core, it defines who can access it, how it's protected through its lifecycle, and how data is classified.[25] Data with low identifiability and low sensitivity, like general demographic trends, can be classified for public access. Data that is identifiable but not highly sensitive, such as an internal employee directory, would be classified for confidential or restricted access, available only to authorized users within an organization. Data that is both highly identifiable and highly sensitive. For instance, HIV patient's status must be assigned with the strictest accessibility level, often accessible to the data subject, and limited numbers of professionals with a direct and lawful duty of care.[26] The assessment of how sensitivity could be based on two factors: (i) the risk of re-identification from anonymised data (plus the sensitivity of the underlying data), and (ii) the sensitivity related to opinions, beliefs, or sexual orientation.[27]

19 Ibid.
20 Gadotti, A., Rocher, L., Houssiau, F., Creţu, A., & De Montjoye, Y. (2024). Anonymization: The imperfect science of using data while preserving privacy. *Science Advances*, *10*(29). https://doi.org/10.1126/sciadv.adn7053.
21 Ohm, P. (2010). "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review.*
22 Ibid.
23 Ibid.
24 Rumbold, John M.M., and Barbara K. Pierscionek. 2018. "What Are Data? A Categorization of the Data Sensitivity Spectrum." Big Data Research 12 (July): 49–59. https://doi.org/10.1016/j.bdr.2017.11.001.
25 "How Does Data Governance Manage Sensitive Data?" 2025. Milvus.io. 2025. https://milvus.io/ai-quick-reference/how-does-data-governance-manage-sensitive-data.
26 Ibid.
27 Ibid, 21.

Appendix

Data Type	Potential Sensitivities & Inferences	Example in the Cambodian Context
Purchasing Habits	Can reveal health conditions, financial status, lifestyle choices, and location patterns. Data-driven inferences can expose highly personal information.	A history of payments at a specific pharmacy could suggest a chronic illness.
IP Address	It has the potential to identify where you live.	
Occupation	It can be sensitive depending on national security implications, social stigma, or an individual's desire for privacy. It is a strong indicator of social and economic class.	An individual working for a politically sensitive Non-Governmental Organization (NGO) may not want their occupation publicly known. This information could be used to infer their political leanings or social standing.
Opinions	Expressed views, especially on political or social issues, can be highly sensitive. They may be deemed inappropriate or incompatible with an individual's professional role.	A government official expressing strong, critical political views on Facebook could face professional repercussions.
Age	It can be sensitive as it determines eligibility or ineligibility for certain rights, services, or obligations. This can lead to discrimination or unwanted inclusion/exclusion.	Age to serve in the military, to retire, or receive a pension.
Pregnancy	This is a sensitive health datum that can lead to significant discrimination, particularly in employment (e.g., being passed over for a job or promotion). It can also reveal information about personal relationships that may be socially disapproved of.	An employer might illegally discriminate against a pregnant woman, assuming she will be less committed to her job.

C. Access Rights

This final pillar of classification determines who can lawfully view, use, or share a piece of data, translating risk assessment into operational rules.[28] These rules are grounded in distinct legal principles, such as the right to public transparency and the fundamental right to individual privacy.[29] Classifying data based on identifiability and sensitivity logically determines the final pillar: *defining who has the legal right to access it*.

28 International Commisioner's Office. "What Is the Right of Access?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-is-the-right-of-access/.

29 Ibid.

The default assumption for government-held information, also known as Public data, is generally assumed to be accessible to everyone.[30] This legal notion encourages citizens to hold the government accountable and also drives innovation.[31] On the other hand, in the context of personal privacy, the legal standing is that the data subject is the only one who can access their data.[32] Any other access to an individual's information, a company, or the government may have to a person's data must be justified by a specific and legal basis, such as the person's express consent, a contract requirement, or a court order.[33] Moreover, just because the company has access to data, it does not mean they can freely use and share data.[34]

In the current Cambodian context, the Draft Law on Digital Government (LDG) serves as a legal foundation for the idea of transparency, which empowers citizens and fosters innovation. Its establishment of an "*Open Data*" category offers the legal foundation for granting the public access to information held by the government.[35] This not only makes accountability possible, but it also gives scholars and companies the starting point for developing new services that will benefit society and the economy. Second, the LPDP upholds the fundamental right to privacy.[36] Assuming that people have an inherent right to control their information, this law makes the "*data subject*" the primary owner of rights.[37] The LPDP establishes the legal foundation for the most limited degree of access, particularly with regard to "*sensitive personal data*," where any other party's access necessitates a specific and legitimate reason, like express consent.[38]

II. Current Developments in Cambodia's Legal Framework for Open Data Governance and Data Classification

The Open Data scene in Cambodia is still in its infancy.[39] It is not specifically governed by any rules or regulations, and the commercial sector is not legally required to make data available to the public. However, recent legislative developments show that Cambodia is taking foundational steps to build its data governance framework.[40] The Cambodia National AI Strategy has firmly stipulated data as fundamental for the country's digital development.[41] The Strategy defined data as the "*food for AI*," essential for innovation and advancement of new technologies.[42] It calls on all institutions

30 Saxena, S., & Muhammad, I. (2018). The impact of open government data on accountability and transparency. *Journal of Economic and Administrative Sciences.*, *34*(3), 204–216. https://doi.org/10.1108/jeas-05-2017-0044
31 Ibid.
32 Helena U. Vrabec, *Data Subject Rights under the GDPR: With a Commentary Through the Lens of the Data-driven Economy*, Oxford University Press, 2021.
33 Ibid.
34 Senigaglia, Roberto, Claudia Irti, and Alessandro Bernes, eds. *Privacy and Data Protection in Software Services*. Singapore: Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-16-3049-1.
35 "Draft Law on Digital Government of the Kingdom of Cambodia", OD Mekong Datahub, 2025, https://data.opendevelopmentcambodia.net/laws_record/draft-law-on-digital-government-of-the-kingdom-of-cambodia.
36 "Draft Law on Personal Data Protection", Open Development Cambodia.
37 Ibid.
38 Ibid.
39 Sokhna Vor, "*How Data-Driven Technology Can Upgrade Cambodia's E-government",* Konrad Adenauer Stiftung, Cambodia, (2020), https://www.kas.de/documents/264850/7993338/Chapter+9.pdf/39084bee-3b38-3973-dcf6-e91c539a048b?version=1.0&t=1579758149758.
40 Ibid.
41 "Draft National Artificial Intelligence Strategy 2025-2030 (Version 5)", OD Mekong Datahub, 2025, https://data.opendevelopmentcambodia.net/en/library_record/draft-national-artificial-intelligence-strategy-2025-2030-version-5.
42 Ibid.

to "*properly and securely collect and store data*" and to consider "*releasing the data openly or sharing some of it*".[43] This high-level commitment to creating a data-rich environment for innovation is the primary driver behind the country's recent legal developments in data governance.

Furthermore, the LDG provides a clear blueprint for how Open Data will actively enable innovation. Article 27 mandates that Application Programming Interfaces used for Open Data must be properly documented, promote interoperability, and explicitly "*encourage and enable innovation*."[44] This provision, combined with the law's stated preference for "*open source software*," shows that the government's goal is not merely to release data, but to create a functional, developer-friendly ecosystem.[45] Nevertheless, to achieve the above goals, it requires a regulatory environment that encourages participation.[46]

The lack of a formal structure for data classification and sharing makes it difficult to access the very data that would otherwise support research and development, hindering evidence-based policymaking and limiting local innovation.[47]

For the first time, the LDG creates a legal mandate for data classification. It states that government data shall be classified as "*top secret data, confidential data, and Open Data*".[48] At the same time, the LPDP provides the necessary substance by defining key risk-based categories, such as personal data and sensitive data, which require the highest levels of protection.[49] The LPDP does not explicitly provide for data classification mechanisms; however, the concept of data sensitivity is implicitly present in the broad definition of personal data, which includes elements related to physical, physiological, genetic, mental, economic, cultural, or social identity.[50] Furthermore, the LPDP provides that personal data should be further pseudonymized as another protective measure for data storage.[51]

There is still a significant disparity between the proposed laws and policies that have been discussed. Although the National AI Strategy presents an Open Data classification, for this idea to be secure and effective, it requires a broader context. A review of the sensitivity and personal nature of the information must be conducted before determining whether it can be shared publicly, with clear guidance from the principles of the LPDP. However, this measure does not establish a precise definition, despite the LPDP suggesting a risk-based approach to handling personal data. There is a lack of clarity regarding legal compliance. The possibility of an unintentional violation could discourage both public and private entities from revealing non-essential information once the LPDP goes into effect. Such reluctance would stifle Cambodia's goals for Open Data, limiting access to the resources needed for research and development.

This situation calls for regulatory clarification. By establishing a harmonized classification framework, Cambodia can ensure that data released to the public has been properly assessed

43 Ibid.
44 "Draft Law on Digital Government of the Kingdom of Cambodia", OD Mekong Datahub.
45 Ibid.
46 "Cambodia 2040 Economic Development." 2020. Konrad Adenauer Stiftung, Cambodia. June 9, 2020, https://www.kas.de/en/web/kambodscha/ausgaben/detail/-/content/cambodia-2040-economic-development.
47 OECD, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers, No. 222, OECD Publishing, Paris. (2013-06-18), http://dx.doi.org/10.1787/5k47zw3fcp43-en.
48 "Draft Law on Digital Government of the Kingdom of Cambodia", OD Mekong Datahub.
49 "Draft Law on Personal Data Protection", Open Development Cambodia.
50 Ibid.
51 Ibid.

for privacy risks, making the Open Data system safe for citizens and providing the clarity needed to foster innovation. Therefore, developing a robust and effective data classification procedure is an essential step in the development of Cambodian policy.

III. Comparative Analysis

European Union's General Data Protection Regulation

Cambodia's rapid digital transformation, aimed at fostering economic growth and societal development, inherently relies on effective data governance. In this context, the GDPR serves as a highly relevant benchmark for assessing and improving data classification practices in Cambodia. The primary reason for this suitability lies in the architectural similarities between Cambodia's nascent legal framework, particularly its LPDP, and the GDPR.[52] The LPDP, currently in its draft stages, borrows extensively from GDPR's principles, including definitions of personal and sensitive data, data subject rights (e.g., right to information, access, rectification, erasure, data portability), and obligations for data controllers and processors.[53] This alignment signifies Cambodia's intention to adopt international best practices, making a comparative analysis with GDPR not just academic, but pragmatic for policy development and implementation.

First, it is to assign clear roles and responsibilities. At its core, the essential way to effective data governance is to define a clear role and responsibility for how an organization manages personal data. While the LPDP is expected to mandate a Data Protection Officer (DPO), an independent and empowered supervisory authority is crucial for effective oversight, enforcement, and providing clear guidance.[54] The current LPDP leaves too much to delegated regulations ("*prakas*"), and potentially limiting its scope to only the private sector might hinder comprehensive public sector oversight.[55] It requires the appointment of a DPO under specific circumstances, particularly for public authorities or organizations involved in large-scale processing of sensitive data or regular and systematic monitoring of data subjects.[56] An independent and empowered supervisory authority is also crucial for effective oversight, enforcement, and providing clear guidance. While Cambodia's LPDP is expected to mandate a DPO, the current draft potentially leaves too much to delegated regulations ("*prakas*"), and possibly limiting its scope to only the private sector might hinder comprehensive public sector oversight.[57] This gap in unified guidance could lead to inconsistent application across different government entities. Nonetheless, the cost of a dedicated DPO can be substantial for Small and Medium-sized Enterprises (SMEs). Therefore, a nuanced assessment is needed to determine the scale of business and specific sectors that would necessitate a full-time DPO, perhaps allowing for external DPO services or a more flexible approach for smaller entities, similar to how some GDPR member states offer guidance or exemptions for micro-enterprises.

52 Ibid, 9.
53 PPC Land, "Cambodia announces comprehensive data protection law," PPC Land, last modified July 23, 2025, https://ppc.land/cambodia-announces-comprehensive-data-protection-law/.
54 DataGuidance, "*GDPR v. LGPD*," DataGuidance, accessed August 18, 2025, https://www.dataguidance.com/sites/default/files/gdpr_v_lgpd_revised_edition.pdf.
55 Graham Greenleaf, "Cambodia's draft data privacy law: Too much is left to delegated prakas," Privacy Laws & Business International Report, February 2025, https://www.privacylaws.com/reports-gateway/articles/int193/int193cambodia/.
56 Spirion, "Data Classification (Data Management): A Complete Overview," Spirion, accessed August 18, 2025, https://www.spirion.com/data-classification.
57 Graham Greenleaf, "Cambodia's draft data privacy law: Too much is left to delegated prakas," Privacy Laws & Business International Report, February 2025, https://www.privacylaws.com/reports-gateway/articles/int193/int193cambodia/.

Second, organizations should enforce data minimization strictly through conducting a detailed and annual data audit. This aligns with GDPR's principle of "*data minimization*," which stipulates that personal data should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.[58] A thorough data audit helps an organization understand precisely what data it holds, where it is stored across its systems, its category of risk, and how it is classified. It helps to ensure you know what data you hold, where it is stored, what category of risk it is, and how it is classified.[59] For instance, sensitive data such as health information or other PII information shall require additional safeguards.[60] This practice allows organisations to enforce appropriate security measures while making sure they only process the data necessary for the intended purpose. It also makes organisations stay up to date with new technologies and business needs. Furthermore, this continuous review process ensures that data practices stay up-to-date with new technologies, evolving business needs, and changing regulatory landscapes, fostering an environment where innovation can thrive on reliable and well-managed data.

Third, Cambodia can further strengthen its data classification and governance by adopting a proactive approach to "*Privacy by Design*" and "*Data Protection by Default*," core tenets of GDPR. These principles dictate that data protection measures should be integrated into the design of new systems and services, rather than being an afterthought. This includes implementing privacy-enhancing technologies like pseudonymization and encryption from the outset and ensuring that the most privacy-friendly settings are the default. For instance, when developing new e-government portals or digital payment systems, data classification and protection controls should be foundational elements of the system architecture. This proactive stance significantly reduces the risk of data breaches and non-compliance, thereby building greater public trust for the widespread adoption of digital services and the success of a burgeoning digital economy.

A. Public Sector

Public sector in Cambodia faces unique challenges stemming from fragmented data silos, which lead to inconsistent data classification, duplication, and significant hurdles in cross-agency data sharing. Government ministries and departments often operate independently, using diverse systems that may not interoperate, resulting in a chaotic data landscape. This fragmentation makes it incredibly difficult to implement unified data classification standards and enforce consistent data handling practices across the entire government. To address these systemic issues, the Cambodian government must develop and enforce a unified National Data Classification Framework for all public authorities. This framework should clearly define data categories (e.g., Public, Internal, Sensitive, Restricted), assign explicit data ownership and stewardship roles within each government entity, and mandate specific security controls and data lifecycle management policies for each classification level.[61] This would standardize data handling across government, promoting interoperability and secure data sharing for improved public services. Finally, establishing a strong, independent supervisory authority with the

58 Akamai, "What Is Data Classification? | Akamai," Akamai, accessed August 18, 2025, https://www.akamai.com/glossary/what-is-data-classification.

59 Bradshaw, Aaron. 2024. "GDPR: Data Compliance Best Practices for 2025." Alation.com. 2024. https://www.alation.com/blog/gdpr-data-compliance-best-practices-2025/.

60 PPC Land, "Cambodia announces comprehensive data protection law," PPC Land, last modified July 23, 2025, https://ppc.land/cambodia-announces-comprehensive-data-protection-law/.

61 UK Parliament, "Sharing Public Sector Data," UK Parliament Postnote, last modified January 28, 2022, https://researchbriefings.files.parliament.uk/documents/POST-PN-0664/POST-PN-0664.pdf.

mandate and resources to oversee data governance across all public sector entities would be critical for ensuring accountability and consistent enforcement of data classification standards.

B. Private Sector

Cambodian private sector entities, particularly SMEs face unique challenges in adopting comprehensive data classification due to limited resources, expertise, and a lack of awareness regarding LPDP. While large corporations might have the means to implement sophisticated data governance frameworks, SMEs often struggle with the technical and financial burden. They may lack dedicated IT security teams or the budget for advanced data classification software. Furthermore, many businesses, especially those not engaged in international trade, might not fully grasp the long-term benefits of data classification beyond basic security, which can lead to inadequate protection of sensitive customer or proprietary data. To address these issues, the Cambodian government and relevant authorities should provide accessible guidelines and tools tailored for SMEs. This could include issuing practical checklists, template data classification policies, and educational materials that explain the importance of data classification in simple terms.[62] Additionally, incentivizing adoption through grants, tax breaks, or subsidized training programs could significantly encourage SMEs to invest in data governance.

C. Non-Governmental Organizations

NGOs in Cambodia often handle some of the most sensitive personal data collected from vulnerable populations in areas such as health, human rights, and social welfare. This includes "special categories of personal data" under GDPR, such as health status, racial or ethnic origin, or political opinions, which demand the highest level of protection.[63] Compounding this is the fact that many Cambodian NGOs receive funding from international donors, particularly from the European Union (EU), who impose its stringent data protection requirements. This creates a complex compliance landscape where NGOs must navigate both local regulations (once fully enacted) and international standards. Coupled with typically limited budgets, technical expertise, and potentially high staff turnover, establishing and maintaining robust data classification frameworks becomes a significant challenge for these organizations. Therefore, for NGOs, the core recommendation is to develop tailored data protection policies that clearly define data classification levels for the specific types of data they handle. This policy should emphasize the treatment of sensitive personal data, outlining strict access controls, encryption protocols, and data retention schedules. Given the nature of their work, NGOs must prioritize obtaining explicit, informed, and truly voluntary consent for data collection, clearly communicating data usage purposes in a culturally sensitive and understandable manner, as emphasized by GDPR's consent requirements.[64]

62 Proofpoint US, "What Is Data Classification? - Definition, Levels & Examples," Proofpoint US, accessed August 18, 2025, https://www.proofpoint.com/us/threat-reference/data-classification.

63 TechGDPR, "GDPR Compliance for NGOs and Social Enterprises," TechGDPR, accessed August 18, 2025, https://techgdpr.com/industries/gdpr-compliance-for-ngos-and-social-enterprises/.

64 EvalCommunity, "GDPR and International Development: Balancing Data Privacy with Development Goals," EvalCommunity, accessed August 18, 2025, https://www.evalcommunity.com/international-development/gdpr-and-international-development/.

Singapore Best Practice

As a leading digital economy within ASEAN, its approach is a particularly relevant benchmark. Singapore employs a dual-track system, offering a comprehensive yet adaptable blueprint for both the private and public sectors. The first track is the principles-based Personal Data Protection Act (PDPA), which provides the necessary legal flexibility for businesses to innovate. The second is its structured Government Data Architecture (GDA), which creates a strategic framework for public services. Additionally, the Singapore Data Management Guideline offers a 3-tier data classification system for non-governmental organisations. This combination presents a proven roadmap for balancing innovation with protection and offers critical, actionable insights for Cambodia.

A. Public Sector

The GDA of Singapore demonstrates how a nation can go from silos of data to secure, streamlined, and dynamic data collaboration.[65] As Cambodia attempts to realize its recent legal structures, the opportunity for such an architecture exists as a translatable guiding principle appropriate for any context. It is not a data-driven technical infrastructure but a socio-technical approach that answers the public sector triad of data problems: poorly constructed data quality, inter-agency distrust, and bureaucratic complication.[66]

The GDA is built on the three pillars of strategy. The first challenge the GDA solved was the quality of data. It focuses on time, energy, and resources to discover and maintain high-value "*Core Data.*"[67] By making one agency the Single Source of Truth (SSoT) for every essential data set, the government holds itself responsible for the quality, accuracy, and maintenance of data.[68] This ensures all ministries work from the same authoritative source, eliminating the inconsistencies that arose from decentralized systems. The second challenge the GDA solved was the trust issue. The second pillar is "*Trusted Centres*".[69] This is an infrastructure through which data is shared, meaning a secure, audited route.[70] Instead of attempting to share thousands of data sets with dozens of agencies and carrying the risk of untrustworthy, undocumented, ad-hoc arrangements, data flows through a central, trusted agent.[71] This fosters trust and encourages data sharing while diminishing the risks of privacy breaches and improper uses.[72] The third challenge the GDA solved was the Open Data initiative. With the GDA, there exists one portal through which eager public officials can have access to otherwise much-needed data. It is projected that without this single access point, public officials would waste invaluable time seeking multiple sources of Open Data across a million portals, transforming days' worth of information accumulation, weeks, into a matter of days.[73]

65 Chin Hui Han, "Using Data Securely." 2020. March 3, 2020 https://psdchallenge.psd.gov.sg/ideas/work-better/ask-a-pro-using-data-securely.
66 Ibid.
67 Koh Eng Chuan and Peng Yuxiang. "Data Governance and Data Integration in Singapore." *Statistics Singapore Newsletter*, no. 2 (2024), https://www.singstat.gov.sg/-/media/files/publications/reference/ssn224_pg27-29.ashx.
68 Ibid.
69 Ibid.
70 Ibid.
71 Ibid.
72 Ibid.
73 Singapore's Open Data Portal, https://data.gov.sg/.

With these three initiatives, Cambodia can realistically apply its newly drafted legislation on Data Governance. First, with the LDG provision that a Digital Government Committee will be formed. Such a committee should be statutorily required to lead an interministerial discussion to assess what are Cambodia's 3-5 most critical "*Core Datasets.*"[74] For each of these datasets, there must be one Ministry as the SSoT.[75] Secondly, to facilitate safe and secure access to the Core Datasets, pursuant to the LDG, Cambodia must create a National Data Exchange Centre, which will operate as a Trusted Intermediary. This body will be under the auspices of the Digital Government Committee, and its activities will be governed solely by the security provisions of the LDG, which means that any data exchanges will be safe and secure. Its operations would be strictly governed by the security requirements of the LDG, ensuring that all data transfers are secured. Third, to provide for the need of the LDG Article 27 and to foster creativity around APIs, Cambodia should create a Government Data Portal.[76] This is essentially the front-facing exposure to an Open Data initiative and should start as a Data Catalogue, essentially a simple repository that provides what data sets there are, and who owns them. This is an important first step to making any government data accessible and discoverable, the building blocks of research and innovation that support Cambodian national strategies.

B. Private Sector

Data protection laws are a major reason why organizations are driven to sort and organize their data.[77] For the private organizations in Singapore, the key legal instrument is the PDPA 2020.[78] Instead of mandating a specific 3-tier classification system, the PDPA takes a principles-based approach. It does not say data must be classified as Tier 1, 2, or 3.[79] Instead, the protection obligation is the legal basis. As stated in Section 24 of the PDPA, it imposes a legal obligation that requires companies to implement *reasonable security management* to protect personal data.[80] This is an implication of data classification. This act requires a company to conduct a risk assessment on the data it possesses, and based on that, it must implement appropriate security controls.[81] The Personal Data Protection Commission (PDPC) interpreted the term *reasonable* as security arrangements that must be "*commensurate with the sensitivity of the data in question*" and "*Therefore, a higher standard of protection is required for personal data that is more sensitive in nature, such as financial or medical information…*".[82] This set a legal mandate for companies to

74 "Draft Law on Digital Government of the Kingdom of Cambodia", OD Mekong Datahub.
75 Asian Development Bank and Amazon Web Services (AWS) Institute, *Data Management Policies and Practices in Government* (2022), https://d1.awsstatic.com/institute/ADB-AWSI-Data-management-policies-and-practices-in-government.pdf.
76 "Draft Law on Digital Government of the Kingdom of Cambodia", OD Mekong Datahub.
77 Dr. Fabian Ibel. "*Where law meets Innovation: Structuring Data for Compliance and AI*".
78 PDPC. "PDPA Overview." Www.pdpc.gov.sg. 2025. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.
79 Ibid.
80 Ibid.
81 Ibid.
82 Napier, Drew, Chong Lim, Kin, and Su-Anne Chen. n.d. "The Legal 500 Country Comparative Guides Singapore Data Protection & Cybersecurity Contributor Drew & Napier LLC." https://www.drewnapier.com/DrewNapier/media/DrewNapier/The-Legal-500-Comparative-Guides-Data-Protection-Cybersecurity-2024-Singapore-chapter.pdf.

identify and provide stronger protection for sensitive data and to classify data based on risk.[83] Moreover, the PDPC's "*Guide to Developing a Data Protection Management Program*" recommends that an organisation's data inventory should include information on "*the classification of the data to manage user access*".[84] This shows that classification is an officially recommended best practice by the regulators.

Similarly, Cambodia's LPDP requires data controllers to implement security measures based on the "*risks of personal data processing that may impact the rights and freedoms of a data subject*."[85] To fulfil this duty, companies must assess their data to understand those risks, which means they must classify it.[86] The LPDP defines sensitive personal data, which gives companies a clear starting point. Any data falling into these categories (health, race, political opinions, biometrics, etc.) must be treated as the highest risk category and requires the strongest security measures.[87] Furthermore, the draft requires companies to develop internal regulations on personal data protection.[88] This is where companies can establish their own internal data regulation policy in which they can adopt the 2-3 levels of data sensitivity (Public, Internal, Confidential/Sensitive).[89] Moreover, Cambodia should explicitly interpret the "*risks of personal data processing*" under Article 20 LPDP to mean that security measures must be commensurate with the sensitivity of the data.[90] This approach creates a clear requirement for all companies to conduct risk-based data classification. This provides the private sector with the flexibility to create its internal policies, as required by Article 39 LPDP, while ensuring a high standard of protection for sensitive information, thereby fostering the legal certainty needed for innovation.[91]

C. Non-Governmental Organization

As Cambodia's new data protection laws come into force, NGOs face a unique and critical challenge. They often handle some of the most sensitive information in the country, related to vulnerable populations, health, and human rights. For this sector, Singapore's Data Management Guidelines for the Social Service Sector offers a particularly relevant and practical blueprint for compliance and ethical data stewardship.

The Data Management Guideline adopts a risk-based approach to data classification for non-governmental organisations.[92] It uses a pragmatic, 3-tier classification system based on a single question: "*What is the impact if this data is leaked?* "[93]

83 Ibid.
84 PDPC, "Developing a Data Protection Management Programme.", Www.pdpc.gov.sg. 2023. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Protection-Management-Programme-(Aug-2023).pdf.
85 "Draft Law on Personal Data Protection", Open Development Cambodia.
86 Ibid.
87 Ibid.
88 Ibid.
89 Ibid.
90 Ibid.
91 Ibid.
92 Data Management Guide, National Council of Social Service, 2021. https://file.go.gov.sg/dmgss.pdf.
93 Ibid.

- **Internal Sensitive:** Data that would cause serious damage or sustained emotional injury to individuals.
- **Internal General:** Data that would cause short-term reputational embarrassment but not severe harm.
- **External:** Data that would cause little or no damage.

This risk-based approach directly aligns with the core requirements of Cambodia's LPDP. The "*Internal Sensitive*" category in the Singaporean guideline is a practical implementation of how to handle the "*Sensitive personal data*" defined in the LPDP.[94] Furthermore, the obligation to apply the "*most stringent level of access controls*" to this sensitive data is a direct answer to the LPDP's requirement in Article 20 to implement security measures based on the "*risks of personal data processing that may impact the rights and freedoms of a data subject*."[95]

In this regard, Cambodian NGOs must take the following proactive measures to prepare for the new legal landscape. Firstly, NGOs can develop an internal data policy based on the above model. This involves identifying all the data they hold and classifying it based on the potential harm a leak could cause to their beneficiaries. Data that falls under the LPDP's definition of "*Sensitive personal data*" must automatically be placed in the highest risk category.[96] Secondly, the risk assessment process will help NGOs adhere to the "*data minimization*" principle in Article 6 of the LPDP.[97] By understanding the sensitivity of the data they collect, NGOs can and should challenge themselves to collect only the absolute minimum information necessary to achieve their mission, thereby reducing their risk profile.

IV. Conclusion

In conclusion, the gap in data classification in Cambodia presents a multifaceted challenge to the nation's innovation agenda. By failing to systematically categorize and manage data, Cambodia risks compromising data security, impeding data-driven insights crucial for new product development, and hindering its ability to participate fully in the global digital economy. Addressing this gap requires a concerted effort to finalize and implement robust data protection laws, develop clear national data classification standards, and build capacity across both public and private sectors. Cambodia does not need to start from scratch when there are best practices to learn from GDPR and Singapore, the perfect balance of strict and business-friendly regulation. Only then can Cambodia truly unlock the transformative potential of its digital economy and foster an environment where innovation can flourish securely and responsibly.

94 "Draft Law on Personal Data Protection", Open Development Cambodia.
95 Ibid.
96 Ibid.
97 Ibid.

ABOUT THE AUTHORS

Sereivathna Bunny

Postgraduate Student at University of Glasgow specializing in Technology and Regulation Law

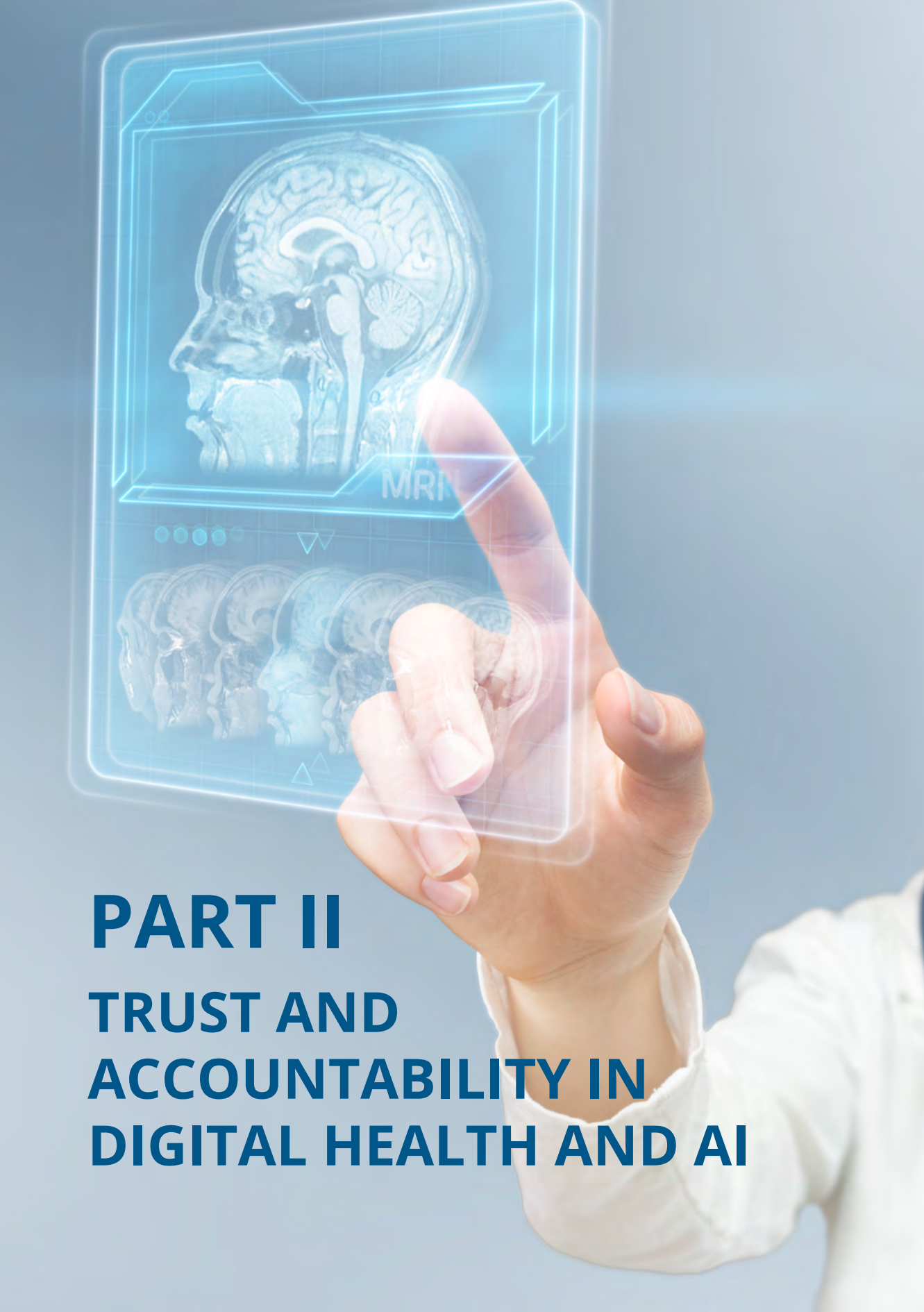
Sereivathna is the recipient of the Chevening Scholarship and an alumni of YSEALI Academics Fellowships. Previously, she served as the Program Manager for Rule of Law projects at the Konrad Adenauer Stiftung Cambodia. Her professional experience centers on the critical intersection of legal frameworks and its intersection with the emerging technologies. Sereivathna's current research focuses on areas including Data Privacy, the Future of FinTech, and the ethical governance of AI.

Sreykun Bunthoeun

LLM at the University of Göttingen specializing in Intellectual Property and Information Technology Law

Sreykun is a KAS EIZ scholar and was previously a Junior research associate at KAS Cambodia. She obtained her LLB from the English language-based Bachelor of Laws program from the Royal University of Law and Economics. She specialized in legal research and writing, partcularly in the field of Digital Law, Data Protection, and Human Rights.

This page is intentionally left blank.



PART II

TRUST AND ACCOUNTABILITY IN DIGITAL HEALTH AND AI

BUILDING TRUST IN AI: HOW STANDARDIZATION CAN SECURE THE FUTURE OF AI ADOPTION

Tom Lebrun

I. Introduction

The accelerating diffusion of artificial intelligence (AI) technologies across critical social functions (credit adjudication, medical diagnosis, logistics optimisation) has elevated "trust in AI" from a marketing slogan to a constitutional imperative. Yet the very attributes that render contemporary AI systems valuable (such as adaptive autonomy and seamless cross-border scalability) also strain the doctrinal apparatus of public law and the practical capacities of market surveillance. Laws struggle to keep pace with the rapid evolution of machine learning. Regulators lack the evidence needed for effective enforcement after the fact, and citizens are left facing decisions whose origins are uncertain. Against this backdrop, technical standardization has emerged as the favoured instrument for operationalising abstract legal principles into supposedly verifiable controls. International standards bodies such as ISO, IEC, and the ITU now frame their project lists around governance processes, risk-management protocols and documentation duties tailored expressly to AI life cycles. Parallel initiatives within the European Union, the United States, and multiple G-20 economies seek to incorporate those standards, either by reference or by functional equivalence, into binding legislative schemes. Thereby creating a multi-layered architecture in which private consensus instruments crystallise into public-law obligations.

This article interrogates the promise and peril of that architecture. Part I situates the rise of standards-based governance in the broader context of AI regulation, tracing the migration from prescriptive statutes to framework legislation that delegates technical detail to consensus bodies. Part II dissects the internal tensions that beset AI standards, namely the practical challenges of interpretability and interoperability when supposedly technical standards aim to safeguard fundamental rights. Part III shifts the lens from legal form to epistemic effect, examining how dominant language models standardise linguistic representations and thereby exercise *de facto* regulatory power over knowledge production. Part IV contends that the ultimate efficacy of standards will turn on a fundamentally diplomatic question: who sets the performance thresholds (metrics) that delimit acceptable residual risk, and in what forum are those thresholds negotiated?

The analysis shows that the line between informal industry rules and formal legal accountability is becoming less clear, suggesting that technical standardization should be seen not only as an engineering process but also as a field of geopolitical competition. By mapping these dynamics, the article seeks to furnish policymakers, standards developers, and legal scholars with an integrated framework for assessing when, and under what institutional safeguards, technical standards can secure the future of AI adoption rather than merely certify its expansion.

II. From Legal Regulation of AI to Technical Regulation: The Emergence of Standards-Based Governance

AI systems are marked by rapid iteration cycles, inherent opacity (the "black box" phenomenon),[1] and involve many layers of development and suppliers. Traditional legislative processes, which are designed for comparatively stable technological domains, therefore struggle to map granular

1 CASTELVECCHI, Davide, "Can we open the black box of AI?", *Nature News*, 2016, vol. 538, no 7623, p. 20.

technical risks to normative obligations.[2] There is nothing new there: parliamentary committees routinely depend on expert testimony to compensate for limited in-house technical proficiency (it has been the case for a long time for deeply technical areas, such as health). This well-known asymmetry produces a persistent "knowledge gap" which is more important and impactful when technologies are as pervasive in our world as they are today. Major technology conglomerates have capitalised on the foregoing complexity to advocate for a regulatory paradigm centred on voluntary or consensus-based standardization.[3] Their submissions to consultation processes frequently emphasise the impracticability of prescriptive, code-level statutory rules and the comparative agility of international standards bodies (e.g., ISO/IEC, IEEE) to update technical benchmarks.[4]

While such arguments underscore legitimate advantages of standards (flexibility, global interoperability, etc.), they simultaneously shift normative authority from democratically accountable fora to expert-driven consortia in which industry wields significant influence. Without calibrated public oversight, standards may reflect market incumbents' architectural preferences more than the broader public interest. It's only logical in a free market. Contemporary digital-economy instruments increasingly adopt the "law as framework" model, whereby primary legislation articulates high-level principles and defers operational specifics to delegated acts, technical standards, or certification schemes. The European Union's Artificial Intelligence Act (EU AI Act) exemplifies this evolution, as it establishes delegates (partly) conformity to harmonised standards for implementation details.[5] Such delegation is intended to preserve technological neutrality and future-proof the legal order. However, it also renders the enforceability of statutory rights contingent upon the timely development and periodic revision of standards that translate abstract legal duties (e.g., "transparency") into supposedly verifiable technical criteria. Absent coordinated governance between regulators and standards-development organisations, this layered system risks fragmentation, regulatory arbitrage, and uneven market access, thereby undermining the very trust it seeks to cultivate.

This situation makes sense if one takes a little step back. Historically, international standards have been drafted by industrial consortia for clearly circumscribed industrial purposes.[6] Whether determining the tensile strength of steel or the chemical composition of food-grade plastics, the drafting paradigm has privileged what one calls the "performance principles",[7] which means that the standard does not dictate "how" to achieve a result, only the measurable outcome to be attained (e.g., "shall withstand continuous exposure to 220 °C for a minimum of one hour"). This outcome-orientation maximises design freedom while delivering predictable, verifiable benchmarks for market surveillance authorities and supply-chain auditors. That legacy paradigm now encounters the "new world" of socio-technical standardization characteristic of AI. Traditional committee experts are steeped in deterministic product specifications, line-by-line normative clauses, and mechanical test methods. By contrast, AI governance requires

2 KAMINSKI, Margot E., "Regulating the Risks of AI", *BUL Rev.*, 2023, vol. 103, p. 1347.
3 ZIELKE, Thomas, "Is artificial intelligence ready for standardization?", *Systems, Software and Services Process Improvement: 27th European Conference*, EuroSPI 2020, Düsseldorf, Germany, September 9–11, 2020, Proceedings 27, Springer International Publishing, 2020, pp. 259-274.
4 ROBERTS, Huw and ZIOSI, Marta, "Can we standardise the frontier of AI?", *Available at SSRN 5271446*, 2025, p. 19
5 See Articles 40-41 of the EU AI Act.
6 RUSSELL, Andrew L., "Standardization in history: a review essay with an eye to the future", *The standards edge: Future generations*, 2005, vol. 247, pp. 1-17.
7 ISO/IEC DIRECTIVES, Part 2, Principles and Rules for the Structure and Drafting of ISO and IEC Documents, 2021, Article 5.4.

discursive considerations such as bias mitigation, transparency reporting, and human-oversight protocols, domains unfamiliar to classical standards engineers.[8] Paradoxically, though (or is it?), recent AI standards are increasingly less technical in the classical sense. Instruments such as ISO/IEC 42005 (AI Impact Assessment) and ISO/IEC 23894 (AI Risk Management) prescribe governance processes, accountability structures, and documentation requirements rather than component-level tolerances.[9] Those texts read closer to soft-law corporate governance codes than to engineering blueprints. This shift reflects legislators' deliberate reliance on standards to fill regulatory detail, but it also raises justiciability concerns. The more a standard looks like policy advice, the harder it is to test or verify through traditional conformity assessment methods. When the topic is AI risk management and AI impact assessment, that could be an issue.

AI systems indeed mediate more of our access to employment, healthcare, credit, and public services. Standardization is therefore intervening upon areas historically safeguarded by constitutional and human-rights law - non-discrimination, privacy, freedom of expression, just to name a few. Standardization technical committees must now encode safeguards that translate abstract rights into operational requirements. Yet the institutional design of standards bodies (consensus-based, mostly industry-funded, and *de jure* technocratic) was never intended to adjudicate normative hierarchies among competing rights or to embody democratic legitimacy. Consequently, without robust liaison mechanisms linking legislators, civil-society organisations, and standards-development organisations, performance-based AI standards risk ossifying market norms that fall short of fundamental-rights jurisprudence.

III. The Internal Tensions of Technical Standardization in Artificial Intelligence

Can we tackle such a challenge? This is not an easy task, notably due to the internal tensions of technical standardization. A first source of doctrinal uncertainty arises from the intrinsic dualism between *shall* clauses, which create binding normative obligations, and *should* clauses, which merely offer non-binding guidance.[10] Although this drafting technique preserves the malleability required to accommodate rapidly evolving technologies, it simultaneously undermines potential legal certainty. Conformity-assessment bodies depend upon unequivocal, verifiable statements. When essential controls are formulated conditionally or relegated to non-mandatory annexes, auditors must interpret the spirit rather than apply the letter of the standard.[11] This interpretative burden is particularly problematic where a legislature (such as the EU AI Act) confers a presumption of conformity only upon harmonised standards whose mandatory provisions map directly to the operative statutory articles. In the absence of a sufficient density of *shall* clauses, a framework standard may at best assist but will never in itself satisfy the legislator's requirements.

8 HÖGBERG, Charlotte, "Stabilizing translucencies: governing AI transparency by standardization", *Big Data & Society*, 2024, vol. 11, no 1, pp. 1-14.

9 ISO/IEC 23984:2023 - Information technology - Artificial intelligence - Guidance on risk management and ISO/IEC 42005:2025 Information technology - Artificial intelligence (AI) - AI system impact assessment.

10 ISO, Foreword – Supplementary Information, available at: https://www.iso.org/foreword-supplementary-information.html [last accessed – 2025-06-10].

11 GOODMAN, Ellen P. and TREHU, Julia, "Algorithmic auditing: Chasing AI accountability", Santa Clara High Tech LJ, 2022, vol. 39, 38.

The contrast between ISO/IEC 42001:2023, entitled "Artificial Intelligence Management System",[12] and the forthcoming European Quality Management System (QMS),[13] being drafted under CEN-CENELEC/JTC 21, illustrates the point. ISO/IEC 42001 adopts the familiar management-system architecture derived from ISO 9001 and ISO 27001.[14] It obliges organisations to adopt governance processes, yet it refrains from prescribing metrics or performance thresholds, leaving the identification of key risk indicators to the discretion of the operator. By comparison, the European QMS is expected to translate the EU AI Act's obligations into prescriptive controls because the European Commission stated that ISO/IEC 42001 was clearly not enough for Europe.[15] The coexistence of these two regimes creates a structural tension. ISO/IEC 42001 offers a globally applicable baseline that can be adapted to diverse legal orders, whereas the European QMS privileges strict alignment with regional legislation. Dual certification and overlapping documentation may thus become unavoidable transaction costs unless the international standard is itself revised to a more granular level of prescription (which probably will not happen, due to the current and understandable dynamics at stake here). A further tension concerns the lingering vacuum in relation to performance metrics. Historically, AI standards have declined to mandate uniform indicators of accuracy, robustness, or bias. The heterogeneity of use-cases, the velocity of technological progress, and competitive sensitivities surrounding benchmark disclosure have all militated against such prescriptions. Nonetheless, specialised initiatives are emerging. ISO/IEC TS 4213:2022, for example, codifies common methodologies for evaluating machine-learning classification,[16] but does not specify any threshold. A draft European standard, prEN JT021025,[17] seeks to establish test protocols for computer-vision systems, and ISO/IEC AWI TR 23281,[18] provides a taxonomy of natural-language tasks that foreshadow potential metric normalisation. These instruments, however, are sector-specific and hierarchically subordinate to management-system standards. They do not bind operators.

In sum, contemporary AI standardization oscillates between formulations that are so generic as to risk diluting legal obligations and prescriptions so detailed as to threaten international interoperability. Achieving the requisite equilibrium demands sustained coordination among legislators, standards-development organisations, conformity-assessment bodies and affected stakeholders. Without such coordination, the promise of standards-based governance may degenerate into a costly and fragmented patchwork that erodes both market confidence and regulatory efficacy. Another challenge is how to make standards enforceable when they try to turn broad legal values (like health, safety, and human rights) into technical rules. Current approaches propose a step-by-step process, such as identifying risks, estimating them, evaluating their impact, and deciding how to manage them. The goal is to match technical safety controls with legal protections. But it's still unclear how to turn legal principles (like fairness, non-discrimination, or due process) into engineering tasks that can be tested or measured. This

12 ISO/IEC 42001:2023 - Information technology - Artificial intelligence – AI Management System.
13 As the QMS is currently being drafted, there is no official reference.
14 ISO 9001:2015 Quality management systems — Requirements and ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
15 SOLER GARRIDO, Josep, DE NIGRIS, Sarah, BASSANI, Elias, SÁNCHEZ, Ignacio, EVAS, Tatjana, ANDRÉ, Antoine-Alexandre, et BOULANGÉ, Thierry, "Harmonised Standards for the European AI Act", joint research center, science for policy brief, 2024, p. 6.
16 ISO/IEC TS 4213:2022 Information technology — Artificial intelligence — Assessment of machine learning classification performance.
17 As the standard is not published yet (and could very well never be), providing a reference is impossible.
18 ISO/IEC AWI TR 23281 Artificial intelligence — Overview of AI tasks and functionalities related to natural language processing.

creates a gap between law and engineering. The result is a mixed method that satisfies neither side. Engineers face vague, untestable rules, while legal experts see core rights being weakened into optional procedures. The EU AI Act nonetheless mandates precisely such an alignment. Article 9 imposes a formal risk-management system for all high-risk AI, explicitly requiring that the residual risk evaluation take into account impacts on health, safety, and fundamental rights.[19] The Commission's standardisation request therefore instructed CEN-CENELEC/JTC 21 to codify acceptance criteria capable of demonstrating conformity to these rights-based objectives.[20] This delegation intensifies the interpretability problem. Conformity-assessment bodies must turn broad claims about privacy, fairness, and avoiding harm into clear and repeatable checks, even when reliable metrics are lacking. This task is made harder by interoperability challenges.

A further layer of complexity arises from the divergent conceptions of "safety" that prevail in engineering and legal communities. In the engineering vernacular, safety often conflates with cybersecurity. The integrity, availability, and confidentiality of digital assets constitute the central object of protection. Legal doctrine, by contrast, apprehends safety primarily in relation to the physical or psychological integrity of natural persons – this is how the EU AI Act addresses it. Needless to say, this conceptual bifurcation jeopardises consistent implementation. The cumulative effect of these interpretability, interoperability, and implementation gaps leaves operators exposed to risk even when they have diligently applied the best available standards. This situation is even more pressing as AI itself has a structuring effect that is often not addressed, neither in standards nor in regulation.

IV. Language, Cognition and Power: The Structuring Effects of AI Models

AI systems are not inert computational artefacts. They constitute socio-technical assemblages that inscribe, reproduce, and ultimately reify a particular vision of the world.[21] Contemporary large language models, by design, generate utterances on the basis of probabilistic inference across vast corpora of textual data. The statistical objective (i.e., to predict the most probable next token) inevitably privileges the centre of the distribution.[22] In practical terms, the model converges upon the linguistic median: it outputs what is statistically most common, most repeated, most "average." That optimisation paradigm, while empirically effective, is neither culturally neutral nor politically indifferent. It embeds into every generated sentence the epistemic priors and normative assumptions latent in the underlying data (and the ponderation decided by the engineers). The phenomenon is readily observable when juxtaposing models trained on distinct geopolitical corpora. For example, ChatGPT, developed and fine-tuned within a North American (even Californian) epistemic milieu, tends to reflect the related ideology: a secular faith in technological progress, a rhetorical embrace of individual autonomy, and an

19 See Article 9, of the EU AI Act.

20 European Commission, COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, 2023, available at: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en [last accessed – 2025-06-10].

21 JOHNSON, Deborah G. et VERDICCHIO, Mario, "The sociotechnical entanglement of AI and values", *AI & SOCIETY*, 2024, pp. 1-10.

22 The model cannot, without deliberate counter-balancing intervention, amplify perspectives that the data do not sufficiently encode.

irrepressible optimism regarding market-driven innovation. DeepSeek, trained predominantly on Chinese-language data and subject to a markedly different regulatory context, produces a discursive register that is more deferential to social order, more constrained on questions of political pluralism, and more attuned to collective harmony than to individual self-realisation. Neither model is "biased" in the pejorative sense of procedural error. Each is, rather, a faithful statistical mirror of the linguistic patterns that prevail in its respective information environment.

To summarize, whereas technical standards traditionally codify product specifications, language-model outputs progressively stabilise semantic and ideological baselines. This shift has important legal implications. When a small number of AI models influence how language is used, they can begin to shape public communication in ways that resemble the role of traditional rule-makers. The challenge, therefore, is not merely to audit datasets for overt bias or to append content-moderation heuristics. It is to recognise that probabilistic optimisation intrinsically favours central tendencies, and that such tendencies seldom coincide with the normative commitment to pluralism embedded in the diverse societies we live in. A governance architecture that seeks to "secure the future of AI adoption" to reprise the promise evoked in the preamble has no other choice but to confront this structural tension. The progressive migration of information retrieval from indexed search engines to conversational "answer engines" portends a structural realignment of knowledge power to support this massive shift of the knowledge economy. Industry commentary already treats the imminent eclipse of conventional web search as a foregone conclusion. Users, indeed, increasingly solicit direct responses from large language models rather than sift through link lists, a shift that commentators liken to the transition from card catalogues to digital databases.[23] Google itself has accelerated the trend by unveiling an "AI Mode" that recasts results pages as dialogic exchanges, thereby positioning its proprietary model, Gemini, as the primary epistemic gatekeeper.[24] The influence of these systems goes well beyond making things easier for users. If only a few large language models control how we search and retrieve information, the way researchers cite and find academic work could be seriously harmed. The canonical pathways by which research is surfaced (bibliographic databases, keyword search, citation networks, etc.) depend on supposedly neutral indexing.[25] A conversational agent that synthesises an "authoritative" answer without exposing its source graph deprives researchers of the critical apparatus needed to verify provenance and contest interpretation. Early studies on the integration of generative AI into the research workflow already warn that the opacity of model outputs strains traditional definitions of research integrity.[26]

23 XIONG, Haoyi, BIAN, Jiang, LI, Yuchen, et al., "When search engine services meet large language models: visions and challenges", in IEEE Transactions on Services Computing, 2024, pp. 4458-4577.

24 SAEIDNIA, Hamid Reza, "Welcome to the Gemini era: Google DeepMind and the information industry", in Library Hi Tech News, 2023, pp. 1-6.

25 KAMOUN, Ahmed, MAILLÉ, Patrick, et TUFFIN, Bruno, "Evaluating the performance and neutrality/bias of search engines", in Proceedings of the 12th EAI International Conference on Performance Evaluation Methodologies and Tools, 2019, pp. 103-109.

26 Academic publishing confronts a parallel disruption. Editorial policies of course struggle to delimit permissible uses of generative AI for drafting, reviewing and even authoring manuscripts. The phenomenon is no longer hypothetical: fully AI-generated papers have begun to clear peer review, confounding established attribution norms and inflaming concerns that periodicals may devolve into mere validation layers for text produced elsewhere. Should this trajectory continue, the very function of the scholarly journal, as a curated forum for incremental, contestable knowledge, risks obsolescence. See VASCONCELOS, Sonia et MARUŠIĆ, Ana, "Gen AI and research integrity: Where to now? The integration of Generative AI in the research process challenges well-established definitions of research integrity", in EMBO Reports, 2025, vol. 26, no 8, pp. 1923-1928.

From a governance perspective, freedom of expression, academic freedom, and the public's right to receive information presuppose a pluralistic media ecology. Where knowledge curation migrates to opaque probabilistic systems, classical regulatory tools such as competition law, media pluralism rules, and scientific-integrity standards must therefore be re-examined. Could standards really be the answer to those issues?

V. Governing AI Means Fixing Thresholds: A Fundamentally Diplomatic Question

In contemporary practice, the decisive power over technical thresholds (accuracy floors, robustness margins, rates of permissible false positives, etc.) rests predominantly with the corporations that design, train, and deploy large-scale AI systems. Neither the EU's forthcoming harmonised standards nor the rest of the world's voluntary instruments prescribe universally binding figures. At most, they articulate process requirements and illustrative benchmarks, inviting providers to select the concrete values that will later be presented to auditors. The EU's own Joint Research Centre concedes that standards may not be able to prescribe accuracy metrics and thresholds for every high-risk AI system[27], emphasising the discretion left to providers to "select relevant and effective" figures consistent with Article 15 of the AI Act.[28] Parallel dynamics are visible in the United States, where the NIST AI Risk Management Framework, while comprehensive in its taxonomy, remains agnostic as to any specific numerical targets, leaving their determination to "organisation-defined parameters". Whether this allocation of authority ought to change is contested. On the one hand, delegating threshold-setting to industry harnesses specialised knowledge and avoids the rigidity inherent in *ex ante* legislation. On the other hand, it engenders a legitimacy deficit. The metrics that delimit acceptable error rates in, say, credit scoring or medical triage directly condition the enjoyment of fundamental rights, yet are calibrated by entities with commercial incentives to minimise compliance friction. The OECD has initiated a public consultation precisely on this point, seeking views on "approaches, opportunities and limitations for establishing risk thresholds for advanced AI systems".[29] That the exercise is framed as multistakeholder diplomacy rather than unilateral state action underscores the political delicacy of reallocating the power to define technical acceptability.

If the axis of threshold decision-making is to shift, it will not be sufficient merely to transpose the task from private hands to traditional regulators. One emergent proposal involves the creation of fiduciary institutions, or "data trusts", capable of acting as neutral stewards. A data trust, structured under trust law, holds data or model artefacts in the public interest and is mandated to negotiate access terms, establish evaluation metrics, and enforce accountability on behalf of data subjects and affected communities.[30] Pilot studies in Québec,[31] illustrate how such trusts could negotiate both training-data governance and performance-threshold commitments, offering an institutional home for decisions that are simultaneously technical and normative.

27 SOLER GARRIDO, *et al.*, supra.
28 See Article 15, of the EU AI Act.
29 OECD AI Policy Observatory, Public consultation on AI risk thresholds, available at: https://oecd.ai/en/site/ai-futures/discussions/risk-thresholds-consultation [last accessed – 2025-06-10].
30 HOUSER, Kimberly A. et BAGBY, John W., "The data trust solution to data sharing problems", *Vand. J. Ent. & Tech. L.*, 2023, vol. 25, p. 113.
31 HULIN, Anne-Sophie, "De la fiducie de données en droit civil québécois: étude exploratoire pour un outil en construction", *McGill Law Journal*, 2021, vol. 67, no 2, pp. 119-156.

Changing how we govern AI risk thresholds will require careful negotiation between different regulatory approaches, industrial goals, and cultural attitudes toward risk. Deciding what counts as "acceptable risk" is not just a matter of data or evidence. It reflects deeper societal values like fairness, safety, and openness to innovation. A lasting solution must come from agreement among standards bodies, regulators, civil society, and the companies whose technologies make such governance possible and necessary. Until such a multilateral architecture is formalised, the practical authority to define AI performance thresholds will continue to reside, by default, with the corporations that create the technology, leaving the promise of rights-respecting AI contingent upon private calculations of reputational and commercial risk. That's the game, of course, but if performance thresholds constitute the operative hinge on which rights-respecting AI governance turns, the forum in which those thresholds are negotiated becomes a geopolitical matter. And on that aspect, the institutional landscape is unfortunately fragmented. On one axis stand the classical organs of public international law, most visibly the United Nations system, whose charters endow them with a (mostly) universal membership and a mandate to articulate global public goods. On the other axis operate the formal standards-development organisations such as ISO, IEC, and the International Telecommunication Union (ITU), which possess the technical secretariats, working-group infrastructures, and consensus procedures required to translate high-level principles into auditable clauses. This situation causes at the very least two structural challenges.

First, it proliferates partially redundant normative instruments whose cumulative opacity hampers compliance. Governments and enterprises are confronted with parallel guidance from UNESCO, the ITU, ISO/IEC JTC 1/SC 42, and, many other *ad hoc* initiatives.[32] Second, the absence of a canonical venue for threshold-setting encourages forum shopping. Private actors favour the body most aligned with their strategic interests, while states leverage institutional pluralism to advance competitive industrial policy under the banner of technical cooperation. Against this backdrop, diplomatic fora acquire renewed importance. Multilateral diplomacy can supply the legitimacy and political equilibrium that purely technical bodies lack, while technical bodies can endow diplomatic declarations with the precision and enforceability that political resolutions seldom achieve. The challenge lies in engineering an interface regime that allocates agenda-setting, negotiation, and adoption functions across these institutions without reproducing the current fragmentation.

Concurrently, courts and regulators increasingly treat harmonised standards as integral components of positive law, thereby blurring the boundary between voluntary compliance and legal obligation. The Court of Justice of the European Union, in *James Elliott Construction v. Irish*

32 Over the past decade, the dramaturgy of standardisation has shifted from an inter-state contest for influence to a hybrid terrain in which multinational firms deploy proprietary norms as vectors of soft power. Microsoft's *Responsible AI Standard, v2*, a 100-page internal code that prescribes life-cycle documentation, release criteria and error-budget thresholds, illustrates how a single corporation can promulgate de facto rules that shape global supplier contracts and third-party audits well before any public body has spoken. Because the standard is expressly calibrated to "ensure compliance with emerging AI laws and regulations," it functions as anticipatory regulation and positions its author as an agenda-setter in legislative consultations. This privatisation of normativity complicates the classical view of standards as neutral technical artefacts. They now operate as instruments of corporate diplomacy, conferring first-mover advantage and reputational capital on their sponsors.

Asphalt (C-613/14),[33] characterised harmonised construction-product standards as forming part of EU law to the extent that they concretise essential requirements of a directive, therefore pushing for standards to be freely accessible. This decision has been confirmed recently in *Public. Resource.Org Inc. v. Right to Know CLG* (C-588/21).[34] In the United States, multiple federal agencies incorporate private standards by reference into the Code of Federal Regulations, rendering them legally binding. The United States Court of Appeals for the Fifth Circuit ruled recently (2024) in favor of *P.S. Knight Company Limited*, holding that once model codes or standards are incorporated into law, they acquire the status of law itself and may therefore be reproduced or distributed.[35] The cumulative effect of those decisions on a global scale seems pretty clear: it is a "juridification" of standards.

The commercial landscape is adapting accordingly, but it will take some time. ISO's digital "SMART Standards" initiative and allied programmes that market "standardisation as a service" envision modular, machine-readable fragments sold via subscription APIs, enabling firms to embed compliance checkpoints directly into their pipelines.[36] National bodies such as ILNAS in Luxembourg explicitly frame this approach as "technical standardisation as a service" within their digital-economy strategies, positioning standard-setting as a revenue line and a policy lever simultaneously.[37] These models invert the historical funding structure of standardisation. Instead of indirect cost recovery through print sales and conference fees, value is extracted through continuous digital licensing, data analytics and bespoke conformity modules. Taken together, these developments erode the classical legal hierarchy theorized by Kelsen in which treaties sat atop legislation, legislation above standards, and standards above private specifications. Corporate frameworks now rival intergovernmental norms in prescriptive detail, and courts elevate selected standards to the rank of binding laws. The social contract probably needs to be renegotiated on that aspect.

VI. Conclusion

AI governance now stands at an inflection point where the structural logic of technical standardisation intersects with the constitutional commitments of how legal texts are drafted and the strategic calculations of geopolitical rivals. This article has demonstrated that standards are no longer peripheral soft-law artefacts. Once referenced by legislation or embedded in global supply contracts, they equal statutes in normative force while remaining less transparent in authorship and less pluralistic in representation. The ensuing hybrid regime delivers tangible benefits (global interoperability, rapid update cycles, empirically grounded best practices, just to name a few), but it also reallocates decisional authority from parliaments to expert

33 Court of Justice of the European Union, 2016, C-613/14, *James Elliott Construction v Irish Asphalt.*
34 Court of Justice of the European Union, 2024, C-588/21, *Public.Resource.Org Inc. v Right to Know CLG.*
35 Fifth Circuit Court of Appeal, 2024, Case No. 23-50081, *Canadian Standards Association v. P.S. Knight Company Limited*.
36 IEC/ISO, "IEC/ISO SMART Standards Initiative Explained", 6 June 2023, available at: https://www.iso.org/news/ref2687.html [last accessed – 2025-06-10].
37 IEC, "Luxembourg highlights role of technical standardization in adoption of artificial intelligence", *E-tech*, Issue 05/2021, available at: https://etech.iec.ch/issue/2021-05/luxembourg-highlights-role-of-technical-standardization-in-adoption-of-artificial-intelligence [last accessed – 2025-06-10].

committees and, increasingly, to the companies that furnish both the data and the metrics by which compliance is measured. Three conclusions follow. First, AI cannot be secured by standards prescriptions alone. Because probabilistic optimisation centralises linguistic and cognitive authority, any credible governance architecture must incorporate safeguards for pluralism. Second, threshold-setting is irreducibly political. The acceptable risk in credit scoring or autonomous driving is a distributive choice that must be negotiated in public, not silently calibrated by private engineering teams. Third, the "juridification" of standards demands a reciprocal democratisation of the standard-setting process. If harmonised texts are to carry the weight of law, they must be drafted and revised under procedural guarantees commensurate with that weight. This is currently not the case.

ABOUT THE AUTHOR

Tom Lebrun

Standards Council of Canada, Lecturer AI Law at Université Laval, Québec City

Tom's work focuses on bringing together diverse international perspectives to advance the governance, regulation, and standardization of artificial intelligence on a global scale. As AI Standardization Policy Lead within the Data and Artificial Intelligence Governance Program at the Standards Council of Canada. With over ten years of experience, he contributes to the development of national and international strategies, fostering collaboration between governments, industries, and global partners. For the past six years, he has taught AI law, policy, and regulation at several universities, primarily at Université Laval in Québec City. Tom holds a doctorate (summa cum laude) specializing in AI-generated texts, as well as LL.B. and a LL.M. from the Sorbonne Law School (Université Paris 1 Panthéon-Sorbonne).

BUILDING TRUST IN THE AGE OF DIGITAL MEDICINE: COMBINING TECHNICAL AND LEGAL REGULATION

Élise Degrave

Olga Thiry

I. Introduction

It is clear to everyone that medicine is now also undergoing increasing digitization, which is accelerating today thanks to the deployment of artificial intelligence. At the heart of these developments are patient data, more specifically 'personal data' relating to their health. For the sake of clarity, we will refer to this data as 'health data' in this study.

Thanks to technology, this data is collected by healthcare providers, stored in databases, reused by healthcare partners, interpreted by artificial intelligence to aid decision-making, and so on. Ultimately, technology promotes more accurate and rapid diagnoses, supports the detection of abnormalities on X-rays, and encourages personalized care through the analysis of patients' genetic characteristics, their level of risk, etc.[1]

These technical deployments often involve the collection and multiple reuses of patient health data. However, this means telling patients: "Give us your most intimate data, it will be stored in a digital format – an intangible format over which you will have no control – and then it will be reused many times by a multitude of healthcare providers. It's for your own good, trust us." That's precisely the point. In this technical, complex, intangible, and often unclear context, particularly for patients, what about trust? Trust cannot be decreed by law. It must be inspired by strong technical and legal guarantees. So how can we build patient trust in the era of digital medicine?

The question is particularly acute at a time when digital abuses are creating mistrust among the public. Among these, we are seeing a proliferation of scandals concerning the misuse of personal data, sometimes even with the complicity of the government. Among other examples, in Belgium in 2022, a draft bill organized the transfer of citizens' health data to insurance companies. The disclosure of this text in the media caused a public outcry, and the minister responsible shelved it for the time being.[2] Added to this are cyberattacks targeting hospitals, which, despite improved security measures and a stronger legal framework, continue to cause significant damage, amounting to as much as €5 million, as was recently highlighted before the Chamber of Representatives of the Belgian Federal Parliament.[3] Furthermore, when it comes to digital health, the internet giants known as GAFAM are never far away, siphoning off our data often without our knowledge and by all means possible, including from our wrists when we wear smartwatches connected to their systems. They have also become major players in the 'battle for generative AI in healthcare',[4] which further clouds the actual fate of the health data we share on a daily basis.

In this study, we focus on how patient trust can be supported by regulation, both technical and legal. In this regard, Belgium, a pioneer in the implementation of a unique architecture for secure health data processing, will be the focus of our analysis of technical regulation in this

1 For more details on this topic, see J.-L. Fraysse, « L'intelligence artificielle dans le domaine de la santé (IAM) : avancées, enjeux des données et régulation éthique, le point de vue d'un professionnel de santé », *Espace européen des données de santé et IA. Enjeux juridiques et défis de mise en œuvre* (Dir. N. De Grove-Valdeyron), Toulouse, Presses de l'Université Toulouse Capitole, 2025, p. 305 et s.

2 On this topic, see E. Degrave, *L'Etat numérique et les droits humains,* Académie royale de Belgique, coll. L'Académie en poche, Bruxelles, 2024, pp. 11 et 12.

3 Le Spécialiste. L'Actualité des médecins spécialistes, « Combien coûtent réellement les cyberattaques aux hôpitaux belges ? », 15 April 2025 available here: https://www.lespecialiste.be/fr/actualites/e-health/combien-coutent-reellement-les-cyberattaques-aux-hopitaux-belges.html.

4 Mind Health, « Exclusive study. Le bilan des initiatives des GAFAM dans la santé en 2023 », https://www.mind.eu.com/health/industrie/etude-exclusive-le-bilan-des-initiatives-des-gafam-dans-la-sante-en-2023/.

area. This experience will be linked to current developments in the European Health Data Space and the accompanying European legal regulation.

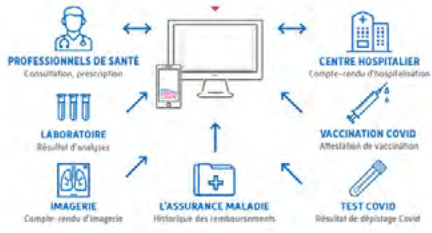
II. Technical Regulation of Digital Medicine

From Paper Files to Smartphone Screens – From Siloed Medicine to Networked Medicine

In just a few years, we have gone from paper files containing medical documents to viewing our health status on a computer or smartphone screen. This transformation has been made possible by the technical infrastructure of digital medicine, which has moved from 'siloed' medicine to 'networked' medicine.

Siloed administration, typical of the paper-based world, meant that each administration worked separately from the others, without exchanging information. Since the 1990s, it has been moving towards networked administration based on data decentralization,[5] as envisaged for the new European Health Data Space, which will be detailed later.

Siloed medicine[6]



Networked medicine[7]

The starting point is an obvious observation: the deployment of digital technology enables effective collaboration between administrations, which can quickly exchange information about citizens. This has led to a desire to encourage 'synergies between the various departments and levels of public authority',[8] with the aim of simplifying procedures and processes for citizens in general (in the social security sector, for example) and patients in particular (in the health sector).

Two Founding Principles of the Network Model

This unique model for exchanging information between government agencies in general and between healthcare providers is based on two key principles.

5 For more details, see. E. Degrave, *L'e-gouvernement e la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, coll. Crids, 2014, pp. 33 à 101. On the societal challenges related to this model, see E. Degrave, *L'Etat numérique et les droits humains,* Bruxelles, Académie royale de Belgique, coll. L'Académie en poche, 2024, p. 144.

6 Diagram from here : https://nurseandco.be/pour-qui/institutions/.

7 Diagram from here : https://www.ch-narbonne.fr/creer-et-utiliser-son-dossier-medical-partage/ For the Belgian network, see the e-health platform detailed here : https://www.ehealth.fgov.be/fr.

8 Commission for the Protection of Privacy (hereinafter « CPVP »), Opinion No 41/2008 of 17 December 2008 on a request for an opinion concerning the preliminary draft law on the establishment and organization of a Federal Service Integrator, No 5.

Firstly, it is a "network" Institutions working in the same area of government (social security, health, etc.) are identified and placed within a network. This is how the social security network and the health network, in particular, came into being in Belgium.

Secondly, Belgian digital administration is based on the 'decentralization of data'. In other words, within this network, the proverb 'don't put all your eggs in one basket' is applied to reduce the risk of hacking. This involves distributing data among the institutions in the network and deciding which type of data is stored in which institution. In this way, data is only stored in one copy, in one institution in the network, which is also responsible for the reliability of that data.

Reuse of Data within the Healthcare Network

Decentralization of data requires that the reuse of this data within the network be organized. This is why a new type of tool is being placed at the heart of this network of institutions: the service integrator, also known as an 'information exchange platform' or 'crossroads bank'. In short, the service integrator is a technical infrastructure, placed at the heart of a network of administrations, which is responsible for ensuring the electronic exchange of information from various authentic sources within this network. Thus, when a healthcare provider needs data that it does not have, it simply contacts the service integrator, which then contacts the institution holding the requested data and forwards it to the institution that requested it.

"Privacy by Design" Ahead of its Time

The network model was ahead of its time in embodying the concept of privacy by design, one of the important principles of the GDPR, which requires privacy protection to be taken into account from the design stage of the tool. This provision of the GDPR embodies the strength of technical regulation, which supports the legal regulation that the GDPR also embodies when it grants rights to patients, as we will see later.

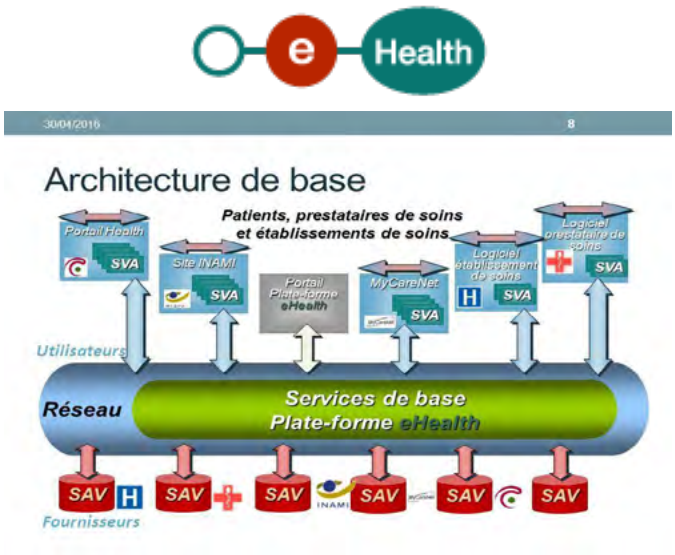
It is precisely this concern for privacy protection in the very architecture of the network model that led to the decision to organize administration into networks, and in particular, networked digital medicine. At the same time, this concern led to the abandonment of the data centralization model, which was discussed, for example, during the SAFARI,[9] project in France. The French government wanted to assign each citizen a unique identification number for all public files, in order to facilitate the consolidation of their information. The fierce opposition to this project led to the adoption of the Law of 6 January 1978 "on information technology, files and freedoms" and the establishment of the "Commission nationale de l'informatique et des libertés" (CNIL). This model was not followed by Belgium, due to concerns that it would increase the risk of data hacking by consolidating all citizen data in a single location.

The "e-health" Network

In Belgium, the sectoral health network has been in existence since 2008. At its core, the eHealth platform, organized by the legislator,[10] acts as a service integrator. This network brings together healthcare providers, hospitals, mutual insurance companies, and administrations involved in healthcare.

9 SAFARI stands for « système automatisé pour les fichiers administratifs et le répertoire des individus ».

10 See the Law of 21 August 2008 on the establishment and organization of the eHealth platform and various provisions, *MB,* 13 October 2008.



Example of a service integrator: e-health platform, at the heart of the healthcare network

A concrete example of the benefits of this model is the electronic prescription system. Since 15 September 2021, doctors, dentists, and midwives have been required to use the electronic prescription system.[11] These are sent directly to the e-health platform. Thanks to an application set up for this purpose, pharmacists can download the prescription directly from the system, after verifying the patient's identity via their electronic identity card. There is therefore no longer any need to use paper. This has certain advantages, such as being able to obtain a prescription renewal without having to go to the doctor's office. However, feedback on the implementation of the system indicates certain difficulties: for example, due to errors made when entering the prescription, some men have been prescribed contraceptive pills. It can also be confusing not to have the prescription in your wallet and not really know what has been entered for you, especially since accessing this information online is not the easiest thing to do, particularly because the Belgian online identification system is not very smooth.[12]

III. Legal Regulation of Digital Medicine

The Dual Objective of the GDPR: Protection and Circulation

After analyzing the Belgian 'networked' system, we will analyze how personal data, and more specifically health data, is protected and shared in accordance with European legislation. The circulation, sharing, and reuse of such data are both essential and sensitive, both economically – for innovation, research, and development – and from a human and ethical perspective, given their sensitive nature.[13]

11 Seehttps://www.inami.fgov.be/fr/themes/soins-de-sante-cout-et-remboursement/les-prestations-de-sante-que-vous-rembourse-votre-mutualite/medicaments/prescrire-un-medicament/obligation-de-prescrire-les-medicaments-de-facon-electronique.

12 Seehttps://www.pharmacie.be/Pharmacy/Article/aller-chercher-ses-medicaments-avec-sa-carte-didentite~641.

13 J.-M. Van Gyseghem, M. Knockaert, A. Gobert and M. Rappe, « Les données et leur circulation en droit de l›Union européenne (II) - La donnée à caractère personnel et sa réutilisation », *J.T.*, 2024/8, p. 121.

When it comes to personal data, the GDPR aims to achieve two objectives: to enable the free movement of personal data while protecting it.[14] At present, the free movement of data, especially in the field of health, has become a crucial issue: removing barriers to the flow of personal data within the Union responds to the growing demand for data availability, which is a prerequisite for the further development of new technologies, particularly artificial intelligence systems.[15] However, this consideration conflicts with the desire to protect individuals from the development of new information and communication technologies, which is the other objective of the GDPR.[16] In practice, how does the European Union approach this difficult balance between protecting citizens' data and developing innovation, for which data is the very essence? The following paragraphs will attempt to answer this question once we have examined the legal framework applicable to health data.

A. Data Protection

a. Definition: 'Health Data'

How is health data legally defined in European law? According to the GDPR, it is 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the health status of that person'. Consequently, this concept revolves around two poles: data relating to the physical or mental health of a natural person, on the one hand, and data relating to the provision of healthcare services, on the other, insofar as these two categories reveal information about a person's state of health. According to the Court of Justice of the European Union, this concept must be interpreted broadly and consists of 'any information relating to any aspect, both physical and mental, of a person's health'.[17]

b. 'Identified or Identifiable' Person

Furthermore, in order for information to be classified as 'personal data', the person concerned by the information being processed must be identified (distinguished from other members of the group to which they belong) or identifiable (the person is not yet identified, but it is possible to do so, either directly or indirectly).[18] This means, for example, that someone, somewhere, is able to say who is behind a particular number.

More specifically, health data is part of a special category of personal data due to the nature, sensitivity, and risks associated with its processing (= operation performed on data),[19] Indeed, the unlawful use of this category of data, which is likely to reveal intimate information about a person, can have serious repercussions on that person's rights and freedoms.[20]

14 GDPR, Article 1 and Recital 10.
15 H. Kranenborg, « About Profiles, Profiling, Data Availability and AI: The Return of the Second Objective of the GDPR? », *EDPL*, 2025/1, p. 10.
16 J. Herveg and J.-M. Van Gyseghem, « Titre 16 - L'impact du Règlement général sur la protection des données dans le secteur de la santé » in *Le règlement général sur la protection des données* (RGPD/GDPR), 1st édition, Bruxelles, Larcier, 2018, p. 704.
17 Ibid, p. 709 ; C.J.C.E., 6 novembre 2023, arrêt *Bodil Linqvist*, aff. C-101/01, obs., C. de Terwangne, « Affaire Linqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, pp. 67-99.
18 Ibid, p. 709.
19 For a full definition, see GDPR, Article 4.
20 GDPR, Recital 75.

c. Obligations of the 'Data Controller'

The person who processes the data will be referred to as the 'data controller' and, in this capacity, will be required to comply with a series of rules. Firstly, for all personal data, certain 'general' principles must be respected: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and finally, confidentiality. For health data, the GDPR has introduced a general prohibition on processing (with exceptions), given that such data is likely to infringe on fundamental freedoms or privacy. Despite this general prohibition, several exceptions are provided for: consent of the data subject, performance of an obligation, processing for archiving or scientific research purposes, etc. It should be added that Member States have the option of introducing additional conditions or limitations for the processing of such data. It is therefore entirely possible – if the principles laid down by the GDPR are respected – to use health data for research purposes and to contribute to the creation of innovations.

d. The Patient's Rights Over their Data

Individuals whose health data is processed, referred to as 'data subjects', are granted a series of rights by the GDPR to enable them to exercise control over their data. There are eight such rights: the right to information, the right of access, the right to rectification, the right to erasure, the right to be forgotten, the right to restriction of processing, the right to data portability, the right to object to data processing, and the right not to be subject to automated individual decision-making. It is the responsibility of the data controller to ensure that these rights are effectively implemented, so that the data subject can exercise them fully.

B. Data Sharing

a. The Regulation on the European Health Data Space

The European Union aims to become a global leader in digital transformation by encouraging the use and development of digital technology while ensuring its reliability.[21] This strategy has led to the adoption of several regulations, including the European Regulation on the European Health Data Space (hereinafter 'EHDS Regulation'), which entered into force in March 2025.[22]

This regulation establishes the architecture of the European Health Data Space (EHDS). The EHDS is based on a model of data decentralization. Health data is not centralized in a single location but is accessible, under certain conditions, via national contact points that enable the secondary and cross-border use of Europeans' health data.[23] This model is well known to the Belgian public authorities, as mentioned above. Once fully implemented (the process is expected to be completed around 2034), it should have changed the management of electronic health data in healthcare and the rules for accessing data for research, innovation, regulation and public policy purposes.[24]

21 For more information, see https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_fr.
22 H. Kranenborg, *op. cit.*, p. 14.
23 EHDS Regulation, Article 79.
24 S. Slokenberga, S., K. Ó Cathaoir and M. Shabani, *The European Health Data Space: Examining A New Era in Data Protection*, 1st ed., Routledge, 2025, p. 2.

The COVID-19 pandemic has played a significant role in this regulatory process of accelerating the move towards "digital health": it "*has highlighted the imperative of having rapid access to high-quality electronic health data for the purposes of preparing for and responding to health threats, as well as for prevention, diagnosis and treatment, and for secondary use of these electronic health data*".[25] By enabling secure and transparent data exchange, the EHDS Regulation aims to transform healthcare for everyone – patients, professionals, researchers and industry.[26] It builds on key existing EU legal frameworks, such as the General Data Protection Regulation (GDPR), the Data Governance Act (DGA), the Data Act (DA), and the Network and Information Systems Directive.

b. 'Primary' and 'Secondary' uses

In practice, the EHDS Regulation allows for the 'unlocking' of health data, which involves improving individuals' access to and control over their electronic health data (primary use) and facilitating the reuse of data (secondary use) for research and innovation.[27] It aims to transform the health data sharing regime while preserving the rights of data subjects (listed above).[28]

c. Links with the Artificial Intelligence Act (AI Act)

The new EHDS Regulation contributes to the development of research and innovation – including the development of artificial intelligence systems in medicine – and is an extension of another European legal instrument, the Artificial Intelligence Act (AI Act). The latter, which establishes different rules and obligations depending on the risks that an 'artificial intelligence system' is likely to present, aims to "*[...] promote the development, use and adoption of AI in the internal market, while ensuring a high level of protection of public interests, such as health and safety, and the protection of fundamental rights [...]*". Together, these regulations aim to "*[...] reconcile innovation and responsibility, ensuring that AI systems become widespread in various healthcare environments and that health data is available for research and clinical use without compromising privacy or security.*"[29]

C. The Limits of Legislative Intervention: Practical Considerations

All these regulations, in particular the GDPR and the EHDS Regulation, aim to achieve admirable objectives in the field of healthcare. Nevertheless, we would like to examine the potential difficulties involved in implementing these standards.

a. Circulation and Protection: An Impossible Reconciliation?

The GDPR seeks to strike a balance between the individual's right to data protection and privacy and the collective interest in the (re)use of personal data. Similarly, the EHDS Regulation and

25 EHDS Regulation, Recital 2.

26 For more information, see https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en.

27 Y. Tolias, « Des données de santé à la fourniture de soins : comment l'IA, le Règlement IA et l'EHDS façonnent l'avenir des soins de santé », *Espace européen des données de santé et IA. Enjeux juridiques et défis de mise en œuvre* (Dir. N. De Grove-Valdeyron), Toulouse, Presses de l'Université Toulouse Capitole, 2025, p. 13; D. Spajić, « Transforming the secondary use of patient data in the European Health Data Space: A challenge for the patient's right to medical confidentiality ? », *The European Health Data Space: Examining A New Era in Data Protection*, 1st ed., Routledge, 2025, p. 88.

28 S. Slokenberga, S., K. Ó Cathaoir and M. Shabani, *op. cit*., p. 3.

29 Y. Tolias, *op. cit.,* p. 26.

the AI Act aim to ensure the reliability of digital technologies while promoting their use and development.[30] These ambitious and promising objectives may be difficult to achieve in the medical sector, where the patient-doctor relationship is based on one fundamental pillar: trust.[31] How can this trust be maintained given the tension between data protection – and therefore minimization – and openness to data sharing, particularly 'across borders' within the European area?

In this regard, improving the availability of health data and facilitating access to it has not been an easy task for European legislators.[32] Indeed, there has been discussion of the impact of the GDPR on the EHDS Regulation with regard to the secondary use of health data.[33] For the sharing and use of personal data for scientific research purposes in the field of health, the GDPR requires the implementation of appropriate safeguards to protect the rights and freedoms of data subjects.[34] These safeguards must ensure the establishment of technical and organizational measures, in particular to ensure compliance with the principle of data minimization.[35] In this regard, it is stipulated that the EHDS Regulation provides a legal basis in accordance with the GDPR for the secondary use of electronic personal data, including safeguards allowing the processing of special categories of data.[36] Furthermore, it indicates the desire to 'ensure a high level of data protection, security, confidentiality and ethical use *[...]*'.[37] Despite these commitments and safeguards, will it really be possible, in practice, to reconcile the protection of individuals' data while allowing innovation, which thrives on large amounts of data, to flourish?

Let's take a concrete example: a patient's right to access their data. In order to effectively exercise this right, the data subject must obviously be allowed to access their data when they request it, as required by the GDPR. With the adoption of the EHDS, this data will be consulted and potentially reused, and it is equally important that the data subject is also informed of these actions concerning their data. In this way, the person will be able to make an informed decision about the use of their data and, if they so wish, exercise their right of access. This approach makes it possible to give concrete expression to this right of access, strengthen patient confidence in the medical profession and ensure that patients obtain and, above all, exercise the guarantees granted to them.

b. Fragmentation of Systems and Legal 'Lasagna'

Within the European Union, data protection rules are now part of a broad and complex legal framework, creating a risk of legal 'uncertainty' around data in several sectors, including healthcare. Furthermore, it should not be forgotten that the governance of research data falls within the competence of the Member States. The latter have a high degree of autonomy in drafting laws that determine who, based on the legal grounds prescribed by the GDPR, and in what circumstances, access to health data should be granted. Therefore, despite the adoption

30 H. Kranenborg, *op. cit.*, p. 17.
31 D. Spajić, *op. cit.*, p. 101.
32 S. Slokenberga, S., K. Ó Cathaoir and M. Shabani, *op. cit*., p. 3.
33 Ibid.
34 GDPR, Articles 89 §1 & 9 §2, point j).
35 M. Kogut-Czarkowska and M. Shabani, « Federated networks and secondary uses of health data: Challenges in ensuring appropriate safeguards for sharing health data under the GDPR and EHDS », *The European Health Data Space: Examining A New Era in Data Protection*, 1st ed., Routledge, 2025, p. 88.
36 Required under Article 9 §2, points g) to j) GDPR.
37 M. Kogut-Czarkowska and M. Shabani, op. cit., p. 235; EHDS Regulation, Recital 4.

of regulations such as the EHDS, differences between Member States' healthcare systems may complicate the harmonization of health-related aspects. In this regard, in the field of health as elsewhere, it is crucial, from the legislator's point of view, to ask whether the rules and means put in place are truly adapted to the realities on the ground (difficulty of application, comprehension, etc.). Indeed, the law can sometimes be perceived as a complex 'legal lasagna' that is difficult to understand for those who are required to comply with and apply it.

To promote innovation in the healthcare sector, will the EHDS Regulation, combined with other instruments such as the GDPR and the AI Act, succeed in overcoming all these obstacles? Only time will tell. In any case, they have the merit of illustrating the European legislator's desire to be at the heart of innovation by supporting its development, while not neglecting citizens and their rights.

IV. Conclusion

In the era of digital medicine, building patient confidence in a new system over which they have no control remains a major challenge. While the European regulatory arsenal and technical architecture lay the groundwork for a solid framework, their complexity can lead to misunderstanding and mistrust. In the future, it will be necessary to ensure clearer implementation, effective access to rights for patients, and more transparent data governance. This major challenge is twofold: preserving individual freedoms while allowing medical innovation to develop. This fragile balance calls for constant vigilance and open dialogue between all stakeholders, healthcare professionals, technology specialists, and lawyers.

ABOUT THE AUTHORS

Élise Degrave

Élise is a professor at the UNamur's Faculty of Law, the head of the E-government research team at Namur Digital Institute (Nadi/Crids), and a co-director of the E-government Chair at the University of Namur. She holds a PHD in Legal Sciences from the University (2013) with her thesis published by Larcier with reference to e-government and protection of privacy. Élise's research now focuses on the usage of personal data by the State, Digital Social Inequalities (Digital Device), automations of citizens' rights and control, as well as transparency of the Public Sector algorithm.

Olga Thiry

Olga is a research assistant at the Faculty of Law at the University of Namur (Belgium). She is a member of the Namur Digital Institute (section CRIDS) as well as the e-Government research team at the Namur Digital Institute.

COMPLIANCE AND RISK MANAGEMENT OF AI SYSTEMS IN INSURANCES

Osiris Moukoko Priso

I. Introduction

On 19 February 2020, the European Commission published a White Paper on Artificial Intelligence (AI), along with a report addressing the implications of artificial intelligence, the Internet of Things, and robotics on safety and liability. Following extensive debates among Member States and European institutions, Regulation (EU) 2024/1689 of the European Parliament and of the Council, establishing harmonized rules concerning artificial intelligence,[1] was published in the Official Journal of the European Union.

This regulation introduces a risk-based framework, imposing differentiated obligations on AI providers and users, while complementing existing regulatory instruments, 'such as the General Data Protection Regulation (GDPR), data protection law, insurance law, and intellectual property law'. As such, purely "*internal*" AI systems do not present the same level of sensitivity or risk as AI systems used for evaluating the creditworthiness of individuals or assessing risk within the context of mutual and health insurance.

This article aims to outline the key challenges and legal principles relevant to the insurance sector, and to propose an initial compliance methodology—particularly in light of the many parallels and convergences among the various European regulatory frameworks.

II. The Legal Framework of AI Systems: Principles and Challenges for the Insurance Sector

While the new AI Regulation introduces additional obligations for all economic stakeholders, the insurance sector must delineate which algorithms fall within its scope **(2.1)**, taking into account the intended purposes of these algorithms to determine the applicable obligations **(2.2)**, and ensure that the use of AI remains consistent with data-related obligations, particularly those concerning personal data **(2.3)**.

Scope and Limitations of the AI Regulation

Legal distinction between algorithm and AI System - The definition set out in Article 3 of the AI Regulation states that an artificial intelligence system is "*an automated system designed to operate with varying levels of autonomy and that may demonstrate adaptability after deployment, and which, for explicit or implicit objectives, infers from the inputs it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*."

Recital 12 of the AI Regulation further clarifies that "*[...] the definition should be based on the essential characteristics of AI systems that distinguish them from software systems or simpler traditional programming approaches and should not encompass rule-based systems that execute operations solely as predefined by natural persons. A key feature of AI systems is their capacity for inference, which includes training, a degree of independence from human action, and functioning without intervention*."

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence.

In practical terms, this leads to two guiding questions: does the algorithm autonomously produce its own operational rules, and is it capable of generating outputs? If the answer is affirmative, any insurance provider utilizing such algorithms will be subject to the obligations outlined in Chapters III, IV, and V of the AI Regulation. Ultimately, this legal distinction determines whether or not a significant portion of the regulation, particularly the provisions concerning high-risk AI systems,[2] will apply.

Provider and deployer, roles and obligations - The scope of this regulation is broad. It applies to all providers or "deployers" whose AI systems are marketed, used, or manufactured within the European Union.[3] Any natural or legal person, whether public or private, may fall under the category of provider or deployer of an AI system. A provider,[4] is defined as the natural or legal person who places an AI system on the market, as understood under EU law. A deployer is the entity that uses the AI system within the context of a professional activity.[5]

For the insurance sector, these definitions are critical, as they determine the extent of their compliance obligations.

Three scenarios may be identified:

- You are a **provider**: you are required to supply, among other things, the technical documentation 'Article 11 and Annex IV', as well as any other applicable obligations, particularly those related to high-risk AI systems.
- You are a **user**: who has supplied data to a provider who developed an AI system on your behalf: you are similarly required to obtain this technical documentation and cooperate with the provider to ensure regulatory compliance.
- You are a **deployer**: you must request access to the technical documentation and comply with the obligations set out in Article 26.

The potential liabilities vary according to these roles, but may also be cumulative:

- For example, a **provider-insurer** may incur non-contractual liability for breach of obligations related to the development of a high-risk AI system under the AI Regulation. These include documentation and compliance obligations, particularly under Article 16, and primarily concern the system's design and training phases prior to market placement;

2 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence.

Article 6:

***"1.** An AI system that is placed on the market or put into service, whether or not it is independent of the products referred to in points (a) and (b), shall be considered high-risk when the following two conditions are met:*

***(a)** the AI system is intended to be used as a safety component of a product covered by the Union harmonization legislation listed in Annex I, or the AI system itself is such a product;*

***(b)** the product whose safety component referred to in point (a) is the AI system, or the AI system itself as a product, is subject to third-party conformity assessment with a view to being placed on the market or put into service, pursuant to the Union harmonization legislation listed in Annex I.*

***2.** In addition to the high-risk AI systems referred to in paragraph 1, the AI systems listed in Annex III shall also be considered high-risk."*

3 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 2.

4 Ibid.

5 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Recital 13.

- A **deployer-insurer** may face contractual liability towards policyholders for issues arising from the use of a high-risk AI system, 'e.g., unintended discrimination, system error, consequences of unlawful decisions' under Article 1217 of the French Civil Code, or non-contractual liability under Articles 1242 and 1245;[6]
- A **deployer-insurer** may also seek contractual redress from the provider, and vice versa, under Article 26, which obliges the deployer to implement appropriate technical and organizational measures, monitor the system, and use it in accordance with the technical documentation provided by the provider.

It is therefore essential for the compliance and legal teams to clearly define roles and associated risks for internal use.

The Central Role of AI System Purposes in the Risk Classification Framework

For all insurance stakeholders, particularly providers and deployers, the regulation establishes a classification of AI systems based on the level of risk they pose to society. The four categories are: unacceptable risk systems,[7] high-risk systems, limited-risk systems,[8] and minimal-risk systems. This classification entails the application of various obligations related to control, documentation, and transparency. According to Chapters II and V of the regulation, which detail the obligations specific to AI systems, the intended purpose is the key criterion for distinguishing among the legal regimes applicable to each category.

Specifically, Article 6 of the AI Regulation stipulates that certain systems may be designated as high-risk by the Commission, and Annex III enumerates those that are automatically considered as such. From an insurance perspective, identifying the purpose of a system is critical. On the one hand, this means that not every algorithmic system or AI system implemented by an insurance company is automatically classified as high-risk. Some internal systems may fall under the limited-risk or minimal-risk categories. On the other hand, this implies that within the insurance domain, the following systems will be considered "high-risk":

- AI systems are intended for assessing the creditworthiness of individuals or establishing their credit score, excluding those used for detecting financial fraud.
- AI systems are intended for risk assessment and pricing in the context of life and health insurance for individuals.

Just as identifying an entity's role along the AI system value chain is important, defining the intended use of AI systems is equally vital for determining applicable obligations. If acting as a provider, the entirety of Chapter III of Regulation (EU) 2024 applies to the AI systems deployed in this context, 'e.g., AI systems used in credit insurance, life insurance, mutual insurance, or health insurance'. For insurers acting solely as deployers, as defined by Article 2 of the AI Regulation, they must comply with the provisions and obligations outlined in Articles 14, 26, and 27, which include human oversight, technical and organizational measures, logging requirements, Data Protection Impact Assessments (DPIA), and fundamental rights impact analyses.

6 "Liability for defective products" under the French Civil Code, Articles 1245 et seq.
7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 5.
8 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 50.

In summary, the regulation requires stakeholders to control the risks associated with deploying such technologies, to clearly prohibit uses that involve unacceptable levels of risk as defined by law, and to impose risk management obligations on providers and, 'in some cases, 'deployers' of all other AI systems.

The Challenge of Data Usage by Insurers within AI Systems: A Delicate Coordination between the AI Regulation and Other Legal Frameworks

The interplay between the GDPR and the AI Regulation is a major issue in the deployment of AI systems. As a reminder, Articles 5, 6, and 9 of the GDPR govern the processing of personal data, regardless of its use. Insurance companies are subject to this framework and must, in particular, define robust and legitimate purposes, establish a legal basis as per Article 6, process only data necessary to achieve those purposes, and, where applicable, rely on a derogation from the general prohibition on processing sensitive data.[9] Among the key concerns for insurance companies are the use of sensitive data and compliance with the principle of data minimization.

Regarding the use of sensitive data, it is important to recall that derogations from the prohibition are only permitted under specific conditions. Among these, three are particularly relevant :

1) Consent,
2) Reasons of substantial public interest,
3) Processing is necessary for compliance with obligations or the exercise of rights in the field of employment law.

In principle, relying on consent is risky, as it must be specific, informed, unambiguous, and most importantly, freely given. Courts generally interpret this requirement with reference to the absence of harm in the event of refusal,[10]—an argument difficult to uphold if the data is used by an AI system assessing risks 'e.g., risk of non-payment, health risk', and which may result in a denial 'e.g., refusal to grant an insurance contract for a loan', thus constituting an automated decision-making process. In the case of non-mandatory insurance, or even mandatory insurance that does not constitute a right, consent cannot be validly used, except potentially during the training phase of the AI.

On the other hand, the other two derogations could be used by insurers:

- First, reasons of substantial public interest, which, according to Recital 52, must and can be provided for by Union or national law. In this respect, Annex III of the AI Regulation clearly implies that access to complementary social coverage or insurance qualifies as a "right to essential private services and public services and social benefits," and is thus of particular importance.
- Second, with regard to employment-linked health mutuals, the justification of fulfilling obligations of the data controller under employment law appears equally relevant and appropriate. Specifically, Article L.911-1 of the French Social Security Code, which mandates the selection of a supplementary health mutual by employees, should

9 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, Article 9.

10 Conseil d'Etat, November 4, 2020, n°432656, *La Quadrature du Net.*

constitute an exception applicable exclusively to mutual insurers—a view shared by the CNIL.[11] However, the CNIL considered that outside this mutual insurance context, the legal framework remains insufficient. Such a perspective paradoxically suggests that data only constitutes a matter of substantial public interest when used within the scope of an AI system.[12]

In addition, these requirements must be reconciled with those established by French domestic law. Articles L.111-7 and L.111-8 of the Insurance Code establish a prohibition on discrimination on grounds such as 'sex, pregnancy, and certain health data', supplemented by provisions of the AERAS Convention for specific situations, 'loans, mutual insurance'. Furthermore, mutual insurance providers are prohibited from collecting or using medical information under Article L.112-1 of the Mutuality Code.

Ensuring compliance with the principle of non-discrimination is therefore crucial. To this end, Article 10 of the AI Regulation specifically authorizes the use of sensitive data—under Union law—as defined in the GDPR, to prevent discrimination. This derogatory purpose enables insurers and mutuals to ensure that their AI systems do not unintentionally produce biased outcomes and, importantly, allows for corrective measures to prevent such biases.

Beyond these theoretical considerations, we propose a practical compliance methodology for high-risk AI systems and the data they process. Obligations under the Data Act are not addressed in this section.

III. Methodology and Recommendations for Compliance Implementation

From a practical standpoint, ensuring compliance involves addressing three key areas: the responsibility borne by the insurance provider throughout the various phases of the AI system's lifecycle; the handling and governance of data used within the AI system; and, finally, how to guarantee transparency and control over the system from the users' perspective.

The goal of this compliance process is to prevent any non-compliance risks—whether arising from internal inaction, poor coordination between the Data Protection Officer (DPO), legal department, Chief Information Security Officer (CISO), and IT department, or a lack of clarity regarding the respective roles of providers and deployers.

Identifying the Entity's Role

The first step is to determine whether the organization qualifies as a provider or a deployer. As a reminder, Article 3 of the AI Regulation defines a provider as "a natural or legal person, public authority, agency, or other body that develops or has developed an AI system or a general-purpose AI model and places it on the market or puts it into service under its own name or trademark, whether for a fee or free of charge"—in other words, the party responsible for designing the AI system.

11 CNIL, legal analysis addressed to supplementary health insurance providers, [online], consulted on August 4, 2025, https://www.cnil.fr/sites/cnil/files/atoms/files/analyse_juridique_adressee_aux_organismes_de_complementaire_sante.pdf.

12 The combined reading of Article 10(5)(2) of Regulation (EU) 2024 and Annex III of Regulation (EU) 2024 only addresses data in the context of an AI system.

Conversely, a deployer is defined in the same article as "*[…] a natural or legal person, public authority, agency, or other body using an AI system under its own authority, except when the system is used in the course of a purely personal, non-professional activity*." The deployer is the entity that uses the high-risk AI system in a professional context and makes it available to employees, agents, or volunteers.

This classification may also result from a risk and liability mitigation strategy. Three cases may be distinguished:

- The insurance company commissions a firm to develop a high-risk AI system, which it then uses itself—it is considered a **deployer**.
- The insurance company designs and develops a high-risk AI system in-house, which it then uses—it is both **provider** and **deploye**r; if it does not use the system but sells it or makes it available to subsidiaries, it is the provider, and the subsidiaries are **deployers**.
- The insurance company commissions a firm to develop a high-risk AI system, but provides the training or test data—in this case, it is a **deployer**, but must also comply with principles governing the use of training or test data, or ensure their correct application.[13]

The key issue is understanding the legal obligations likely to apply to the company, particularly if the regulatory provisions are triggered.

Distinguishing the Types of Algorithms Used

The use of algorithms or mathematical formulas is already common in the insurance industry 'e.g., among actuaries and statisticians'. It is therefore crucial to assess whether and how such activities fall within the scope of the AI Regulation. In this regard, reference to Article 3 and Recital 13 is essential. It is necessary to assess whether the algorithms in use are capable of inference as defined by the Regulation—that is, whether they can modify their own rules in order to generate the most appropriate outcome.

Here are two illustrative examples:

- A model involving predictive analysis of future claims based on mixed data, 'e.g., clients and others': if the training data enables the algorithm to infer and refine its own rules, the system is subject to the high-risk AI regime.

A well-known mathematical model applying fixed weightings to multiple client data points and merely executing predefined human rules qualifies as an algorithm under the law but is not subject to the AI Regulation.

Classifying Data Sets and Their Relationship to AI Systems

Pursuant to Article 3 of Regulation (EU) 2024/1689, training data,[14] testing data,[15] and validation,[16] data must be distinguished, as must the data used within the AI system itself. These data sets may

13 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 10.

14 The data used to provide an independent evaluation of the AI system in order to confirm the expected performance of that system prior to its placing on the market or putting into service.

15 The data used to evaluate the trained AI system and to set its non-trainable parameters as well as its learning process, notably to avoid underfitting or overfitting.

16 The data used to train an AI system by adjusting its trainable parameters.

include customer or prospect data, data purchased or shared from a partner, or data obtained through research—each subject to a variety of applicable legal frameworks, 'AI Regulation, GDPR, and Intellectual Property Code'.

This classification is crucial for determining the applicability of Article 10 of Regulation (EU) 2024/1689 and identifying who bears the associated obligations. Article 10 establishes a data governance system requiring documentation of design choices, data collection processes, processing operations used in data creation and enrichment, and bias assessment procedures. In other words, it concerns the role and handling of data within the AI system. In some cases, testing data may fall outside the IT system itself; in such cases, even as a deployer, an insurer may be subject to some obligations normally assigned to AI providers during the system design phase.

To better address the documentation requirements and the interplay between various legal frameworks 'AI law, intellectual property, personal data, insurance law, and anti-discrimination provisions', the following classification of data sets is recommended:

- Data sets used in the context of high-risk AI systems—that is, data involved in the various phases of high-risk AI systems;
- Test data sets, as defined by the regulation;
- Other data sets—that is, those never used at any stage of a high-risk AI system.

Ensuring Compliance in the Use of Data, Including Personal Data

This point follows logically from the previous one. Across all datasets, personal data in particular must be protected.[17] Accordingly, each "data controller" under the GDPR must, at a minimum, complete a processing record, inform individuals of the processing purpose, and ensure mechanisms are in place for exercising data subjects' rights.

The data controller must also ensure the following:

- **Compliance with the principles of lawfulness and data minimization**,[18] and, where applicable, documentation of the chosen legal basis—whether legitimate interest or consent—depending on which appears most appropriate. This entails refraining from using data that is not strictly necessary for the processing purpose, and questioning whether the use of AI is justified compared to a less intrusive system. Furthermore, the invocation of legitimate interest must account for specific obligations in the insurance context, including compliance with anti-discrimination prohibitions, whether stemming from national law or the AI Regulation, 'e.g., bias correction'.[19] Consent, for its part, may only be relied upon if it is clear, unambiguous, and—above all—freely given.[20]

17 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, Article 3.

18 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, Articles 5-6.

19 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 10.

20 Conseil d'Etat November 4, 2020, n°432656, *La Quadrature du Net.*

- **Refusal to consent** must not result in any detriment to the data subject. This implies that insurers should only process the data of individuals who have freely and unequivocally agreed to such use. The use of "contract performance" as a legal basis is excluded, as it is difficult to justify why training data for AI would be necessary to perform an insurance contract, especially since such contracts have existed for over a century without AI.
- **Data minimization** will be challenging to implement, particularly in cases of full dataset collection.[21] Even when relying on legitimate interest, the full collection of personal data groups should be avoided unless it can be duly justified, 'e.g., demonstrating why data on users aged 25–40 or over 60 is relevant';
- **Guaranteeing the exercise of rights** by implementing prior notice, an opt-out mechanism to prevent unwanted processing, and the possibility for rectification. The CNIL also recommends the implementation of technical data tracking measures to ensure effective data erasure;
- **Ensuring individual awareness** through technical documentation, particularly to justify, if applicable, the impossibility of re-identifying individuals once training data has been integrated into the AI system;
- **Clearly defining the processing purpose**, especially when sensitive data is used for bias correction. In such cases, the use of personal data must comply not only with Article 9 of the GDPR, but also with Article 10(5) of the AI Regulation, which requires that the data be strictly necessary to control the risks associated with high-risk AI systems.
- **As documentation responsibilities** fall on the data controller, they must be ensured by the provider during the system design phase, and subsequently by the deployer during the system's operational phase.

Document the compliance of High-Risk AI System

It is the responsibility of operators—particularly AI system providers—to ensure compliance with the principle of control over AI systems, including through the following actions:

- **Implementing a risk management system**,[22] that is, conducting a thorough and continuous analysis and update of the AI system. This includes identifying and analyzing known or reasonably foreseeable risks, evaluating the consequences of reasonably foreseeable misuse, assessing other potential risks, and adopting measures capable of mitigating known and foreseeable risks. The objective is to perform a "*permanent*" and "*iterative*" risk assessment that ensures risk levels remain acceptable in light of the AI system's intended purposes, and to eliminate risks wherever possible;

21 CNIL, Deliberation SAN-2024-014, September 26, 2024, paragraphs 49 to 77 ; CNIL, Deliberation SAN-2023-008 ; CNIL, Deliberation SAN-2020-003.

22 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 16.

- **Adopting a governance system for training data** that respects privacy,[23] and mitigates bias;
- **Establishing a comprehensive compliance documentation set**, including a technical document that demonstrates compliance with regulatory requirements and describes the AI system,[24] an operational manual intended for deployers, and technical and organizational measures, 'such as human oversight, action traceability within the AI system, and adequate security guarantees aligned with other European frameworks, including the GDPR';
- **Ensuring the completion of a fundamental rights impact assessment** for high-risk AI systems. This requirement applies to entities delivering public services, banks, and insurance providers. The goal is to assess the risks such systems may pose to the fundamental rights of individuals,[25] similar to the Data Protection Impact Assessment (DPIA). Some elements of these two analyses may overlap;
- **Guaranteeing human oversight** of the high-risk AI system, and when personal data is involved, complying with Article 22 of the GDPR—particularly in cases involving automated decision-making. This includes providing an explanation of how the algorithm works and offering possible redress mechanisms;
- **Providing a user manual** supplied by the AI system provider to guide deployers in its proper use.

IV. Conclusion

The evolving European regulatory framework for artificial intelligence (AI), particularly under Regulation (EU) 2024/1689, introduces a paradigm shift for the insurance sector. It compels both AI providers and deployers to adopt a proactive, structured approach to compliance. At the heart of this regulation lies a risk-based classification system, where AI systems are evaluated according to the societal risks they pose, ranging from minimal to high-risk. For insurance actors, AI systems related to creditworthiness assessments or life and health insurance pricing are often deemed high-risk, triggering the full scope of regulatory obligations. Understanding one's role—whether as a provider, deployer, or hybrid actor—is a prerequisite for compliance. This determination governs the allocation of duties concerning documentation, transparency, risk management, and accountability. Moreover, distinguishing between simple algorithms and AI systems capable of autonomous inference is critical in identifying regulatory applicability. A central challenge lies in the lawful and ethical use of data.

The intersection of the AI Regulation with the GDPR, along with national laws (such as the French Insurance Code and Mutuality Code), requires insurers to navigate sensitive issues, including data minimization, legal basis for processing (consent or legitimate interest), and the use of sensitive data for bias correction. Data governance must extend beyond technical design to include privacy preservation and non-discrimination safeguards. Practical compliance steps

23 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 10.
24 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 11.
25 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, Article 27.

must include classification of data sets (training, testing, operational), robust documentation, and the implementation of mechanisms ensuring data subject rights. Importantly, providers must establish iterative risk management procedures, document their systems extensively, and ensure human oversight throughout the AI system's lifecycle. In sum, compliance with AI regulations is not merely a legal necessity but a strategic imperative for the insurance industry. It demands interdisciplinary coordination, technical vigilance, and a commitment to fundamental rights. Ensuring transparency, accountability, and risk mitigation is not only essential to regulatory alignment but also critical to maintaining trust in AI-driven insurance practices.

ABOUT THE AUTHOR

Osiris Moukoko Priso

Senior Consultant

Osiris Moukoko Priso is a Legal & Compliance Manager and Data Protection Officer at Numéricité, leading a team that has supported over 100 startups and public institutions in building agile, GDPR-compliant digital solutions. A recognized expert in digital, AI, and data protection law, he has worked internationally with Expertise France and the World Bank, delivering comparative legal studies on data, AI, and digital transformation across Africa and Asia. As a lecturer and speaker, he shares a forward-thinking vision of ethical and innovative digital governance that empowers organizations and protects citizens.

LAW IN THE LOOP: GOVERNING EHEALTH PLATFORMS IN CAMBODIA

Sor Samnangvathana

Yean Solina

Simon Burlinson

Dr. Elias J. Engelking

I. Introduction: From Legal Lag to Legal Leadership

Cambodia's healthcare system is experiencing a rapid digital transformation, spearheaded by eHealth platforms such as Peth Yoeung and MeetDoctor. These platforms serve approximately 500 health facilities nationwide, spanning public hospitals, private clinics, and primary care centers, which equate to approximately 80% of the private market. By integrating end-to-end functions—electronic health records, digital prescriptions, logistics for pharmaceuticals, and payment workflows—these digital intermediaries have evolved into core providers of health services rather than mere IT tools.

Although Cambodia's Digital Health Strategy 2024–2035,[1] acknowledges this shift, the nation's enabling statutes and sub-decrees remain anchored to analog assumptions: healthcare facilities are physical structures, providers are exclusively human, and services flow through brick-and-mortar institutions. This disconnect between statutory architecture and digital reality is a common feature of emerging economies, but it is not immutable.

Across ASEAN, innovative regulatory models demonstrate how law can serve as a proactive catalyst for safe, trusted, and rapid innovation. Singapore's modular licensing regime for healthcare services,[2] Malaysia's national AI governance sandbox for healthtech,[3] and Indonesia's ehealth regulatory sandbox,[4] illustrate how regulatory agility and robust safety standards can coexist, particularly in cybersecurity, smart hospital infrastructure, and AI-driven clinical workflows. These examples show that legal frameworks can underwrite, not undermine, technological progress.

Rather than viewing Cambodia's current legal inertia as a unique hindrance, this article situates the country within a broader regional transition. We argue that Cambodia can move beyond reactive legislation by introducing culturally grounded, data-driven legal innovations that set standards, ensure accountability, and strengthen public trust in digital health. The objective is not merely to catch up, but to position Cambodian law as a strategic asset, guiding the healthcare sector toward sustainable, inclusive digital leadership.

Legal Gaps in the Current Framework

Digital Health Platforms (DHPs) no longer just link the clinician and patient. They orchestrate an entire value chain that stretches from upstream data donors and AI developers to downstream payors and public regulators, with cloud hosts, diagnostics labs, and third-party plug-ins in between. Each actor performs a discrete function—data curation, model training, workflow integration, clinical adoption, or financial settlement—yet their actions converge in a single point-of-care decision. When something goes wrong, liability is therefore seldom traceable to a single node; it propagates along the chain.

1 Ministry of Health. (2024). "*Digital Health Strategy 2024–2035*". Phnom Penh: Ministry of Health.
2 Government of Singapore. (2020). *Healthcare Services Act 2020*.
3 Malaysia Digital Economy Corporation, "*National Artificial Intelligence Roadmap 2021-2025*", Cyberjaya, 2021, available at: https://dig.watch/resource/malaysia-national-artificial-intelligence-roadmap-2021-2025 [last accessed - August 5, 2025].
4 Ministry of Health of Indonesia. (2022). *Regulation No. 24/2022 on Digital Health*. Jakarta: Government of Indonesia.

A. Absence of Platform Licensing Law

Cambodia's current legislation licenses individual health professionals,[5] yet remains silent on DHPs—becoming the setting where AI assistants routinely act as "*co-clinicians*," triaging symptoms, drafting prescriptions, and even initiating insurance claims. This unresolved classification leaves regulators without a basis to decide (i) whether a platform must register with the Ministry of Health (MoH), (ii) what technical and clinical standards must be met before AI-mediated care goes live and (iii) which sanctions apply when algorithmic or system failures cause patient harm—while the disciplinary measures in Article 15 of the 2016 Law,[6] still apply only to natural persons.

Comparative jurisdictions have moved ahead: Singapore's Healthcare Services Act 2020,[7] creates a risk-tiered licensing system that escalates obligations in line with the potential harm posed by each digital service.[8] Cambodia's lack of an equivalent instrument blurs whether an eHealth platform assumes provider-level duties of care or merely the intermediary responsibilities set out in the E-Commerce Law 2000.[9] This Article outlines a light-touch accreditation pathway (in Section 3 below) that could serve as a transitional solution while a dedicated licensing decree is prepared.

B. Data Stewardship and Patient Agency

The final version of the Draft Law on Personal Data Protection (LPDP),[10] designates health information as sensitive personal data and requires explicit, revocable consent before any processing. Article 32 grants individuals a right to data portability, while Article 20 obliges controllers to adopt appropriate security safeguards. Yet DHPs currently can store and analyse medical records without the MoH guidance on how to fulfil these obligations in practice.

- Consent capture: in Cambodia's mobile-first yet low-literacy landscape, workable consent may need to be both understandable and revocable. Approaches such as voice-prompt flows in Khmer or a simple "*tap-to-withdraw*" button could be considered; exploratory piloting would help determine whether patients fully understand the implications and can act without assistance. Such approaches would help satisfy the LPDP's requirement under Article 8 for explicit, revocable consent.
- Data portability: the right to obtain and transfer one's health data will remain largely theoretical unless export tools match local bandwidth conditions and handset capabilities. Early ideas include letting users quickly download their health data either as a standardized FHIR file or a simple PDF summary. Similar to the U.S. Blue Button initiative. Further dialogue could examine practical aspects such as file-size limits and which clinical data elements might warrant prioritisation. Facilitating such transfers would operationalise LPDP Article 32 on data portability.

5 Law on Regulation of Health Practitioners, NS/RKM/1116/014, Cambodia, Articles 7–11.
6 Law on Regulation of Health Practitioners, NS/RKM/1116/014, Cambodia, Article 15.
7 Healthcare Services Act 2020, Singapore, Part 2, ss. 9-9A.
8 OECD, "*OECD Regulatory Policy Outlook 2021*", Paris, 2021, pp. 183 – 196, (arguing that tiered obligations allow regulators with limited capacity to focus supervision on the highest-harm services) available at: https://doi.org/10.1787/38b0fdb1-en [last accessed – 26 May 2025].
9 Law on Electronic Commerce, NS/RKM/1119/017, Cambodia, Article 24.
10 Draft Law on Personal Data Protection, "Final Version", Cambodia, dated 23rd June 2025.

- Patient dashboards: a bilingual dashboard (Khmer and English) might enable users to view, correct, or delete their records in real time, while complementary offline or assisted-access channels—such as community health-worker support or facility-based kiosks—could also be explored, especially for populations with limited digital or health literacy. Providing these functions could demonstrate practical compliance with LPDP Articles 8, 20, and 32.

International practice is moving from proprietary notions of data ownership toward a trust-infrastructure model based on stewardship, interoperability, and federated-learning architectures that keep raw data in-country while sharing only model parameters. The EU GDPR,[11] already allows for the operationalisation of data portability, for example, through API-enabled patient portals. Without a sector-specific *Prakas*, Cambodian platforms lack a blueprint for translating LPDP Articles 8, 14, and 32 into user-centred consent dashboards, structured data exports, and robust local-language interfaces.

C. Algorithmic Decision-Making and Legal Liability

DHPs increasingly embed Artificial Intelligence modules that screen symptoms, suggest differential diagnoses, optimise imaging workflows, or generate draft prescriptions. As these systems evolve from isolated tools to agentic services—running continuously and autonomously across multiple points of care—questions of who is liable when an algorithm harms a patient become acute.

Cambodia presently lacks any statute or *Prakas* assigning responsibility among developers, clinicians, platform operators, and data controllers when AI outputs prove erroneous. Existing provisions on professional negligence (e.g., Law on Regulation of Health Practitioners)[12] assume a human decisionmaker; the E-Commerce Law-,[13] covers content intermediaries, not medical algorithms. Consequently, patients and platforms alike face legal uncertainty. Because algorithmic outputs ripple through multiple decision points—from triage to imaging to prescribing—any governance solution must adopt a systemic, rather than incident-specific, view of liability.

Comparative reference points

- **European Union**: the AI Act 2024,[14] classifies health-related AI systems as high-risk- (Annex III). It layers mandatory safeguards—transparency, human oversight (Article 14), postmarket monitoring (Article 72) on top of the general product safety law.
- **Singapore**: the Artificial Intelligence in Healthcare Guidelines (MOH & Synapxe — formerly IHiS, Version 1.1, 2021) remain the only published healthcare-specific AI rules; however, Singapore's Health Sciences Authority introduced a 2024 Change Management Programme for AI/Software Medical Devices,[15] signalling a move toward lifecycle oversight and risk tiering.

11 General Data Protection Regulation (EU), 2016/679, European Union, Article 20.
12 Law on Regulation of Health Practitioners, NS/RKM/1116/014, Cambodia, Article 15.
13 Law on Electronic Commerce, NS/RKM/1119/017, Cambodia, Article 24.
14 AI Act 2024 (EU), 2024/1689, Annex III; Articles 14 & 72.
15 Health Sciences Authority, "*Medical Device Guidance GN-37: Change Management Program (CMP) for SaMD, including Machine-Learning-Enabled SaMD*", Singapore, 2024, available at: https://www.hsa.gov.sg/docs/default-source/hprg-mdb/regulatory-updates/industry-briefing-on-cmp-for-samd_slides.pdf [last accessed – 26 May 2025].

- **United States:** the FDA "*Predetermined Change Control Plan*" concept allows continuous learning- software while keeping a licensed clinician "*in the loop*."[16]

These frameworks illustrate two emerging principles: (i) graded obligations that escalate with clinical risk and (ii) systemic accountability that extends beyond a single algorithm to the entire care pathway.

Issues for exploration in Cambodia

- **Defining human oversight:** in a mobile-first system where triage suggestions are auto-inserted into the clinician's queue, what constitutes meaningful oversight? Is a quick onscreen check sufficient, or must the doctor actively interrogate the model's reasoning?
- **Attributing fault:** harm may arise at any link of a Digital Health Platform's multisided value chain: a developer writes flawed code; a data supplier uploads biased training sets; the platform configures the model incorrectly; a clinician accepts the suggestion uncritically; or an insurer automates claims based on biased algorithms. Given this chain of embedded decisions, any future liability regime will need mechanisms—joint and several or proportionate—to allocate responsibility across all participating actors, rather than isolating the clinician or the platform alone.
- **Post-deployment monitoring**: without a national incident-reporting register for AI errors, systemic faults could go undetected. A MoH *Prakas* could invite platforms to submit periodic safety and bias audits, borrowing the post-market monitoring logic from the EU.

Invitation rather than prescription: policymakers might explore a graduated AI oversight regime—adapting LPDP data governance duties, leveraging existing clinical licensing structures, and piloting sandbox clauses for novel AI modules—before issuing a comprehensive liability statute.

D. Interoperability and Data Exchange Law

Cambodia's draft Cybersecurity Law defines health-related services as part of the nation's Critical Information Infrastructure (CII),[17] and assigns regulatory responsibility for such infrastructure to the relevant sector ministry.[18] Yet no statute or *Prakas* stipulates how DHPs should exchange clinical data in a safe, structured, and rights-preserving manner.

The National Digital Health Strategy 2023–2030,[19] calls for "*open APIs and common data standards*," but its recommendations are aspirational and non-binding. As a result, many public and private hospitals and clinics still exchange medical, laboratory, and imaging reports over Telegram; hospital information systems remain siloed; and emerging DHPs tend to build proprietary gateways—hindering continuity of care and fragmenting patient records.

16 U.S. Food and Drug Administration, "*Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan*", Silver Spring, MD, 2021, available at: https://www.fda.gov/media/145022/download [last accessed – 26 May 2025].
17 Draft Cybersecurity Law, Cambodia, Article 3(19).
18 Draft Cybersecurity Law, Cambodia, Article 9.
19 Ministry of Health, *National Digital Health Strategy 2023–2030*, Phnom Penh, 2023.

By contrast, Estonia's XRoad,[20] and the UK's NHS Spine,[21] operate under binding legal mandates that hard-wire standards such as HL7 FHIR into national infrastructure legislation. Singapore's National Electronic Health Record (NEHR),[22] and London's "*One London*" platform,[23] further show how middleware and federated APIs can bridge legacy systems while preserving patient control.

Ethical framing: interoperability is not merely a technical plumbing issue; it is an ethical pre-condition for data stewardship, continuity of care, and patient mobility. A legal framework that mandates baseline standards—while allowing incremental legacy integration—would anchor trust and prevent digital fragmentation.

Issues for exploration in Cambodia

- **Health-specific Interoperability Decree:** a MoH *Prakas* could codify a "*minimum technical baseline*" (e.g., FHIR R4 resources for demographics, encounters, and diagnostics), mirroring Estonia's legal reference to XRoad schema.
- **Certification Pathway:** platforms connecting to the national health network could be certified against that baseline, using a light-touch self-assessment plus external audit akin to the UK's NHS Digital "*Data Security and Protection Toolkit*."

II. Legal Innovations for Governing eHealth

Legal Instrument Options

Digital health is already here. What is missing is an enabling legal toolkit that can mature in step with clinical practice. The instrument below mirrors approaches that have proven workable elsewhere in ASEAN and could be adapted to Cambodia without waiting for an entirely new statute.

- **Interministerial *Prakas* on eHealth Platform Licensing:** a joint *Prakas* issued by the MoH and the Ministry of Commerce (MoC) could treat a digital platform as a "*health service intermediary*". This would clarify when a licence is required, which safety controls must be in place before launch, and how liability is shared when something goes wrong. A risk-tiered model—similar to Singapore's Healthcare Services Act Schedule 3—would scale obligations according to patient impact. The legal hook lies in the Law on Regulation of Health Practitioners (2016), Articles 12 and 24, read together with the Law on E-Commerce (2019), Articles 24 - 28.
- **Health Data Protection Guidelines under the LPDP:** once the LPDP is promulgated, the MoH could issue sector-specific guidelines that translate general duties into clinical practice. Key elements include layered consent flows, a default export format based on HL7 FHIR bundles, and a security baseline aligned with ISO 27799. These measures would operationalise LPDP Articles 7, 15, and 32 while giving smaller clinics ready-to-use templates.

20 *X-Road Act* (Estonia), RT I, 12.06.2015, 11, § 3.
21 *Health and Social Care Act 2012* (UK), s. 255.
22 Singapore Ministry of Health, "All Private Hospitals Commit to Enhancing Health Data Sharing for More Seamless Care Delivery," press release, Singapore, 9 Nov 2024, available at: https://www.moh.gov.sg/newsroom/all-private-hospitals-commit-to-enhancing-health-data-sharing-for-more-seamless-care-delivery [last accessed – 26 May 2025].
23 NHS Digital, "*Data Security and Protection Toolkit Guidance*", London, 2023, available at: https://www.dsptoolkit.nhs.uk/ [last accessed – 26 May 2025].

- **Health Sector-Cybersecurity Directive:** the draft Cybersecurity Law designates health services as CII and assigns the MoH as the competent regulator for health. A directive, developed with the Digital Security Committee at the Ministry of Posts and Telecommunications (MPTC), could adopt ISO 27799 (Health informatics — Information security management) as the baseline control catalogue and align with Singapore's Cybersecurity Code of Practice,[24] for CII (Healthcare), as well as Malaysia's Health Data Framework Baseline Controls. This would put a clear floor under platform security without prescribing a single technical architecture.
- **Code of Conduct on AI in Healthcare:** a profession-led code, endorsed by the MoH and the medical councils, could set expectations for explainability, documented human oversight, bias monitoring, and scheduled post-deployment audits. The document could draw on the EU AI Act (Annex III) and Singapore's AI in Healthcare Guidelines (2023),[25] while remaining light enough to update regularly. Because it is soft law, compliance could be made a condition for sandbox participation or for renewal of a platform licence.
- **Governance Mechanism for Cross-Ministerial Coordination:** all four instruments would benefit from a standing Joint Oversight Committee comprising the MoH, MPTC, MoC, and the Personal Data Protection Regulatory Committee. Regular reporting and an open consultation channel with industry associations would keep the regime adaptive and transparent.

Regulatory Sandboxes for Digital Health

In highly regulated sectors like health, traditional regulatory frameworks often struggle to adapt to emerging technologies. Regulatory sandboxes offer a pragmatic solution: they are controlled, time-bound testing environments that allow innovators to experiment with new digital health solutions under regulatory supervision. These environments may include temporary waivers and enable regulators to observe how innovations function in practice before making binding regulatory decisions. According to the World Bank,[26] regulatory sandboxes for digital health can facilitate early evidence generation, reduce time to market, and improve stakeholder trust by clarifying risks, benefits, and regulatory requirements. Well-designed- sandboxes let regulators and innovators learn together without exposing patients to unmitigated risk. Cambodia could embed such a mechanism in sub-legislation rather than waiting for an act of Parliament.

Legal Hook:

Law on Regulation of Health Practitioners (2016), Article 71 (c) empowers the MoH to authorise experimental service models by *Prakas*. A single Inter-ministerial *Prakas* on Digital-Health Sandboxes—co-signed by MoH, MPTC, and the Personal Data Protection Regulatory Committee—could therefore lawfully carve out a regulatory sandboxing regime for DHPs.

24 Cyber Security Agency of Singapore, "Cybersecurity Code of Practice for Critical Information Infrastructure (Second Edition)", Singapore, 2022, available at: https://www.csa.gov.sg/legislation/codes-of-practice [last accessed – 26 May 2025].

25 Ministry of Health & Health Sciences Authority, "Artificial Intelligence in Healthcare Guidelines (AIHGle)", Singapore, Edition 1.0, 2023, available at: https://isomer-user-content.by.gov.sg/3/9c0db09d-104c-48af-87c9-17e01695c67c/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf [last accessed – 26 May 2025].

26 World Bank Group, "Regulatory Sandboxes for Digital Health: A Tool for Safe Innovation in Health Technology Regulation", Washington, D.C., World Bank, 2025, pp. 2–4; 6–8 & 13, available at: https://documents1.worldbank.org/curated/en/099011825011040830/pdf/P175075-0c729174-1c7a-4f04-9bb2-4127f301c037.pdf [last accessed – 2 June 2025].

Core design parameters

1) **Clear public guidelines –** a published sandbox rulebook spells out objectives (*innovation vs. policy-focused*), eligibility, compliance duties, and entry/exit criteria.
2) **Limited scope & duration –** authorisation valid for 12–18 months, renewable once. The derogation covers licensing and certain advertising restrictions, but never malpractice or criminal liability.
3) **Mandatory data protection compliance –** participants must appoint a Data Protection Officer, file a Personal Data Impact Assessment under LPDP Article 19, and encrypt data to at least ISO 27799 standards.
4) **Supervisory oversight –** regular progress reports and the right for the MoH to suspend trials upon safety signals.
5) **Structured exit or scale-up –** clear decision gates at months 12 and 18: (a) graduate to a full eHealth platform licence; (b) extend under stricter conditions; or (c) terminate with mandatory data deletion.
6) **Public-private cocreation space –** every cohort includes at least one research institution or "*living lab*", mirroring the model used in Singapore's Telemedicine Regulatory Sandbox (2018–2020).

Comparative evidence from ASEAN

- **Indonesia** – OJK Innovation Centre for Digital Technology (ICDX): during COVID-19, a Jakarta hospital piloted an AI-driven ICU triage algorithm under sandbox waiver; evaluation showed a 15 % reduction in ventilator utilisation.[27]
- **Singapore** – MOH Telemedicine Sandbox (2018–2021): the sandbox "Licensing Experimentation and Adaptation Programme (LEAP)" co-created governance measures with industry; its objectives met, MOH discontinued the sandbox in Feb 2021 and launched a Voluntary Listing of Direct Telemedicine Providers so patients could identify providers adhering to these measures.[28]
- **Malaysia** – MDA "RegLab" for medical device- software (2023): allowed startups to trial AI dermatology apps while MDA drafted its Software as a Medical Device (SaMD) -Guideline.[29]

Benefit for Cambodia: applied to the Cambodian context, a digital health sandbox under the MoH leadership, targeting use cases like AI diagnostics, clinical decision support, or teleconsultation, could enable safe, stepwise innovation. Beyond temporary regulatory flexibility, a sandbox functions as a trust-building mechanism: it requires innovators to co-design metrics with regulators, share de-identified results, and generate local evidence. This reduces legal uncertainty, supports iterative policy development, and signals openness to investment. A public "*Sandbox Outcomes Report*" could feed into eHealth platform licensing (see Section 3.1) and inform updates to the forthcoming Digital Health Strategy 2026–2030.

27 Otoritas Jasa Keuangan, "Laporan Tahunan OJK 2021" (Annual Report 2021), Jakarta, 2022, p. 42, available at: https://www.ojk.go.id/id/datadanstatistik/laporantahunan/Documents/Laporan%20Tahunan%20OJK%202021.pdf.

28 Ministry of Health Singapore, "Voluntary Listing of Direct Telemedicine Service Providers to Help Patients Make Informed Choices", Press Release, 26 February 2021, available at: https://www.moh.gov.sg/newsroom/voluntary-listing-of-direct-telemedicine-service-providers-to-help-patients-make-informed-choices [last accessed – 26 May 2025].

29 Ministry of Health Malaysia & Futurise, "Online Healthcare Services (OHS) RegLab – Guideline Overview", Cyberjaya, 2023, available at: https://www.futurise.com.my/index.php/ohs-reglab/ [last accessed – 26 May 2025].

Principle-Based and Co-Regulatory Governance

Fast-moving technology favours laws that state what outcomes matter (principles) and let lower-level, rapidly updated instruments decide how to meet them (codes, standards). Cambodia can achieve this with concise MoH regulations that reference accredited industry guidelines.

Legal foundation

- Law on Regulation of Health Practitioners (2016) Article 5 – empowers the relevant medical councils under the MoH to set professional standards.
- E-Commerce Law (2019) Articles 29-33 – creates a duty of care applicable to digital services.
- LPDP Articles 6-14 – embeds cross-sector principles (lawfulness, transparency, purpose limitation).

Core principles and their practical expression

Principle	How it shows up in practice
Accountability	Each platform names a senior 'Responsible Officer' and files an annual duty-of-care report.
Patient agency & data stewardship	Granular consent dashboard; secondary use only with explicit opt-in.
Explainability & human oversight	Licensed clinician reviews any AI-generated clinical advice before release.
Interoperability & portability	HL7 FHIR R4 discharge summaries issued within 24 h.

Co-regulatory tools

1) **Accredited industry codes –** a recognised digital health code becomes a licence condition once the MoH approves it by *Prakas***.**
2) **Standards recognition list –** MoH publishes accepted international standards (ISO 27799, IEC 823042); self-certification allowed, subject to spot audit.
3) **Independent conformity assessment –** third-party labs or universities conduct annual reviews and report findings to the MoH.
4) **Comply or explain transparency –** large platforms (more than 10,000 monthly active users) must publicly justify deviations from the code.
5) **Stakeholder council –** a semi-annual forum of the MoH, data protection authority, professional bodies, industry representatives, and patient groups, updates principles and resolves grey zones.

Regional precedents

- Singapore – Model AI Governance Framework v2.0: principles endorsed by regulator; sectors add detailed notices.
- Indonesia – MoH Regulation 24/2022: sets out abroad accountability clause while delegating technical specifics to professional associations.

Principle-based, co-regulatory governance delivers legal certainty without rigidity. A short 'Principles for Safe Digital Health' *Prakas* can stay relevant for years, while accredited codes and standards evolve as technologies and risks change.

III. A Philosophy of Regulation for eHealth Platforms

The legal governance of DHPs in Cambodia demands more than additional statutes; it requires a redefinition of the purpose and method of law in a setting of rapid technological change. Two complementary ideas – legal minimalism and digital constitutionalism – provide a roadmap that is simultaneously agile and rights-anchored.

Legal Minimalism: Light-Touch Regulation with Clear Guardrails

Legal minimalism relies on broad principles, guidance documents, and controlled risk sandboxes rather than exhaustive codes. To date, the MoH has not issued dedicated guidance on teleconsultation or e-prescriptions. Adopting such nonbinding instruments would offer immediate clarity on professional duties while statutory reform is underway. These soft-law instruments are possible because the Draft Cybersecurity Law designates health services as critical information infrastructure entities and authorises sector ministries to issue implementing measures.[30]

International experience confirms the value of minimalism. Under Singapore's *Healthcare Services Act 2020,* the Health Sciences Authority operates the LEAP Regulatory Sandbox, allowing innovators to test new digital health products within predefined risk parameters.[31] A similar sandbox, issued by *Prakas*, would let Cambodian platforms pilot AI-supported triage, Teleconsultations, or automated claims while the MoH monitors safety.

Minimalist tools could include:

- Guideline on Good Platform Practice (GPP) for Digital Health, setting baseline expectations for accountability, data stewardship with patient agency, and human oversight.
- Model consent language for teleconsultation, available in Khmer and English.
- A tiered licensing notice that links higher risk functions (e.g., automated diagnosis) to stricter reporting, leaving low risk functions under general professional law.

Because guidance is easier to revise than legislation, MoH can update requirements after each sandbox cohort, creating an iterative cycle of policy learning. In a low-capacity environment, this flexibility is an asset, not a weakness.

30 Draft Cybersecurity Law, Kingdom of Cambodia, Articles 3(20) & 7.
31 Healthcare Services Act 2020 (Singapore), § 6 and First Schedule; LEAP Sandbox Notice No. 3/2021.

Digital Constitutionalism: Embedding Rights and Dignity in Code

Flexibility must be anchored in non-negotiable rights. Digital constitutionalism holds that core values – privacy, dignity, equity, and accountability – should be built into digital infrastructure from the outset. The Constitution of Cambodia guarantees the incorporation of international human rights norms and protects the privacy of correspondence.[32] The LPDP classifies health data as sensitive and requires explicit, revocable consent.[33]

These high-level protections need sectoral activation. A health-specific *Prakas* on Digital Consent could operationalise LPDP duties by mandating consent dashboards, Khmer language prompts, and one-click withdrawal mechanisms. The same instrument could require explainability statements for any AI that influences clinical or reimbursement decisions, drawing on the European Union's Artificial Intelligence Act for technical benchmarks.[34] International Covenant on Civil and Political Rights,[35] incorporated via the Constitution Article 31, further supports a right to protection against arbitrary or unlawful interference with digital health data.

Digital constitutionalism also protects against future risks. By embedding duties of fairness, non-discrimination, and transparency into platform code and contracts, Cambodia can preserve "*Digital Dignity*": the right of individuals to fair, explainable, and non-discriminatory algorithmic treatment. This principle will remain relevant as cloud analytics, generative AI, and cross-border data flows evolve.

Concluding Synthesis

Legal minimalism and digital constitutionalism are not opposing theories. Minimalism supplies the agile instruments – guidelines, sandboxes, and model clauses – that keep regulation light yet responsive. Constitutionalism supplies the immutable rights that any innovation must respect. Together, they form twin pillars for governing DHPs in Cambodia and can be implemented through two complementary steps:

1) Issue a MoH *Prakas* establishing a Digital Health Sandbox for platforms designated as part of the health sector's CII under Article 7 of the Draft Cybersecurity Law, and develop accompanying operational guidelines.
2) Issue a MoH Prakas on Digital Consent and Algorithmic Fairness, giving operational effect to LPDP Arts 9 and 13 and Constitution Article 40.

Adopting both steps would allow Cambodia to experiment boldly while ensuring that every new service respects privacy, equity and accountability from the outset.

32 Constitution of the Kingdom of Cambodia, Articles 31 & 40.
33 Draft Law on the Protection of Personal Data, Kingdom of Cambodia, Articles 7 & 15.
34 Regulation (EU) 2024/865 on Artificial Intelligence, European Union, Articles 9 & 14.
35 International Covenant on Civil and Political Rights, Article 17.

IV. A Cambodian Jurisprudential Identity for Digital Health Law

Cambodia's digital health moment is not simply a technical question of new rules; it is a constitutional question of what kind of legal order the Kingdom wishes to project into cyberspace. The Legal Lens frames the dilemma succinctly: the same norm can operate either as a brake on innovation or as its catalyst. We distil three indigenous pillars—public trust, Buddhist ethics, and hybrid legalism—that can turn Cambodian law from a reactive follower into a proactive architect while remaining culturally resonant.

Public Trust as Legal Infrastructure

Relational trust has long substituted for formal paperwork in Cambodian health care: patients consult village *Kru* before doctors, and licensing boards are trusted only insofar as they echo communal norms. Digital platforms magnify this dynamic—if users do not trust a tele-doctor's credentials or an app's fee transparency, no statute will save adoption.

Legal lever: the *Law on Commune/Sangkat Administration 2001*, Article 43, already recognises local councils as first-line dispute settlers. A forthcoming *Prakas on Trust & Transparency in Digital Health* could extend that logic online by mandating:

1) Plain Khmer terms of service and data use notices;
2) A redress portal supervised by the local Ombuds-mechanism;
3) Digital credential badges that pull licence status from professional council APIs.

Effect: trust mechanisms move from optional UX widgets to enforceable duties. The platform becomes liable for removing a provider whose licence has lapsed, while patients gain a culturally familiar channel for grievances.

Buddhist Ethics – from Non-Harming to Digital Compassion

Theravāda principles permeate Cambodian public life. The Constitution (Articles 31 & 43) elevates Buddhism and fundamental rights; ***ahiṃsā*** (non-harming) and ***karuṇā*** (compassion) therefore offer a normative bridge between secular regulation and moral legitimacy.

Operationalising Non-Harming

- Human in the loop: Any AI triage tool that classifies a case as high risk must trigger synchronous human review; failure constitutes negligence per proposed *Prakas*.
- Respectful consent: Digital consent screens must present risks and alternatives in accessible Khmer, reflecting relational integrity rather than a perfunctory click.
- Stewardship, not ownership: Health data are held *for* the patient, not *by* the platform; withdrawal of consent requires erasure except where retention is mandated by law.

Legal vehicle: insert a values preamble "*Inspired by the principles of non-harming and compassion [...]"* into any Digital Health Services Sub-Decree. Courts may then interpret ambiguous provisions e.g., algorithmic explainability, in favour of patient welfare.

Hybrid Legalism and Customary Flexibility

Cambodia's jurisprudence is already plural: French civil code structure, Buddhist moral authority, and donor-driven "*development law*" coexist. Rather than forcing digital health into a single mould, regulators can choreograph layered governance.

Precedent: *Prakas 488/20 on Village Health Support Groups* blends MoH standards with community-drafted bylaws, demonstrating how formal and customary rules can coexist in the health domain.

Interagency alignment: A joint MoH–MPTC *Prakas* on Digital Health Data could weave sector-specific safeguards (consent dashboards, mandatory FHIR APIs) into the LPDP draft, Article 23b and 28 cross-border transfer test. This avoids duplicate notification regimes and provides a single window for compliance.

Layered enforcement

- Hard law where risk is acute (AI dosing algorithms analysed as Class III medical devices).
- Soft law where experimentation is needed (sandbox guidelines).
- Customary mediation for low-value disputes (reuse of communal reconciliation).

Trust embedded as legal infrastructure, compassion encoded as non-harming safeguards and adaptive pluralism that allocates the right tool to each risk tier—together these form a distinctly Cambodian legal lens for governing multi-sided DHPs. They translate international best practices into idioms that Cambodian citizens already recognise and respect.

V. Conclusion: From Legal Lag to Legal Leadership

Cambodia now stands at a crossroads. DHPs already deliver consultations, diagnostics and reimbursement across the Kingdom, yet the governing statutes still assume a brick-and-mortar hospital model. In Sections 1–5, we argued that Cambodian law must do more than catch up: it must leap ahead and become a form of digital infrastructure in its own right.

Law as Digital Infrastructure: digital technologies prosper when the underlying protocols are modular, interoperable, and adaptive. Legal instruments must adopt the same design philosophy. Rather than one omnibus eHealth Law, Cambodia should rely on *platform-specific Prakas*, guidelines, timeboxed regulatory sandboxes under the authority of the MoH, MPTC and sectoral guidelines issued pursuant to the forthcoming LPDP. These tools can be revised on short cycles, allowing the ruleset to coevolve with technological practice.

Trust and Cultural Resonance: section 5 demonstrated that relational trust, Buddhist ethics of non-harming and compassion, and Cambodia's hybrid legal tradition can transform abstract compliance into lived legitimacy. Embedding these values turns law into a trust engine rather than an external constraint.

Regional Leadership: ASEAN is converging on baseline rules for data, AI, and cross-border services. By operationalising a *trust-based, culturally grounded, yet interoperable* legal architecture, Cambodia can move from norm-taker to norm-shaper in regional dialogues.

This is the moment to bring law into the loop

By grounding digital health transformation in Cambodia's enduring motto—Nation, Religion, King (ជាតិ សាសនា ព្រះមហាក្សត្រ Constitution of the Kingdom of Cambodia, Article 4), the Kingdom can ensure that legal innovation advances public welfare, reflects compassionate values, and reinforces legitimate governance.

When legal codes iterate as fast as software updates, they cease to be speed bumps and become highways—paving a path toward safer, more equitable, and more innovative health care for every citizen of Cambodia.

By embracing legal minimalism, digital constitutionalism, and a distinctly Cambodian jurisprudential identity, the Kingdom can convert legal lag into legal leadership—and ensure that its citizens benefit fully and safely from the digital health transformation.

ABOUT THE AUTHORS

Samnangvathana Sor

Senior Consultant of Corporate and Commercial Practice, DFDL, Phnom Penh, Cambodia; Co-Chair of the Healthcare Committee of EuroCham Cambodia.

Vathna is currently a Senior Consultant in DFDL's Corporate and Commercial Practice in Phnom Penh, providing advisory services on matters related to M&A, Corporate Compliance, Labour, Immigration, and Commercial Law. Across sectors, she has experience with Health Care, Tourism, Hospitality, F&B, and Education, which includes IPO and Licensing matters. Partaking in support of resolving labor disputes at the Arbitration Council Foundation. Vathana holds am LL.M (Transnational law and Business University, Seoul), LL.B (Royal University of Law and Economics, Phnom Penh) and B.Ed. in English (RUPP).

Yean Solina

Of Counsel, ANANT Law Firm, Phnom Penh, Cambodia; Co-Chair of the Healthcare Committee of EuroCham Cambodia.

Solina is a Lawyer specializing in health, life science law, insurance and social protection. She has advised the Ministry of Health on pharmaceutical legislations and supported foreign companies entering the Cambodian market. Her client include international organization such as the International Labor Organization. She was appointed by royal decree to the Ministry of Justice's Legislative and Judicial Council (2020) and as an independent member of the Non-Bank Financial Services Authority (2021). Solina holds an MBL from (Jean Moulin University Lyon 3) and two bachelor's degrees: one in Comparative Law from (Lumière University Lyon 2 in France), and an LL.M from the (Royal University of Law and Economics in Phnom Penh).

Simon Burlinson

Solicitor and Senior Consultant, DFDL, Phnom Penh, Cambodia; Member of the Healthcare Committee of EuroCham Cambodia.

Simon is currently a Senior Consultant within the ralm of Corporate & Commercial Group based in Cambodia. He works with clients ranges from single, multi-jurisdictional mergers, cross-border acquisitions and disposals, joint venture structures, project development as well as financial arrangements in relation to technology, healthcare and energy sectors. He is a registered English-qualified solicitor and holds a BSc. (Hons) in Pharmacology & Toxicology.

Dr. Elias J. Engelking

Senior Consultant, Intercare Hospital, Phnom Penh, Cambodia; Advisor, German Development Cooperation (GIZ) GmbH; Cooperation Doctor, German Embassy, Phnom Penh; Trusted Doctor, Swiss Development Cooperation (SDC), Phnom Penh; Co-Chair of the Healthcare Committee of EuroCham Cambodia

Dr. Elias is a German-trained general surgeon and emergency physician with extensive experience in Europe, Africa, and Southeast Asia. He advises Intercare Health Group and Cambodian Government institutions on behalf of the German Development Cooperation (GIZ) on health system reform, digital transformation, and innovation. His current work centers on building digital health platforms, advancing AI governance, and strengthening accreditation and quality assurance in health professions education. He has authored and co-authored multiple publications on law, innovation, and health governance, including forthcoming contributions to Law and Innovation.

PART III

INNOVATION GOVERNANCE BEYOND THE MARKET

IS DELIBERATION POSSIBLE HERE? THE RISE AND FALL OF OPEN CONSULTATION PLATFORM VTAIWAN

Poren Chiang

I. Introduction

The rapid development of emerging technologies, often propelled by disruptive business models, presents a formidable challenge to existing regulatory frameworks. In the last decade, policymakers have been struggling to respond to the public's calls for regulatory intervention, as the collateral impact of technological advancements rewrites the very fabric of society.[1]

This is believed primarily due to the unprecedented complexities that undermine traditional policymaking approaches. First, significant information asymmetries often exist between policymakers and social actors, stemming from the highly technical or specialized nature of these sectors. Regulators may lack the necessary knowledge to fully grasp the potential and limitations of new technologies in question. Second, there is considerable uncertainty surrounding regulatory solutions and their potential outcomes. The effectiveness of interventions and the possible existence of unintended consequences in novel sectors are difficult to predict. Furthermore, these disruptions also play differently on different sectors of society: a new food delivery platform might introduce convenience to its users, but it may also inadvertently hike up the menu price for the dine-in customers. Regulators must quickly sort out those who will be negatively impacted, and the shockwave may be widespread. Lastly, policymaking processes often require deciding the trade-offs between over- or under-regulation, and the regulators are often at risk of overlooking potential harms or stifling economic development.[2] It is no wonder why that the public and the private sectors are looking for policy tools to tackle this problem.

vTaiwan,[3] came to the spotlight amid this search for the anticipatory policymaking holy grail. Started as one of the novel alternatives to administrative consultation from the cabinet, the vTaiwan platform runs a deliberative process to bring stakeholders and concerned citizens to collectively work towards a resolution. Through the utilization of discussion tools like Pol.is,[4] vTaiwan has helped the Taiwan government build a bigger consensus, navigating the deep water of regulatory adjustments with relative ease.

One of the most prominent successes made by vTaiwan was Uber's compliance with local taxi laws. When the ride-sharing giant began its operation in Taiwan, it considered itself exempt from the existing legal frameworks and actively refused taxation, fueling a year-long cat-and-mouse chase with Taiwan's transportation authority. This intense administrative brawl involved hefty fines from the ministry and widespread media campaigns from Uber, where the company went to great lengths to rally its users against the government.[5] vTaiwan trod into this volatile situation with its iterative process and digital tools, finding a common ground for all actors that eventually led to Uber's compliance.

1 Cecilia Kang & Adam Satariano, "As A.I. Booms, Lawmakers Struggle to Understand the Technology", New York Times, Mar 03, 2023. https://www.nytimes.com/2023/03/03/technology/artificial-intelligence-regulation-congress.html.

2 Araz Taeihagh, M Ramesh, Michael Howlett, "Assessing the regulatory challenges of emerging disruptive technologies", in *Regulation & Governance* 15, Wiley, 2021, pp. 1009–1019. https://doi.org/doi:10.1111/rego.12392.

3 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

4 Christopher Small, Michael Bjorkegren, Timo Erkkilä, Lynette Shaw, Colin Megill, "Polis: Scaling Deliberation by Mapping High Dimensional Opinion Spaces", in *RECERCA: Revista De Pensament I Anàlisi* vol. 26(2), Spain: Universitat Jaume I, 2021. https://doi.org/10.6035/recerca.5516.

5 Kuo-Wei Wu, Shun-Ling Chen, Poren Chiang, "Open with Caution: How Taiwan Approaches Platform Governance in the Global Market and Geopolitics", in *Perspectives on Platform Regulation*, Germany: Nomos, 1st, 2021, pp. 165–186. https://doi.org/10.5771/9783748929789-165.

Since then, the vTaiwan initiative has become nothing short of a crown jewel among civic tech communities, celebrated as a pioneering example of how deliberative democracy could not only resolve immediate conflicts but also help regulations anticipate innovation. BBC described the platform as 'a consensus-building social network' that 'may have a tremendously valuable lesson for us all',[6] while scholarly works lauded its ability to attract 'thousands of young people who had never participated in politics" and build a network that may be mobilized on other national issues 'such as the fight to limit the impact of Covid-19.[7] The perception of vTaiwan being a dynamic, democratizing force, capable of fostering civic engagement and legislative agility, sounds almost mythological, portraying it as almost the saviour of democracy.

However, a decade and several iterations of topics on the platform later, the initial fever around vTaiwan has largely waned. While the Uber case remains as its model success, the platform itself has mostly fallen out of the public eye. A closer examination reveals a significant decline in its active use and governmental engagement: there have been no new proposals from the government since 2020, and the majority of completed projects on vTaiwan date back to before 2017.[8] Projects like the regulation of online liquor sales and efforts towards procurement open data failed to achieve the same level of legislative integration or impact. This stark reality begs critical questions: If vTaiwan was such a groundbreaking success, why are we not seeing more agencies involved with the platform? Does the deliberation process genuinely save the regulatory environment from the condemnation of "*slowpoke*," or was the Uber case an anomaly?

This article aims to dive into the bold claim behind vTaiwan – that deliberative democracy can fundamentally transform regulatory processes. The first section describes the origin of vTaiwan and the deliberation process it had set up. The second section will address the "*failed*" cases — proposals stuck in limbo or purposefully ignored by the lawmakers. The final section will dissect the underlying reasons behind the decline and subsequent fall of deliberative law adjustments on the vTaiwan platform through the analysis of available interviews and field data. By examining the disparity between its celebrated initial success and its current reduced impact, we seek to understand the systemic challenges that ultimately limit the transformative potential of such initiatives in the realm of regulatory reform.

II. The Origin and the Deliberative Process of vTaiwan

The vTaiwan initiative is a consensus-building platform from g0v, the self-organized, polycentric civic tech community,[9] in Taiwan. It is independently run by community volunteers, aiming to 'gather opinions, facilitate discussions, and build consensus' via the usage of 'digital tools and the participation of diverse stakeholders.' The project was established more than a decade ago, and the current working group still hosts weekly meetups to develop potential topics.[10]

6 Carl Miller, "Crossing Divides: How a social network could save democracy from deadlock", BBC, Oct 29, 2019. https://www.wired.com/story/taiwan-democracy-social-media/.

7 Lex Paulson, "Introduction - Reinventing democracy: New modes of representation", in *The Routledge Handbook of Collective Intelligence for Democracy and Governance*, Routledge, 1st, 2023, pp. 143–152 &148. http://doi.org/10.4324/9781003215929-8.

8 vTaiwan, "vTaiwan – Digital Economy Regulation Online Consultation". https://vtaiwan.tw - last accessed May 2025.

9 g0v.tw, "g0v Manifesto", 2019. https://g0v.tw/intl/en/manifesto/en/ - last accessed May 2025.

10 vTaiwan, "vTaiwan Working Group General Info", on *g0v HackMD*, 2023. https://g0v.hackmd.io/@vTaiwan/rkxAt4oTla - last accessed June 2025.

Surprisingly, even with its long history of autonomy, vTaiwan had its roots in administrative involvement since its inception. The idea to have a consultation mechanism out in the open was initially conceived by then-cabinet member Jaclyn Tsai during one of g0v's bimonthly hackathons. Seeking to reform the regulatory landscape to support tech startups, the minister proposed to run an online platform to collect public input on legalizing close companies and crowdfunding campaigns. The discussion will be held online, producing several iterations of drafts, before being consolidated into a formal bill proposal by the corresponding governmental agencies. With the aid from g0v community members like Audrey Tang and Peggy Lo, an online Discourse forum,[11] was quickly set up in January 2015, marking the start of vTaiwan initiative.[12]

In the early days of vTaiwan, the rulemaking process was heavily inspired by the RegulationRoom initiative,[13] from Cornell.[14] For each regulatory issue, the proposing agency shall provide introductory text, potential topics to develop, applicable glossaries, and other additional materials that help make the case; contracted facilitators from III Science & Technology Law Institute, a quasi-governmental think tank, would convert the documents into formats suitable for online collaboration, which are then published to vTaiwan's web forum. Community moderators help facilitate discussions, collect questions for the agencies to answer, and organize a *working group* consisting of active participants and public servants. The working group is charged with assembling policy recommendations and, after a few iterations of revision, producing a draft bill for the agency to adopt. Relevant materials and discussions will be publicly archived, while parts of the forum will be kept open to track the legislation progress.[15]

Two of the less controversial topics, regulating crowdfunding platforms and legalizing close companies, were proposed by the Financial Supervisory Commission and the Ministry of Economics, respectively, to kickstart the platform. As the process matured, more deliberation methods and digital tools were integrated to vTaiwan. In order to reach consensus, facilitators started to utilize the Focused Conversation Method (ORID) to categorize participants' speech into objective facts ("*O*"), reflective feelings ("*R*"), interpretations based on their values ("*I*"), before the group finally came to their decisional moments ("*D*").[16] Online collaboration tools were also put on the center stage at this era — realtime text editors like Hackpad encouraged parallel, asynchronous discussion, transcript hosting platform SayIt enabled pin point citation of ideas or statements, and GitBook helped generate paginated e-books for final presentation.[17] The product of the discussion is not of a raw consensus, but a so-called "*Coherent Blended Volition*" — a "*conceptual blend*" of a diverse group of people that 'incorporates the most essential elements of their divergent views.'[18]

11 "What is Discourse?", Civilized Discourse Construction Kit Inc., 2025. https://www.discourse.org/ - last accessed June 2025.

12 Audrey Tang, Peggy Lo, et al, "vTaiwan.tw Executive Yuan Online Consultation Platform", on *g0v Hackpad*, 2014. https://g0v.hackpad.tw/vTaiwan.tw--oWRxOF4ilfx - last accessed June 2025.

13 Cynthia R. Farina, Josiah Heidt, Mary J. Newhart, Joan-Josep Vallbé, "RegulationRoom: Field-Testing An Online Public Participation Platform During USA Agency Rulemakings", Cornell e-Rulemaking Initiative, 2012. https://scholarship.law.cornell.edu/ceri/10.

14 Audrey Tang, Peggy Lo, et al, "vTaiwan.tw Executive Yuan Online Consultation Platform", on *g0v Hackpad*, 2014. https://g0v.hackpad.tw/vTaiwan.tw--oWRxOF4ilfx - last accessed June 2025.

15 Audrey Tang, "vTaiwan.tw Process", on *g0v Hackpad*, 2015. https://g0v.hackpad.tw/vTaiwan.tw--yIoh6OFRR8o - last accessed May 2025.

16 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

17 Mei-Chun Lee, "The Nobody Movement: Civic Hackers and Digital Activism in Taiwan", Taipei: Spring Hill, 2025, pp. 205–213.

18 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

Six months after vTaiwan launched, 11 other issues ranging across labor, tax, cyberbullying, and information security were submitted to the vTaiwan platform.[19] The consultation process itself were also formalized into four stages: (1) Proposal stage, where an agency actively submits an issue to vTaiwan or passively agrees to open up discussion with the public; (2) Opinion stage, where general opinions are collected online to build up the argument landscape; (3) Reflection stage, where facilitators host hybrid consultation meetings with multiple groups of stakeholders; and (4) Legislation stage, where the final consensus is reached and presented as a statement, policy, or draft bill.[20] In September, the legislature passed the corresponding law amendments for close companies, 3 months after the consultation process concluded. This marked vTaiwan's first political success,[21] clearing the path for its model case — Uber's compliance — to happen.

Anchoring the Uber Fleet

Perhaps one of the best examples of disruptive innovation, Uber, the car-hailing and ride-sharing app giant, has been in constant battles with city governments since its very first day of entering the market. Debuted in 2011, Uber introduced a long-overdue change to the transportation industry — passengers may now quickly match and get cars dispatched to their destination, all within a single tap from their mobile app. The reception was exceptional, as Uber's user base and market value skyrocketed, but it had also managed to irritate transportation officials and the taxi industry in almost every city it operated in.[22]

The disgruntlement from the cab drivers is not difficult to understand: from fares, fleet size, to operating areas, taxi services have been tightly regulated by their cities throughout their existence. To the licensed operators, Uber was exploiting the market with an unfair advantage, in most cases, they are allowed to operate free of the rules, regulations, and licensing requirements of traditional taxis.[23] However, maintained that it was not subject to such regulation, as they considered themselves merely a tech company that matches people with drivers, not an actual provider of rides. The overly optimistic, almost audacious interpretation certainly did not entertain city commissioners around the globe, as fines and lawsuits began to accumulate against Uber's then-illegal operation.[24]

Despite its mixed reputation, Uber entered the Taiwan market in 2013 as it expanded its global presence. Initially positioned as a high-end transportation service, Uber Taiwan was able to steadily establish a user base among tech entrepreneurs without raising too many eyebrows.[25] However, when it rolled out UberX in 2014 to compete with local taxis, unions and the chamber

19 vTaiwan, "vTaiwan.tw" (archived version), Jun 10, 2015. https://web.archive.org/web/20150610030545/http://www.vtaiwan.tw:80/ - last accessed June 2025.

20 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

21 Liz Chen, "Exclusive Interview with Minister without Portfolio Jacyln Tsai: Industrial Experts, Come Serve and Reshape the State Apparatus", *Inside*, Aug 26, 2015. https://www.inside.com.tw/article/4927-tsai-yu-ling-interview - last accessed June 2025.

22 Brian X. Chen, "A Feisty Start-Up Is Met With Regulatory Snarl", New York Times, Dec 2, 2012. https://www.nytimes.com/2012/12/03/technology/app-maker-uber-hits-regulatory-snarl.html - last accessed May 2025.

23 Luz Lazo, "Cab companies unite against Uber and other ride-share services", The Washington Post, Aug 10, 2014. https://www.washingtonpost.com/local/trafficandcommuting/cab-companies-unite-against-uber-and-other-ride-share-services/2014/08/10/11b23d52-1e3f-11e4-82f9-2cd6fa8da5c4_story.html - last accessed May 2025.

24 Brian X. Chen, "A Feisty Start-Up Is Met With Regulatory Snarl", New York Times, Dec 2, 2012. https://www.nytimes.com/2012/12/03/technology/app-maker-uber-hits-regulatory-snarl.html - last accessed May 2025.

25 Liz Chen, "High-End Car-Summoning Service Uber Rolling into Taipei", *Inside*, Jun 10, 2013. https://www.inside.com.tw/article/2545-uber-taipei - last accessed June 2025.

of commerce swiftly came together to launch large-scale protests against Uber. UberX identified itself as a "*rental car with paired drivers*" service that offered substantially lower rates than the regulated taxi base fare. Such framing also means that UberX circumvented most of the local safety regulations imposed on taxis — such as mandatory background clearance for drivers or transparent window panes for vehicles — a gesture taxi unions considered unfair competition.[26] Taiwan's Ministry of Transportation and Communications began cracking down on Uber and its drivers after its refusal to register as a taxi service, imposing over US$1.16 million in penalties in less than one year.[27] To the regulatory authorities, Uber actively rejected regulation, avoiding mandatory insurance, and most importantly, evading taxes via overseas payment processors.[28]

Even the agencies must admit, however, that the convenience of Uber did introduce a much-needed innovation for the ride-hailing market, and there should be *some* way for the new form of taxi operation to be legalized. This gap in knowledge opened up a crack for public input. vTaiwan, around the same time, it had just wrapped up its pilot projects and was deciding on the next issues to tackle. In June 2015, about 30 community members voted in an internal poll to take on issues related to sharing economy — specifically Airbnb and Uber — into development. With the coordination from Minister Tsai and the agencies,[29] the vTaiwan community began preparing the topic for public discussion with STLI contractors.

To better congregate the diverse opinions from the crowds, vTaiwan utilized a new online tool named Pol.is to collect input from the general public.[30] Pol.is works by letting the facilitator "*seeds*" the opinion space with different comments and asking participants to vote if they side with them; participants may choose "*agree*," "*disagree*," or "*pass*". They are also allowed to add additional comments for others to vote on, if there were any particular perspectives not mentioned. The Pol.is website will visualize the ideological distribution of different actors in real time, grouping participants with similar views and showing potential middle grounds two groups might have in common.[31] After a full month of online opinion collection, 925 participants voted on 145 comments. Two distinct but similarly-sized opinion groups could be identified: one emphasized outlawing unlicensed passenger vehicles, noting the illegal operations and opaque management drew safety concerns; the other praised how Uber broke the market dominance of taxi fleets, stating their preference for the higher quality Uber service over regular taxis.[32] Both groups agreed that safety is the top priority, that regulations shall be fair and adaptive to sociotechnological advancements, and that there shall be proper driver screening and insurance coverage.

26 Wen-Bing Su, "Ministry of Transportation to Investigate Whether Uber Operates Illegally", *iThome*, Jul 9, 2014. https://www.ithome.com.tw/news/89285 - last accessed Jun 2025.

27 Shelley Shan, "Uber and its drivers pay NT$37.59 million in fines", *Taipei Times*, Aug 14, 2015. https://www.taipeitimes.com/News/taiwan/archives/2015/08/14/2003625338 - last accessed May 2025.

28 Kuo-Wei Wu, Shun-Ling Chen, Poren Chiang, "Open with Caution: How Taiwan Approaches Platform Governance in the Global Market and Geopolitics", in *Perspectives on Platform Regulation*, Germany: Nomos, 1st, 2021, pp. 165–186. https://doi.org/10.5771/9783748929789-165.

29 Liz Chen, "Exclusive Interview with Minister without Portfolio Jacyln Tsai: Industrial Experts, Come Serve and Reshape the State Apparatus", *Inside*, Aug 26, 2015.https://www.inside.com.tw/article/4927-tsai-yu-ling-interview - last accessed June 2025.

30 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

31 Christopher Small, Michael Bjorkegren, Timo Erkkilä, Lynette Shaw, Colin Megill, "Polis: Scaling Deliberation by Mapping High Dimensional Opinion Spaces", in *RECERCA: Revista De Pensament I Anàlisi* vol. 26(2), Spain: Universitat Jaume I, 2021. https://doi.org/10.6035/recerca.5516.

32 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

Facilitators from STLI summarized these voices, and an online-offline hybrid consultation meeting was called in August 2015. Different stakeholders — regulatory agencies, scholars, taxi unions, community members, and Uber Taiwan,[33] — came to the understanding that Uber had to comply with legal requirements of insurance and driver training, while the regulatory environment and the existing taxi service needed to catch up with market demands. The administration moved to adopt the consensus formed within Pol.is and at the meeting, and a revised, more permissive regulation on automobile transport services came into effect one year later. App-based taxi services are now free to operate as long as they do not undercut regulated taxi fares, provide sufficient driver transparency, and pay their proper sales tax per ride.[34] This marked a rare truce between Uber and the existing taxi services, in a time when Uber was still at war with different countries.[35]

This coherent blended volition of the Uber issue, however, did not seem satisfactory to Uber themselves. More specifically, the built consensus and the newly introduced diversified taxi service regulation still require drivers to hold a commercial driving license. The requirement, though easy for UberBlack transportation service to meet, sets a much higher bar in the ridesharing economy Uber sought to tap into. Uber persisted in its position to not be put under taxi services but a new category of service for ridesharing, calling taxi regulations in many countries "*outdated*" and "*no longer a good fit for ridesharing enabled by a smartphone*."[36] At the same time, Uber had already accrued a total of NT$66.05 million for its failure to register, operating with unlicensed drivers, and other 465 violations.[37] It also had not paid its commercial tax. Instead, Uber opted for a full-blown newspaper campaign to call on the President of Taiwan to "*Progress Together*" under the façade of the Sharing Economy Industry Association.[38]

This did not play well with the legislators. In the same month, the legislature amended the *Highway Act* by raising the maximum fine for illegal passenger transportation services to NT$25 million ($780,000), 16 times higher than the previous limit.[39] The Highway Bureau, seeing the uncooperative nature of Uber, started slapping heavy penalties for their illegal acts. Uber finally had to halt its ridesharing operation in February 2017 after accumulating US$10 million in fines.[40] Up until this point, Uber still directed their users to voice their dismay toward the

33 "Opinion Collection on uberX Private Car Operation' Consultation Meeting", on *g0v Hackpad*, Aug 27, 2015. https://g0v.hackpad.tw/2015-08-27-uberX--y4uRD0dNFMq - last accessed May 2025.

34 Hsiao Yu-Tang, Shu-Yang Lin, Audrey Tang, Darshana Narayanan, Claudina Sarahe, "vTaiwan: An empirical study of open consultation process in Taiwan", published on SocArXiv, 2018. https://doi.org/10.31235/osf.io/xyhft.

35 Audrey Tang, "Uber responds to vTaiwan's coherent blended volition", Pol.is blog on *Medium*, May 23, 2016. https://blog.pol.is/uber-responds-to-vtaiwans-coherent-blended-volition-3e9b75102b9b - last accessed May 2025.

36 Damian Alexander Kassabgi, "Regulated ridesharing: How Taiwan could achieve it", Uber, Dec 14, 2016. https://newsroom.uber.com/taiwan/twrseng/ - available at https://web.archive.org/web/20170228061404/https://newsroom.uber.com/taiwan/twrseng/.

37 Faith Hung, "Uber says disappointed by Taiwan law raising ride-sharing fine to highest level globally", Reuters, Dec 17, 2016. https://www.reuters.com/article/technology/uber-says-disappointed-by-taiwan-law-raising-ride-sharing-fine-to-highest-level-idUSKBN1452AC/ - last accessed May 2025.

38 Kuo-Wei Wu, Shun-Ling Chen, Poren Chiang, "Open with Caution: How Taiwan Approaches Platform Governance in the Global Market and Geopolitics", in *Perspectives on Platform Regulation*, Germany: Nomos, 1st, 2021, pp. 165–186. https://doi.org/10.5771/9783748929789-165.

39 Faith Hung, "Uber says disappointed by Taiwan law raising ride-sharing fine to highest level globally", Reuters, Dec 17, 2016. https://www.reuters.com/article/technology/uber-says-disappointed-by-taiwan-law-raising-ride-sharing-fine-to-highest-level-idUSKBN1452AC/ - last accessed May 2025.

40 Jethro Mullen & Yuli Yang, "Uber suspends its service in Taiwan as fines mount", CNN, Feb 2, 2017. https://money.cnn.com/2017/02/02/technology/uber-taiwan-suspending-service-fines/ - last accessed June 2025.

government.[41] The administration did not back off, however, and Uber Taiwan eventually conceded. resuming their service within regulatory bounds two months later. Uber, while still operating as a technology platform company, will drop its ridesharing service and delegate the actual operation of transport services to local fleets.[42] A later court decision set aside Uber's fines due to a technical error in jurisdiction, bringing the long-stretching saga of Uber's compliance to its finale.[43]

It would be hard to say this is a total win-win for the stakeholders: Uber did get to conduct business in Taiwan, even expanded into delivery platforms afterwards, but its transportation service effectively pivoted into yet another taxi app. The part that would be most impactful and market-intrusive — ridesharing — was just left behind.[44] However, the competitive pressure from Uber significantly catalyzed the emergence of similar ride-hailing apps, some even from the largest taxi fleets themselves,[45] and "the Uber case" is still celebrated as vTaiwan's most significant success.

Shifting Headwinds

The rather unfortunate case of online liquor sales, meanwhile, allows us to really see the challenges of vTaiwan. The Taiwanese *Tobacco and Alcohol Administration Act* forbids any means of alcohol sales that cannot verify their consumers' age. The statute literally listed vending machines and e-commerce as some of the examples, banning the operation of online wine stores. As online shopping became popularized, merchants began advocating for lifting the restriction; independent brewers especially considered the law a hindrance to their development, as it prevented them from reaching their customer base.

The issue was brought to vTaiwan in early 2016, and an amendment that would allow convenience store pick-ups was passed by the cabinet.[46] Unexpectedly, the bill was retracted from the legislature a few months later in the new government term. The new administration cited uneasiness from social welfare groups as the reason behind walking back.[47]

41 Kuo-Wei Wu, Shun-Ling Chen, Poren Chiang, "Open with Caution: How Taiwan Approaches Platform Governance in the Global Market and Geopolitics", in *Perspectives on Platform Regulation*, Germany: Nomos, 1st, 2021, pp. 165–186. https://doi.org/10.5771/9783748929789-165.

42 J.R. Wu, "Uber resumes ride-hailing service in Taiwan after talks with authorities", Reuters, Apr 13, 2017. https://www.reuters.com/article/us-uber-tech-taiwan-idUSKBN17F0KB/ - last accessed June 2025.

43 Chang-Shun Lin, "Supreme Administrative Court Ruled En Banc: The Highway Agency Has No Jurisdiction Over Fining Uber", Central News Agency, Sep 18, 2020. https://www.cna.com.tw/news/asoc/202009180254.aspx - last accessed June 2025.

44 Yi-Hsuan Lee, "Exclusive Interview with Uber Taiwan General Manager: Changing the Consumers' Ride and Delivery Habits with 'Deals Too Good to Resist'", on *CommonWealth Magazine*, Sep 26, 2023. https://www.cw.com.tw/article/5127502 - last accessed June 2025.

45 Audrey Tang, "Uber responds to vTaiwan's coherent blended volition", Pol.is blog on *Medium*, May 23, 2016. https://blog.pol.is/uber-responds-to-vtaiwans-coherent-blended-volition-3e9b75102b9b - last accessed May 2025.

46 Shiao-Tien Tang, "Executive Yuan Greenlit Online Alcohol Sales, Limited to Convenience Store Pickup", ChinaTimes, Apr 28, 2016. https://www.chinatimes.com/realtimenews/20160428003692-260405.

47 Chih-Rong Kuo, "Online Alcohol Sales Scrapped! Major Policy Reversal as Executive Yuan Withdraws Bill from Legislature", Business Next, Aug 27, 2016. https://www.bnext.com.tw/article/40741/BN-2016-08-27-201942-44 - last accessed June 2025.

From the surface, this could've been considered a betrayal of the deliberative process. However, upon further inspection of the recorded meeting minutes, it became apparent that the citizen groups had never agreed on the proposed compromise in the first place. The plan was to launch convenience store pick-ups as a pilot all along.[48]

This exposed the underlying fragility of vTaiwan. The amendment was never a manifestation of the deliberation process, but a reflection of the political will behind it. This is better shown in the number of topics progressed through vTaiwan over the years (*Table 1*), where the change of administration in 2016 significantly curbed the ability to formulate new issues.

Table 1: Topic status progression on vTaiwan, 2015–2020

Year	Initiated	Drafted	Concluded
2015	11	8	3
2016	5	3	5
2017	7	8	1
2018	1	4	8
2019	1	1	0
2020	1	0	0

Despite the setbacks, a new wave of proposals still found their way through vTaiwan. Audrey Tang, also a long-time participant of the vTaiwan mechanism, was appointed to the cabinet to oversee digital transformation in the governmental body in 2016. She took over Jacyln Tsai's previous position to bring agencies to the stakeholder meetings while still accepting topic submissions from vTaiwan's community.

Topics from late 2016 to 2017 were mostly revamps of existing commercial law submitted by the Ministry of Economics, with the crackdown on non-consensual private images (revenge porn) being the sole topic proposed by the participants. This aligned with Tang's commitment to serve as a servant for the public servants and not to force agencies to partake in the procedure,[49] but without the will of a political figure, the decline of new initiatives had also turned apparent once the backlogs cleared out.

Meanwhile, Taiwan's online participation platform JOIN had just gained traction among grassroots movements. The JOIN platform offers a petition-based mechanism for the crowd to demand public answers from the agencies. Proposals are vetted for their wording and validity before entering a 60-day petition collection phase. Agencies are required to produce an official response within two months once 5,000 endorsements are collected. In a 2021 study, the JOIN platform had accumulated 9,729 issues that passed the 5,000 petition threshold, and 5,074

48 "March 31, 2016 [vTaiwan Virtual World Law Adjustment] Online Consultation Meeting (10): Accompanying Measures for Allowing Online Alcohol Sales", published on YouTube, Mar 31, 2016. https://www.youtube.com/live/BXa0Bqn02UI - last accessed June 2025.

49 g0v contributors, "Digital Minister: New Challenges of g0v × gov", published on g0v Hackpad, https://g0v.hackpad.tw/ep/pad/static/zZD5rfTKDNg - last accessed July 2025.

issues were verified by the agencies as policy-related.[50] Though agencies are not required to provide meaningful commitments or facilitate changes, some of the petitions did successfully spin up stakeholder meetings and hearings. Supporters of online liquor sales actually tried one more time to get the law revised in 2021 through this platform, though still rejected by the agency.

The form of stakeholder meetings was also being institutionalized at the moment. Through the establishment of Participation Officers,[51] at different levels of bureaucracy, cross-agency and public-private collaborations could happen much easier with a designated point of contact. POs not only bridge between external actors and the internal wiring within the agency, they also provide important institutional knowledge and act as the catalyst for the agency to adapt to changes. By 2022, a total of 120 collaborative meetings had been held, working on topics proposed from the JOIN platform or internally by POs themselves.[52]

In contrast, submissions from government agencies to vTaiwan ceased in late 2017. As official proposals became a rarity, the platform's only activity consisted of contracted law firms seeking aid to produce their policy reports; this practice also came to a halt when the pandemic struck in 2020.[53] As the community drifted apart from the government, members utilized the weekly meetups to discuss recent events and deliberative methods to this day.

III. The Question of Deliberation and Democracy

In the previous sections, we have examined two of the most iconic topics vTaiwan handled, along with its rise and subsequent decline. So what exactly made vTaiwan fail to address so many other issues that JOIN platform or collaborative meetings did?

The most apparent reason is the role of cabinet members behind what was advertised as a community governance model. Mei-Chun Lee pointed out in her field studies that vTaiwan bears an overdependence on political appointees for its legitimacy. As participant Billy Lin noted, a majority of vTaiwan's success stemmed from Minister Jacyln Tsai's contribution, 'as she could move issues she desire[d] to vTaiwan' and handle the logistics after the consultation concluded. The issues, however, were mostly the ones the minister cared about; and without statutory power or the authority coming from the minister-without-portfolio,[54] the agencies have no obligation to cooperate with dozens of tech-savvy "*concerned citizens*." This legitimacy problem also extends to the JOIN platform—even with 5,000 petitions (about 0.025% of total eligible voters), agencies might still consider citizen groups or legislators as more representative of the people's voice. Digital democracy still builds on representative politics and bureaucracy.

50 Hsin-Ying Huang, Mate Kovacs, Victor Kryssanov, Uwe Serdült, "Towards a Model of Online Petition Signing Dynamics on the Join Platform in Taiwan", in *2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG)*, IEEE, 2021, 199-204. https://doi.org/10.1109/ICEDEG52154.2021.9530852.

51 Public Digital Innovation Space (PDIS), "Directions for Implementing the Role of Participation Officers in the Executive Yuan and Subordinate Agencies", Dec 4, 2017, https://po.pdis.nat.gov.tw/en/directions/ - last accessed July 2025.

52 Public Digital Innovation Space (PDIS), "List of Collaborative Meetings", 2022, https://cm.pdis.nat.gov.tw/list/ - last accessed July 2025.

53 Mei-Chun Lee, "The Nobody Movement: Civic Hackers and Digital Activism in Taiwan", Taipei: Spring Hill, 2025, pp. 205–213.

54 Ibid.

The second reason lies behind the consensus-building method (coherent blended volition) vTaiwan cherishes. Yu-Shan Tseng pointed out that the so-called consensus does not resemble what participatory democracy scholars consider deliberation but rather relies on the logic of simple majoritarianism based on decisions that are already more or less made.[55] In the Uber case, instead of addressing the underlying social-economic inequalities, algorithmic reordering for plural opinions on Pol.is removed, details and nuances needed for deliberation—the point of the ridesharing economy was completely missed at the end of the day, and the opinion groups congregated on ideological statements that partially contributed to the "*tax vs. innovation*" tension.

The third reason is the unsustainability of the vTaiwan community model itself. In an interview, community moderator KY noted the involvement of STLI facilitators that handled plenty of the administrative burdens within the process; nevertheless, due to their status as a contractor, they were prone to the influence of the minister without portfolio. vTaiwan is actually 'more of a public sector-driven innovation than a community-led participation,' and to actually make the process open and participatory to the citizens, it was up to the goodwill of community moderators to monitor the production quality, the representativeness of stakeholders, and to participate in the discussions in person.[56] The sheer amount of workload was overbearing for virtually any volunteer.

Of course, not every democratic experiment is perfect, and the vTaiwan community still has its heritage and successes. However, with its fundamental issues on deliberation method and democratic legitimacy, vTaiwan is far from the *deliberative democracy* or *digital democracy* savior its advocates portray.

IV. Epilogue: Moving Past the Myth of Panacea

To the participants of vTaiwan, the trouble was that the platform was marketed as a democratic 'panacea from the Far East island nation,' an orientalist image painted by open government advocates to miraculously solve democratic challenges. To make progress is easy, KY warned, as agencies could just gather a bunch of puppet stakeholders and accept whatever proposals the public suggested. Though without real deliberation, the consultation process would merely become a tainted act of *openwashing*.

We have already seen similar cases in France. In an open letter, a coalition of NGOs in France condemned "the government increases consultations to give the impression to civil society that they 'co-construct' policies of the country, but they stay deaf [sic] to calls of citizens and to those of their representatives, as soon as the subject raised or the tone do[es] not please them."[57] By selectively utilizing the consultation process, the government could "*borrow*" into the voice of the people with little consequences.

55 Yu-Shan Tseng, Liquid Democracy: A Comparative Study of Digital Urban Democracy, UK: Wiley, 1st, 2025, pp. 112&166.
56 Appendix I-2: "vTaiwan" Interview, in *Civic Technology and Its Role in Digital Democracy: Case Studies of Taiwan, Japan, and South Korea*, Taiwan: Ministry of Digital Affairs, 2024, pp. 61–84.
57 "Open Government in France: an Empty Promise?", published on La Quadrature du Net, Dec 9, 2016. https://www.laquadrature.net/en/2016/12/09/Open-Government-France-an-Empty-Promise/ - last accessed June 2025.

This is not limited to countries alone. In 2023, a restructured vTaiwan community joined forces with Chatham House and the AI Objectives Institute to run a pilot program for OpenAI to identify the priorities in AI governance. The assembled international and local cohort, which one might think should be formulated similarly to a multi-stakeholder group, was instead overly-represented by males in the AI industry and snowballed connections.[58] This raised the concern of tech companies taking advantage of the deliberative process and community reputation for advancing specific narratives.

Ultimately, the vTaiwan methodology produces just enough rough consensus with its digital tools. For meaningful participation, political figures need to relinquish part of their control to the citizens on agenda setting; [59] to achieve meaningful deliberation, administrative procedures shall adopt proper stakeholder assessment and data collection process.[60] Future initiatives must move beyond single-issue successes and find ways to embed deliberative processes more deeply into the standard operations of government agencies. For deliberation to happen here, democracy must first be possible here.

ABOUT THE AUTHOR

Poren Chiang

Member, Digital Law Task Force, Judicial Reform Foundation, Taiwan

Poren is a Digital Law researcher based in Taiwan. He holds an LL.M. from UCLA School of Law, specializing in Digital Law and Policy. An active software developer, he has collaborated with civic tech communities and free software initiatives on both legal and technical matters. His research focuses on digital governance, open data, and data surveillance. He is currently advocating with civic groups in Taiwan for a proper Digital Bill of Rights (DBR).

58 Flynn Devine, Alex Krasodomski-Jones, Carl Miller, Shu Yang Lin, Jia-Wei Cui, Bruno Marnette, Rowan Wilkinson, "Recursive Public: Piloting Connected Democratic Engagement with AI Governance", vTaiwan × OpenAI, 2023. https://vtaiwan-openai-2023.vercel.app/Report_%20Recursive%20Public.pdf.

59 "2016 vTaiwan & Join Platform Analysis Interview (Audrey Tang)", published on SayIt Archive. https://sayit.archive.tw/

60 Ibid.

REGULATING INNOVATION THROUGH EXTRA-FINANCIAL INFORMATION

Jonathan Keller

I. Introduction

Is a company's ultimate goal being to optimize, no matter what, the valuation of the shares to generate a return on investment to shareholders? Beyond the sole question of the purpose of capitalism, the main difference with non-profit organisations (NGO), the distribution of responsibilities between stakeholders of a company, i.e., the management and shareholders, has to be questioned. The sole function of managers used to ensure the return on investment (ROI) to investors,[1] at the point that, in 2012, Leo STRINE - Chief Justice of the Delaware Supreme Court - declared that generating maximal value for shareholders is enshrined in hard law.[2] However, without questioning the drive for profits, the evolution of the society integrated new actors into the notion of stakeholders, such as workers, contractual parties, and geographical neighbourhood entities. In 2014, the United States (US) Supreme Court overturned that vision in *Burwell v. Hobby Lobby* by holding that the duties of managers extend beyond assuring a sole return to investors.[3] Even if theorized in the 1970s,[4] this extension is updated on the premise of a finite world by aiming mainly to reduce corporates' impacts/abuses on the environment. Various actions are available, such as environmental bonds,[5] or extra-financial reporting;[6] the first incentives manage investors' expectations on the ROI or furnish alternative valuation,[7] where the reporting obligation has to reveal the true state of health of the company to potential or actual shareholders.[8] This last obligation lies on the Corporate Social Responsibility (CSR) principle, but not exclusively. Many US,[9] and European Union (EU),[10] laws enforce a liability regime for disclosing corporate's actions into extra-financial information to notify shareholders fully of any danger to the value of the corporation.[11] This information shall therefore contain markers on the (1°) corporate actions and strategy on social and environmental, (2°) human and financial means

1 *Michigan Supreme Court, Dodge v. Ford*, 170 N.W. 668, 684 (Mich. 1919) "*A business corporation is organized and carried on primarily for the profit of the stockholders*."

2 Leo E. Strine Jr., *Our Continuing Struggle with the Idea That For-Profit Corporations Seek Profit*, *Wake forest Law review*, Vol. 47, p. 135, (2012), "The corporate law requires directors, as a matter of their duty of loyalty, to pursue a good faith strategy to maximize profits for the stockholders."

3 134 S.Ct. 2751, 2771 (2014). While it is certainly true that a central objective of for-profit corporations is to make money, modern corporate law does not require for-profit corporations to pursue profit at the expense of everything else, and many do not do so. For-profit corporations, with ownership approval support a wide variety of charitable causes, and it is not at all uncommon for such corporations to further humanitarian and other altruistic objectives.

4 See Roberta Dahl, "After the revolution", 80-87 (rev. ed. 1990), commented in Vincent M. Di Lorenzo, "Equal Economic Opportunity: Corporate Social Responsibility in the New Millennium", 71, *University Colorado Law Review*, vol. 51 (2000), Available at: https://scholar.law.colorado.edu/lawreview/vol71/iss1/4 (last consultation 10/06/2025).

5 Di Zhou & Alexios Kythreotis, "Why issue green bonds? Examining their dual impact on environmental protection and economic benefits", *Humanities and Social Sciences Communications*, volume 11, 2024.

6 Madison Condon, "Green' Corporate Governance" In *Oxford Handbook of Corporate Law and Governance*, 2nd ed., *Boston Univ. School of Law Research Paper No. 4556184*, Available at SSRN: https://ssrn.com/abstract=4556184 (last consultation 10/06/2025).

7 Such as less taxes (see footnote 5).

8 Hereinafter we will refer to both actors as "shareholders".

9 Congress of United States, An Act To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes, Pub. L. 107–204, also known as SOX.

10 European Parliament and the Council, Directive (EU) 2022/2464 of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (OJ L 322, 16.12.2022, pp. 15–80) also known as "CSRD Directive" and Directive (EU) 2024/1760 of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (OJ L, 2024/1760), 5.7.2024 also known as "Due Diligence Directive".

11 Jeffrey Bauman, Alan Palmiter & Frank Partnoy, *Corporations law & policy*, Thomson West, 6th ed., 2007, p. 1164, spéc. p. 721 recalling, for the SOX (footnote 9) the existence of « directors' and officers' liability insurance (« D&O Insurance ») which exclude from this coverage any « material misrepresentation » i.e. « *extensive descriptions of the corporation and its finances, including the latest annual report, and financial statements.* » see also « *The insured must disclose knowledge* » *of "any act, error, or omission which might give rise to a claim under the policy*".

to implement this strategy, and (3°) the results. Among other topics, "sustainability reporting" which gathers data on environmental topics (ex: carbon footprint, energy savings) and on the due respect to human rights.[12] It is important to emphasize that this extra-financial reporting is written by managers to report their actions to shareholders,[13] and to "*federal bureaucrats (...) patrol(ing) the markets.*"[14]

This long development introduces two main aspects of our thematic: the reconsideration of the theory of the agency,[15] questioning the liberties granted to the management to produce wealth, and the possibility of including the impacts of artificial intelligence (AI) within the sustainability reports. The exercise is perilous since those reports aim at the socio-environmental impacts of companies. More precisely, is the choice for a manager to replace all or part of his workforce by AI subject to being validated by the shareholders, to a vague environmental reporting, or to the sole directors' discretion?

The US Securities and Exchange Commission (SEC) answered partially to this question on 3rd January 2024 by replying to a claim formulated by AFL-CIO Equity Index Funds on the basis of Rule 14a-8(i)(7).[16] This article grants to any qualifying shareholder,[17] the right to force the (management of the) company, through an order issued by the SEC, to include a resolution and supporting statement in the company's proxy materials for its annual meeting. As such, AFL-CIO Equity Index Funds is a labour union acting as a shareholder against Disney,[18] and Apple,[19] respective, management to include in the shareholders' reports all developments regarding the use of AI and the associated ethics code. Thus, the sustainability report including socio-environmental actions shall now take into consideration major technology choices made by the management, since those choices have a societal impact on the human workforce. This strategy allows union labours to go through the window (*as a shareholder*) when the door was closed (*as a labour union*) by the management.

The social prudence prophesied by Asimov's Caves of Steel,[20] to ease the social acceptability of robots through the guarantee of the artificial life's harmlessness, was dismissed in our reality. Newspaper headlines such as What Jobs Will AI Replace First?,[21] witnesses this choice. The Fourth Industrial Revolution,[22] is marching and raises the threat of global computerization, implying

12 See Infra II.A. on the blur around this notion.
13 William W. Bratton and Michael L. Wachter, *Shareholders and Social Welfare*, *Seattle University law review*, Vol. 46, p. 489 (2013), spec. p. 495.
14 Ibid.
15 i.e. "*directors and their executives are appointed to run the corporation on behalf and for the benefit of shareholders*" definition provided by M. Yan, "Corporate Social Responsibility versus Shareholder Value Maximization: Through the Lens of Hard and Soft Law", *Northerwestern journal of International law & business,* vol. 47 (2019), available at https://scholarlycommons.law.northwestern.edu/njilb/vol40/iss1/2, (last consultation 10/06/2025) pp. 45-86, spec. pp. 54-55.
16 Code of Federal Regulation, 17 CFR § 240.14a-8 - Shareholder proposals.
17 See the conditions in Article 14a-8(ii)b.
18 US Securities and Exchange Commission, Reply of the 3rd of January 2024 to the Walt Disney Company, available at https://www.sec.gov/files/corpfin/no-action/14a-8/nlpcdisney11524-14a8inc.pdf (last consultation 12/06/2025).
19 US Securities and Exchange Commission, Reply of the 3rd of January 2024 to Apple Inc, available at https://business.cch.com/srd/AppleInc_.pdf (last consultation 12/06/2025).
20 Isaac Asimov, *The caves of steel*, Doubleday, 1954.
21 Bernard Marr, "What Jobs Will AI Replace First?", in *Forbes*, 2024, available at: https://www.forbes.com/sites/bernardmarr/2024/06/17/what-jobs-will-ai-replace-first/ ; comp. Ben Lutkevich, "Will AI replace jobs? 18 job types that might be affected" in *TechTarget*, 2025, available: at https://www.techtarget.com/whatis/feature/Will-AI-replace-jobs-9-job-types-that-might-be-affected enumerating "legal" as one of the most threatened work by the AI (last consultation 10/06/2025).
22 Simona Abis, Laura Veldkamp, "The Changing Economics of Knowledge Production", *The Review of Financial Studies*, volume 37, issue 1, 2024.

the necessity for workers to adapt or to be replaced by a machine. Offering the choice of the technology to the sole management was, until AI, a liberty which was not generating a real social revolution since the necessity of human agents. The generalisation of AI, however, questions the very identity of actors such as Disney and the "spirit embedded". The SEC's rejection of the defendant's claim underlines the complexity of the deployment of AI within a corporation by the management, by restraining their power (II). However, extra financial information is very far to solve any matter on our issue. The applicable texts are blurry and therefore leave a real margin of appreciation with an *ex post* control to a third party (III).

II. The Choice of AI for a Corporation: A "New" Class Struggle

When the Means of Production become Workers

To appreciate fully this problematic – *the soft control of shareholders on the use of AI deployed within one's company* - it is necessary to limit the width of technology to our subject. Even if both companies quoted the first White House's 'AI Bill' of October 2022, this text needs to be discarded from further discussion. Designed to have more symbolic value than normative one, this text was one of the many repealed at the beginning of Trump's administration,[23] to be replaced by ones of his own.[24] Where Biden's act assimilated AI as a software 2.0,[25] Trump's one, enacted after the SEC's rejection, refers to a real legal definition of AI,[26] close to Article 3(1) of the EU's AI Act.[27] Those two texts include some autonomy of the AI to distinguish it from the software underlining this way of its novelty.[28] However, those legal definitions are organic, general, and rarely functional.[29] Thus, to narrow down our problem, we need to define the AI questions within the SEC's cases threatening the human workforce.

23 White House, Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30 october 2023, available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (last consultation 10/06/2025).

24 White House, Executive Order 14179, *Removing Barriers to leadership in artificial intelligence*, January 23, 2025, available at https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/ (last consultation 10/06/2025).

25 Automated systems" defined "*any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities*"

26 15 U.S.C. 9401(3) : "*The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to-(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.*"

27 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) , PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.

28 AI system as "*a machine-based system (...) designed to operate with varying levels of autonomy and (...) exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*".

29 The rare functional definitions of AI systems within the EU AI's act aim to qualify such systems as "forbidden" or "high risk" (see Annexe 1).

- Firstly, platforms such as "Uber" need to be excluded from our problematic since the work relationship was initially designed to be ruled by algorithm.[30]
- Secondly, we need to stress the difference between the situation where the AI systems are replacing the human workforce with the one where AI is merely tools for work.
    - For example, the"Algorithm management" described as "*increasing automation will reduce the strains of unfilling tasks, making space for human creativity and ingenuity to flourish*",[31] or "AI agents" described as a "*software entity that employs AI techniques and has agency to act in its environment based on set goals, which means it can decide which actions to perform and has the ability to execute them.*"[32]

In both subcategories, AI is a tool at the service of the workers, fulfilling this way the computer science's promise.[33] Furthermore, the inherent risks embedded within, mainly excessive surveillance before getting data to replace humans.[34] Still, those different AIs are tools to accompany human workers, not autonomous systems replacing the workforce. The aforementioned regulations, particularly the EU AI Act, address or prohibit some AI functionalities.

AI functionalities such as generative AI - producing text, images, videos, or other forms of white collar labor – are considered as general AI systems. Thus, the appreciation or mitigation of any risk will be minimal through the assessment of any impact of fundamental rights,[35] or through deceptions to end-users.[36] None of those two situations applies within the automation of human labor, excluding those of further considerations. Disqualifying generative AI as a "high risk AI" frees providers or users from any prior formality. Readers will acknowledge that the EU AI Act is explicitly aiming at certain functionalities, as social scoring, über-surveillance,[37] or discrimination, as a high risk. Therefore, the replacement of the human workforce by AI systems for shareholder value maximization,[38] is possible. Formulated another way, negative social impacts due to massive layoffs are not a considerable factor, and the involvement of the remaining humans in the creation of content will be enough to discard any transparency duty or any kind of prior assessment. Few legal provisions are obviously framing the deployment of a new technology within a company.[39] Those legal rules are weak since workers do not have real control over the means of production, particularly if those are surveilling them after being trained on their digital footprint, or to put another way, AI tools could be seen as interns trained to replace the human workforce.

30 See Jamil Rabih, "Uber and the Making of an Algopticon – Insights From the Daily Life of Montreal Drivers", in *Capital & Class*, "Machines & Measure", Ed. by Phoebe Moore et al., available at SSRN: https://ssrn.com/abstract=3490030; also see Gérard Haas & Marie Torelli, "Comme un patron : UBER dirige, contrôle et sanctionne !", *Blog du Cabinet Haas*, 06 march 2020, available at https://info.haas-avocats.com/droit-digital/comme-un-patron-uber-dirige-controle-sanctionne (last consultation 10/06/2025).

31 Theo Cox and Gerard Rinse Oosterwijk, *Algorithmic management in the workplace*, available at https://feps-europe.eu/wp-content/uploads/2024/09/Algorithmic-management-in-traditional-workplaces.pdf (last consultation 10/06/2025).

32 IBM AI ethic board, *AI agents : opportunities, risks and mitigations*, 2025, available at https://www.ibm.com/granite/docs/resources/ai-agents-opportunities-risks-and-mitigations.pdf (last consultation 10/06/2025).

33 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 1 "informatic technology must be at the service of every citizen" (« L'informatique doit être au service de chaque citoyen. »).

34 Daryl Lim, "Determinants of Socially Responsible AI Governance", 25 *Duke Law & Technology Review* 183-232 (2025) Available at: https://scholarship.law.duke.edu/dltr/vol25/iss1/5 (last consultation 10/06/2025).

35 AI Act: Article 9(2)-a on high risk, Article 27 on the methodology and information expected.

36 Digital Service Act (Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC OJ L 277, 27.10.2022, p. 1–102): Article 25 on online interface design; AI Act: Article 5(a) on the prohibition of subliminal techniques enhanced by AI.

37 See Jamil Rabih, "Uber and the Making of an Algopticon – Insights From the Daily Life of Montreal Drivers", note supra.

38 M. Yan, "Corporate Social Responsibility versus Shareholder Value Maximization: Through the Lens of Hard and Soft Law", supra.

39 Infra I.B.

The action led by the ACL-CIO Index Funds is interesting for many points. It is relevant to see a union acting as a shareholder to use the master's tools, not to dismantle the master's house,[40] but to save white collar workers, as graphic designers from Dall-E® or Midjourney®. This situation is far from Brian Merchant's Luddites,[41] justifying violence against machines in the name of workers' rights facing automation. The use of the shareholder rights approach by a union is original, since historical unions' approach focused more on labor laws resistance.[42]However, instrumentalizing the use of shareholders' prerogatives by a union to exercise a tougher control on the management diminishes the uncertainty of social or legal struggles. The disclosure of the use of AI systems and the ethical codes attached to extra-financial documents may create a relevant alternative to the name & shame practices used by unions to denounce management's behavior.[43] Furthermore, such disclosure will allow the shareholders to appreciate the ethical values held by the management: Disney, for example, to uphold the company's values by providing only human-generated content. As we will see at the end of this article, ethical codes bind the management's behaviour through a liability regime lying on consumer law.[44]

The Choice of Technology by the Management

SEC's replies have a broader effect than this particular case since they triggered a reform of the Commission's interpretation of Rule 14a-8(i)(7). This new interpretation perceives broadly issues related to social and ethical concerns, regardless of their economic relevance or significance to a particular company,[45] and thus limits management power on "ordinary business" exclusion. This exclusion rests on two central considerations relating to (i) the proposal's subject matter, i.e. subject "*so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight*",[46] and (ii) the degree to which the proposal "micromanages" the company, i.e. through "*probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment*".[47] As we will explain in this paragraph, choices of technology have been raised on the latest consideration. Of course, the use of Microsoft Office suites for workers has, *prima facie,*[48] little or no impact on shareholders since such software are tools *per se*. On the other hand, laying off workers to replace them with AI is a social concern eligible to Rule 14a-8(i)(7).

As a prior announcement, the SEC's 2014 reply is quite enlightening regarding its very procedure for implying the right to shareholders to appreciate the use of such novel technologies as financial information. Such judgment constitutes a SEC's case law reversal on such a matter,

40 To paraphrase Audre Lorde, "The Master's Tools Will Never Dismantle the Master's House" in *Sister Outsider*, Crossing Press ed., United States, 1984.
41 Brian Merchant, *Blood in the machine*, Little, Brown and Company, United States, 2023, p. 496.
42 Félix Tréguer, L'Utopie Déchue, Fayard, 2019, telling the action of Laurent Chemla and Stephane Bortzmeyer to support the CGT at the dawn of automatisation.
43 Nicole Stolowy, Hervé Stolowy, "Name and Shame: A Comparative and International Analysis of Whistleblowing Laws", *HEC Paris Research Paper*, 2022, No. LAW-2023-1491, Available at SSRN: https://ssrn.com/abstract=4380430 (last consultation 10/06/2025).
44 Infra II.B.
45 Securities and Exchange Commission, *Staff Legal Bulletin* No. 14M (CF) (SLB 14M) of 12 feb. 2025.
46 Securities and Exchange Commission, *Release No. 34-40018* (May 21, 1998).
47 Ibid.
48 Ministerie van Justitie en Veiligheid (netherland justice office), *DPIA Office 365 for the Web and mobile Office apps*, 20 June 2020, https://slmmicrosoftrijk.nl/wp-content/uploads/2021/07/200630-DPIA-Office-for-the-Web-and-mobile-Office-apps.pdf (last consultation 10/06/2025) pointing all the personal data issues on the use of Microsoft's Office.

since the Commission tended to qualify the choice of technologies by companies,[49] as business matters related to practices and operations.[50] Such reversal may be justified both by the very use of AI but also by the nature of the main proponent,[51] who triggered this litigation: one of the main federations of labor unions in the United States.

The fact that direct collective bargaining has few effects on AI as a workforce. Even if local laws enacted in US are pushing to consult labor unions prior to any AI deployment,[52] Trump's proposal, the *One Big Beautiful Bill Act,*[53] will create a moratorium on State AI legislations. Formulated another way, Section 43201 of this proposal will preempt several enacted and proposed restrictions by prohibiting any state or local enforcement "*limiting, restricting, or otherwise regulating*" AI models, AI systems, or automated decision systems. In Europe, apart from Germany's labor law,[54] such consultation is not mandatory. The French example is relevant to underline the collective bargaining and its very low impact. The *Comité social et économique* (CSE), created by articles L 2311-1 to L2311-2 *du Code du travail*,[55] acts as employees' delegates,[56] or combines the responsibilities of works councils,[57] CHSCT,[58] and employees. Employers need to consult this committee prior to any technology update within the company to appreciate the impact on employees' health and working conditions. Even if this procedural consultation is more formal,[59] than effective, the CSE cannot oppose the deployment of a new technology without real threats to health or security of the workers. Of course, the CSE represents workers, but as a company organ. It is neither a labor union nor a shareholder,[60]

Thus, the weakening of the theory of the agency initiated by the SEC only benefits directly to shareholders and not to labor unions or representatives' organs. The company's ordinary business operations are delegated exclusively to the executive board to avoid any micromanagement,[61]

49 Constant case law: SEC, AT&T Inc., 13 February 2012, rejecting the request of a report on financial and reputational risks posed by continuing to use technology that inefficiently consumed electricity.

50 Constant case law: see SEC Westinghouse Electric Corporation, 27 Jan. 1993, rejecting the request of shareholders to access policies, guidelines, and actual practices of an unprofitable subsidiary, see also SEC JPMorgan Chase & Co., 21 March 2023, refusing the request on company business practices that prioritize non-pecuniary factors when it comes to establishing, rejecting, or failing to continue client relationships.

51 It is interesting to see that in Disney's case the New York City Employees' Retirement System, the New York City Fire Pension Fund, the New York City Police Pension Fund and the New York City Board of Education Retirement System were also co-filers.

52 New York City, local law 144 of 2021 updated on 5th July 2023, Illinois HB3773 of 8th august 2024, Colorado *Consumer Protections for Artificial Intelligence*, SB24-205 of 17 may 2024 and New Jersey, *Assembly bill 5053*, 9th Dec. 2024.

53 H.R.1 - One Big Beautiful Bill Act 119th Congress (2025-2026).

54 Where Union Labor are powerful and negotiated since 2010 the limitation of automation.

55 Ordonnance n° 2017-1386 du 22 septembre 2017 relative à la nouvelle organisation du dialogue social et économique dans l'entreprise et favorisant l'exercice et la valorisation des responsabilités syndicales, JORF n°0223 du 23 septembre 2017.

56 For company having less than 11 employees.

57 Upto the number of employees within the company.

58 « *Comité d'hygiène, de sécurité et des conditions de travail* », described by Article L. 4612-1 du code du travail as contributing to physical and mental health of employees and to improve working conditions.

59 See Tribunal judiciaire de Nanterre du 14 février 2025, Corinne Baron-Charbonnier, « Décision du Tribunal judiciaire de Nanterre du 14 février 2025 : quel rôle pour le CSE dans les phases d'implantation de l'IA en entreprise ? », 30 April 2025, https://www.lamy-liaisons.fr/eclaireurs-du-droit/decision-du-tribunal-judiciaire-de-nanterre-du-14-fevrier-2025-quel-role-pour-le-cse-dans-les-phases-dimplantation-de-lia-en-entreprise/ (last consultation 10/06/2025) where an AI deployment was cancelled due to the absence of a prior consultation.

60 Prior to the redaction of this article, several French union labours explained to us that it was not their "historical" and "social" "DNA" to become shareholders to use those kind of rights.

61 SEC, Staff Legal Bulletin No. 14L, 03 Nov. 2021, available at https://www.sec.gov/rules-regulations/staff-guidance/staff-legal-bulletins/shareholder-proposals-staff-legal-bulletin-no-14l-cf (last consultation: 07 may 2025): "*This approach is consistent with the Commission's views on the ordinary business exclusion, which is designed to preserve management's discretion on ordinary business matters but not prevent shareholders from providing high-level direction on large strategic corporate matters*."

Among those exclusive delegations, day to day life operation such as the choices of the product created, the way of distribution, the distributors and the choice and implementation of new technology used or developed by the company,[62] the latter being negated in the present cases. Both companies' reply summons the AI definition in the White House's bill is being construed as an old technology with a limited impact on the company,[63] and, with the reinforcement of the SEC jurisprudence,[64] to support their position by limiting AI's effects on social concerns.

III. Social Impacts of AI as an Extra-Financial Information: An Accountability Means

Principles and Limited Applications of the Extra Financial Information

Certain public policy rules ensure that shareholders benefit from trustworthy information on the corporate life from the executive management.[65] This accounting information constitutes a guarantee of good governance for investors. As mentioned above, the weakening of the theory of the agency is being exacerbated by the extra financial information required by recent EU legal frameworks. This new framework requires the management to take into consideration societal parameters.[66]

These texts provide a standardized framework on environmental, social, and governance information, the *European Sustainability reporting standards*, to companies. However, the social aspect is quite limited,[67] even for the Due diligence directive.[68] Those texts are part of the *European Green Deal*, and human rights are addressed through the spectrum of environmental sustainability of the product/service. More specifically, indicators are mainly aiming:

- the social condition of the workers, such as the benefit of a work contract including the working hours,[69] social coverage, the wages.[70]
- The number of lawsuits related to human rights infringement, as discrimination,[71] or any accident related to work.[72]
- Even if collective bargaining, including collective labor agreements, is a criterion, the impact of this indicator seems limited.

62 Disney, p. 5 " *routine operations, including those with respect to content development and distribution, supply chain management, contract management, financial management and planning, and management*".
63 Disney, pp. 4-5; Apple p. 5.
64 Modestly, the case law quoted by the representatives of Apple and Disney are not convincing.
65 See for example in United States, Foreign Corrupt Practices Act (FCPA) Act of 1977 (15 U.S.C. §§ 78dd-1, et seq.) enacted for making it unlawful to make payments to foreign government officials to assist in obtaining or retaining business followed by the Federal Sarbanes–Oxley Act of 2002 mandating certain practices in financial record keeping and reporting for corporations (Pub. L. 107–204, 116 Stat).
66 Ref. Footnote supra 9.
67 The ESRS are divided in 4 topics; the environmental one is the more important one.
68 Since only the chain of activity was preferred to the chain of value reducing drastically the *ratione materiae* to the sole contractors upstream and excluding downstream contractors, whereas the CSRD Directive aims the workers of the chain of value.
69 S1-6 indicator detailing the numbers of permanent employees, temporary workers and contractors.
70 If the wages are decent (S1-10 indicator) or if there is any discrepancies between man/woman (S1-16 indicator).
71 ESR S1 – 17 indicator is also including slavery and child labor.
72 S.1.-7 indicator.

- The existence *per se,* of such contracts assumes fair governance, also problematic, since it lies on the corporate values to conduct business.
    - The existence of a code of conduct implementing the detection of infringement or corruption, 'including lobby activities'.[73].

Such a summary brings back to the same criticism developed on the technical standard ISO 26000 meant to "*operationalize*", i.e., to bend the duties of the transnational companies, the United Nations Global Compacts.[74]

Even if CSRD and Due Diligence directives standardized the reporting, those texts are developed on a consensus based on what corporates, particularly their own managements, wish. Such corporate legal bargaining reveals imperfect indicators by design. Alas, the inclusion of AI in such reporting will – in European law – at least be reflected mainly on their energetic aspects or on the training of necessary staff,[75] – which is basically already a legal obligation.[76] The variation of human labor is not a meaningful criterion to take into consideration. It is, however, important to underline two main points to understand plainly our issue.

Finally, even if the CSRD and duty vigilance directive are creating an extra-financial information duty, the modalities of this duty are – at least on digital issues – soft. Where its implication for the environmental cost is "*easy*" to calculate,[77] the very question of the societal impact of digital activities, and now from the AI, is quite controversial.[78] There is a real risk of underestimating such impacts, but more precisely a real industrial work of undermining those assessments to limit corporates' liability on their social impacts. The enforcement of EU 2025/794 Directive,[79] also known as the Omnibus directive, reflects such endeavour by undermining the EU Green Claim Directive, aiming to harmonise labels and certifications.[80] Another example of such setbacks, extra-financial information is due every five years instead of every year, and the width of the stakeholders to think about. Such deregulatory policies also exist in the US, as the Trump AI Act shows.

"Accountability" by Default

Since the legal framework presented above creates an information duty benefiting a wider notion of stakeholders, its digital aspects fall within the scope of the principle of accountability, which can be summarized as an obligation for a company to take all compliance steps to avoid

73 G.3 and G1-5 indicators.

74 V. J. Pitseys, C. Ruwet, *La mise en récit comme source de motivation et de légitimation au cœur des nouvelles techniques de régulation*, Droit et société, 2014/1 n° 86 | p. 13.

75 To keep a control on the AI deployment for example, see Winston Maxwell, Le contrôle humain des systèmes algorithmiques, thèse HDR, Droit. Université Paris 1 Panthéon- Sorbonne, 2022. ⟨tel-04010389⟩.

76 Article 4 of AIA, Article L4121-1 (on the duty of the employer to provide a training) and L6321-1 (on the right of the employee to be trained with new tools to keep his/her work) *du code du travail.*

77 For example, the 5G's environmental impact negotiation were focusing on whether the antenna was on or off, if the electrical power was solar or from a nuclear plant, if the antenna was in the shade or in plain sun… Many criteria leading to an artificial decrease of the environmental impact.

78 Jonathan Keller, "Droit de l'environnement et numérique" in *Numérique, droit et société*, Dir. Bénédicte Bévière-Boyer & Dorothée Dibie, 2022, Dalloz, Collection : Thèmes & commentaires, Actes.

79 Directive (EU) 2025/794 of the European Parliament and of the Council of 14 April 2025 amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain corporate sustainability reporting and due diligence requirements (Text with EEA relevance) PE/6/2025/REV/1, OJ L, 2025/794, 16.4.2025.

80 Proposal for a Directive on substantiation and communication of explicit environmental claims (Green Claims Directive) COM/2023/166 final.

any heavy penalty. The very difference of regimes stands on the availability and goal of the information. Where the extra-financial information shall reveal the company's impact on society to shareholders to advise them on keeping or purchasing shares, the documents realized by the data processor in the name of the principle of accountability – such as impact assessments,[81] – are being stored as proof of compliance for the competent national authority.[82] Thus, the information provided is completely different from one document to another. Furthermore, companies do not publish impact assessments since it may state internal cybersecurity setups, and such publication may create vulnerabilities. We stressed above that, aside from issues such as discrimination, surveillance, or grading employees, AIs are not considered high risk or as subject to DPIA. The deployment of AI to replace the human workforce may alas, be limited in some way to the sole extra-financial information.

This sole publication does not mean that management is totally free since, even if all legal means are extinguished, the technique called "name and shame" is being used by non-governmental organizations to reveal corporate malpractice. The data is extracted from the extra-financial information and compared with open-source intelligence.[83] Once there is a high likelihood that an offence was constituted, those non-profit corporations contact the press to ensure the public institution follows up on the lawsuit. However, the notion of "offence" must be understood widely by incorporating the breach of the ethical code by the management has been judged, in the US, as a deceptive practice based on Article 5 of the FTC Act.[84]

In this case, NGO may raise the issue by collecting proves of such infringement to underline commercial and political statements with reality. Still, our situation is far from this idea, since the search for profit by using new technologies instead of human labour is not a crime. However, the bad buzz around such practices may limit such behaviour as the misuse of workers' personal data or production of those data, illegally obtained, to train the AI deployed within the company.[85] Even if the legal implications and effects of such litigious AI are still objects to scholarly discussion, we could assimilate with an illegal product,[86] being used/distributed by a company, justifying human workers' return. In the first hypothesis, the AI editor has to replace the problematic IT system with a compliant or to take the necessary measures to regularise the situation.[87] The second situation is quite different since the in-house AI system shall be put in hold until its compliance with regulatory rules. In such a case, it is possible for workers to reclaim redress in the name of labour laws.[88]

Prima facie, the interpretation of the SEC's replies to Apple and Disney could be a real object of rejoicing since the race to automation will be counterchecked by shareholders on legal grounds and not left to the sole management's full discretion. The different IT scandals revealed the indifference of the general public to the contents' recipes; the price is still a primordial factor.

81 DSA's Article 34 on systemic risk, GDPR's Article 35 on high risk, AAI's Article 27 on fundamental rights impact assessment.
82 Article 29, Opinion 3/2010 on the principle of accountability, 13 july 2010, WP 173, p. 19, spec. p. 5, §12.
83 Such as domestic or international news, patents or scientific literature.
84 US Supreme Court, *Nike, Inc. v. Kasky*, 539 U.S. 654 (2003), about the right of a private party to seek redress for a company's allegedly false and misleading statements about the production of the goods that the company sells, if the private party himself did not rely on those statements, purchase the goods, or suffer any actual injury by reason of such reliance.
85 See in US for illicit use of proprietary data to train machine learning system, District court for the district of Delaware, 2 febr. 2025, Thomson Reuters enterprise center c/ Ross intelligence inc., n° 1:20-cv-613-SB.
86 See in France Cass. Com. 25 June 2013 n°12-17.037 on the illicit transfer of non-compliant personal data.
87 Which the generic warranty stipulation in IT contract.
88 See supra about the prior communication of the deployment to workers.

However, the public disclosure of AI and ethical guidelines extends the stakeholders' definition,[89] offering new means of control to third parties, i.e., civic society. Naturally, shareholders value more ROI than social aspects. Of course, one solution may be to create "social bonds" on the model of the environmental ones to create incentives to keep a human workforce within companies. However, as the CSR and environmental standards certified by dubious labels revealed, a high risk exists in reality to facilitate the conduct of business.

ABOUT THE AUTHOR

Jonathan Keller

Independant researcher

Jonathan holds a PhD in Law and specializes in Data Protection and Intellectual Property. As a research engineer, he works on legal issues related to new technologies. He lectures at several universities and contributes to interdisciplinary research programs. A prolific author, he regularly speaks at conferences and participates in institutional expert groups.

89 Edward Freeman, and John McVea, "A Stakeholder Approach to Strategic Management", *Darden Graduate School of Business Administration University of Virginia*, Working Paper No. 01-02 (2001). Available at SSRN: http://dx.doi.org/10.2139/ssrn.263511 (last consultation 10/06/2025).

This page is intentionally left blank.

KONRAD ADENAUER STIFTUNG

Konrad-Adenauer-Stiftung Cambodia
House No. 4, Street 462, Khan Chamkar Mon
P.O.box 944, Phnom Penh, Kingdom of Cambodia
Telephone : + 855 23 966 171
E-mail : Office.Phnompenh@kas.de
Website : www.kas.de/cambodia
Facebook : www.facebook.com/kaskambodscha
Instagram : www.instagram.com/kas_cambodia

9 789996 390739