Seven Perspectives for Realizing a Data-Driven Society

I. Core vision of a data-driven society

"On the threshold of the 21st century, Japan must take revolutionary yet realistic actions promptly, without being bound by existing systems, practices and interests, in order to create a 'knowledge-emergent society,' where everyone can actively utilize information technology (IT) and fully enjoy its benefits."

This is the first sentence of the e-Japan Strategy adopted by the IT Strategy Headquarters (Advanced Information and Telecommunications Network Society Promotion Strategic Headquarters) in January 2001. Some 20 years have passed since the conception of the e-Japan Strategy, and while Japan has become the world's most advanced in developing broadband infrastructure, including optical fiber networks, digitalization in various areas, including government, healthcare, and education, has been noticeably slow. We will examine the reason behind this from two aspects. First, looking at the corporate management level of digital investment, digital investment in Japan has been primarily aimed at cost reduction. It has not focused on creating new value or revenue opportunities. Another criticism is that digital investment has focused only on easy-to-reach and visible areas, such as advanced terminals and high-speed lines (digitization), thus turning the means into the end. On the other hand, digital investment has lacked a BPR-oriented[2] perspective that reviews the business process itself (digitalization).

The other aspect is that digital technology providers have been reluctant to adopt

---

[1] This proposal is a summary, made as comprehensively as possible, of the discussion at the DPFJ. Still, there may be cases in which the opinions of individual DPFJ members (incorporators and proponents) or the opinions of organizations to which they belong differ from those expressed in this proposal.

[2] BPR (Business Process Reengineering) means not merely the introduction of digital equipment and services but also a fundamental review of the business process itself, taking advantage of the characteristics of digital technology.

openness, which ensures the interoperability of different devices and services, even amid rapid technological innovation. They prefer to protect their current interests (old systems) and pursue vendor lock-in. At the same time, new digital technologies have focused on the supply-oriented perspective of technological feasibility, lacking a perspective that considers how to solve problems facing the real world with familiar digital technologies and whether the solutions are self-sustainable and scalable.

Data-driven society / a society we should strive for

Japan faces a wide range of challenges, but one of the biggest is population decline. Japan's population is estimated to decline to about 60 million in 2100[3]. This is about half the population at its peak in December 2004 (about the same as the population at the end of the Taisho era, some 100 years ago). If no measures are taken, the significant contraction of the economy will likely have serious consequences, including fiscal deficits, increased social security costs, and a decline in diplomatic power (proportional to economic power).

In this context, data is the key to a thriving economy in the 21st century. Through the collection, accumulation, and analysis of big data, it is necessary to shift from problem discovery to problem-solving, from past analysis to future prediction, and from partial optimization to overall optimization while utilizing artificial intelligence.

In doing so, it is vital to maintain the cycle of (a) identifying issues in our socio-economic framework, (b) studying solutions to those issues using IoT devices, etc., (c) verifying the operational feasibility of the solutions, (d) improving the solutions. Data circulation that transcends the boundaries between the real world and cyberspace is at the core (vision) of an ideal data-driven society.

Furthermore, in the past few years, we have experienced two ongoing global crises: COVID-19 and the invasion of Ukraine. Amid these global crises, the pros and cons of digital technology are also becoming more evident than ever before. It is the responsibility of our generation to take the lessons learned and implement them in society.

Based on these fundamental concepts, the following summarizes the seven perspectives required to achieve a data-driven society.

---

[3] "Population Projections for Japan's Future (2017 Estimates)," National Institute of Population and Social Security Research (July 2017).

II. Data-driven society: the seven perspectives

1. A problem-solving society

We are in the process of building a data-driven society. We will solve various issues facing the economy and society through big data analysis and solution development and operation. The quantity, quality (granularity), and distribution speed of data will be crucial for building a problem-solving society in the face of rapid population decline and severe fiscal constraints in the future.

Therefore, (1) developing a data linkage infrastructure, (2) establishing the right to self-manage data, and (3) accelerating government digitalization will be extremely important.

1-1) Developing data linkage infrastructure

Until now, attempts at informatization (digitization) have focused only on areas such as administration, education, and healthcare. The walls of vested interests have largely thwarted even these attempts. However, if we envision a data-driven society, data linkage (systems of systems functioning as a unified virtual system) that transcends the boundaries of such areas (systems) will play an important role.

To achieve this kind of data linkage, it is essential to ensure interoperability among data sets by standardizing data formats, to develop a trading market for data distribution, to realize data linkage (by third parties) through the use of common APIs (Application Programming Interface), and to ensure interoperability among data linkage infrastructures. To break down barriers between areas, we should adopt a cross-industry approach rather than separate, industry-specific methods in developing an environment to promote data distribution. In addition, we need to change tacit know-how into established knowledge by combining lifeless data collected by the IoT (Internet of Things) with human actions (know-how) through data linkage, and build a framework for the next generation to share this knowledge.

It is also necessary to expedite the creation of an institutional framework for data[4] linkage. For example, the European Commission has published a framework for data-related laws. Japan must also urgently consider an institutional framework[5] (data competition law) to

---

[4] Here, data includes personal and non-personal data generated by IoT devices, etc.

[5] In February 2022, the European Commission published "Data Act : Proposal for a regulation on harmonized rules on fair access to and use of data." This proposal is based on the European Data Strategy

promote data utilization and prevent data monopolization (oligopoly). This future legislation must work in conjunction with the Personal Information Protection Law (protection and utilization of personal information) and establish a competitive framework in the digital market (prevention of oligopoly and promotion of competition in the digital market).

1-2) Establishing the right to self-manage data

Given that data monopolization by platform operators is the primary obstacle to sound competition, it is necessary to establish a mechanism that incorporates the right to self-manage data by design, from the institutional- and system-design-stages, when developing a data linkage infrastructure.

In building a mechanism that allows self-management and distribution of information belonging to and generated by oneself based on one's clear intention, it is necessary to realize a cooperative system of authentication consisting of trust services such as electronic certificates stored in smartphones through public-private partnerships, proof of authenticity of data holders, verification of data non-tampering, timestamps for data transmission, and confirmation of delivery (e-delivery). These trust services should be interoperable through a coordinated system by Europe and other major countries.

1-3) Accelerating government digitalization

In September 2021, Japan launched the Digital Agency to lead the government's digital policy. The digitalization of the public sector is essential for realizing a problem-solving society, and we look forward to the efforts of the Digital Agency. For the government's digitalization efforts, three points are of immediate importance: ensuring openness, making the benefits visible, and opening up the system, as well as strengthening the governance of organizations.

First, openness (transparency) in system procurement and policy-making processes must be maintained continuously. In particular, measures closely related to people's lives,

---

(February 2020). It aims to make more data available to society as a whole, including making the data generated by IoT devices accessible to the users of the devices (whether natural or legal persons) and, upon their request, to third parties other than the manufacturers of the devices in question (data owners) for a reasonable fee (excluding gatekeepers as defined in the Digital Markets Act). The Commission also plans to publish industry-specific data bills in the future, such as for health care, automobiles, etc.

such as cloud computing of government information systems pursued by the Digital Agency, have many stakeholders and require a careful review process. We would like to see the Digital Agency take the initiative in creating a forum for a wide variety of discussions, information dissemination, and exchanging opinions that make maximum use of digital technology.

Second, it is indisputable that the purpose of government digitalization should be to improve its usefulness to the people. At the same time, however, it must also be clear what added value digitalization will bring to the relevant agencies within government departments. Therefore, a new budget system that provides incentives to the various ministries is worth considering: e.g., a mechanism whereby a portion of the cost savings from digitalization is used for new policy areas.

In addition, consideration should be given to adopting openness for a one-stop government system. As with the opening of APIs for information systems in private financial institutions, we should establish a mechanism that enables private companies to become aggregators and competitively provide one-stop government services by opening APIs for government information systems and freely combining authentication infrastructure, data (public databases), system functions, etc. Such efforts, with the Digital Agency taking the initiative to solve issues, can be beneficial in terms of identifying bottlenecks that prevent the openness of administrative systems through collaboration with the private sector.

2. A decentralized and shared economy

With the advent of digital technology and the widespread use of the Internet in the private sector, Web 1.0 became a reality, enabling traditional media and a wide variety of information providers, including businesses, to deliver information online to users. Web 1.0 was followed by the emergence of Web 2.0, a world in which the general public, who had previously been merely information users, could transmit and share information widely. In the evolution of a Web 2.0 society, platform operators appeared as third parties that acted as intermediaries between information providers and information users. While the existence of platform operators has been credited with dramatically improving the efficiency of information access, various problems have been pointed out, as described below.

In the world of digital technology, for example, computing capacity has responded to the needs of the time through a mix of centralization and decentralization, from the era of mainframe-centered centralization (of computer resources) to the age of

decentralization with the spread of personal computers, to the return of centralization through cloud computing, to partial decentralization through the use of edge computing, and so on.

How will we address the issues that platform operators are facing? When considering the answer, it could become a discussion on how to deal with platform operators, who represent an era of centralization, and how to shift the emphasis from over-centralization toward decentralization slightly.

In this sense, the society we should aim for is a decentralized and shared economy (the best mix of decentralization and centralization), and two critical issues for consideration here are (1) advancement of measures to enforce platform responsibilities and (2) utilization of blockchain technology (to accommodate Web3).

2-1) Promoting measures toward platform operators

In an era where data plays a central role in our socio-economic system, platform operators are taking advantage of the characteristics of two-sided markets[6], the network effect[7], zero marginal costs[8], and non-competing goods[9] to increase their market dominance and exercise market dominance over other sectors. In particular, the personal information that platform operators obtain goes far beyond the benefits that users receive in return and provides excess profits to the platform operators. As a result, a concentration of wealth may lead to economic stagnation through underinvestment and over saving while the labor share remains low. To solve these problems, reviewing the operation of competition laws, promoting data distribution, and creating new markets will be necessary.

First, concerning reviewing the operation of competition laws, the current Antimonopoly Act lacks the criteria for recognizing the market dominance of platform operators. It has

---

[6] A two-sided market means that the platform operator's market consists of two markets: a market for trading between the platform operator and the companies operating on its platform, and a market for trading between the platform operator and the users (end users). The conversion and accumulation of value take place across these two markets.

[7] A network effect is a process whereby the following occurs; an increase in the number of platform users leads to the accumulation of personal information about users, and businesses seeking this accumulated personal information further participate in the platform. The number of businesses participating in the platform increases the number of options available to users, which leads to a further increase in the number of users.

[8] In the case of digital goods, the marginal cost becomes zero because there are no additional costs associated with producing additional goods.

[9] Data is a non-competitive good because its value does not decrease when one person consumes (uses) it, and others can benefit from the same value.

become challenging to prove abuse of market dominance, such as predatory fees. Therefore, it is necessary to consider revising the law to a new competition law, modeled after the European Digital Markets Act and others, and including an ex-ante regulatory element that applies regulations to platform operators that exceed a specific size[10]. To measure a specific scale, in addition to sales, the government could adopt indices that accurately reflect the reality of Internet-related markets, such as the number of monthly active users (MAU), the number of registered users, etc.

In addition, platform operators often bundle their services. Therefore introducing a mechanism to disclose the structure and process of how these businesses make profits from user data is also worth considering, such as independently recording revenue for business units that have acquired MAUs above a specific size. Based on such a mechanism, there could be a functional separation of platform operators (e.g., limiting mutual use of personal data between different services or allowing competing operators to use data under identical conditions provided that they pay appropriate compensation) with objectively recognized market dominance[11].

Next, from the standpoint of facilitating data distribution, ensuring data portability, which allows platform operators to retrieve stored data (personal and corporate data) on their own and transfer this data to another entity, is a possible solution. Developing information banks and data distribution markets that delegate these business processes to third parties will also contribute significantly to data distribution. In particular, developing a data distribution market will effectively clarify the economic value of data as an intangible asset.

Furthermore, to encourage the creation of new markets, it is imperative to improve workforce skills and, specifically, to create an environment that fosters digital human capital. Measures to support venture businesses will also be essential. In doing so, it is

---

[10] Competition laws generally have an ex-post regulatory character. Ex-post regulation will continue to be effective, but the government should consider another approach (considering ex-ante regulatory elements referred to in these recommendations) in cases where conventional regulatory measures are difficult to apply, such as in digital markets. For example, dominant-carrier regulation in The Telecommunications Business Act is intentionally ex-ante. In contrast, the Antimonopoly Act provides ex-post regulation, and there have been considerations that their overlapping application (from differing angles) may be possible in some cases (see "Guidelines for Promotion of Competition in the Telecommunications Business Field" by the Japan Fair Trade Commission and the Ministry of Internal Affairs and Communications). Still, it would be necessary to reorganize these factors between business laws and new competition laws once again.

[11] From a standpoint of eliminating market dominance, one method to achieve this, called functional separation, is to create an information barrier or other organizational and operational separation between the division with market dominance (A) and other divisions (B) to ensure equality between the entity that owns A and other competing entities that use A. If this functional separation is not enough, there is also a technique known as structural separation, which organizationally separates A from B.

necessary not simply to transplant overseas business models to Japan but to actively support initiatives for distinct capabilities that aim to develop unique technologies, establish profit models, and help foster the development of companies that can expand globally in the future. It is also essential to create a community for such distinct skills.

2-2) Utilizing blockchain technology (compatible with Web3)

Recently, services utilizing blockchain technology (distributed ledger technology) have developed rapidly. The spread of crypto assets such as Bitcoin has been a typical example. Still, we can expect various applications such as NFTs (non-fungible tokens), decentralized finance (DeFi), and distributed autonomous organizations (DAOs) to emerge. Web3, with its related technology suite and developed business model, has also gained high expectations. However, such applications are still in their infancy.

Indeed, while web 1.0, which offered information from suppliers to users in one direction, has progressed to web 2.0, where both sides supply information in either direction, platform operators have gained market dominance by intervening between suppliers and users in web 2.0 and have distorted market competition. We must counter the presence of such entities with corrective measures, urgently.

Concurrently with these measures, however, it will be essential to discuss the future landscape of cyberspace. Although it is not yet certain whether the world of Web3 will arrive, discussions of the significance and state of the decentralized and shared economy that Web3 embodies provides an excellent opportunity to consider the future of the Internet's service layer.

We can expect Web3 to foster loose communities of service providers and users, but it is unlikely that Web3 will encompass all socio-economic activities. Instead, we can expect a long coexistence between a traditional centralized society and a decentralized, shared society such as Web3, where the latter gradually takes over.

Therefore, it is best to precisely follow trends in Web3 and only facilitate clarification of the minimum required targets, such as ensuring transparency and accountability of business models, etc. It would also be best to further accelerate Web3-related innovation by clarifying operational policies (ensuring policy predictability), such as implementing specific rules through a soft-law approach only and not through hard laws and regulations. On the other hand, it is also important to analyze trends in Web3 through fixed-point observation.

3. Converged content distribution

The digital content market is worth over ¥13 trillion[12], and its growth will have significant economic ripple effects. In addition, digital content has cultural ripple effects, such as improving a nation's image and cultural understanding. Therefore, it is essential to implement vitalization programs to expand the size of the market and bring its output up to the optimal level for society. On the other hand, there has been a debate on the nature of digital content policy in terms of the need for procedures to protect the standards of expression and pluralism while curbing uneconomical external factors such as inappropriate content.

However, the environment of the digital content market is changing radically. Content production, distribution, and consumption have become wholly digitalized, with everything processed as data. Content has become one of the key digital goods in a data-driven society. In particular, since the web 2.0 era, the market environment has become one in which everyone is both a creator and a user (consumer) of content. In Web3, the use of NFTs (a concept of scarcity for digital goods) and the use of complex cyberspaces such as the metaverse is growing, and new forms of secondary content use, sharing, circulation, etc., have emerged. In addition, we expect the environment surrounding communities and media to change even more rapidly, including using DAOs.

Under these circumstances, conventional content policies have based themselves on differences in utilization technologies and transmission channels, and it is upon these policies that policymakers have discussed intellectual property strategies and IT strategies separately while shaping policy. However, given the radical changes in the digital environment described above, it is necessary to examine once again the nature of converged content distribution within the overarching digital policy framework. In addition, as cross-border digital content distribution becomes increasingly significant, it is also necessary to maximize the global distribution of content.

Therefore, to promote the distribution of converged content, it is vital to (1) achieve flexibility in content distribution, (2) ensure media diversity without limitations due to transmission channels, and (3) address global issues.

3-1) Achieving flexibility in the content distribution environment

---

[12] ("Japan and World Media x Digital Content Market Database 2022 Vol. 15 [Preliminary Report]", February 2022, Human Media, Inc.)

In the past, there have been discussions about the convergence of telecommunications and broadcasting. The discussions of the public nature of broadcast media and those of the development of transmission channels sometimes became conflated in the process, leading to confusion. An important principle to keep in mind is that the function of providing information (content production) by broadcast media, including local media, is essential in society and should be highly valued. In addition, as issues such as the spread of fake news and slander on social networking services become increasingly prevalent, the function of the media (including its role as a fact-checking organization) to earn society's trust should continue to be highly valued.

In the EU, instead of basing regulations on transmission channels, webcasting, like broadcasting over the airwaves as a non-linear service, is regulated as an audiovisual service[13]. Additionally, non-linear on-demand services are also subject to rules such as not including content that incites racial or religious hatred and separating advertisements from programming.

Video sharing platform services are also subject to the above regulations. In the future, UGC (user-generated content), shared on social networking services and other platforms, will also be subject to content moderation and other rules[14].

In the future, Japan must seriously consider shifting to a system of regulations that considers the social impact of content and broadcast media, rather than dichotomizing regulations into telecommunications and broadcast media.

In addition, content distribution infrastructure should continually develop, maximizing its efficiency by introducing cloud services and shared facilities to continue to fulfill its role as broadcast media in the future.

3-2) Ensuring media diversity without limitations due to transmission channels

If access to broadband services through optical fiber networks (including 5G/6G) becomes a universal service, large-capacity video transmission services such as IP multicast will be available across Japan without regional disparities. Therefore, to secure broadband transmission lines at a minimum national level while avoiding overlapping investment, it may be possible to systematically allow a portion of the broadcasting transmission network to be wireless.

In addition, a content policy that goes one step ahead in terms of its reach should be

---

[13] See the EU's AVMSD (Audiovisual Media Services Directive) and DSM (Digital Single Market Strategy).

[14] These regulations will be applied under the DSA (Digital Services Act), to be enforced in the future.

considered, such as the introduction of a (pay-as-you-go) subscription model on a collaborative content distribution platform and the use of NFTs to guarantee the rarity of content and its distribution.

3-3) Addressing global issues

As digital content distribution across borders increases, it is becoming increasingly important to ensure proper transactions between global platform operators and content providers and to take measures to protect consumers. In addition, anti-piracy measures should not be confined to a single country but rather require cooperation among nations and coordination among private businesses operating on a global scale. Furthermore, many issues need urgent sorting out regarding the metaverse and NFTs, such as the lack of domestic and international systems to protect developers' rights and avatars.

To this end, implementing "digital special zones" to identify institutional or customary obstacles to the distribution of digital content and redefining the rules should be encouraged through international collaboration, and establishing review panels of relevant parties should be considered to strike a balance between protection and utilization (creation). At the same time, efforts should be made to develop content-creating human capital that can work globally.

4. Data risk management

In a data-driven society where digital technology permeates society and data circulates beyond the boundaries of the real and cyber worlds, managing data risks to protect data from tampering thoroughly is essential. As already mentioned, if data linkage (a system of systems) that extends beyond individual domains advances through digital technology, the effects of data tampering will not be confined to a single realm; they will extend to the entire socio-economic system. Moreover, the greater the influence of data, the more significant its impact on our socio-economic system.

Therefore, from a data risk management perspective, we will address two points: (1) promoting risk countermeasures that transcend organizational boundaries and (2) establishing data security measures.

4-1) Promoting risk countermeasures that transcend organizational boundaries

Given the growing severity of cyber threats and the rising geopolitical risks in the Asia-Pacific region, there is an urgent need to create a framework for comprehensive risk assessment in cyberspace as part of digital policy. Since the boundaries between public and private sectors, domestic and foreign in cyberspace, are ambiguous, there is an urgent need to organize risk assessment systems and allocate roles related to risk response between public and private sectors.

In particular, it is important to envision a wide range of risk scenarios in cyberspace (more severe than ever before) and to consider a wide range of issues such as the division of roles between the public and private sectors for each case, information sharing, and coordination mechanisms, and to share rational and objective decision-making in advance to keep residual risks within an acceptable range. In particular, while being conscious of recent heightened geopolitical risks, we expect precise examination by the government from a perspective of how to maintain the functions of critical infrastructure sectors in the event of a centralized cyber-attack with suspected state involvement (mission assurance to prevent the breakdown of essential services and ensure their continuity of provision).

4-2) Establishing data security measures

Data security will become much more important in a data-driven society. To ensure confidentiality, integrity, and availability, which are the cornerstones of information security, first, from the perspective of confidentiality, it is necessary to consider, for example, that highly confidential data held by public entities should be stored in Japan, where domestic laws secure it. Specific consideration should also be given to the organization of data supply chains. In addition, efforts should be made to develop guidelines to promote the use of a Software Bill of Materials (SBOM)[15] to address software supply chain risks.

In addition, countermeasures against fake news are necessary to secure data integrity. In the recent invasion of Ukraine, the mass dissemination of fake news has caused a great deal of confusion. In some aspects, fact-checking organizations' efforts have minimized these situations' deterioration. Regularly, efforts are made to minimize fake news suspected of state involvement (e.g., labeling with alerts and warnings, banning retweets, and suppressing displays) as countermeasures. Still, there are many issues to consider, such as whether maintaining a similar system in emergencies is sufficient and how to

---

[15] In the U.S., a federal government initiative, the Executive Order on Improving the Nation's Cybersecurity (May 2021), addressed SBOMs. In July of the same year, the NTIA of the Department of Commerce drafted and published "The Minimum Elements for a Software Bill of Materials."

establish a strategy for the state to analyze false information as part of its security measures[16].

Furthermore, it is necessary to hasten discussions on how the right of cyber-self-defense should be exercised (including the scope of permissible active defense) in cases where cyber-attacks cause extensive damage and have suspected state involvement.

5. Internet freedom

The Internet is now the basic infrastructure of our socio-economic system. Because of this, the management and operation systems of the Internet (Internet governance) is an essential subject of discussion that affects the nature of the Internet. The Internet has developed based on the principle of Internet freedom, allowing different networks and applications to interoperate beyond the bounds of national regulations and controls while maintaining the basic principles of autonomy, decentralization, and cooperation. However, while taking into account the fact that the Internet was developed and operated as a U.S. research and development project (NSFNET) until its commercialization (opening to the private sector) in 1991, the critical issue is the extent to which government reach should be allowed in the Internet's management and operation systems. The recent invasion of Ukraine has been a significant catalyst for deepening these discussions.

Thus, the essential discussions on Internet freedom are (1) the application of international rules in cyberspace, (2) the acceleration of free cross-border data distribution, (3) Internet governance in a broad sense, plus (4) Japan's contribution to promoting international discussions.

5-1) Application of international rules in cyberspace

First, there is a debate about the extent to which national (government) reach is acceptable from a security standpoint in cyberspace. The pros and cons of applying international law in cyberspace have been discussed at the United Nations Group of Government Experts (GGE).

---

[16] The EU Digital Services Act (DSA) includes a crisis response mechanism that allows the state to be involved in social media under a state of emergency. In Japan, in addition to discussing what constitutes a state of emergency, it is necessary to carefully consider the balance between security and freedom of expression/freedom of the press.

In this debate, there is a divide between the former Western Bloc that believes that conventional international rules should apply to cyberspace as they are, and China, Russia, and others. China, Russia, and others claim that the U.S. controls current cyberspace (Internet) rules. Many developing countries also share this view[17].

In light of the fact that severe cyber-attacks were conducted along with armed attacks in the invasion of Ukraine, it is necessary to advance more concrete discussions on the application of international law in cyberspace, including how the right of self-defense should be exercised.

5-2) Acceleration of free cross-border data distribution (international digitalization agreements)

Discussions on the nature of cross-border data distribution began in the 1980s and were gradually encompassed in the discussions on the liberalization of trade in services at the WTO. Today, it is common to offer services (and acquire personal information, etc.) from outside of a country's sovereignty. There is a trend toward data localization in some countries to prevent data from leaking overseas. However, there are also concerns that data localization will create barriers in borderless cyberspace, impeding free economic activity and undermining the right to know by undermining the free distribution of knowledge and information.

Therefore, rather than aiming for commonality of systems across countries, such as ensuring transparency for data distribution, ensuring the interoperability of data across sectors, ensuring privacy and security for data handling, and realizing a trust service system, countries should aim for a standard interface between each nation's system where differences exist and ensure the interoperability of mechanisms for cross-border data distribution. The first step should be to build consensus for international collaboration among like-minded countries and then to work toward loose cooperation (bilateral or intra-regional cooperation agreements) in the form of international digital agreements.

---

[17] The former Western Bloc, including the U.S., Japan, and Europe, argue that because private investment built cyberspace, it is reasonable to assert that private activities in cyberspace should be as free as possible, that governments should keep regulation to a minimum, and that existing international law should apply in cyberspace.

 In contrast, China, Russia, and others argue that the current cyberspace is based on U.S.-led rules, that each state must manage cyberspace in the name of national sovereignty, and that while international laws, such as the UN Charter's provisions on national sovereignty, peaceful dispute resolution, and non-interference in internal affairs are important (applicable), the application of the right of self-defense and international humanitarian law lacks validity.

5-3) Realization of Internet governance in a broad sense

The issues of applying international rules in cyberspace and accelerating the free movement of data across borders are the essence of Internet governance in the narrow sense of the term. However, Internet governance in a broad sense is also critical in ensuring Internet access worldwide, both in regular times and in emergencies.
It is expected that discussions on universal connectivity of the Internet and strengthening public support for human capital development in developing countries will become more concrete. Now that COVID-19 has further heightened awareness of the importance of digital technology, we must reaffirm the importance of closing the gap between countries (regions/peoples) that have access to the Internet and those that do not and take concrete action to address this issue.

5-4) Japan's contribution to promoting international discussion

The Internet Governance Forum (IGF) was established at the World Summit on Information Society (WSIS), held in November 2005, and has convened annually. The IGF will be held in Japan in the fall of 2023. In preparation for the IGF meeting in Japan, industry, academia, and government should work together to develop a new agenda[18] for Internet governance and a future action plan (the IGF is currently scheduled to be held until 2025) and to take action to realize an undivided world through the Internet with Japan taking the lead in this effort.

6. Transparency of rules

In traditional discussions, the rules considered were legal regulations (hard laws). Laws and regulations fall into two broad categories: economic regulations and social regulations. Economic regulations, which seek order in the economic system, have undergone a series of deregulations in line with emphasizing market competition and reducing the degree of government reach. On the other hand, there have been an increasing number of issues that are difficult to deal with under conventional economic regulations, such as the rise

---

[18] The agendas for discussion could include the application of international rules in cyberspace (5-1), free cross-border data distribution (5-2), Internet governance in a broad sense (5-3), and international harmonization of rules (7-2).

of platform operators. On the other hand, the importance of social regulations has gained wide recognition from the standpoint of user protection, etc. Still, some rules are not appropriate to enforce through legislation or compulsory measures, and some regulations have frameworks that cannot keep up with reality because of rapid technological innovations.

In considering digital policy, amidst the remarkable technological innovation and changes in market structure, there is a need to reach a consensus on what form of rules is appropriate to apply in which cases, including co-regulation through public-private partnerships and self-regulation by the private sector. In addition, these rules should aim to achieve the following three goals: promoting competition (including improving user convenience), ensuring privacy, and ensuring security. When these three factors are balanced, we can say that trust is established in cyberspace.

Although the rules for digital policy are diverse, they must meet the requirements of (1) ensuring effectiveness and (2) ensuring transparency and predictability.

6-1) Ensuring the effectiveness of rules

In the digital marketplace, for example, dramatic changes are taking place in the state of telecommunications networks. Hardware and software in network functions are increasingly separated, with software offered as a cloud service to define hardware functions. Additionally, AI-based orchestration (resource allocation) is now taking place virtually. The current Telecommunications Business Act, based on conventional principles of equipment installation, does not account for this kind of hardware/software separation.

Therefore, concrete discussions should take place to significantly revise the framework of the Telecommunications Business Act, a rule that may become ineffective in the future. In doing so, the scope of discussion should include NNI (Network/Network Interface) and SNI (Service/Network Interface) openness, including openness through APIs.

6-2) Ensuring transparency and predictability of rules

In the case of self-regulation and co-regulation, which are gaining importance as rule-making instruments emphasizing soft law, the government summarizes the primary policy direction, private organizations and businesses play a proactive role in its implementation, and the government objectively evaluates their effect. Organizing the criteria for achieving transparency and objectivity in self- and co-regulation (i.e., establishing

guidelines) is necessary.

In doing so, we must be clear about the benefits we seek from co-regulation, etc. This is because it is necessary to avoid, for example, administrative negligence attempting to avoid the costs associated with the enactment of hard laws or the use of co-regulation or other measures when stricter regulation is more appropriate because of lobbying from regulated businesses. It is also necessary to ensure consistency with the EU[19] and other bodies pursuing similar initiatives.

In considering the transparency of rules, we also have to consider the wide range of subjects to which these rules apply. For example, decisions made by AI are not made by an objective and lifeless entity but rather by learned data and algorithms set up by the developer. Therefore, it is necessary to promote the development of tools and guidelines to ensure the transparency of algorithms.

7. International harmonization of rules

The traditional telecommunications world has emphasized ensuring interoperability, enabling the interconnection and operation of telecommunications networks in various countries. Standardization has been promoted mainly by the International Telecommunication Union (ITU), the oldest UN organization dedicated to such matters. However, rapid technological innovation has increased the importance not only of official standardization (de jure standards) but also of de facto standards created by the competition clause. Furthermore, as the Internet spread around the world, maintaining the principles of independence, decentralization, and cooperation while ensuring interoperability, rule formation in the form of standardization was not limited to technical aspects but expanded into a wide range of socio-economic areas such as government reach in cyberspace, freedom of expression, measures against slander and libel, prevention of fake news, and so on. While the expansion of such rule formation is in a sense natural since digital policy is something that involves all areas, on the other hand, there have been

---

[19] In May 2015, the European Commission adopted and published the Principles for Better Self- and Co-regulation. The Principles fall into 2 phases, the conception and implementation phases of the regulation, each with 5 points of consideration (10 points in total). (https://digital-strategy.ec.europa.eu/en/news/principles-better-self-and-co-regulation-endorsed-better-regulation-package#)

an increasing number of cases in which the agendas and conflicts of interest of various countries have come to light.

In cyberspace, where there are no national borders, we need (1) harmonization of rules/interoperability and (2) international harmonization of soft laws.

7-1) Harmonization of rules / interoperability

Since borderless cyberspace requires effective, transparent, and predictable rules, an international discussion is necessary. In doing so, it is essential to ensure interoperability to accommodate differences in regulations, rather than standardizing or making rules identical.

In today's borderless cyberspace, where service providers offer their services in multiple countries, the extraterritorial application of regulations through hard laws would result in a situation where a single country is subject to various legal systems, and domestic operators subject to these regulations would not be able to cope with such a situation. Therefore, it is essential to continue carrying out policy dialogue (including developing assessment tools for interoperability) and other ongoing implementations to achieve international harmonization (interoperability) of hard laws.

7-2) International harmonization of soft laws

International collaboration efforts are required not only in hard law but also in rule formation with emphasis on soft law, such as self- and co-regulation. So far, however, there have been no examples of such international collaboration.

For example, in Japan, the debate over network neutrality has emphasized rulemaking (guideline-making) based on a co-regulation approach, whereas other countries have adopted various strategies. For this reason, it is vital to deepen the discussion on current issues of network neutrality in international forums, etc. These discussions are directly related to the debate over Internet governance.

III The next stage

This text summarizes the discussions that have been held since the establishment of the DPFJ in September 2021 through online meetings and open conferences [20] and is

---

[20] DPFJ was established in September 2021 and simultaneously published five discussion agendas: (1) Basic perspectives on digital policy in a data-driven society, (2) Global borderlessness and the state of

organized into seven perspectives that provide a digest of the key issues surrounding digital policy.

The DPFJ will continue to promote in-depth discussion of the seven perspectives while simultaneously considering the need to discuss the following three items from medium- to long-term perspectives.

First, it is necessary to envision concretely (model) what a digital society will look like in the mid- to long-term. In this text, we have presented a data-driven society as something to strive for. However, digital policy is related to all socio-economic structures, and while recognizing rationally that digital technology is an excellent tool for controlling (and in some cases monitoring) society and the economy, Japan, as a country that protects democracy, freedom of the press, and freedom of expression, needs to consider how to use digital technology and how to establish and implement rules and regulations for the use of digital technology to be in line with its identity as a nation.

Second, all stakeholders need to be involved in the above discussions. While there have been suggestions that policy discussions in the past were biased toward suppliers (industry), recently, there has been an increased emphasis on measures from the user's perspective, such as consumer protection. However, as discussed from a Web3 standpoint, the distinction between providers and users will disappear in the future, and it is necessary to redefine civil society and consider the nature of the democratic process in envisioning a medium- to long-term digital society in an age where everyone is a participant in cyberspace.

Third, there is also a need to create an environment that widely recognizes the role of rule conception and facilitates multi-layered discussions. We should recognize that rule conception in a digital society is an issue that the government should strategically address, including rule conception from a problem-solving standpoint that is independent of any single organization, democratic and diverse rule conception that enables the fair distribution of legitimate benefits, and harmonization of domestic and international rules.

---

digital policy, (3) Impact of structural changes in digital markets on digital policy, (4) Data-driven society and the direction of intellectual property and content policy, and (5) the state of rules in a data-driven society. Accordingly, the DPFJ held a panel discussion commemorating its establishment, entitled "Japan: A Digitally-Defeated Nation. Which Digital Policies Should be Discussed Now?"

Subsequently, "Open Conference: Digital Policy in a Data-driven Society" was held twice in January 2022 and March 2022 as plenary sessions, bringing together the discussions of each focus group and building on the above agendas.

For more information, see the DPFJ website (https://www.digitalpolicyforum.jp).

This document is a draft and will be finalized by summer this year after soliciting opinions through social networking services. Subsequently, the DPFJ will continue discussions on digital policy (Phase II) and, as necessary, compile and disseminate proposals on essential issues to the public, such as the emergency proposal issued in March 2022[21].

End

---

[21] "Lessons Learned from the Invasion of Ukraine and Digital Technology," DPFJ (March 2022). Based on this urgent proposal, an emergency open conference was held that same month.