T20 Policy Brief

G20 BRASIL 2024

T20 Brasil 2024 Let's rethink the world

Task Force 05

INCLUSIVE DIGITAL TRANSFORMATION

Sustainable Cyber Governance: Balancing Security and Development

Kenneth Wong, Partner, PricewaterhouseCoopers (Hong Kong Special Administrative Region of the People's Republic of China)

Danny Weng, Partner, PricewaterhouseCoopers (the People's Republic of China)

Limin (Duncan) Ding, Senior Manager, PricewaterhouseCoopers (Hong Kong Special Administrative Region of the People's Republic of China)

Yuntong (Sara) Qu, Senior Associate, PricewaterhouseCoopers (the People's Republic of China)

Bokyung Kim, Senior Associate, PricewaterhouseCoopers (Republic of Korea)

Min Hyuk (Tory) Kim, Associate, PricewaterhouseCoopers (Hong Kong Special Administrative Region of the People's Republic of China)

TF05

Abstract

The preceding T20 summits advocated for the enhancement of global cyber resilience, highlighting Public-Private Partnership ("PPP") and International Cooperation ("IC"). Echoing these discussions, the Brazil presidency is further underscoring cybersecurity and digital governance.

Our research revealed that while governments acknowledge their pivotal role as regulators in fostering cyber resilience, many face the challenge of balancing between security and development. We observed overly stringent regulations falling into the Policy Implementation Gap, where well-intended regulations inadvertently impede innovation and dampen socio-economic growth. To assist nations in developing sustainable regulatory frameworks and promote cross-national dialogue, this policy brief proposes to the G20 economies to establish a **Cybersecurity Legislation Advisory Group ("CLAG")** with two primary objectives:

1) Create a **Legislation and Information Repository ("LIR")** featuring a comprehensive, multilingual collection of global cybersecurity legal frameworks, including legislations, regulations, statutes, guidelines, recommendations, etc. The LIR, as a universally accessible resource for both the public and private sector stakeholders, is intended to facilitate research and comparative studies. Harnessing G20's resources and AI solutions, CLAG could deliver accurate English renditions that will significantly lower the linguistic barrier for stakeholders seeking to understand the global cybersecurity legal landscape, thereby fostering a collaborative approach in navigating the harmony between security and development in digital governance.

2) Form a dedicated **Research & Advisory Team** to undertake a comprehensive global comparative analysis utilizing the LIR. This team will coordinate the **Trio Initiative**, comprising: the drafting of a Playbook for cybersecurity legal framework

design and implementation, the publication of Annual Reports on legal landscape trend analysis, and the coordination of Exchange and Advisory Programs to facilitate customized consultations between experts and policymakers. These initiatives are intended to support the development of affordable, equitable, and well-balanced cybersecurity legal frameworks that drive sustainable economic growth while bolstering cyber resilience. These efforts shall emphasize individual country's unique national circumstances and socio-economic development priorities, grounded in the principles of PPP, IC, and the overarching G20 agenda.

Diagnosis of the Issue

Characterized by the advanced use of AI, IoT, and big data, our society now entered the post-digital era, moving beyond mere digitization into a phase where digital technology is deeply integrated into all aspects of our lives. This evolution, however, presents significant challenges in digital governance and cyber resilience, areas where G20 has been actively engaged through initiatives such as the establishment of the Digital Economy Working Group ("DEWG")[1], the Cybersecurity Dialogue in Saudi's presidency[2], the key declarations from Bali[3] and Osaka[4], and various Ministerial Meetings throughout India[5], Italy[6], and other summits. These efforts underscore the G20's commitment to unifying the global vision of fortifying cybersecurity postures, emphasizing the notions of International Cooperation ("IC") and Public-Private Partnership ("PPP").

1. National Commission for the Control of Protection of Personal Data – Morocco, "Digital Economy Working Group", Global Privacy Assembly, September 2022 https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.c.-Digital-Economy-Working-Group-English.pdf
2. G20 Information Centre, "Ministerial Declaration", G20 Research Group and the University of Toronto, July 22, 2020 http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html
3. Indonesia 2022, "G20 Bali Leaders' Declaration", 15-16 November 2022 https://www.g20.in/en/docs/2022/G20%20Bali%20Leaders%27%20Declaration,%2015-16%20November%202022.pdf
4. G20 Japan 2019, "Osaka Declaration on Digital Economy", January 25, 2019 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf
5. G20 India 2023, "G20 4th Digital Economy Working Group Ministers' Meeting", August 24, 2023 https://static.pib.gov.in/WriteReadData/specificdocs/documents/2023/aug/doc2023824243701.pdf
6. G20 Italia 2021, "The Digital Ministers approves a Declaration identifying 12 actions to accelerate the digital transition of the economy and governments", August 5, 2021 http://www.g20italy.org/the-digital-ministers-approves-a-declaration-identifying-12-actions-to-accelerate-the-digital-transition-of-the-economy-and-governments.html

Our research on the global cybersecurity legislation insights revealed that governments worldwide, echoing G20's endeavours, are investing more resources in building legal frameworks to navigate and address these challenges presented by the post-digital age[7]. While cybersecurity laws are vital for digital security and resilience, crafting them requires a nuanced approach that harmonizes the imperatives of robust security with the essence of sustainability and innovation. We observed instances where countries, particularly those in the nascent stages of cybersecurity legislation development, enforce overly stringent laws modelled on those of more developed nations, only to encounter a Policy Implementation Gap ("PIG"). This gap is the discrepancies between the intended policy design and the actual outcome of the implementation, characterized as unaffordable and unsustainable for both the regulators and the complying parties post-implementation[8]. PIG often arises from insufficient engagement with those directly responsible for implementation during policy formulation and a lack of feasibility assessment on resource availability for sustainable execution of the policy[9]. This misalignment can impede innovation and socio-economic growth, presenting policymakers with the arduous task of balancing security with development.

Our research, driven by the goal of solving important problems in our society and building trust in the global community in the realm of combatting cybercrime, aims to shed light on these widespread regulatory challenges, particularly in developing countries, and emphasize G20's strategic role in bridging this gap. Past G20 efforts have

7. PwC, "Cybersecurity Legislation Insights", 2023 https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/cybersecurity-legislation-insights-v1.pdf
8. PwC, "Cybersecurity Legislation Insights"
9. Muhammad Abdullahi, Nooraini Othman, "Bridging the Gap between Policy Intent and Implementation", Perdana Centre of Science, Technology andInnovation Policy, Universiti Teknologi Malaysia. Kuala Lumpur, August 15, 2020 https://core.ac.uk/download/pdf/338813565.pdf

mainly focused on raising awareness and building consensus on the importance of cybersecurity governance. The time has come and there is an urgent need to provide more concrete guidance to nations on establishing balanced, cost-effective, and practical legal frameworks. Addressing this gap is not only pivotal for bolstering global cybersecurity but also resonates with the G20's mission to foster economic stability and sustainable growth.

Recommendations

To strike a balance between the need for having stringent cybersecurity legislations and fostering innovation, and to bridge the gap between the good intention of a policy and the actual outcome of the implementation, the proposed approach is the establishment of the Cybersecurity Legislation Advisory Group ("CLAG"). Recognizing that cybersecurity is a shared responsibility that requires nation-states to fight as a united front, this initiative aims to serve as a pivotal international platform that facilitates the establishment of a global baseline standard in designing well-balanced cybersecurity frameworks and that ensures both digital security and economic vitality are sustained.

The establishment of CLAG could be led by the Digital Economy Working Group ("DEWG"), which carries an existing focus on cybersecurity discussion and initiatives. The DEWG's mandate to address digital transformation challenges makes it a suitable party to initiate the CLAG, ensuring the advisory group's efforts in cybersecurity legal frameworks are aligned with the broader digital economy goals of G20 and benefit from DEWG's established framework for IC and PPP[10].

10. G20 India, "The Fourth Meeting of Digital Economy Working Group & Digital Economy Ministers' Meeting of G20", Accessed April 1, 2024. https://g20.negd.in/#:~:text=The%20Digital%20Economy%20Working%20Group,inclusive%20social%20and%20economic%20growth.

The CLAG is recommended to be structured with two main functions: the Legislation and Information Repository and the Trio Initiative, which includes the Playbook, Annual Reports, and Exchange & Advisory Programs. The general structure and functions of the CLAG are provided below (Figure 1), illustrating how the key functions shall be managed and key principles be integrated.

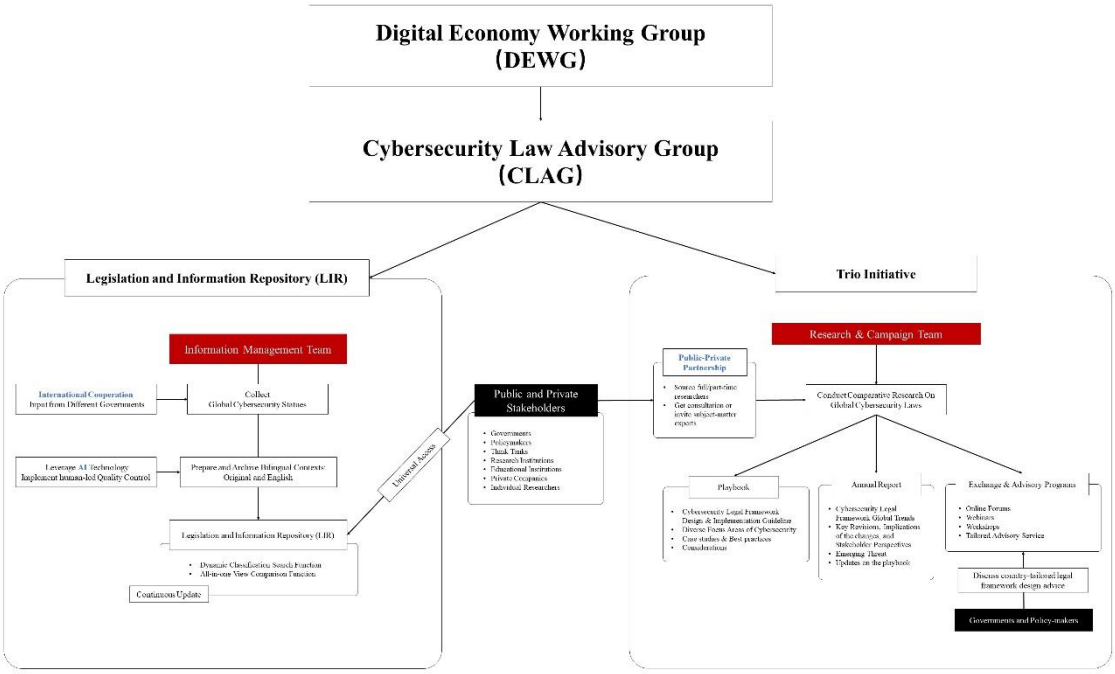

FIGURE 1. The Structure and Functions of CLAG

The Legislation and Information Repository ("LIR")

LIR is an extensive digital library, encompassing a wide array of cybersecurity-related legal frameworks and materials such as laws, legislations, regulations, guidelines, recommendations, news, etc., universally accessible to both the public and private stakeholders. The 'Information Management Team', shall be tasked with curating this global collection, initially focusing on the frameworks of G20 member states and broadening to that of all nations across the globe. The collection process will leverage G20's robust information-sharing networks and established channels of international cooperation to gather contributions from government entities and private research

institutions. The collected documentation will undergo a translation process, facilitated by Artificial Intelligence ("AI") technology, to produce English renditions. While reaping the efficiency of AI integration, the process will be overseen by human-led quality control to ensure that the original contexts are accurately maintained.

The concept of LIR was incepted from the pain points encountered during our comparative study on global cybersecurity legislation[11], where we found legal documents are typically available only in local languages and dispersed across various sources. The language barrier and the fragmentation of source data posed significant hurdles to timely and effectively analyse and understand the rapidly shifting field of cybersecurity legal framework. LIR aims to address such obstacles in research by offering a unified, linguistically accessible, and easily navigable cybersecurity legal information database platform, thereby stimulating the innovation of academia, business organizations, or government institutions. Enhanced accessibility of information and lowered language barriers would create greater opportunities for insights to be unearthed, which would then enable more informed decision-making by policymakers, especially those of developing nations.

To attain optimal utility and enhance research efficiency, LIR's user interface should be equipped with dynamic and customizable search functions, featuring clear data categorization and organized archiving. For instance, upon searching for a specific country, instead of displaying a random assortment of documents and links, the system will present documents categorized by their focus areas (such as critical infrastructure, sector-specific regulations, or incident response) and compliance requirements, ranging from mandatory regulations to guidelines and pertinent news. Moreover, a pivotal feature of LIR, aimed at enabling efficient comparative analysis of various legal frameworks, is

[11] PwC, "Cybersecurity Legislation Insights"

the 'All-in-one View' comparison tool. This functionality is integral to the overall user experience of the platform's design, enabling users to conduct side-by-side evaluations and increase research productivity. Visual illustrations of these design principles are provided below (Figure 2), illustrating the user-focused aspects of the interface.

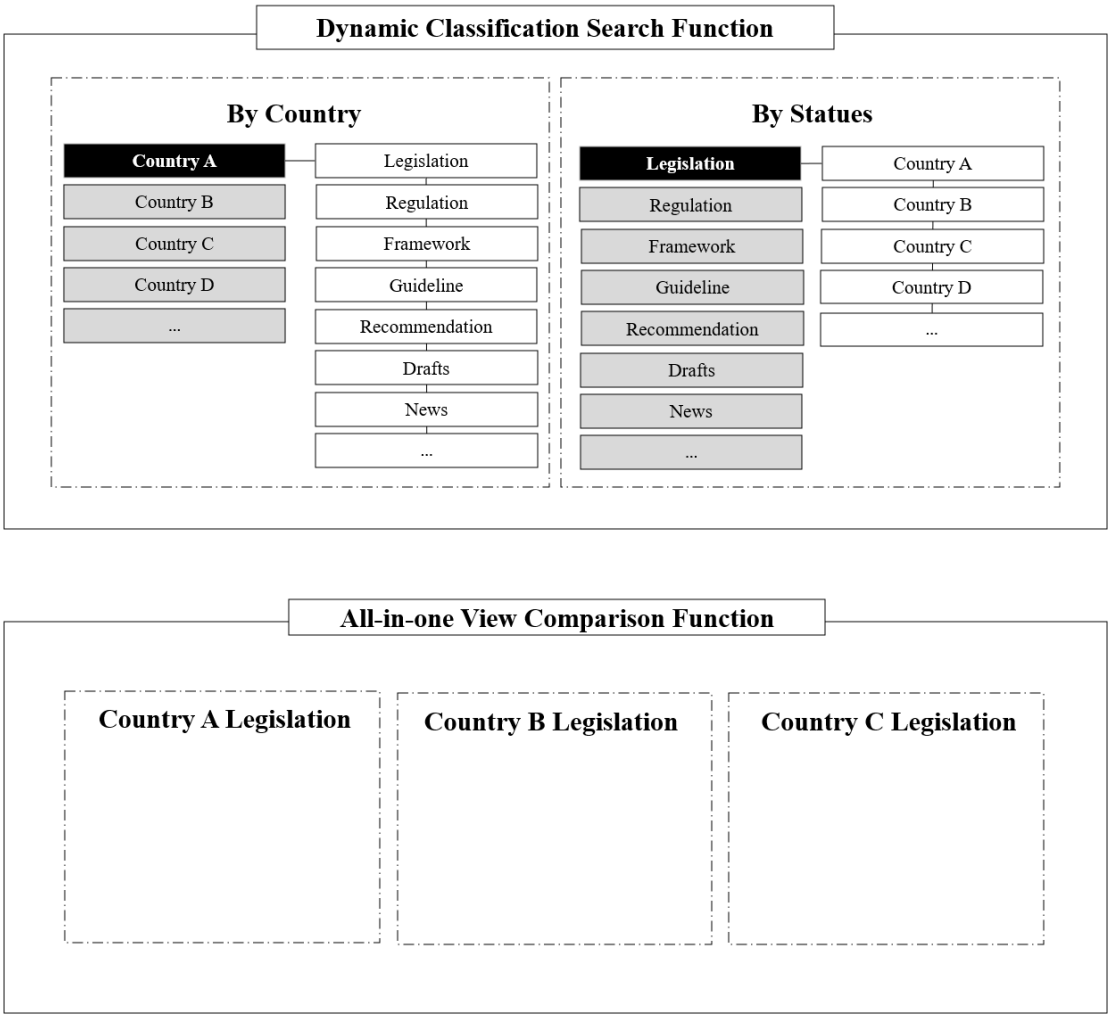

FIGURE 2. Visual Illustrations of LIR's design interface

The Trio Initiative

In the global cybersecurity domain, nations universally share the imperative to bolster cyber resilience. Thus, the characteristics of universal applicability and scalability stand as the cornerstones for creating impactful G20 initiatives. At the same time, however, our

research noted that there is no one-size-fits-all approach when designing cybersecurity legal frameworks[12]. Every government has its unique national circumstances and development priorities, which its legal frameworks should be based upon and tailored to.

The 'Trio Initiative,' with its multifaceted approach, adeptly navigates this dichotomy through its three-pronged approach:

1) *Playbook* on cybersecurity legal framework design and implementation
2) *Annual Reports* on global cybersecurity legal landscape trend analysis
3) *Exchange and Advisory Programs* for country-tailored discussions

A dedicated team, namely the 'Research & Advisory Team', shall take the lead on the three initiatives. Emphasizing the shared responsibility principle of cybersecurity and the value of Multi-Stakeholder Partnership (MSP)[12], the team will collaborate closely with diverse academic entities, think tanks, and industry experts under the PPP model. Harnessing LIR's database, the team shall conduct a thorough comparative analysis of global cybersecurity legal frameworks to gain a deeper understanding of the problems, challenges, opportunities, insights, and considerations that can assist countries, especially those in the early stages of cybersecurity legislation development, create affordable, balanced, and efficient legal and regulatory frameworks.

The Playbook, envisioned as a general roadmap, outlines the methods and considerations for designing legal frameworks across various cybersecurity domains, including incident response, cybercrime, and data privacy. While providing guidelines on regulatory strategies and capacity building, the playbook shall emphasize the considerations on affordability and multistakeholder engagement, aiming to reduce the risk of PIG occurrence. The guidelines shall be supported with best practices and case

[12] PwC, "Cybersecurity Legislation Insights"

studies to enhance the reader's understanding of the principles behind the considerations and serve as a source of benchmarking. Primarily targeting the policymakers, the playbook will be universally accessible to all public audiences, focusing on creating a broader impact with high scalability.

The Annual Report is an informative provision that highlights the significant shifts and notable trends that occurred in the year's global cybersecurity legal sphere. The report may feature evaluative country-specific case studies on the repercussions of legal adjustments, showcasing best practices or lessons learned. Additionally, it aims to collate perspectives and insights from a broad spectrum of stakeholders, including sectoral regulators, industry leaders, and members of civil society, to highlight the frontline experiences on the effectiveness and implications of the legal changes, thereby reducing the risk of PIG occurrence. Emerging cyber threats and challenges may also be elucidated, emphasizing how legal frameworks are adopted to address, or falling short of, them.

The report serves to aid governments in better understanding the evolving landscape, thereby facilitating informed decision-making in policy development. Furthermore, it aims to benefit businesses, academia, and individuals by providing a clearer understanding of changes in the rapidly evolving legal environment and threat landscape, enabling better compliance, risk management, and strategic planning. Through disseminating knowledge, highlighting the voices of the frontline, and fostering a collaborative approach, this initiative resonates with the notions of shared responsibility and intends to assist stakeholders in adapting proactively in the ever-shifting cybersecurity domain.

The *Exchange and Advisory Programs* are the interactive arm of the Trio Initiative, designed to complement the scalability of the Playbook and universality of the Annual Reports with a bespoke touch. These programs, possibly in the form of seminars or

webinars, will feature the contributions from researchers and experts involved in the Playbook and the Annual Reports, offering deep dives into the insights gained from global cybersecurity legal frameworks comparative analysis. While opening to all members of the public, the programs' core value lies in facilitating bespoke exchanges and advisory, allowing policymakers to engage directly with experts for custom solutions reflective of their unique national contexts. The G20's extensive experiences in orchestrating international collaborations and leveraging PPP models position it as an ideal facilitator for these impactful programs.

Scenario of Outcomes

This Policy Brief highlights the intricate challenge of finding the balance between crafting robust cybersecurity legal frameworks and nurturing innovation and socio-economic growth, amidst the complex and evolving landscape of digital threats. It underscores the necessity for bolstered International Cooperation and Public-Private Partnership, proposing the creation of a comprehensive Legislation and Information Repository and the launch of the Trio Initiative. These measures aim to address the challenges posed by the post-digital era through the G20 framework and cultivate sustainable methodologies to enhance global cyber resilience.

The potential outcomes of the G20's adoption of these recommendations are vast, encompassing both immediate benefits and long-term transformations. The enhancement of collaboration and the refinement of legal frameworks, designed to be more affordable and effective, are poised to effectively reduce the Policy Implementation Gap. This reduction promises to alleviate resource misallocation and ambiguities surrounding the enactment and compliance with cybersecurity regulations, thereby safeguarding innovation and socio-economic development from being inadvertently hindered by the very efforts to raise cyber resilience.

Nevertheless, the path to these advancements is laden with challenges and necessitates careful negotiation of trade-offs. The task of maintaining and updating the LIR's database in the face of rapid cyber threat evolution presents a complex challenge, which the paper proposes to address by adopting a phased approach, initially concentrating on the provisions of G20 nations before broadening its scope to other nations globally. The comprehensive objectives of the Trio Initiative, which span the creation of a guideline playbook, the publication of annual reports, and the orchestration of extensive exchange

and advisory programs, demand considerable expertise and resources. In this context, the G20's role as a facilitator between nation-states as well as diverse sectors is pivotal. Needless to mention, it is imperative to fully exploit the Public-Private Partnership to tap into the vast reservoir of the private sector's resources and knowledge.

The long-term trajectory of the cybersecurity legal landscape is poised for significant evolution should the G20 community fully embrace these recommendations. Positioned at the vanguard of these initiatives, the G20 has the potential to empower nations, particularly those in the developing world, to adeptly manoeuvre through the intricacies of the post-digital age, establishing an unprecedented global benchmark for collaboration and innovation in the realm of cybersecurity legal framework development. This progressive shift towards a more informed, considerate, and proactive approach to cyber governance is expected to enhance global cyber resilience substantially.

References

G20 India, “The Fourth Meeting of Digital Economy Working Group & Digital Economy Ministers’ Meeting of G20”, Accessed April 1, 2024. https://g20.negd.in/#:~:text=The%20Digital%20Economy%20Working%20Group,inclusive%20social%20and%20economic%20growth.

G20 India 2023, “G20 4th Digital Economy Working Group Ministers’ Meeting”, August 24, 2023 https://static.pib.gov.in/WriteReadData/specificdocs/documents/2023/aug/doc2023824243701.pdf

G20 Information Centre, “Ministerial Declaration”, G20 Research Group and the University of Toronto, July 22, 2020 http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html

G20 Italia 2021, “The Digital Ministers approves a Declaration identifying 12 actions to accelerate the digital transition of the economy and governments”, August 5, 2021 http://www.g20italy.org/the-digital-ministers-approves-a-declaration-identifying-12-actions-to-accelerate-the-digital-transition-of-the-economy-and-governments.html

G20 Japan 2019, “Osaka Declaration on Digital Economy”, January 25, 2019 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf

Indonesia 2022, “G20 Bali Leaders’ Declaration”, 15-16 November 2022 https://www.g20.in/en/docs/2022/G20%20Bali%20Leaders%27%20Declaration,%2015-16%20November%202022.pdf

Muhammad Abdullahi, Nooraini Othman, “Bridging the Gap between Policy Intent and Implementation”, Perdana Centre of Science, Technology andInnovation Policy,

Universiti Teknologi Malaysia. Kuala Lumpur, August 15, 2020

https://core.ac.uk/download/pdf/338813565.pdf

National Commission for the Control of Protection of Personal Data – Morocco, "Digital Economy Working Group", Global Privacy Assembly, September 2022

https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.c.-Digital-Economy-Working-Group-English.pdf

PwC, "Cybersecurity Legislation Insights", 2023

https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/cybersecurity-legislation-insights-v1.pdf

G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

Let's rethink the world

CEBRI Rethink Tank

FUNDAÇÃO ALEXANDRE DE GUSMÃO

ipea
Instituto de Pesquisa Econômica Aplicada