INSTITUTE OF STRATEGIC & INTERNATIONAL STUDIES (ISIS) MALAYSIA

focus

PP5054/11/2012 (031098)
12/2022 ISSUE NO. 17

Digital rights in cyberspace

Society should take lead on digital rights

Internet still too toxic for women

Speech mustn't fall under social media giants' purview

Content

Editorial team

Farlina Said
Joann Saw
Tan Wan-Peng
Zul Izwan Hamzah

Design by
Mohd Farouf Sahal

Published by
Institute of Strategic & International Studies (ISIS) Malaysia
1, Persiaran Sultan Salahuddin
50480 Kuala Lumpur, Malaysia

Editor's Note

This ISIS Focus on digital rights has been long in the making. From the first virtual workshop held during MCO 2.0 in early January 2022 to the time of writing in May – the final product has gone through Malaysia in lockdown, transition towards endemicity and a new government.

Thus, the editorial process has seen the growth, use and impact of Malaysia's digital spaces. Prior to the pandemic, internet access was framed as one of connectivity focused on addressing the availability and cost of access to the world wide web. However, the pandemic uncovered the potential of digital services, where individual access to the internet mitigated impacts of Covid-19, whether for education, employment or to fulfil daily needs in the form of groceries.

The use of cyberspaces for social networking and discourse has continued. This was best illustrated in the 15th general election, where Malaysians used digital spaces to educate and participate in politics. The online space also acquired its own "parliamentary seats" – P223 (Facebook), P224 (Twitterjaya) and P225 (TikTok), adding to the existing 222.

The year 2022 also saw the risks in increased digitisation. Coverage of large-scale data breaches shows that data collected require sufficient protections. The data of 22.5 million Malaysians born between 1940 and 2004 were allegedly sold online and a hacker also released information on five million AirAsia passengers. Such breaches should be investigated. The preferred outcome is an improvement in data management because to scale back digitisation may be a little too late.

Responsibilities need to be distributed. Unauthorised access can be undiscovered gaps in systems exploited by interested actors. However, vulnerabilities can also include failures in digital literacy whereby an individual is unaware of the phishing trap activated by a click.

Yet underlying these digitisation trends are the traditional harms exacerbated by the use of ICT. There can be gendered experiences of cyber, especially for women whose personal data, information or images are leaked to great detrimental impact on their career or reputation.

Further, a multiethnic, multicultural nation, such as Malaysia, is sensitive to critical conversations. There are fears that discourse online can turn into mobilisation platforms or escalate racial tensions. The digital environment is not pristine and can contain inauthentic experiences whether they are offline interventions from cybertroopers or distortions from AI algorithms. These factors are monitored by platforms but mismatches in policies can boost certain messages and exacerbate misinformation or hate speech.

To improve systems, processes and awareness, this ISIS Focus explores the concept of digital rights, which are human rights suited for the digital age. The purpose may be to guide advocacy in a landscape where jurisdiction and responsibilities can appear confusing. It can also be the stepping stone to increasing the capacity of the general population who would have to navigate cyberspaces. The conversation on rights should decide the expectations an individual has of the government and private sector, while raising personal awareness.

The six writers here have explored digital rights, ranging from a conceptual framework to the right to access and digital inclusivity. They also touch on the risks of a data-rich environment, necessity of having technologists on board in discussions about digital rights, concerns over the privatisation of free speech and protecting women in digital spaces. A whole-of-society approach needs to be considered. We are most grateful to Global Partners Digital for the opportunity to produce this ISIS Focus and its support.

Malaysia was on a positive trajectory for digital adoption even prior to the pandemic. However, the possibilities and perils of digital spaces and services will only increase. Through this issue, we hope to contribute to a developing discourse on protecting Malaysians online.

Data-centred rights to forefront

As more aspects of life become digitalised, governance must focus on harm in tech

By Dr Tan Jun-E

The rapid advancement of digital technologies presents a multitude of novel and complex challenges to the protection of human rights, especially violations that cut across the digital and physical.

I would like to offer a conceptual framework for digital rights in general and from there, zoom into data-centred rights, one of the less-discussed aspects of digital rights, which deserve more attention for the societal implications for years to come.

Conceptual framework for digital rights

One of the problems of advocating for digital rights is a lack of consensus of what the concept means. From a 2019 study, interviewing 24 digital rights advocates and activists from Malaysia, the Philippines and Thailand, a conceptual framework was built to encapsulate four main spheres of digital rights.

These are:

The first two spheres depend on whether "the digital" is seen as a space where we conduct activities, such as when we are online or as data representation of physical entities, whereby its use or manipulation can have real-life consequences. The last two focus more on developmental aspects, of access and of having a say in the direction and regulation of the digital.

In Southeast Asia, the movement focused mostly on human rights translated to digital spaces, notably on issues such as freedom of expression and online gender-based violence. Access to the digital was not a key focus, possibly because governments there had worked on digitalisation and connection as a matter of priority. Participating in digital governance was mainly at national or subnational levels on influencing government policy on ICT, with forums for international standards setting mostly out of reach.

Digital harms and society

As we stand in 2022, the area of digital rights is still quite underdeveloped in the region, even when risks and harms rise from the permeation of technologies in our daily lives. AI technologies, for instance, offer personalised content, such as social media feeds, recommendation and online shopping.

While offline, our movements are increasingly digitised and tracked and monitored by corporations and government bodies. In Malaysia, we already see the use of some of these technologies in public services, such as Penang's facial recognition technology for CCTV surveillance to combat crimes or the court systems in Sabah and Sarawak piloting predictive statistical analyses, with the intention of moving towards machine learning to assist in decisions on sentencing for drug and rape offences.

"As we stand in 2022, the area of digital rights is still quite underdeveloped in the region, even when risks and harms rise from the permeation of technologies in our daily lives.

While there has been little reporting on the efficacy and safety of these systems in the Malaysian context, similar implementations elsewhere have raised concerns, such as facial recognition systems and risk-recidivism software use in the United States, which amplify racial biases and marginalising the marginalised further.

Another example of decision-making based on data and digital bodies that has an outsized impact on society is the social credit system in China, which rates the behaviour of citizens, companies, and even government agencies, and offers rewards or punishments accordingly.

Governance of data and AI applications

There are at least two ways to view this problem of protecting data-centred rights. The first is to

Classification	Explanation	Example
Unacceptable risk	AI systems considered a clear threat to safety, livelihoods and rights of people	Social credit scoring by public authorities Toys using voice assistance that encourages dangerous behaviour
High risk	AI technology that could put the life and health of citizens at risk or create an adverse impact on fundamental rights Stringent oversight mechanisms to be implemented before distribution	AI in critical infrastructure AI in scoring of exams AI application in robot-assisted surgery Administration of justice and democratic processes
Limited risk	AI systems with a clear risk of manipulation	Chatbots
Minimal risk	AI system that can be developed and used subject to existing legislation without additional legal obligations	AI-enabled games Spam filters

"While offline, our movements are increasingly digitised and tracked and monitored by corporations and government bodies. In Malaysia, we already see the use of some of these technologies in public services

procedures to protect privacy and security. This is typically managed at an organisational level. The scope of data protection covered should not be limited to personal data representing people, but also non-personal data and metadata from which inferences can be made.

The second is to govern the applications that make use of this data. In 2021, the European Union released a draft of its proposed Artificial Intelligence Act, which may set a worldwide standard for AI regulation (as did the General Data Protection Regulation or GDPR for data protection). Notably, the act classifies and regulates applications by level of risk imposed on EU citizens by any AI application.

Applications that pose "unacceptable risk", such as subliminal manipulation and exploitation of vulnerable groups, social-credit scoring by public authorities, real-time biometric identification systems in public spaces, are prohibited outright.

"High-risk" applications, such as AI used in applications for recruitment, assessing consumer creditworthiness, safety critical systems, will be subjected to more regulatory oversight than "low or minimal risk" applications (e.g. AI chatbots, spam filters and most other AI systems).

As with most initiatives like this, the devil is in the details and many have offered in-depth analyses and critiques about the proposals. In general, it is a good move away from industry self-regulation, as well as narrowly defined and poorly applied AI ethics. Situating AI technologies in their application and societal contexts, with a risk-based approach, is another layer to protect data-centred rights.

A conceptual breakdown of digital rights offers clarity of the problem areas and we see that each sphere comes with its historical context, stakeholders, existing research and advocacy issues. The breadth of what is covered can then be mapped out to address gaps and form bridges among state and non-state actors.

While all spheres of digital rights are important and have real-life implications, the area of data-related rights is the least-understood and the fastest growing. As Malaysia moves ahead with its Digital Economy Blueprint and National Fourth Industrial Revolution (4IR) Policy, it will also have to keep abreast of the global landscape of AI regulations to ensure that risks of the technologies do not outweigh their potential benefits.

Dr Tan Jun-E
Senior research associate, Khazanah Research Institute (KRI)

What are digital rights?

Based on Dr Tan Jun-E's ***conceptual framework for digital rights in Southeast Asia***

As technology becomes intertwined with human lives, the maintenance of human dignity, equality and freedom becomes an online and offline endeavour. Definitions may vary but the four ways to contextualise digital rights include:

01 Conventional human rights enshrined in Universal Declaration of Human Rights translated to digital space

Article 2 - Everyone is entitled to all the rights and freedoms in this declaration, without distinction of any kind.

Article 12 - No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon honour and reputation.

Article 18 - Everyone has the right to freedom of thought, conscience and religion; including freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19 - Everyone has the right to freedom of opinion and expression; including freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

02 Data-centred rights

- Governance of data privacy and cybersecurity
- Any form of data – be it online activity, biometric data, such as medical and financial data – is a representation of individuals and should be protected

03 Rights to access digital spaces and services

Aside from content traversing in cables and communication lines, communication in the digital space is shaped by the private sector, social media companies and algorithms. These can determine the range of access and expressions individuals have in the digital space.

04 Rights to participate in governance of the digital

Multistakeholder approaches to governing the digital environment. As cyber is a multistakeholder environment, protecting cyberspace requires various stakeholders, inclusive of the private sector and civil society.

Digital rights must trump all in digital transformation

Malaysia should include the marginalised as internet rules every aspect of life

By Dr Rachel Gong

Public policy tends to prioritise economic development and growth. However, as our social lives and public services become increasingly digitally dependent, policymakers must recognise that digital transformation is an all-of-society process that includes social wellbeing and human rights, economic development and growth. Digital policy can no longer focus primarily on the digital economy while neglecting digital society.

Having a digital society mindset involves thinking about development and design, not just for productivity and efficiency, but also for inclusivity and the public interest, recognising and observing human and digital rights.

A society-first policy framework recognises that the challenges facing a digital society are to be solved not with just technical solutions but also social solutions that protect digital rights.

Digital rights part of digital inclusion

Digital rights are simply "human rights in the internet era". Human rights, such as the right to receive and impart information, right to privacy and right to education, all have to be protected online as offline. One way to do this is by developing and implementing digital policies that prioritise inclusion.

Digital inclusion is a broad policy driven approach towards ensuring "all individuals and communities, including the most disadvantaged, have access to and use of information and communication technologies (ICTs)". Digital inclusion must evolve as technology advances. It requires intentional strategies and investments to reduce and eliminate historical, institutional and structural barriers to technology.

Digital inclusion goes beyond closing the digital divide. Building more infrastructure, improving network performance and developing devices and apps that are easier to use and more secure are important technical solutions to the problem of the digital divide.

But digital inclusion also requires social solutions to address social inequalities and evaluate proactively the societal impact of digitalisation, for example, on educational opportunities, healthcare outcomes and social cohesion. It means recognising the privilege and bias inherent in the design and development of many digital systems, whose unspoken assumptions may not adequately observe or protect digital rights.

Far too often, digital adoption rushes ahead with little consideration of the long-term – and unintended – consequences of the technology.

For example, unregulated data collection and sharing by private social media platforms have diminished both the right to and expectations of online privacy. Similarly, as education systems pivoted to edutech platforms for online learning during pandemic lockdowns, not enough consideration was given to how pupils from low-income households would be able to keep up with their more privileged counterparts, resulting in them being left further behind.

During the Covid-19 pandemic, society crossed a digital Rubicon. The metaverse and web3 are not our current digital realities (and they may never be), nonetheless society is becoming more, not less, digital. Several countries, including Malaysia, are recognising the right to access the internet as human rights. As more people come online, it is important that public policy protects digital rights in an interconnected world.

4 principles for digitally inclusive policies

There are at least four principles that can inform digitally inclusive policies that protect digital rights: inclusive design, valuing user experience, good governance and prioritising the public interests.

Inclusive design Society needs technological tools that can be used meaningfully by all groups of people, including and especially the vulnerable and disenfranchised. For example, having government websites translated into multiple languages, including languages spoken by indigenous and migrants.

Broadly, technological systems and processes need to be designed inclusively, not just tools like websites and apps. This may mean retaining or creating new alternative analogue means to support less digitally connected groups.

"Far too often, digital adoption rushes ahead with little consideration of the long-term – and unintended – consequences of the technology.

For example, the financial services sector encourages cashless transactions and transitioning to digital-first communications. Without non-punitive non-digital alternatives, this transformation is likely to hurt unbanked and underbanked groups with limited digital access and literacy.

Valuing the user experience Good intentions do not always translate

into a positive user experience. For example, satellite connectivity has been tried and tested and refined for decades.

The latest developments promise better speeds and more reliable performance even in inclement weather. However, performance is measured by service providers in terms of signal coverage in ideal conditions and not by day-to-day download speeds that users experience, especially in remote or rural areas.

Nor does following the letter of the law guarantee a good outcome. Platforms may meet legal obligations by requiring users to agree to terms and conditions that govern their use of the platform. In practice, however, users may still find themselves subject to abuse and harassment on the platform. It is incumbent on corporations to take responsibility for addressing the challenges of developing platforms and systems that protect users' rights.

Good governance This is a topic that warrants much more discussion but suffice to say good governance is fundamental in the protection of digital rights. Digital governance ranges from developing secure, integrated and interoperable systems to managing and protecting personal data. These are no longer just national issues but require cross-border regulations in a networked world.

Prioritising public interests Public policies should not privilege the private sector at the expense of the public. While many of the most popular digital applications are private sector products, the backbone of the technology they run on is largely supported by public funds.

The lack of clarity and transparency in the development and procurement of the MySejahtera application was a hard lesson for all parties. Going forward, open access to procurement processes can improve public and private sector accountability.

More engagement with disenfranchised groups

Nations emerging from the depths of the pandemic should prioritise public interest and social wellbeing in their recovery. A key player in promoting digital inclusion and protecting digital rights is the public sector. Per the Universal Declaration of Human Rights, "everyone has the right of equal access to public service in (their) country."

> **"The lack of clarity and transparency in the development and procurement of the MySejahtera application was a hard lesson for all parties.**

The Malaysian government has declared public service delivery to be a priority in Budget 2023, in line with the Digital Economy Blueprint. This includes commitments to closing the digital divide, improving technical competencies among public sector staff and the development of a cloud-computing ecosystem.

These commitments will generate a lot of data. Comprehensive data regulations are needed to govern all the digital data and protect digital rights. Shared standards need to be developed and implemented across systems, for example, regarding data access rights. This requires public servants to be informed, not only about technology, but also about social inequalities and digital rights.

One step towards achieving these goals is for policymakers and tech developers to engage more deeply with groups whose rights are often overlooked, such as people with disabilities, migrant communities and the marginalised.

Policymakers should seek their input when developing public policy. Developers should involve them in testing digital tools and systems before launching them publicly. Like digital transformation, developing inclusive policies that protect digital rights is an all-of-society process.

Dr Rachel Gong
Deputy director of research, Khazanah Research Institute (KRI)

Governments, private sector can no longer dismiss privacy, surveillance concerns in wired age

By Dr Moonyati Yatid

Society should take lead on digital rights

As societies move into the digital era, the context for rights also changes, especially as digital spaces present new prospects for exercising individual and collective rights. Digital rights are seen as an extension of human rights in the digital age – with privacy, safety, security and protection part of the core components.

Surveillance, data protection and privacy have emerged as key issues of citizens' digital rights. For instance, with the development of emerging technologies, such as facial recognition and other surveillance technologies, governments and companies have been collecting data from civilians. The public would trade the loss of privacy for national security, economic stability or other societal benefits.

But state-conducted surveillance for security can reinforce existing biases and build upon harmful cycles. These factors will have an adverse impact on minority communities, disproportionately affecting the marginalised. This is especially prevalent in countries, such as the United States, with its long history of over-surveillance towards communities of colour.

Surveillance can be a tool to empower national security and geostrategic goals. Critics have raised the alarm over surveillance targeting minority groups and infringing on human rights, such as the Uyghur. China is not a stranger to practices of extensive surveillance, especially where thresholds of privacy rights can differ from international standards. Surveillance is codified into national law, such as Hong Kong's "national security law".

A core component of surveillance is data collection and the thresholds of privacy. However, not all thresholds and safeguards reflect similar standards. According to a 2019 study by Comparitech, out of 47 countries assessed, only five have adequate privacy safeguards – all in Europe – and General Data Protection Regulation (GDPR) significantly contributed to this finding.

Outside of the European Union, the study ranked Malaysia number five in the lowest category, after China, Russia, India and Thailand. Malaysia scored poorly for biometric data collection and visual surveillance practices, with further concerns for democratic safeguards. Malaysia has also been impacted by breaches involving financial and medical data. Thus, Malaysia is grappling with thresholds of privacy, awareness and cybersecurity challenges.

The Personal Data Protection Act 2010 (PDPA) is the main instrument safeguarding data management for the private sector. But the legislation contains many gaps that hinder protection in totality.

For one, the PDPA does not include data collected by the Malaysian government and state bodies. In 2018, a study carried out by Ipsos painted Malaysia's correlation between data privacy awareness and trust. While only 44% of Malaysians were aware and have some knowledge about online data privacy, a majority (80%) trusted that the government was doing enough to protect their personal data. However, this correlation might have changed since Covid-19 and the introduction of the MySejahtera application.

MySejahtera and public trust

MySejahtera is Malaysia's contact-tracing application, equipped with geolocation capabilities and designed to collect sensitive data, such as the state of an individual's health. It is one of the most subscribed apps in Malaysia and at the peak of the pandemic, enjoyed an 85% install rate and 92% open rate.

Controversies surrounding users' data protection, data ownership, oversight mechanisms and privacy have not only created awareness but also eroded public trust. Citizens are increasingly questioning if the government can protect their rights in the digital age and whether current laws and policies are effective.

Malaysia had been aggressive in its plans and policies to ensure that the nation embarked successfully on digital transformation. It introduced various polices, such as the National E-Commerce Strategic Road Map, National Industry 4wrd Policy and the most recent MyDIGITAL initiative to "transform Malaysia into a digitally driven, high-income nation and a regional leader in digital economy". While cybersecurity related issues are listed and considered in these national documents, in reality, there are many areas for improvement, especially enforcement.

> **"...state-conducted surveillance for security can reinforce existing biases and build upon harmful cycles.**

Malaysia requires more robust, updated and in-depth legislations that could protect and safeguard its people's digital rights. The rapid growth of technological development and application means that regulations need to be updated at a comparable pace. For instance, although facial recognition technology application is on the rise in Malaysia, there are few laws that govern this space. This needs to change.

Empowering society

While the law is one means of addressing the issue, more importantly, we need to build a society that would advocate digital rights. But how do we do this? And is it effective?

In March 2022, amid concerns over user data privacy in MySejahtera, there was a significant plunge in check-in rates across all states and federal territories. As reported on 12 April 2022, a 30% drop nationally

was observed. Many urged the government to stop requiring the use of the app because of legal and privacy concerns over MySejahtera's data, particularly as the nation transitioned to Covid-19 endemicity. Not long after, it was announced that scanning MySejahtera was no longer needed to enter premises.

In this day and age where strong public pressure could impact on policy directions, it is imperative that society be more aware of our digital rights and continue to advocate to policymakers and technology providers to take higher responsibility and accountability in providing a safe and secure digital space. Government bodies and the private sector also need to assume the highest level of responsibility and provide transparent services to safeguard the public's digital rights.

Last, policies and legal frameworks need to be adequate to create a strong social compact that is inclusive for all parties. Countries have started to address the challenges in a variety of ways.

GDPR, an important component of the European Union's privacy law and human rights law, governs how personal data must be collected, processed and erased. Among others, the law also contains the right to be forgotten, also known as the "right to erasure", where citizens have the power to demand the removal of private information from internet searches. GDPR sets the bar for data protection globally, by guaranteeing the security of personal data in the digital sphere.

Emerging technologies will continue to transform and lead to recognition of new rights in the digital space. How and what path our nation takes in shaping digital rights, the key is to ensure that there would be ample ways to seek justice.

"...policies and legal frameworks need to be adequate to create a strong social compact that is inclusive for all parties.

Dr Moonyati Yatid
Policy analyst, Global Foundation for Cyber Studies and Research

Why should internet be 'wild West' where loss of data is considered a norm?

By Maryam Lee

Seize control of your 'digital twin'

In the late 1990s when the masses began to gather socially online (who remembers the days of Friendster or MySpace?), we did not quite realise just how much we brought the socio-political constructs of our world along with us.

We created accounts on these social networking sites, not quite knowing what to expect. It was a new territory to explore.

Before we knew it, we got used to how these platforms shaped the way we interacted with one another. Could we imagine forms of interaction that did not look like Twitter, Instagram, or TikTok? Unwittingly, we have participated in a large-scale social experiment on how to amplify thoughts, ideas, audience and influence in a new media age.

Digital doppelganger

We create digital twins the moment we translate a piece of information about ourselves into digital information. In one "sign up" click, we create a digital profile of ourselves on the platform's servers and it acts as our proxy to perform social interactions or business transactions. The more we use the platform, the more interactions happen, the more data from which the platform could learn and improve on a user's digital profile.

Over the years, these bits of data accumulate and the average user has no way of knowing just how extensive, let alone accurate, the digital representation of themselves are to the source.

Access to and use of technologies depend on that accuracy. Algorithms are designed to curate digital experience from the data. Algorithms are the rules and conventions our digital twins must adhere to because the system is designed to collect information that way. Data collection is a vital component of the system that allows algorithms to run on the data, thus curating experiences.

While we outsource more and more of our decision-making powers to computers, can we confidently say that our digital twins are safe, wherever they may be?

They are intangible, thus, if malicious actors "kidnap" these digital doppelgangers (via data breach incidents or security leakages), are there repercussions?

We are constantly exposing ourselves via digital footprints left on computer servers all over the world. Actors with the skills and resources to extract the bits of information can follow the trail that leads right to us, making us vulnerable to malicious attacks and putting us in danger. We describe these situations as digital harms.

Value of digital selves

If we value human rights, we should also value our digital counterparts' rights. This perspective on data governance is informed by data-centric digital rights, a perspective that looks at implementation into the data entities that represent the users. Data-centric digital rights are aimed at protecting citizens' rights by implementing transparent regulations to protect them.

There are various actors interested in data. While most of us realise it too late, digital platforms were the first to see the profits from having access and control over millions, even billions, of our digital twins. Shoshana Zuboff, author of the seminal *The Age of Surveillance Capitalism* (2019), calls companies like Facebook a "massive surveillance empire" that makes hundreds of millions in profits selling users' personal information. Their entire business model rests on the basis of extracting and processing vast amounts of personal information to target their users for their "real" paying customers: marketers and advertisers.

At the same time, governments around the world realised how powerful it is to have control over the communication and information infrastructure. Galloway argues that to collect data at such scale, speed and complexity, it surely "represents a radical shift in the balance of power between state and citizen".

If we understand how our data is really us and that we cannot separate our digital twins, then we would understand that this business model makes money off selling us, practically making it a form of digital human trafficking. The harms to our digital entities manifest especially, in this instance, during times of extreme social and political polarisation. The best example was the Cambridge Analytica scandal of exploiting users' data during election campaigns.

Yet, Cambridge Analytica was not the only company implementing these practices. By and large, tech companies are still operating based on the same business model that profits from massive data extraction with no clear, standardised technical assurance that they would not be abused.

The political functions of digital technologies have remained the same: to collect as much data as possible to predict better future outcomes of human behaviour. Despite data protection laws, there is little incentive to move away from this model as hefty fines are regarded as a cost of doing business.

"We are constantly exposing ourselves via digital footprints left on computer servers all over the world.

On top of that, the technical implementation of data protection is not required by the platform providers. A simple privacy policy adapted from a commonly used

> **“We create digital twins the moment we translate a piece of information about ourselves into digital information.**

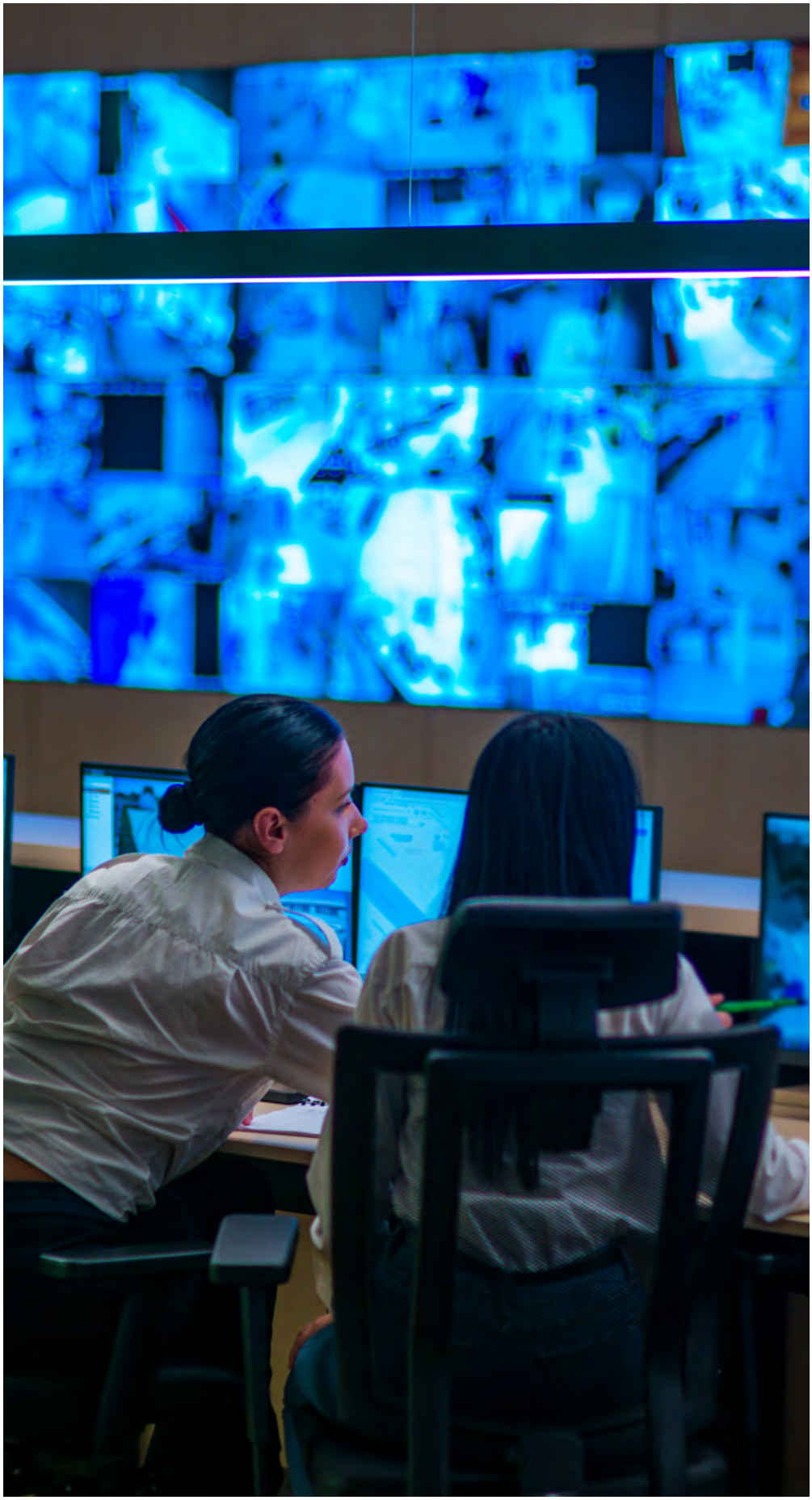
template on the internet is more than enough to satisfy legal requirements of notification and acquiring consent from users. There is no way to audit and validate compliance of data protection without the technical standards to do so. Software should have the same protections for public consumption as any other product or service. Citizens should only concern themselves with acting as responsible users.

With digital rights advocacy actors increasing in recent years, it is only a matter of time before we start mainstreaming the demand for technologies to be made rights respecting by design.

The first step is to get the technologists on board defining and designing the digital future we want – namely one that respects our inalienable human rights to exercise our freedoms, while extending these rights to our digital twins.

Once the rights are codified into law, technological development shall take care of their adoption and distribution. Surely, it sounds simple enough but it would not be easy. Does this digital society model sound too good to be true? Maybe. The least we could do is try.

Maryam Lee
Strategic programme manager,
IO Foundation



Digital jurisdiction in Malaysia

By Farlina Said

Content-related issues

1. Communications and Multimedia Act 1998
2. Penal Code
3. Sedition Act 1948
4. Defamation Act 1957
5. Film Censorship Act 2001
6. Regulating and enforcing bodies: Ministry of Communications and Multimedia (K-KOM), Malaysian Communications and Multimedia Commission (MCMC), Royal Malaysian Police

Data breaches

1. Communications and Multimedia Act 1998
2. Personal Data Protection Act 2010 (private sector and general public)
3. Computer Crimes Act 1997
4. Official Secret Act 1972 (government data practices)
5. Penal Code
6. Regulating and enforcing bodies: National Cyber Security Agency, K-KOM, Personal Data Protection Department, Malaysia Administration Modernisation Performance Unit, Chief Government Security Office, Royal Malaysian Police

Disinformation and misinformation

1. Communications and Multimedia Act 1998
2. Penal Code
3. Regulating and enforcing bodies: K-KOM, MCMC, Royal Malaysian Police

Hate speech

1. Communications and Multimedia Act 1998
2. Penal Code
3. Regulating and enforcing bodies: K-KOM, MCMC, Royal Malaysian Police

Security-by-design approaches

1. Personal Data Protection Act 2010 (but only in principles)
2. Related bodies: National Cyber Security Agency (NACSA), Cybersecurity Malaysia, Sirim

Be flexible

Be empathetic about the home situation of pupils as some may not have available adult supervision or reliable internet.

Protection of children

1. Child Act 2001 and the Child (Amendment) Act 2016
2. Penal Code
3. Communications and Multimedia Act 1998
4. UN Convention on the Rights of Child
5. Sexual Offences against Children Act 2017
6. Regulating and enforcing bodies: K-KOM, MCMC, Royal Malaysian Police, Ministry of Women, Family and Community Development, Education Ministry, Cybersecurity Malaysia

Protection of women

1. Convention on the Elimination of All Forms of Discrimination Against Women
2. Communications and Multimedia Act 1998
3. Anti-Sexual Harassment Bill
4. Regulating and enforcing bodies: K-KOM, MCMC, Royal Malaysian Police, Ministry of Women, Family and Community Development, Education Ministry, Cybersecurity Malaysia

Speech mustn't fall under social media giants' purview

Western standards not applicable in regions without robust democracy, protection of rights

By Harris Zainul

More than ever, our conversations and communications are embedded in social media platforms. In fact, the Malaysian Communications and Multimedia Commission's (MCMC) internet users' survey 2020 highlights how almost 30 million Malaysians are on social media with global numbers upwards of four billion. This, in no small way, is reflected in these companies' immense market capitalisation that often beat or are in the ballpark of the GDPs of developed countries.

With this growing prominence, these platforms' policy decisions decide what can and cannot be said in the new digital public squares. In simple terms, the content moderation policies represent the privatisation of free speech regulation – an area traditionally governed by the state. Whether or not this brings more benefits than drawbacks remains unclear.

The question of what needs to be done, if anything at all, is even more so. Thrown into this complicated mix is how these platforms operate beyond Malaysian jurisdiction, making government oversight and regulation an even more arduous task.

Yet, the increasingly fraught nature of politics globally, hate speech, misinformation and foreign influence operations make it more urgent than ever to answer this question.

Free-speech regulations

On the privatisation of free-speech regulation and potential role(s) of the state, there are at least three schools of thought. The first advocates for content moderation to be left to free-market forces.

Underpinning this is the thinking that the market will incentivise or disincentivise social media platforms to moderate content to maximise user experience and retain market share. Here, users will decide ultimately the extent of content moderation, with little room for state involvement.

This, however, fails to acknowledge the natural monopolies these platforms are, their network effects and how there are few alternatives. For example, TikTok, Facebook, Twitter and YouTube all featured on Cloudflare's top-10 websites with the highest web traffic in late 2021, registering billions of daily users. In Malaysia, according to the MCMC report, use of social media other than Facebook, YouTube, Instagram, Twitter, Google Plus and LinkedIn stood at a measly 0.2% of the population.

Besides that, it also presumes that users will actively seek, understand and compare the content moderation policies to identify which one suits their needs the best. While some platforms – such as Facebook, Reddit and Twitter – have endorsed the Santa Clara Principles, emphasising platforms to communicate "understandable rules and policies", it remains to be seen how many users view these policies.

Transparency calls

With more and more official communications disseminated through government-run social media accounts on these prominent platforms, users will be hard pressed to use a lesser known alternative or to leave well-known platforms altogether.

The second calls for greater transparency in the content moderation decision-making process.

Here, it is argued that transparency will allow observers to scrutinise the platforms' decisions to remove and retain "offensive" content. This has been widely adopted by most platforms through their transparency reports containing information on content removed because of infringement of platform policies, government takedown notices and other grounds.

The third school of thought argues for greater government oversight and regulation of social media platforms.

The argument goes, governments are elected and possess a mandate to determine the redlines of a particular society while legitimising measures to regulate online content. What this argument lacks is a full appreciation of the risks associated if the government in question does not appreciate free speech.

Relatedly, it is not uncommon for less democratic governments to consolidate control over the information environment through legal means. For example, governments have been introducing "fake news" laws in recent years, with official justification being to address the rise in mis- and disinformation online, yet conveniently worded to persecute those speaking inconvenient truths.

"...transparency will allow observers to scrutinise the platforms' decisions to remove and retain "offensive" content.

Further, the recent prominence of propaganda arising out of the Russian-Ukrainian war has led to increased attention on foreign influence operations among governments. While it might still be too early to tell if and how governments will react with new laws regulating speech and content, it remains a concern.

This is due to past government actions in the region against civil society and non-governmental organisations working on human rights issues that are foreign funded. It is no far stretch of the imagination to picture these "pesky" organisations that are often critical of those in power to fall within the

ambit of such new laws.

Digital 'public utilities'

There are two priority areas for immediate consideration.
The first is to treat social media platforms as public utilities.

Similar to physical utilities, such as water, electric and telecommunications, social media companies today play an outsized role in the functioning of society.

This reflects their current prominence and it needs to be emphasised that they are global in nature, with billions of users and many more billions of dollars in their bank accounts. No longer are they start-ups powered by idealistic young founders pulling up their bootstraps.

Shortcomings in their content moderation policies and implementation can lead to real consequences – as seen with the genocide in Myanmar, 2016 US presidential elections and Covid-19 infodemic.

Further, classifying them as digital public utilities can cement their larger responsibilities to the public and sidestep the mess that is whether these platforms are intermediaries for user-generated content.

These responsibilities can come in the form of improved areas for content moderation that are set by democratic governments under a co-regulation framework.

Under this framework, the government outlines areas of priority in the country-specific context, while the platforms are then responsible for monitoring and taking action when justified.

For example, the government can highlight medical misinformation or foreign influence operations as priority areas for the platforms to remove content on legitimate grounds.

Better user experience

When coupled with the requirement for platforms to publish periodic reports on their efforts, compliance and justification – transparency can be more meaningful, with the government able to introduce external accountability mechanisms for any violation.

This more deliberate approach adds democratic legitimacy to content moderation while limiting the potential for government overreach in controlling the information environment. These platforms also benefit from aligning with what society expects from them, contributing to better user experience overall.

Given how there is little to no technological homogeneity underpinning these platforms, the preference for identifying priority areas for action should allow sufficient flexibility on execution.

The second is to address the gap in scholarship and research on this discourse. Most of the discourse on the privatisation of free speech regulation and wider consideration of platform governance is predominantly Western-centric – analysed through Western-lenses tinted with Western norms, politics and culture.

This is abundantly clear in the discourse following Elon Musk's claim to be a "free-speech absolutist" and that Twitter policies should match the laws of a country in which it is operating.

While this might work for the European Union's proposed Digital Services Act, it is not the case in this part of the world where freedom of speech is rarely accompanied by freedom after speech.

With these platforms occupying an outsized position in shaping news and political agendas, it is critical for voices from this part of the world to be reflected in the larger debate on these content moderation policies.

With the genie long out of the bottle when it comes to living our lives on the internet as mediated by these platforms, it is imperative to address these issues the soonest.

"...privatisation of free speech regulation and wider consideration of platform governance is predominantly Western-centric – analysed through Western-lenses tinted with Western norms, politics and culture.

Harris Zainul
Senior analyst

Harris' primary research areas include policy responses to mis- and dis-information; the consequences of mis- and dis-information on democracy and society; and Southeast Asian and Malaysian politics, human rights, and democratisation. His other research areas include China's Belt and Road Initiative, Asean-Korea relations, and the geopolitics of the Mekong River.

Time to enforce strictly laws against those who commit acts of violence online

By Tashny Sukumaran

Internet still too toxic for women

As of mid-2022, an estimated five billion people are online. While this number might not indicate regular internet users (infrequent users, patchy connections and shared devices are included in the total), it remains that more than 60% of the world's population are connected via technology.

While increased connectivity is a positive step – the United Nations passed a resolution declaring access to the internet as human rights in 2016 – we must also acknowledge that it comes with a host of risks that are difficult to address and mitigate, particularly in societies that already do a poor job of protecting the marginalised.

In 2020, during the height of the pandemic, UN Women found that online and IT-facilitated violence against women soared globally as connectivity increased, reporting disturbing statistics. Its findings showed that "physical threats, sexual harassment, sex trolling, sextortion, online pornography (and) Zoom-bombing" all increased. Intimate image abuse continued to be an issue domestically, with Malaysian Telegram groups devoted to sharing and trading illegal pornographic content mushrooming.

Without guaranteed or protected online safety, freedom of speech and access to information are limited despite their fundamental role in the just development of a society. If governments and relevant authorities do not use a firm hand to address gendered online violence, they perpetuate disempowerment and disenfranchisement, removing women from spaces to which they deserve equal access.

According to a UN report on online violence against women and girls that surveyed five Asian countries, the most common form of violence was "sexist or misogynistic comments, or gendered hate speech". This manifested itself not just through written insults and online harassment, but also spreading intimate images non-consensually, disseminating rape footage and live-streaming child sexual abuse.

Statistics hide truth

A study from The Economist Intelligence Unit found that the overall prevalence of violence against women globally was 85%. However, this rate may be understating the real scope of the issue because of underreporting: only one in four women reported the behaviour to the online platform and 14% to an offline agency.

"Without guaranteed or protected online safety, freedom of speech and access to information are limited...

In a preliminary survey carried out by ISIS Malaysia, 46.7% of respondents were aware of the "official" channels through which a complaint could be made, such as turning to the police or the Malaysian Communications and Multimedia Commission (MCMC). Despite this, 56.7% of respondents said that they had "no trust at all" in these official methods while 30% said they had "very little trust". This preliminary survey carried out over 48 hours also listed cyber-harassment (63.6%), hate speech (33.3%) and cyber-stalking (16.7%) as the most common forms of online gender-based violence.

Unfortunately, the myth that to avoid cyberbullying and intense forms of online harassment one could turn off the computer or phone continues to be propagated. Dilpreet Kaur Gill, a co-founder of community-driven online gender-based violence support group CybHer Malaysia, said following a slew of police reports made about non-consensual intimate images being spread in Telegram groups, the police gave "no response". "That's why the team agreed that unless survivors are keen to make a report, we never advise them to do so as a matter of course."

This was the case as far back as 2017, when domestic civil society groups reported that law enforcement groups did not take online gender-based violence seriously.

"Anecdotal cases have shown that where women did report instances of online VAW, their experiences are often trivialised and normalised... Responses by police officers were either dismissive or condescending. Oftentimes the police would tell the victim that there is nothing they could do as it is a 'private affair' or that the victim should just delete his/her account," said the report, which was submitted to the UN Special Rapporteur on violence against women.

State silence

This underscores how those in power do not understand – or choose not to recognise – that online lives are real lives. But the internet is a space of neutral utility: for better or worse, technology is not an ideologically free space and those pretending otherwise are fooling themselves.

It is also disingenuous to claim that the state has no purview to address online gender-based violence: all states have an obligation to protect people from harm, uphold freedom of expression and individual agency and eliminate violence against women. Victim-blaming, laissez-faire attitudes and a patriarchal legal framework are all barriers to justice.

How then can tech companies, regulators and the authorities address online gender-based violence?

First, a robust and progressive regulatory framework must be put into place. At present, the Malaysian Communications and Multimedia Commission accepts complaints

but the majority are related to telecommunications providers and service quality, not rights-related. However, it does address "offensive" content that could incite ill sentiment among the citizenry, such as comments insulting race or religion.

Codifying violence

Therefore, a cohesive and comprehensive definition of what constitutes online gender-based violence – as well as recognition that such behaviour is illegal – must be codified. MCMC should expand its complaint scope to addressing online gender-based violence, holding responsible not just the perpetrators but also secondary transmitters (re-perpetrators).

Second, there must be a change in mindset when addressing any form of gender-based violence. Rape culture, victim-blaming and casual sexism must be addressed through government-spearheaded awareness campaigns that have been formulated and endorsed by reputable women's rights groups and activists.

Finally, technology intermediaries must embrace their important role. Strict user rules must be imposed and enforced. Social media platforms must investigate and respond to reports of online gender-based violence swiftly and decisively, increasing capacity to handle reports.

In a 2018 report, Amnesty International described Twitter as "toxic", highlighting how under the UN Guiding Principles on Business and Human Rights, the platform was duty-bound to "to take concrete steps to avoid causing or contributing to abuses" of non-discrimination and freedom of expression rights. However, not enough has been done to tackle violence against women using the service despite Twitter increasing the size of its reporting team.

Social media platforms – oftentimes the battlefront of most gender-based attacks – are fascinating in that they constitute public spaces peopled by millions, managed and administrated by private entities that are inherently capitalistic.

> **"Social media platforms constitute public spaces peopled by millions, managed and administrated by private entities that are inherently capitalistic.**

While companies can be pushed to protect human rights, it is those who commit the act of violence who are ultimately responsible and, therefore, should be held liable. This can only be done through stringently enforced legislation that protects marginalised groups rather than those in power, holds perpetrators accountable and provides holistic and long-lasting solutions for victims. For too long, sexist and harmful language has been treated as acceptable: a normalised price to pay, as it were, for being a woman online.

Tashny Sukumaran
Senior analyst

Tashny's research interests include domestic politics, labour migration, gender parity and equality, and the regional role and position of international human rights mechanisms. She is the founder of 50-50 Malaysia, a tool to connect policymakers, journalists and the public with female experts in, on or from Malaysia.

By Farlina Said

Difference between personal & sensitive information

Personal data is information (in respect to commercial transactions) which relates directly or indirectly to a data subject. This is information that could identify an individual, such as name or email.

Sensitive personal data contains information, such as health condition, ethnicity or political opinions.

May be categorised differently if handled by the government, as classification refers to the Official Secrets Act 1972 or newer guidelines distributed by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU).

What should I do if data breaches are reported and they affect me?

Malaysia does not mandate compulsory notification of data breaches to users. The PDPA does not even mandate data breach notification to authorities – though these are among the provisions expected to be updated. However, should information of a data breach come to your notice, there are ways to deal with it:

Confirm the data breach or information released. This may be difficult as companies in Malaysia may not be forthcoming on the extent of information stolen or taken.

Change the passwords of related accounts, or if in doubt, all the accounts. Password management is perhaps one of the barriers that could hinder hackers. It should be a best practice to change the passwords and one that is a good length with a combination of letters, numbers and symbol.

Use two-factor authentication (2FA) to increase the steps to authenticate your identity and entry into accounts. This is usually when an individual has to input a series of numbers delivered via mobile connection or SMS. Other ways is to use an authenticator application. Some banks would have SMS alert services for transactions, which could monitor credit card activities.

Invalidate any affected debit or credit card.

Submit a report to the Royal Malaysian Police's commercial crime investigation department for issues on identity theft that results in credit card fraud or other scams leading to commercial losses.

What should I do if data breaches are reported and they affect me?

Malaysian bodies with possible jurisdiction:

PDRM commercial crime investigation department
Tel:
- +603 2610 1559
- +603 2610 1599

CCID infoline (WhatsApp):
+6013 2111 222

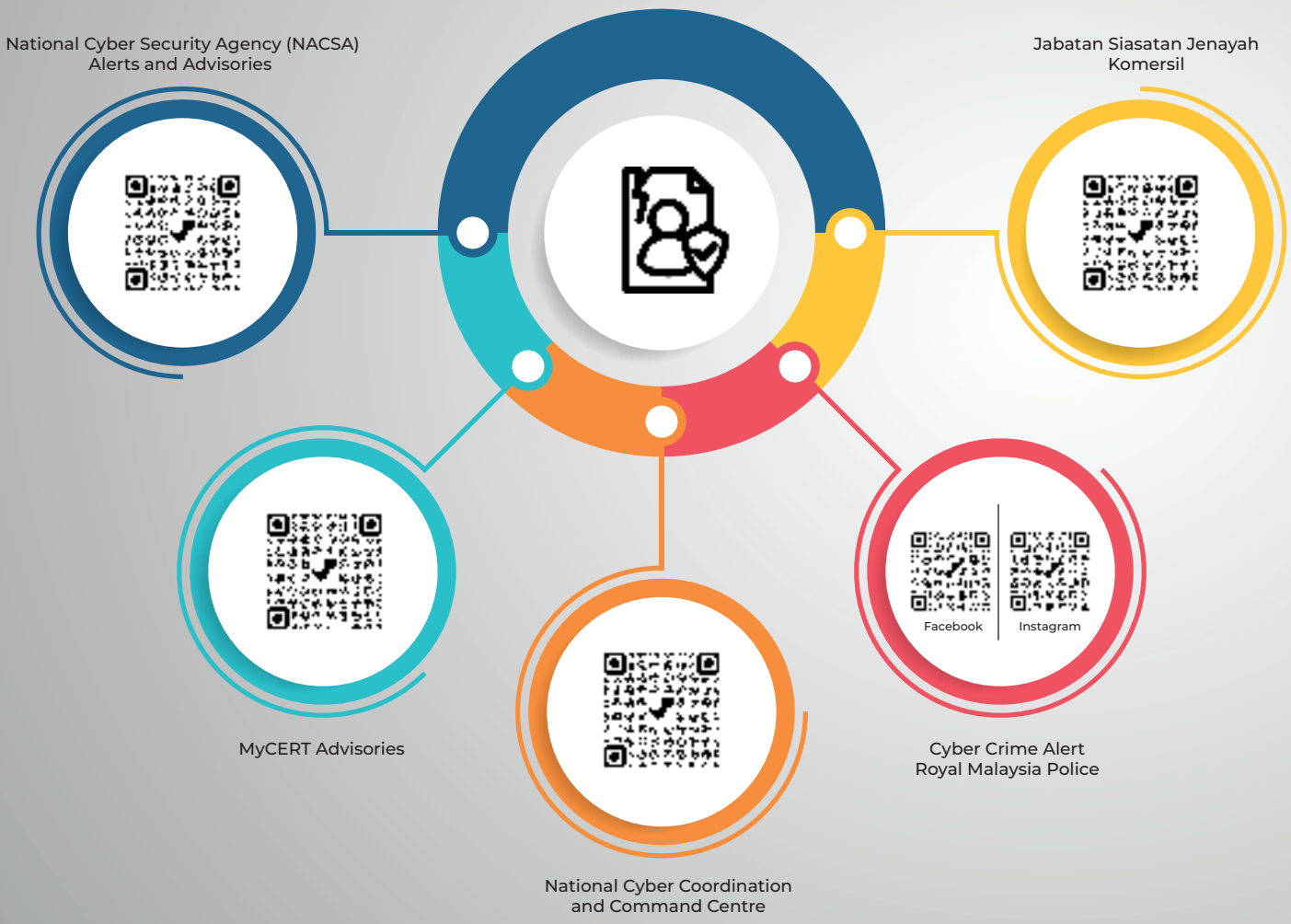
Bank Negara Malaysia
Tel: 1300 88 5465

Communications and Multimedia Content Forum, Malaysian Communications and Multimedia Commission
Email: secretariat@cmcf.my
Hotline: 1800 88 26 23
Tel:
- +603 7954 8105
- +603 7958 3690

Personal Data Protection System by the Personal Data Protection Department
Email: aduan@pdp.gov.my

Cyber999 by MyCERT
Email:
cyber999@cybersecurity.my
Tel: 1300 88 2999
Emergency: +6019 266 5850
SMS: CYBER999 REPORT <EMAIL> <COMPLAINT> to 15888

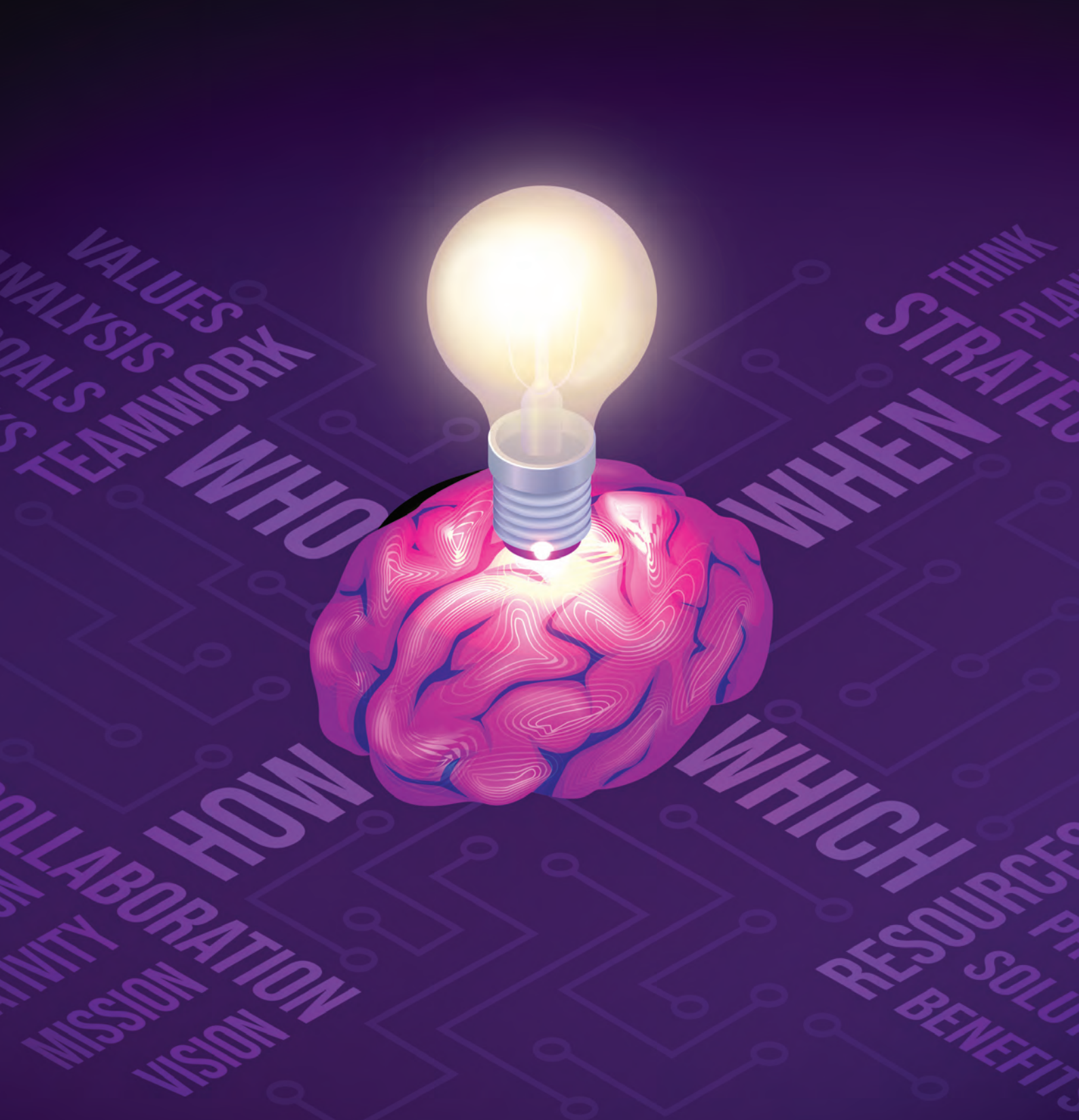
Get updated information on scams, data breaches & online harms



SemakMule Application

GET IT ON Google Play

https://semakmule.rmp.gov.my



ISIS Malaysia, established on 8 April 1983 as an autonomous research organisation, focuses on foreign policy, security studies, economics, social policy, nation-building, technology, innovation and environmental studies.

As a premier think-tank, ISIS Malaysia engages in Track Two diplomacy and fosters regional integration and international cooperation through forums, such as the Asia-Pacific Roundtable (APR), Asean Institutes of Strategic and International Studies (Asean-ISIS), Pacific Economic Cooperation Council (PECC) and Network of East Asian Think-Tanks (NEAT).

Institute of Strategic & International Studies (ISIS) Malaysia

Address: 1, Persiaran Sultan Salahuddin, 50480 Kuala Lumpur, Malaysia
Phone: 603 2693 9366
Email: info@isis.org.my

www.isis.org.my | ISIS_MY | isis_malaysia | ISISMalaysia