SEARCH AND SEIZURE IN THE AGE OF DIGITAL FINANCE: UNDERSTANDING THE PHILIPPINE LEGAL FRAMEWORK REGULATING THE FINANCIAL TECHNOLOGY INDUSTRY AND ITS IMPLICATIONS ON CONSTITUTIONAL RIGHTS

UNIVERSITY OF THE PHILIPPINES
COLLEGE OF LAW

MARIA LOVELYN JOYCE S. QUEBRAR
2013 - 01000

PROF. PATRICIA R.P. SALVADOR-DAWAY
Supervised Legal Research Adviser

SEARCH AND SEIZURE IN THE AGE OF DIGITAL FINANCE: UNDERSTANDING THE PHILIPPINE LEGAL FRAMEWORK REGULATING THE FINANCIAL TECHNOLOGY INDUSTRY AND ITS IMPLICATIONS ON CONSTITUTIONAL RIGHTS

ABSTRACT

Financial technology ("fintech") companies are "industry disruptors"—they have transformed the world of financial services by disrupting traditional financial institutions and altering how we manage our money.[1] Fintech helps expedite processes that once took days, weeks or even months. As the world gradually moves on from the COVID-19 era to the post-pandemic years, fintech has become an integral part of our personal and professional day-to-day life. Indubitably, fintech can become a tool for the protection of liberty and nurturing of prosperity under the rule of law. However, despite strong growth indicators, fintech in the Philippines still faces several challenges, including the balancing of the protection of the users' right to privacy and the upholding of their right against unreasonable searches and seizures. Amidst increasing number of cyberattack threats and data breaches demanding robust security measures,[2]the author aims to recommend solutions to the fintech problem through this paper, which is divided into three major parts: Part I introduces the fintech industry and its history and development; Part II analyzes the different laws governing fintech and the challenges in its regulation; and Part III discusses the future of the industry and recommendations to address the gaps in existing laws in the Philippines regarding protection of data privacy rights

---

[1] *Fintech Disruptors: How Startups are Shaping the Future of Financial Services, available at* https://coda.io/@mukesh-ram/fintech-disruptors-how-startups-are-shaping-the-future-of-financ.

[2] *Fintech in the Philippines: An overview*, ACCLIME, Aug. 31, 2023, *available at* https://philippines.acclime.com/insi-ght/fintech-overview/.

OUTLINE

A. Improving laws and regulations to protect the constitutional rights of Filipinos
B. Striking a Balance between Innovation and Regulation
    1. Equalizing the value of data privacy and law enforcement
        a. Cooperation between government agencies and the private sector
        b. Effective education for fintech users
    2. Enhancing government tools to prevent unreasonable searches and seizures
    3. Increasing the penalty for cybercriminals and other law violators

VIII. CONCLUSION

"Liberty in the constitutional sense must mean
more than freedom from unlawful governmental restraint;
it must include privacy as well, if it is to be a repository of freedom."
—Justice William O. Douglas[3]

"The right to be let alone is indeed the beginning of all freedom."
—Justice Louis D. Brandeis[4]

I. INTRODUCTION

Take a little time and look back to your life during the pandemic. During those days of social distancing, financial technology ("fintech") was the unsung hero in trying to get back the bits and pieces of your pre-pandemic life,[5] such as non-homemade meals, shopping, and payment of bills. As the world gradually moves on to the post-pandemic years, fintech remains to be an integral part of our personal and professional day-to-day life. Traveling to school or your office, you may book a ride-hailing app such as Grab, Joyride, or Angkas, which you pay for through your linked bank or e-wallet account. As you need to get your morning coffee from the nearby café, you pay for your drink by swiping your credit card in the point-of-sale terminal or scanning the QR code on display. Later, when you become hungry for lunch, you order your favorite meal from a food delivery app like Foodpanda. Finally reaching the end of the day, you go to dinner with your friends and split the bill using Gcash or Maya.

Ernst & Young's Global FinTech Adoption Index shows that nearly two-thirds or 64% of the world's population was using fintech applications in 2019, up from 16% in 2015.[6] According to the report, 3 out of 4 consumers had become users of money transfer and payment solutions.[7]

---

[3] Public Utilities Comm'n v. Pollak, 343 U.S. 451, 467 (1952). (Douglas, *J.*, *dissenting*).

[4] Olmstead v. United States, 277 U.S. 438, 478 (1928). (Brandeis, *J.*, *dissenting*).

[5] Stephanie Walden, *What Is Fintech?,* FORBES.COM, July 25, 2022, *available at* https://www.forbes.com/-advisor/banking/what-is-fintech/.

[6] Ernst & Young, *Global FinTech Adoption Index 2019*, ERNST & YOUNG, *available at* https://assets.ey.-com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf

[7] Walden, *supra* note at 5.

As with many emerging technology sectors, fintech can be an ambiguous concept due to the sheer breadth of tools, platforms and services that fall under its yawning umbrella.[8] However, despite strong growth indicators, fintech in the Philippines still faces several challenges, including the balancing of the protection of the users' right to privacy and the upholding of their right against unreasonable searches and seizures. Amidst the increasing number of cyberattack threats and data breaches demanding robust security measures,[9] the author aims to recommend solutions to the fintech problem through this paper, which is divided into three major parts: Part I introduces the fintech industry and its history and development; Part II analyzes the different laws governing fintech and the challenges in its regulation; and Part III discusses the future of the industry and recommendations to address the gaps in existing laws in the Philippines regarding protection of data privacy rights.

II. THE FINTECH INDUSTRY

A. Definition of the Word "Fintech"

Surprisingly, while the term "fintech" is ultramodern, the idea is not brand new.[10] In fact, while Merriam-Webster just added the word to its dictionary in 2018,[11] which means "products and companies that employ newly developed digital and online technologies in the banking and financial services industries,"[12] the concept dates back decades ago.[13] For example, automated teller machines (ATMs) were once considered the cutting edge of fintech innovation, as were signature-verifying technologies first used by banks in the 1860s.[14]

Fintech is a portmanteau for "financial technology." It is a catch-all term for technology used to augment, streamline, digitize or disrupt traditional financial services.[15] The word refers to software, algorithms, and applications for

---

[8] *Id.*

[9] *Fintech in the Philippines: An overview*, ACCLIME, Aug. 31, 2023, *available at* https://philippines.-acclime.com/insi-ght/fintech-overview/.

[10] Walden, *supra* note at 5.

[11] Maria LaMagna, *This 30-year-old financial term was finally added to the dictionary*, MARKETWATCH.COM, Sep. 6, 2018, *available at* https://www.marketwatch.com/story/this-finance-related-term-was-just-added-to-the-dictionary-do-you-know-what-it-means-2018-09-05.

[12] "Fintech." MERRIAM-WEBSTER.COM DICTIONARY, *available at* https://www.merriam-webster.com/dictionary-/fintech.

[13] Walden, *supra* note at 5.

[14] *Id.*

[15] *Id.*

both desktop and mobile, and sometimes it includes hardware, too.[16] Fintech platforms enable run-of-the-mill tasks like depositing checks, moving money between accounts, paying bills, or applying for a loan.[17]

B. Background of the Fintech Industry

Fintech companies primarily utilize technology to carry out core functions offered by financial services, influencing how individuals manage, preserve, borrow, invest, transfer, pay, and safeguard their money.[18] The majority of fintech firms were established after 2000, have secured funding since 2010, and are still in the process of maturing.[19] They facilitate not just the feasibility but also the simplicity of transferring funds between accounts, individuals, nations, and entities. There is no typical fintech company: fintech includes start-ups, growth companies, banks, nonbank financial institutions, and even cross-sector firms.[20]

In establishing a fintech ecosystem, steady demand is crucial as users, including small and medium-sized businesses, require easily accessible financial services lest the ecosystem become completely unviable.[21] Another important consideration is access to capital, as different forms of financing, including private, public, and alternative sources, are driving ecosystem growth in a swiftly evolving landscape to prevent obsolescence.[22]

The interplay between non-financial institutions and fintech is also important, and the results greatly benefit its consumers. Non-financial institutions can access financial instruments through application programming interfaces (API), allowing integration of apps and services using the features of programs that were created by other institutions.[23] The most popular API utilized by the fintech industry are payment gateways, compliance and regulation

---

[16] *Id.*

[17] *Id.*

[18] Max Flötotto, et al., *What is fintech?,* MCKINSEY & COMPANY, Jan. 16, 2024, *available at* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-fintech#/.

[19] Walden, *supra* note at 5.

[20] *Id.*

[21] Kirill Kalashnikov, *Southeast Asia, a vibrant and inclusive fintech ecosystem*, THE ASIAN BANKER, Aug. 30, 2023, *available at* https://www.theasianbanker.com/updates-and-articles/southeast-asia,-a-vibrant-and-inclusive-fintech-ecosystem.

[22] *Id.*

[23] *Id.*

services, anti-money laundering services, and customer knowledge.[24] Embedded finance integrates financial services such as payment processing, lending, and others into the business processes of non-financial companies, which permits the accumulation of user behavior information,[25] resulting into "more personalized and generally better" [26] services.

In developing fintech though API, there are two application models: first is Western, which has a separate application for each product, and second is Asian, which features a so-called "superapp" that combines many different products and functions on one platform.[27] Southeast Asia (SEA) definitely leans towards the second option.[28] Usually, superapps combine taxi hailing, food delivery, fintech products, digital banking, and e-commerce for daily user interaction.[29] One of the more famous brands in SEA is Grab, which offer deliveries, mobility, financial services, enterprise, and others—all through one superapp.[30] These services connect consumers from all walks of life with everyday entrepreneurs, providing enjoyable experiences and fulfilling the everyday needs of millions across 500 cities and 8 countries.[31]

Progressive regulation or government policies regarding markets, taxes, and initiatives also contribute to the development of the financial services industry.[32] Thus, SEA is notably becoming a very favorable environment for a majority of fintech businesses, especially in countries like Singapore, Malaysia, and Philippines, where financial digitalization is a national priority.[33]

C. The Rise of Fintech to Popularity

The most attractive feature of fintech is efficiency. In this fast-paced world where various products and services are available for purchase in different parts of the world, people and industries need something to help them cope, especially when it comes to payments—that something is fintech.

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Creating the superapp*, GRAB, *available at* https://www.grab.com/ph/about/superapp/.
[31] *Id.*
[32] Kalashnikov, *supra* note at 21.
[33] *Id.*

Fintech companies are "industry disruptors"—they have transformed the world of financial services by disrupting traditional financial institutions and altering how we manage our money.[34] Fintech helps expedite processes that once took days, weeks or even months. It also holds the potential to improve financial inclusion. In some parts of the world, where governmental or institutional support is lacking, fintech fills needs for the unbanked.[35] The efficiency of using fintech platforms may be owed to the fact said platforms help users navigate financially complex tasks with little or no interaction with a human at all.[36]

In recent years, fintech has morphed from "being associated with scrappy startups"[37] to "becoming a significant facet of established and legacy financial institutions."[38] Several US banks have already partnered with fintech companies or launched their own fintech initiatives.[39] For instance, Goldman Sachs used fintech to launch an online bank called Marcus in 2016, while JP Morgan Chase invested USD 25 million in fintech startups in 2019.[40]

Another noteworthy attribute of fintech is its sustainability, which has become a priority for many countries in recent years. Fintech, which is inherently green in nature, has become the model industry as nations transition to a low-carbon economy, coupled with amplified regulatory requirements and the growing focus on carbon reporting.[41] Fintech's target consumers, which are millennials and Gen Z, are the most eco-conscious generations.[42] They prefer products and services that align with their values, making the incorporation of sustainability in the business a necessary strategy.[43]

In the Philippines, the popularity of GCash surged during the pandemic as most consumers opted for cashless transactions from online shopping and bill

---

[34] *Fintech Disruptors: How Startups are Shaping the Future of Financial Services, available at* https://coda.io/@mukesh-ram/fintech-disruptors-how-startups-are-shaping-the-future-of-financ.

[35] Walden, *supra* note at 5.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] UOB, PwC, & Singapore FinTech Association, *FinTech in ASEAN 2023: Seeding the Green Transition*, SINGAPORE FINTECH.ORG, *available at* https://singaporefintech.org/wpcontent/uploads/2023/11/5.1_fintech-in-asean-2023.pdf.

[42] *Id.*

[43] *Id.*

payments to transport fares.[44] The mobile payment app, which also offers financial products such as savings accounts, investments, and insurance, has 75 million active users as of 2023, expanding from the 60 million it had in May 2022.[45]

At present, there are several brands in the market that offer alternative solutions to various financing issues. The beautiful thing is, fintech presents itself as an option rather than the only choice. Its presence coincides with traditional payment methods and brick-and-mortar stores. Therefore, the impact of fintech on your life is a personal issue dictated by how many services you choose to interact with—you can go as deep as you want or simply stay surface-level.[46]

D. The Need to Regulate the Fintech Industry

Indubitably, fintech offers a considerable answer to the problems of distance, accessibility, and ease of transaction. In fact, the Bangko Sentral ng Pilipinas (BSP) itself wants half of total retail transactions done electronically, as part of its efforts to cut transaction costs and remove barriers to owning financial accounts.[47]

However, the fintech solution carries along with it a separate mass of troubles. Increased digital use leaves the system open to the risks of hacking and online fraud.[48] Money lost to cybercriminals have continued to rise, with losses due to these illicit activities estimated to have hit PHP 1 billion during the height of the COVID-19 pandemic.[49] As digitalization continues to grow in SEA, regulators must launch suitable legal and regulatory frameworks.[50] However, the challenge lies in information asymmetry given the many complex attributes of these novel business models, and financial products that blur the boundaries

---

[44] Ditas Lopez, *Unauthorized Debits Hit Popular Philippine E-Wallet GCash,* BLOOMBERG NEWS, May 9, 2023, *available at* https://www.bnnbloomberg.ca/unauthorized-debits-hit-popular-philippine-e-wallet-gcash-1.1917659.

[45] Frances Gagua, *GCash eyes "biggest IPO" title, overseas expansion in 2024*, ASIAN BANKING AND FINANCE, *available at* https://asianbankingandfinance.net/cards-payments/exclusive/gcash-eyes-biggest-ipo-title-overseas-expansion-in-2024.

[46] Walden, supra note at 5.

[47] Benjamin Diokno, Speech delivered at the 14th Annual Group of Twenty-Four (G-24) / Alliance for Financial Inclusion Policymakers' Roundtable at the 2022 IMF-World Bank Springs Meetings (Apr. 26, 2022).

[48] Lopez*, supra* note at 44.

[49] *Id.*

[50] *Fintech: A Fine Balance*, ASIAN LEGAL BUSINESS, Aug. 23, 2023, *available at* https://www.legalbusinessonline.-com/features/fintech-fine-balance.

between traditional and innovative ways of doing business whether it involves banking, investments, lending, payments, currency or other fintech.[51]

III. HISTORY AND DEVELOPMENT OF THE FINTECH INDUSTRY

A. The History and Development of the Fintech Industry in Southeast Asia

The rising smartphone consumption have resulted to a growth in usage of digital financial services in SEA, notwithstanding continuous access to traditional banking services.[52] Currently, the region is emerging as a hotspot for fintech innovation across all major areas including payments, lending, insurance and investing.[53]

According to the e-Conomy Southeast Asia Report 2021,[54] usage has increased between 2020 and 2021, recording an annual growth rate ranging from 9% up to 48% across all major digital financial services.[55] Another report by the Robocash Group[56] shows that between 2000 and 2022, the total number of fintechs in SEA rose from 34 to 1,254, with the largest increase occurring between 2015 and 2020.[57]

Based on *Figure 1*, the largest number of companies in SEA operate in India. A total of 541 fintechs are based in India, accounting for 43.1% of all fintechs found.[58] The Philippines comes in the fourth spot, taking up 10% of all

---

[51] *Id.*

[52] Fintech News Singapore*, Is Southeast Asia Entering Its Golden Age of Fintech?,* FINTECHNEWS.SG, Apr. 29, 2022, *available at* https://fintechnews.sg/60785/financial-inclusion/is-southeast-asia-entering-its-golden-age-of-fintech/.

[53] *Id.*

[54] Google, Temasek and Bain & Company, *e-Conomy SEA 2021 The Digital Decade: Southeast Asia's internet economy resurgence is fueling growth across the region,* BAIN & COMPANY, Nov. 10, 2021, available at https://www.bain.com/insights/e-conomy-sea-2021/.

[55] Tom Bleach, *Southeast Asia Sees Number of Fintechs Rise by 3588% Since 2000; Reveals RoboCash Group*, THE FINTECH TIMES, Feb. 11, 2023, *available at* https://thefintechtimes.com/southeast-asia-sees-number-of-fintechs-rise-by-3588-since-2000-reveals-robocash-group/.

[56] Robocash Group, *State of SEA Fintech 2022 Report*, *available at* https://robocash.group/pressroom/substantial-growth-in-payments-transfers-alternative-lending-e-wallets-and-digital-banking-sectors-over-the-past-two-decades/.

[57] Bleach, *supra* note at 55.

[58] *Id.*

the fintechs in the region.[59] When it comes to funding, fintechs in SEA more than tripled to hit a record USD 3.5 billion in the first nine months of 2021, compared to USD 1.1 billion for all of 2020.[60]

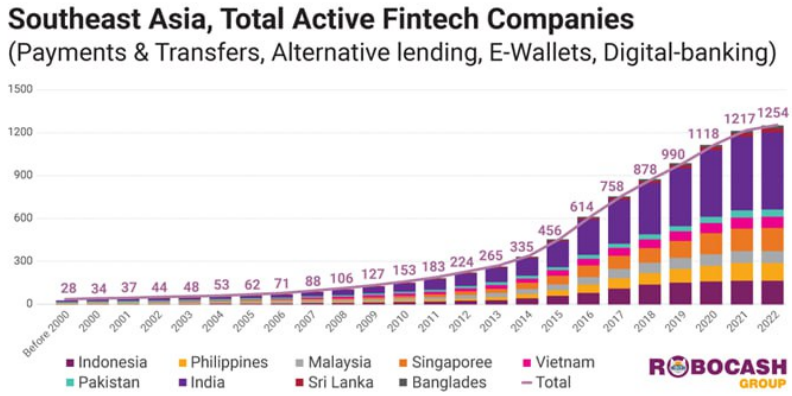

Figure 1. This shows the number of active fintech companies in Southeast Asia in 2022.[61]

In SEA, individuals who are underbanked and unbanked make up more than 70% of the population.[62] Many lack bank accounts, are in debt, and transact mostly in cash, which makes it difficult for them to build credit histories and have access to credit from traditional financial institutions.[63] Relatedly, over of 60% micro, small and medium enterprises (MSMEs), encounter obstacles in securing loans from traditional banks due to high collateral requirements.[64]

With the introduction of new and innovative financial solutions by fintech companies, the way that consumers, including the unbanked and underbanked, and businesses transact has changed dramatically.[65] One concrete example is

---

[59] *Id.*

[60] Deloitte Southeast Asia Innovation Team, *The rise of fintech in Southeast Asia*, Oct. 11, 2022, *available at* https://kr-asia.com/the-rise-of-fintech-in-southeast-asia. *Note that* the fastest growing fintech categories are digital payments and digital lending. In 2021, the digital payments segment saw record funding of USD 1.9 billion, a 244% compound annual growth rate (CAGR) from USD 562 million in 2020. Digital lending also recorded a sizable 78% CAGR to USD 314 million.

[61] Robocash Group, *supra* note at 56.

[62] *The credit landscape in The Philippines is growing according to Mocasa*, TECH COLLECTIVE, May 9, 2023, *available at* https://techcollectivesea.com/2023/05/09/credit-landscape-philippines-mocasa/#:~:text=-The%20credit%20landscape%20in%20The%20Philippines%20is%20growing%20according%20to%20Mocasa&text=Despite%20being%20a%20significant%20regional,population%20is%20unbanked%20or%20underbanked.

[63] Deloitte Southeast Asia Innovation Team, *supra* note at 60.

[64] *Id.*

[65] *Id.*

mobile money, also known as the e-wallet.[66] With SEA's soaring smartphone penetration, e-wallets are now one of the most popular payment methods in the region.[67] Mobile transaction volume in the region reached USD 62.59 billion in 2020 and is expected to rise more than four-fold to USD 268.07 billion by 2025.[68]

The payment landscape across SEA is localized and fragmented, and each country has a preferred e-wallet.[69] Singapore has PayLah! and GrabPay, Philippines has GCash, Indonesia has GoPay, OVO and DANA, Vietnam has MoMo and VNPAY, and Malaysia has Boost and Touch 'n Go.[70] These e-wallets all utilize QR payments, with some offering card options, like GrabPay Mastercard.[71] Scanning QR codes is the most popular way to make digital payments in SEA, largely due to their low operating costs, versatility, and convenience for consumers and merchants.[72]

Another reason why e-wallets are popular in the region is that most SEA residents do not use credit cards. Over 174 million adults in SEA do not have a bank account or credit card.[73] In Thailand, Vietnam, and Indonesia, the number of residents who hold a credit card are about 30%, 11%, and 6% of the population, respectively.[74] QR payments-based e-wallets allow SEA users to make digital payments with only a smartphone and Internet connection.[75]

Notably, the players in SEA's payments sector are not just payment companies—many of them are also e-commerce firms.[76] Therefore, it is not by chance that SEA is witnessing a rapid expansion in digital payments coinciding with a surge in e-commerce. According to the International Data Corporation, e-commerce spending in SEA is expected to rise by 162% to USD 179.8 billion by 2025.[77] Digital payments are expected to account for 91% of e-commerce

---

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *E-Commerce Evolution in Asia and the Pacific*, ASIAN DEVELOPMENT BANK, November 2023, available at https://www.adb.org/sites/default/files/publication/922086/e-commerce-evolution-asia-pacific-opportunities-challenges.pdf.

transactions.[78] The largest markets for e-commerce payments are expected to be Indonesia (USD 83 billion), Vietnam (USD 29 billion), and Thailand (USD 4 billion).[79] As a result, there is a convergence of digital payments, payments infrastructure and e-commerce in SEA, especially among the larger e-commerce players who can leverage their existing customers and merchants to acquire users for their new financial offerings.[80] For example, Shopee has ShopeePay and SeaBank, while GoTo has GoPay and the GoTo financial ecosystem.[81] Lazada has been strengthening its digital finance infrastructure through partnerships, such as those with AmBank in Malaysia, Finaxar in Singapore, DANA in Indonesia, and Asia Kredit in the Philippines.[82]

B. The History and Development of the Fintech Industry in the Philippines

The Philippines is among the fastest-growing economies in SEA, but the primary focus of large traditional banks on wholesale and corporate services has rendered a significant portion of the potential customer base underserved.[83] Another significant challenge is the public's limited knowledge regarding the banking system.[84] Forty five percent of unbanked Filipinos believe that balance requirements would prevent them from opening an account despite existing products with no minimum balance required, while another 40% say that they believe they lack adequate documentation.[85]

Nevertheless, this scenario is evolving swiftly. Two domestic payments services, GCash and Maya, are operating at scale, and international competitors are already vying for position in a swiftly changing and very promising market for digital financial services.[86] Onboarding users is now made easier with the advent of the Republic Act (R.A.) No. 11934 or the SIM Registration Act, linking

---

[78] *Id.*

[79] *Id.*

[80] Deloitte Southeast Asia Innovation Team, *supra* note at 60.

[81] *Id.*

[82] *Id.*

[83] Emmie Abadilla, *PH banks poised for growth but lagging in tech*, MANILA BULLETIN, Aug. 21, 2023, *available at* https://mb.com.ph/2023/8/20/article-871.

[84] Guillaume de Gantès, Hernan Gerson, and Kristine Romano, *On the verge of a digital banking revolution in the Philippines*, MCKINSEY & COMPANY, May 3, 2023, *available at* https://www.mckinsey.com/industries/financial-servi-ces/our-insights/on-the-verge-of-a-digital-banking-revolution-in-the-philippines.

[85] *Id.*

[86] *Id.*

cellular SIM cards with verified users.[87] This guarantees existing and prospective fintechs a share of consumers in the market.

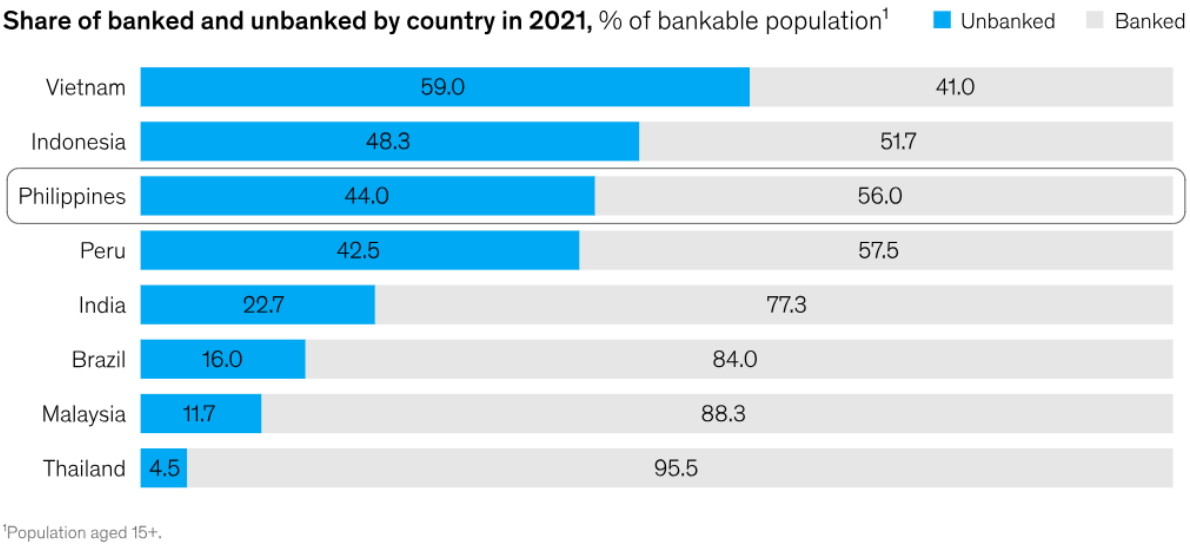

Figure 2. The Philippines has a low rate of banking penetration among peer countries, underscoring the enormous unmet demand for financial services.[88]

Notably, fintech companies within the definition of small or medium sized businesses in R.A. No. 9501 or the Magna Carta for MSMEs[89] are entitled to government assistance for said businesses in the form of, among others, direct and indirect project lending, rediscounting of loan papers and financial leasing.[90] In relation to this, the R.A. No. 11293 or the Philippine Innovation Act aims to incentivize innovative MSMEs through the creation of an innovation fund.[91] It

---

[87] de Gantès, et. al, *supra* note at 84.

[88] *Id., citing* Alliance for Financial Inclusion; Bangko Sentral ng Pilipinas; Bank of Thailand; BSP Financial Inclusion Survey; Economic Intelligence Unit; Global Findex Database 2021; Reserve Bank of India; World Bank; McKinsey analysis, *available at* https://www.mckinsey.com/industries/financial-services/our-insights/on-the-verge-of-a-digital-banking-revolution-in-the-philippines.

[89] Rep. Act. No. 6977, as amended by Rep. Act. No. 9501. § 3. *Micro, Small and Medium Enterprises (MSMEs) as Beneficiaries.* — MSMEs shall be defined as any business activity or enterprise engaged in industry, agribusiness and/or services, whether single proprietorship, cooperative, partnership or corporation whose total assets, inclusive of those arising from loans but exclusive of the land on which the particular business entity's office, plant and equipment are situated, must have value falling under the following categories: micro - not more than P3,000,000; small - P3,000,001 – P15,000,000; medium - P15,000,001 – P100,000,000.

[90] *Fintech Laws and Regulations Philippines 2023-2024*, ICLG.COM, Dec. 7, 2023, *available at* https://iclg.com/prac-tice-areas/fintech-laws-and-regulations/philippines.

[91] *Republic Act No. 11293*, DICT, June 14, 2023, *available at* https://dict.gov.ph/ra-11293/?__cf_chl_tk=LrRAV1ezX8ikOYacwiea2plwjEfMgHa8.IKGFNnlZpM-1709226810-0.0-1511.

also mandates the Intellectual Property (IP) Office to promote and streamline the registration and protection of IP.[92]

Remittances also play an exceptionally vital economic role in fintech, with about USD 30.5 billion in remittances flowing into the Philippines every year.[93] Gcash and Maya are explicitly targeting remittance transactions, disrupting the established model of brick-and-mortar service providers.[94]

In 2020, the BSP issued Circular No. 1105, entitled the Guidelines on the Establishment of Digital Banks.[95] The Circular considers digital bank as a distinct classification of bank and provides the framework for its operation and establishment.[96] Six digital banks are licensed under this dedicated regime, but in August 2021, the BSP imposed a three-year moratorium on the grant of digital banking licenses to closely monitor the performance and impact of the new banking classification on the industry.[97] However, as of 2023, the BSP was already contemplating the lifting of the said moratorium as more players have expressed their interest in joining the industry.[98] With digital banks, opening basic accounts for retail customers now only demands a phone number or an ID card.[99] The BSP's unified QR code payments infrastructure (QRPh) has reduced person-to-merchant (P2M) transaction costs while further expanding the reach of digital payments systems, and the introduction of InstaPay and PesoNet is enabling at-scale transactions via electronic bank transfers.[100] This led to an increasing pressure from fintech companies which drives innovation within the traditional banking sector. For example, BPI, one of the country's largest banks,

---

[92] *Supra* note 90.

[93] *Id.*

[94] *Id.*

[95] BSP Circ. 1105 (2020). Guidelines on the Establishment of Digital Banks, *available at* https://www.bsp.gov.ph/Regulations/Issuances/2020/c1105.pdf.

[96] Dennis Quintero, Kristina Navarro & Danielle Gaite, *Philippines: BSP releases Guidelines on the Establishment of Digital Banks*, BAKER MCKENZIE, Feb. 7, 2021, *available at* https://www.globalcompliancenews.com/2021/02/07/phili-ppines-bsp-releases-guidelines-on-the-establishment-of-digital-banks210121/.

[97] Lawrence Agcaoili, *BSP mulls lifting ban on new digital banks*, THE PHIL. STAR, Oct. 12, 2023, *available at* https://www.philstar.com/business/2023/10/12/2302979/bsp-mulls-lifting-ban-new-digital-banks#:~:text=The%20-BSP%20has%20granted%20digital,Singapore%2Dbased%20digital%20bank%20Tyme.

[98] Ian Cigaral, *BSP: Digital banks struggling with loan collections*, PHIL. DAILY INQUIRER, Jan. 8, 2024, *available at* https://business.inquirer.net/439922/bsp-digital-banks-struggling-with-loan-collections.

[99] de Gantès, et. al, *supra* note at 84.

[100] *BSP Digital Payments Transformation Roadmap 2020-2023*, BSP, *available at* https://www.bsp.gov.ph/Media_And_Research/Primers%20Faqs/Digital%20Payments%20Transformation%20Roadmap%20Report.pdf.

recently launched the Vybe e-wallet on its mobile app, which offers many of the same services as GCash and Maya.[101] At the same time, UnionBank has begun offering fully digital financial services to underbanked consumers via its UnionDigital Bank proposition.[102]

For an entity to become a fintech, an attractive strategy, given the relatively long wait time for a universal banking license and the suspended application process for digital licenses,[103] is purchasing a small rural bank then converting it into a digital banking hub.[104] In the McKinsey report, over 400 rural banks are found to be eligible for this purpose.[105] Seabank Philippines exemplifies this approach in practice. In October 2020, Seabank acquired a majority stake in Banco Laguna Inc, a small rural bank,[106] and in April 2021, it obtained an Electronic Products and Financial Services (EPFS) Type A License, which enabled it to launch its digital-first proposition nationwide.[107]

The extensive yet unexplored opportunities within the growing fintech sector in the Philippines offer significant potential, surpassing any accompanying risks. However, effectively navigating the rapidly evolving digital finance landscape in the Philippines requires a deep understanding of its structural limitations, regulatory environment, economic integration, and global positioning.

IV. REGULATIONS AND COMPLIANCE FOR FINTECH CORPORATIONS: THE IMPACT OF THE GENERAL DATA PROTECTION REGULATION IN SOUTHEAST ASIA AND THE PHILIPPINES

A. The General Data Protection Regulation

Effective starting May 25, 2018, the General Data Protection Regulation (GDPR) is hailed as the toughest privacy and security law in the

---

[101] *Vybe*, BPI, *available at* https://www.bpi.com.ph/personal/bank/digital-banking/mobile/vybe.

[102] *About u*s, UNION DIGITAL BANK, *available at* https://uniondigitalbank.io/en.

[103] de Gantès, et. al, *supra* note at 84.

[104] *Id.*

[105] *Id.*

[106] *History of Seabank*, SEABANK.PH, *available at* https://www.seabank.ph/info/history.

[107] *Seabank's Financial Statements 2021, Notes to Financial Statements*, p. 1, SEABANK.PH, *available at* https://www.seabank.ph/assets/pdf/pages/financial%20statement/Financial_Statement_2021.pdf.

world.[108]According to the World Bank, the GDPR "is the most recent example of comprehensive regulation of data protection and privacy, setting a new threshold for international good practices."[109] Although it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, as long as they gather or cater to data related to people in the EU. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.[110]

In summary, the GDPR protects the following rights of individuals: (1) the right to be informed; (2) the right of access; (3) the right to rectification; (4) the right to be forgotten; (5) the right to restrict processing; (6) the right to data portability; (7) the right to object; and (8) rights in relation to automated decision making and profiling.[111] Generally, the rights of individuals are similar to those under the Data Protection Act, GDPR's predecessor, but these have been significantly strengthened under GDPR and procedures should be in place to cover the new rights that individuals have.[112]

1. *Right to be informed* – This enables individuals to understand what personal information is being gathered about them, the reasons behind it, who is gathering the data, the duration of its collection, how to raise concerns, and whether any data sharing will transpire.[113]

2. *Right of access* - Individuals have the right to submit access requests and obtain information from the organization regarding whether their personal data is being processed.[114] Subsequently, the organization is required to furnish a copy of the individual's personal data and any additional information they possess.[115] Information must be provided within one month of the data subject's requests, rather than the

---

[108] *Data protection and privacy laws*, WORLD BANK, *available at* https://id4d.worldbank.org/guide/data-protecti-on-and-privacy-laws.

[109] *Id.*

[110] *What is GDPR, the EU's new data protection law?,* GDPR.EU, *available at* https://gdpr.eu/what-is gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU.

[111] *GDPR – Key Provisions*, DIXON WILSON CHARTERED ACCOUNTANTS, Mar. 1, 2018, *available at* https://www.dixonwilson.com/technical-updates/gdpr-key-provisions.

[112] *Id.*

[113] *What are 8 Data Subject rights according to the GDPR*, Oct. 16, 2022, *available at* https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/.

[114] *Id.*

[115] *Id.*

previous 40 days.[116] This can be extended to two months if the request is complex and the request can be declined in extenuating circumstances.[117] In most cases, there should be no fee associated with providing this information.[118]

3. *Right to rectification* – This enables individuals to request that the organization rectify any inaccurate or incomplete data they hold about them.[119] If the organization confirms the data is inaccurate, the legal deadline to respond to a request is one month.[120] Upon such a request, the organization must verify the data's inaccuracy and rectify it.[121]

4. *Right to be forgotten* – This is also known as the right to erasure.[122] It means data subjects can request their data to be erased.[123] However, the Information Commissioners Office (ICO) acknowledges that there are legal obligations and professional guidelines that may require data controllers or processors to retain certain kinds of data for specific periods.[124]

5. *Right to restrict processing* - Individuals have the option to ask an organization to restrict the usage of their personal data, although the organization is not obligated to automatically delete it.[125] However, they must refrain from processing in certain situations, such as when data is inaccurate.[126] Once the data is restricted, the organization is prohibited from processing it unless they have obtained consent, require it for legal claims, or need it to safeguard the rights of other individuals.[127]

---

[116] *Supra* note at 110.
[117] *Id.*
[118] *Id.*
[119] *Supra* note at 111.
[120] Id.
[121] *Id.*
[122] *Id.*
[123] *Supra* note at 110.
[124] *Id.*
[125] *Supra* note at 111.
[126] *Id.*
[127] *Id.*

6. *Right to data portability* – This is a new right under the GDPR.[128] Data subjects now have the right to have data transferred to a third-party service provider in a structured, commonly used, and machine-readable format.[129] However, this right only arises where personal data is provided and processed based on consent or when necessary to perform a contract.[130] Individuals can also request that their data be transferred directly to another organization.[131]

7. *Right to object* – This allows individuals to raise objections to the processing of their personal data under specific circumstances, contingent upon the processing purpose and lawful basis.[132] Individuals can also object to data processing based on legitimate interests or tasks in the public interest.[133]

8. *Rights in relation to automated decision-making and profiling* - Strict rules when it comes to the processing of personal data that is done without human involvement are introduced by the GDPR.[134] This includes various forms of profiling, such as evaluating individual job performance, financial status, and behavior, especially if it results in a legal consequence that substantially impacts them.[135] However, it will not apply if the processing is necessary for the performance of a contract, if it is authorized by the law, or if the processing is based on explicit consent.[136]

It is also worthy to note that the size of the sanctions is significant under the GDPR. Organizations that violate the law shall be penalized in the amount of 4% of their global sales for the last 12 months or around 20 million euros for violations of this new set of rules and regulations.[137]

---

[128] *Supra* note at 110.
[129] *Supra* note at 111.
[130] *Supra* note at 110.
[131] *Supra* note at 111.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *GDPR Summary, available at* https://www.gdprsummary.com/gdpr-summary/.

B. The Impact of GDPR in Southeast Asia

The GDPR and other similar regulations worldwide have heightened awareness regarding individual' rights in safeguarding their privacy and overall data protection.[138] In contrast to the EU, the SEA landscape comprises numerous legal systems with varied characteristics and historical backgrounds, making it extremely challenging to generalize the operation of data protection laws in this region.[139] Corporations in these jurisdictions must abide with the complexities inherent in each one while devising a privacy compliance program.[140]

Nevertheless, the Association of Southeast Asian Nations (ASEAN) is catching up, although the development of data protection regulation in its member-countries has progressed to varying degrees.[141] Until recently, Singapore, Malaysia, Thailand, and the Philippines were the only countries with personal data protection laws.[142] The latest country in ASEAN to enact data protection laws is Indonesia, with the Personal Data Protection bill's passage into law in 2022.[143] The remaining countries in ASEAN do not have overarching regulatory frameworks for data protection, although there are laws in specific sectors or for electronic media that regulate personal data. [144]

Due to significant trade between ASEAN and Europe, adherence to EU regulations is increasingly essential for businesses.[145] The GDPR has become the catalyst that compelled several ASEAN countries to review their own data protection laws and possibly develop a similar regulatory framework to protect their citizens and enable local businesses to operate globally through some sort of comity in regulatory approach.[146]

---

[138] Aryashree Kunhambu, *Asia's Regional Data Protection Regulations and its comparison with the GDPR,* Mar. 24, 2022, *available at* https://tsaaro.com/blogs/asias-regional-data-protection-regulations-and-its-comparison-from-the-gdpr/.

[139] *Id.*

[140] *Id.*

[141] Sharon Tan and Nurul Azman, *The EU GDPR's impact on ASEAN data protection law,* FINANCIER WORLDWIDE MAGAZINE, September 2019, *available at* https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law.

[142] *Id.*

[143] DLA Piper, *Data Protection Laws of the World*, DLA PIPER, Jan. 2, 2024, *available at* https://www.dlapiperdataprotection.com/index.html?t=law&c=ID#:~:text=The%20PDP%20Law%20provides%20personal,data%20processor)%20for%20losses%20incurred.

[144] Tan & Azman, *supra* note at 141.

[145] *Id.*

[146] *Id.*

1. Malaysia

Malaysia is currently in the process of reassessing its Personal Data Protection Act 2010 (PDPA) to align it more closely with the GDPR.[147] The Minister of the Communications and Multimedia Ministry, which is the ministry charged with responsibility for the protection of personal data, has stated that one of the objectives of the review of the PDPA is to streamline international requirements on personal data protection, including the many key takeaways of the GDPR.[148] According to the minister, "Malaysia has the PDPA which was formulated in 2010, but after nine years, there are so many new developments and it is important for the existing law to be amended to ensure that we are up-to-date with the current developments."[149] A timeframe has not been set on when the PDPA will be amended. The review of the PDPA began in 2018, but the dissolution of the Malaysian Parliament in 2022 and subsequent general election, put this on hold.[150]

2. Singapore

Singapore's Personal Data Protection Act 2012 (PDPA) is considered to be more pragmatic and favorable for businesses because it includes a broad range of exceptions to consent that organizations can utilize.[151] Even so, the PDPA shares many GDPR principles, in that they both require customer consent for all communications regarding data collection, data processing or disclosure of data.[152] As part of an ongoing review, a discussion paper was issued to introduce the right to data portability, which gives users greater control over the movement of their information across service providers.[153] More recently, Singapore has appointed the Infocomm Media Development Authority (IMDA) as its accountability agent.[154]

---

[147] *Id.*

[148] Kherk Chew, *Malaysia: 90 Days under Malaysia Madani - Personal Data Protection redux*, BAKER MCKENZIE, Mar. 3, 2023, *available at* https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-90-days-under-malaysia-madani-personal-data-protection-redux.

[149] Tan & Azman, *supra* note at 141.

[150] Chew, *supra* note at 148.

[151] Rosalyn Page, *The state of privacy regulations across Asia*, CSO, *available at* https://www.csoonline.com/article/57-2461/the-state-of-privacy-regulations-across-asia.html.

[152] Tan & Azman, *supra* note at 141.

[153] *Id.*

[154] *Id.*

Singapore joined the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CPBR) system in March 2018 and has become the third economy after the US and Japan to operationalize the system.[155] As accountability agents, IMDA will ensure the privacy policies and practices of participating organizations comply with the APEC CBPR and Privacy Recognition for Processors (PRP) through independent third-party assessments before certifying them.[156] By appointing IMDA, Singapore has shown a deep commitment "to pursue a better data protection mechanism that does not hinder innovation and development."[157]

3. Thailand

Thailand's first consolidated law on personal data protection, called the Personal Data Protection Act (PDPA), was initially signed in 2019 but was enforced in 2022 due to the pandemic.[158] As the EU's third-largest commercial partner in ASEAN, businesses in Thailand must integrate GDPR regulations within their processes.[159] While the Thai PDPA reflects concepts developed from Thai perspectives, compliance with the EU GDPR does not necessarily reflect compliance with the Thai PDPA.[160] Therefore, careful examination is crucial in order for companies to fully comply with the PDPA and the GDPR.[161]

The Thai PDPA is applied to organizations that are directly based in Thailand or are based abroad but are involved in controlling and processing goods, services, and consumer behavior data in Thailand.[162] Businesses should be mindful of two data types – a) general data, such as name, date of birth, phone number, etc.; and b) sensitive data, such as racial, sexual, religious, health, political, and biometric information.[163] Overall, the data owner must give explicit consent to approve any acts of collection, use, or disclosure of their personal data.[164]

---

[155] APEC Electronic Commerce Steering Group, *Singapore Joins APEC Data Privacy System*, ASIA-PACIFIC ECONOMIC COOP., Mar. 7, 2018, *available at* https://www.apec.org/press/news-releases/2018/0307_cbpr.

[156] *Id.*

[157] *Id.*

[158] Nguyen Hanh, *Thailand Issues First Personal Data Protection Act*, ASEAN BRIEFING.COM, May 11, 2022, *available at* https://www.aseanbriefing.com/news/thailand-issues-first-personal-data-protection-act/.

[159] *Id.*

[160] Tan & Azman, *supra* note at 141.

[161] *Id.*

[162] Hanh, *supra* note at 158.

[163] *Id.*

[164] *Id.*

The Thai PDPA introduces strict, practical guidelines and penalties for any misuse of personal data, including for e-commerce activities.[165] Public and private companies are obligated to protect confidential data and provide financial compensation for those affected by the data breach.[166] The Act would secure a stable and sustainable environment for e-commerce, especially in dealing with cross-border transfers that already make up half of the online consumer purchases in Thailand.[167] Prior to the Thai PDPA, weak legal measures failed to protect consumers from bank scams and fraud arising from data leakage and identity theft with 32% of Thai tech professionals having reported personal experience with payment fraud in 2019.[168]

4. Indonesia

The Personal Data Protection (PDP) Bill was passed and became law on October 17, 2022 in Indonesia.[169] The PDP Law is the first comprehensive law in Indonesia to govern personal data protection in both electronic and non-electronic systems. It signifies the development of policies on personal data protection and confidentiality and strengthens the protection of the right to privacy.[170]

The PDP Law is closely aligned with international data privacy standards and is largely modelled on the GDPR.[171] It covers data ownership rights, and prohibitions on data use, along with the collection, storage, processing, and transfer of personal data of Indonesian users.[172] It also introduces new concepts, including the requirement for both prior and post notifications to the regulator on cross-border personal data transfers. The new law goes further by introducing criminal sanctions for personal data breaches.[173]

---

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] DLA Piper, *supra* note at 143.

[170] Thales Group, *Personal Data Protection (PDP) Law of Indonesia*, THALES GROUP, *available at* https://cpl.thales-group.com/compliance/apac/indonesia-personal-data-protection-law.

[171] DLA Piper, *supra* note at 143.

[172] Thales Group, *supra* note at 170.

[173] *Id.*

In addition, Indonesia has sector-based laws such as Law No. 11 of 2008 on Information and Electronic Transaction, which was as amended in 2016.[174] This law which requires a party that operates an electronic system to implement security measures to prevent failure or disturbance to the electronic systems, including personal data on such systems, and laws specific to the telecoms, banking, and capital markets sectors.[175]

5. Laos

Laos passed the Law on Electronic Data Protection 2017 which provides data protection to Lao citizens in circumstances where electronic information is collected, accessed, used, or disclosed.[176] The Act provides for general protection to personal information and establishes essential concepts such as consent, data retention and deletion practices, ensuring data accuracy. The Act is supplemented by the Introduction on Implementation of the Electronic Data Protection Act, which sets out examples of how data protection procedures may be implemented by companies.[177]

Furthermore, the Law on Prevention and Combating of Cybercrime 2015 contain provisions which protect data privacy and prohibit the use of personal information which could harm a data subject's reputation.[178]

6. Vietnam

After a protracted period of deliberation, the Vietnamese government ultimately passed the country's "historic," first-ever Personal Data Protection Decree (PDPD) on April 17, 2023, which took effect on July 1, 2023.[179] The PDPD is a landmark legal instrument that integrates all of Vietnam's disparate data protection legislation, with the potential to bring them closer to the GDPR

---

[174] Hanh, *supra* note at 158.

[175] *Id.*

[176] *Lao PDR – Data Protection Overview*, *available at* https://www.dataguidance.com/jurisdiction/lao-pdr.

[177] *Id.*

[178] Hanh, *supra* note at 158.

[179] *Vietnam Personal Data Protection Decree in effect from 1 July 2023*, May 15, 2023, ALLEN & GLEDHILL, *available at* https://www.allenandgledhill.com/vn/publication/articles/23650/personal-data-protection-decree-in-effect-from-1-july
-2023.

requirements.[180] The PDPD will apply to both domestic and foreign individuals/entities that directly engage in or relate to personal data processing activities in Vietnam.

Remarkably, in January 2019, Vietnam passed a controversial cyber security law.[181] The law imposes onerous conditions, like mandatory data localization requirements and cross-border data transfer restrictions by requiring that important data generated or collected by offshore entities in Vietnam be kept onshore.[182] In addition, the privacy regulator has the right to physically inspect the contents of the information stated in the application for the cross-border transfer of personal data and domestic, and foreign service providers must store the users' data in the country for a certain period to be stipulated by the government.[183] It also requires tech companies to share user data if asked by the government and to open a local office in the country.[184]

7. Cambodia

At present, Cambodia does not have a comprehensive data protection law. There are some general protections of personal data, confidentiality and privacy in the Cambodian Constitution, the Cambodian Civil Code, labor law and sector-specific laws governing banking and financial services and medical ethics.[185] However, Cambodia is poised to become the next SEA nation to roll out a personal data protection law which is patterned after the GDPR.[186]According to the Ministry of Posts and Telecommunications, the law would apply to all private entities that collect and use personal data, but not public authorities.[187] Although the proposal, which was drafted in 2023, lays out personal data rights in line with international law, lawyers who reviewed the text said its requirement for local

---

[180] *A Closer Look at Vietnam's First-Ever Personal Data Protection Decree*, TILLEKE & GIBBINS, Apr. 21, 2023, *available at* https://www.tilleke.com/insights/a-closer-look-at-vietnams-first-ever-personal-data-protection-decree/.

[181] Thoi Nguyen, *Vietnam's Controversial Cybersecurity Law Spells Tough Times for Activists*, THE DIPLOMAT, Jan. 4, 2019, *available at* https://thediplomat.com/2019/01/vietnams-controversial-cybersecurity-law-spells-tough-times-for-activists/.

[182] *Id.*

[183] Page, *supra* note at 151.

[184] Hanh, *supra* note at 158.

[185] *Id.*

[186] Fiona Kelliher, *Cambodia's draft data protection law fans fears of government abuse,* NIKKEI ASIA, Dec. 8, 2023, *available at* https://asia.nikkei.com/Politics/Cambodia-s-draft-data-protection-law-fans-fears-of-government-abuse.

[187] *Id.*

data storage and vague language could give companies and the government broad leeway to access or share information without consent.[188]

8. *Myanmar*

There is currently no general data protection law in place in Myanmar. However, it is worthy to note that The Law for Protection of Personal Privacy and Personal Security of Citizens exists,[189] although it does not specifically address the data protection concerns of the citizens. In relation to this, there are calls from multiple sectors for the Myanmar government to establish a Data Protection Law that protects data and human rights.[190]

9. *Brunei*

At present, Brunei has no general data protection laws in effect. Nonetheless, the Authority for Info-communications Technology Industry of Brunei Darussalam serves as the Data Office which is currently developing a new Personal Data Protection law in Brunei Darussalam.[191] The upcoming legislation aims to govern the collection, use and disclosure of personal data by private organizations, in a way that recognizes the obligations of private sector organizations in the collection, use and disclose of personal data, as well as the right of individuals to protect their personal data.[192]

The above analysis of the similarities between GDPR and the data protection laws of SEA countries displays the EU's role in dictating model contractual clauses and best practices that seep into the data protection practices of SEA countries as well.[193] The EU is ASEAN's second largest trading partner

---

[188] *Id.*

[189] The Pyidaungsu Hluttaw Law No. 5 (2017). The Law for Protection of Personal Privacy and Personal Security of Citizens, *available at* https://www.mlis.gov.mm/mLsView.do;jsessionid=E5E1CFF9699C13D-185BF078893C38D54?lawordSn=1023.

[190] *Policy Brief: A Data Protection Law the Protects Privacy: Issues for Myanmar*, MYANMAR CENTRE FOR RESPONSIBLE BUSINESS, *available at* https://www.myanmar-responsiblebusiness.org/pdf/2019-Policy-Brief-Data-Protection_en.pdf.

[191] *Personal Data Protection*, AUTHORITY FOR INFO-COMMUNICATIONS TECHNOLOGY INDUSTRY OF BRUNEI DARUSSALAM, *available at* https://www.aiti.gov.bn/regulatory/pdp/.

[192] *Id.*

[193] Kunhambu, *supra* note at 138.

and the largest provider of Foreign Direct Investments.[194] More importantly, estimated seven million EU citizens that travel to ASEAN countries each year.[195] This means that many organizations within the ASEAN would be required to be compliant with the GDPR.

C. Existing Regulations for Fintech Companies in the Philippines

The dawn of the fintech industry in the Philippines was slow but inevitable, and it did not eventually shine its light upon lawless land. Throughout the years preceding fintech's emergence, there were already laws in place that govern entities involving data and finance.

R.A. No. 9160 or the Anti-Money Laundering Act of 2001 was made to implement the state policy to "protect and preserve the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity".[196] This piece of legislation applies to covered persons as defined by Section X802 of the Manual of Regulations for Banks (MORB) as amended by Section 1 of BSP Circular No. 950,[197] *viz*:

> **Section X802/4802Q.** *Scope of Regulations.* These regulations shall apply to all covered persons supervised and regulated by the Bangko Sentral. The term "covered persons" shall refer to banks, non-banks, QBs, trust entities, non-stock savings and loan associations, pawnshops, foreign exchange dealers, money changers, remittance and transfer companies, electronic money issuers and other financial institutions which under special laws are subject to Bangko Sentral supervision and/or

---

[194] *Data and privacy protection in ASEAN: What does it mean for businesses in the region*?, DELOITTE, 2018, *available at* https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf.

[195] *EU-ASEAN Relations*, EUROPEAN UNION EXTERNAL ACTION, Jan. 30, 2024*, available at* https://www.eeas. europa.eu/eeas/eu-asean-relations_en.

[196] Rep. Act No. 9160 (2001), § 2. Anti-Money Laundering Act of 2001.

[197] BSP Circ. No. 950 (2017), § 1. Amendments to Part Eight or the Anti-Money Laundering Regulations of the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions.

> regulation, including their subsidiaries and affiliates, which are also covered persons, wherever they may be located.[198]

By analogy, fintech companies may be considered as covered persons since their activities are akin to the enumerated entities above. However, a direct application of the Act may prove to be difficult because of how technology has transformed how financial services are delivered.[199]

Another law that affects the fintech industry is R.A. No. 10173 or the Data Privacy Act of 2012. This Act covers anyone who "collect[s], hold[s], process[es] or use[s] personal information,"[200] such as fintech companies which collect personal sensitive information for its operations.[201] The Act requires fintech companies to uphold the data privacy rights of their clients and to adhere to the general principles of data privacy. A very important aspect of the Act is the necessity of consent for personal[202] or sensitive personal information[203] to be processed by a data controller. The data subject[204] must give his or her consent, specific to the purpose prior to the processing, or in the case of privileged information,[205] all parties to the exchange have given their consent prior to processing. Consent must also be evidenced by written electronic or recorded

---

[198] *Id.*

[199] Emerson Bañez, *Fintech Regulations,* PIDS*, available at* https://pidswebs.pids.gov.ph/CDN/EVENTS/001_disini_regulation_of_fintech.pdf.

[200] Rep. Act No. 10173 (2012), § 3 (h). Data Privacy Act of 2012. *Note that* a personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.

[201] Bañez, *supra* note 199, at 23.

[202] Rep. Act No. 10173 (2012), § 3 (g). *Note that* personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

[203] Rep. Act No. 10173 (2012), § 3 (l). *Note that* sensitive personal information refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.

[204] Rep. Act No. 10173 (2012), § 3 (c). *Note that* data subject refers to an individual whose personal information is processed.

[205] Rep. Act No. 10173 (2012), § 3 (k). *Note that* privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

means.[206] Furthermore, the law does not accept implied consent of the data subject.[207] In an effort to comply with the higher standards and obligations set by the GDPR, the Act is now supplemented by rules and regulations mirroring GDPR policies.[208]

A few years later, R.A. No. 10667 or the Philippine Competition Act was passed. This Act seeks to safeguard competitive conditions to enhance the efficiency of market competition.[209] Under the said Act, the Philippine Competition Commission is given the power to review matters related to mergers and acquisitions, including those in the fintech industry.[210]

A more recent legislation is R.A. No. 11055 or the Philippine Identification System Act, which creates a central identification platform for all citizens and resident aliens in the Philippines.[211] This Act mandates the creation of the PhilSys Registry, which is the repository of all data,[212] including the PhilSys Number (PSN), a randomly generated, unique, and permanent identification number that will be assigned to every citizen.[213] Then, the PhilID, which is the physical medium issued to convey essential information of a person such as the PSN, full name, sex, blood type, marital status, place of birth, photo, date of birth and address, will be issued.[214] As fintech companies rely on personal information and are covered by the Know Your Customer (KYC) Policy of the BSP, the PhilID will be sufficient proof of identity to open bank accounts and avail financial services.[215] Refusal to accept the PhilID may result in a monetary fine, if such refusal was without just and sufficient cause.[216] The law also penalizes the

---

[206] Rep. Act No. 10173 (2012), § 3 (b). *Note that* consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

[207] Bañez, *supra* note 199, at 24.

[208] Tan & Azman, *supra* note at 141.

[209] Rep. Act No. 10667 (2015), § 2. Philippine Competition Act.

[210] Bañez, *supra* note 199, at 25.

[211] Rep. Act No. 11055 (2018), § 2. Philippine Identification System Act.

[212] Rep. Act No. 11055 (2018), § 7 (b).

[213] Rep. Act No. 11055 (2018), § 7 (a).

[214] Rep. Act No. 11055 (2018), § 7 (c).

[215] Bañez, *supra* note 199, at 33. *See also* Rep. Act No. 11055 (2018), § 12, ¶ 1 *and* Rep. Act No. 11055 (2018), § 13 (j).

[216] Rep. Act No. 11055 (2018), § 19, ¶ 1.

unauthorized and willful use or disclosure of the data.[217]The implementation of this system may result in an increase of clients for Fintech companies.[218]

Finally, R.A. No. 11934 or the Subscriber Identification Module (SIM) Registration Act (SRA) requires the registration of all SIMs.[219] Unregistered SIM cards will be deactivated, potentially affecting 20 percent of mobile phone users' access to digital payments, electronic transactions, and one-time-pin authorizations.[220] Experts foresee a "boost in e-commerce and fintech adoption and growth in the sense that the process of SIM registration already hurdles the know-your-customer step required when signing up for fintech apps […] and other digital services. The mobile number is now associated with a subscriber."[221] The Act is also seen lessening the proliferation of fraudulent spam messages, as well as boost telecom security efforts.[222]

In addition to Congress, other government bodies and regulatory agencies have issued rules and regulations that directly impact the fintech industry.

D. Regulatory Bodies of the Fintech Industry in the Philippines

1. Bangko Sentral ng Pilipinas

While already existing in the country as early as the 2000s, the actual and material consumption of fintech products occurred during the COVID-19 pandemic, which has expedited the digital transformation of the Philippine economy. Specifically, it gave rise to the expansion of the fintech sector, including the following: digital banking; money service businesses (Electronic Money Issuers (EMIs); Remittance Agents (RAs); Money Changers (MCs)/Foreign Exchange Dealers (FXDs); Virtual Asset Service Providers (VASPs)); Merchant Acquirers and Operators of Payment Systems (OPS); online

---

[217] Rep. Act No. 11055 (2018), § 19, ¶ 5.

[218] Bañez, *supra* note 199, at 33.

[219] Rep. Act No. 11934 (2022), § 4. SIM Registration Act.

[220] *SIM Registration Urged as 20% Risk Losing Access Digital Payments*, FINTECH NEWS PHIL., May 2, 2023, *available at* https://fintechnews.ph/58095/digital-payments/sim-registration-urged-as-20-risk-losing-digital-payments/.

[221] Richmond Mercurio*, SIM registration to boost e-commerce, fintech services*, THE PHILIPPINE STAR, December 15, 2021, *available at* https://www.philstar.com/business/2021/12/15/2147978/sim-registration-boost-e-commerce-fintech-services.

[222] *Id.*

lending platforms (OLP); online trading apps, and other emerging technologies.[223]

According to the General Banking Law, the BSP shall have supervision and exercise regulatory powers over the operations of other financial institutions which under special laws are subject to BSP supervision,[224] as well as other classifications of banks as determined by the Monetary Board of the BSP.[225]

The adherence with the requirement under the R.A. No. 11127 or the National Payment Systems Act and BSP Circular No. 1049 to register with the BSP is exceptionally crucial for fintech companies, specifically those operating a payment system.[226] The said Circular provides for the rules and regulations on the registration of these firms which, in turn, allows the BSP to have oversight of the payment system these mainly online companies operate to ensure that they function safely, efficiently, and reliably, consistent with the central bank's objectives of consumer protection and financial stability.[227] Non-compliance thereto may cause the stopping of operations by BSP. [228]

The BSP has also actively issued regulations crafted to enhance capitalization, governance, and risk management for financial institutions, such as BSP Circular 1137 (Amended Outsourcing and IT Risk Management Regulations), BSP Circular No. 1154 (Prudential Requirements for Digital Banks), BSP Circular No. 1160 (Guidelines on Financial Products and Services Consumer Protection Act), and BSP Circular No. 1166 (Amendments to E-Money and EMI Regulations).[229]

In addition to digital banks and EMIs which were subjected to a BSP moratorium in 2021, the BSP also abruptly introduced another moratorium for new VASP licenses – with the exception for those already existing BSP-

---

[223] *Supra* note at 90.

[224] Rep. Act No. 8791 (2000), § 4. The General Banking Law of 2000.

[225] Rep. Act No. 8791 (2000), § 3.2 (a).

[226] Ralf Rivas, *Bangko Sentral orders Lyka to halt operations*, RAPPLER.COM, July 23, 2021, *available at* https://www.
rappler.com/business/bangko-sentral-orders-lyka-stop-operations-july-2021/.

[227] Frequently Asked Questions (FAQs) on Registration of Operators of Payment Systems, BSP, *available at* https://www.bsp.gov.ph/PaymentAndSettlement/FAQ_OPS_Registration.pdf.

[228] Rivas, *supra* note at 226.

[229] *Supra* note at 90.

Supervised Financial Institutions (BSFIs).[230] The moratorium on digital banks was imposed by the BSP to preserve the level of competition and maintain quality of service among the players, as well as effective regulation of digital banks.[231] On the other hand, the purpose of the EMI moratorium is to allow the BSP to monitor the EMI sector and to prevent the misuse of e-money licenses.[232]

2. Securities and Exchange Commission

In 2021, the Securities and Exchange Commission (SEC) officially launched its PhiliFintech Innovation Office (PIO), with the primary task of regulating the use of fintech in the country.[233] This will be executed through the registration of new players while also establishing first contact with existing fintech companies[234] which have been operating without proper regulation or authorization, or which will introduce new fintech products.[235] The PIO shall "document, analyze, and understand fintech business models and their possible impacts on the market and its participants."[236] Through this, the SEC will be able to effectively protect investors and market participants, while concurrently promote the growth of fintech firms, by formulating and executing regulatory response.[237] The launch aligns with the objective of the SEC to "keep itself adept with the ever-changing developments in the Fintech landscape to determine how it intersects with the jurisdiction of the SEC."[238]

In addition, the SEC has implemented numerous regulations to oversee the fintech sector over the years. In 2019, the SEC issued rules and regulations on Crowdfunding "in recognition of recent financial innovation of raising funds for a venture or business using internet platforms."[239] Moreover, online lending platforms (OLPs) are still subject to a moratorium imposed by the SEC in

---

[230] *Id.*

[231] *Id.*

[232] *Id.*

[233] *Philippine Securities Regulating Agency Launches Fintech Innovation Office*, DISINI LAW, *available at* https://disini.ph/-news/%E2%80%8B%E2%80%8Bphilippine-securities-regulating-agency-launches-fintech-innovation-office/.

[234] *Id.*

[235] *SEC launches new office for fintech innovation*, PNA, July 30, 2021, *available at* https://www.pna.gov.ph/articles/11-48884.

[236] *Id.*

[237] *Id.*

[238] *Introduction to the PhiliFintech Innovation Office*, SEC, *available at* https://www.sec.gov.ph/-philifintech/#gsc.tab-=0.

[239] *Id.*

2021.[240] Lastly, the SEC endeavors to create the Rules on Initial Coin Offering or Digital Assets Offering and Digital Assets Exchange Rules, which are currently being reviewed and revised based on the comments received from several Fintech proponents and the public.[241]

3. Anti-Money Laundering Council

In 2001, Congress created the Anti-Money Laundering Council (AMLC), the Philippines' Financial Intelligence Unit (FIU) tasked to implement the Anti-Money Laundering Act.[242] In our jurisdiction, fintech companies are subject to AML regulations, and part of their obligations under the law include customer identification and screening, transaction monitoring, and reporting of suspicious activities.[243] These regulations ensure that fintech companies are collecting and managing user information securely and performing all necessary checks to stay compliant.[244]

To further strengthen its cause, the AMLC has signed the Information Sharing Protocol (ISP) with the Fintech Alliance.PH, the leading and largest digital trade organization comprised of startups and unicorns collectively generating over 90% of digital-initiated transactions volume in the Philippines,[245] with the goal of fighting against money laundering and terrorism financing in the country.[246] Both parties will be collaborating in the areas of information exchange, and capacity building to enhance each other's abilities to address money laundering, terrorism, and terrorism financing concerns. It also "institutionalizes an effective documentation mechanism that performs targeted suspicious transaction monitoring and reporting and develops valuable or breakthrough investigative leads."[247]

---

[240] *Supra* note at 90.

[241] *Id.*

[242] *Fintech Alliance.PH Inks Agreement With the Anti Money Laundering Council*, Fintech News Philippines, Nov. 15, 2021, available at https://fintechnews.ph/54689/fintech/fintech-alliance-ph-inks-agreement-with-the-anti-money-laundering-council/.

[243] Rep. Act. No. 9160 (2001), § 9.

[244] *AML Compliance in Philippines: Key Regulations Your Fintech Must Know*, Feb. 13, 2023, *available at* https://www.tookitaki.com/compliance-hub/fintech-compliance-philippines-aml-regulations-company-know.

[245] *Who We Are*, FINTECH ALLIANCE.PH, *available at* https://fintechalliance.ph/about-us/.

[246] *Fintech Alliance.PH Inks Agreement With the Anti Money Laundering Council*, FINTECH NEWS PHILIPPINES, Nov. 15, 2021, *available at* https://fintechnews.ph/54689/fintech/fintech-alliance-ph-inks-agreement-with-the-anti-money-laundering-council/.

[247] *Id.*

4. Department Of Information and Communications Technology

The Department of Information and Communications Technology (DICT) is the primary policy, planning, coordinating, implementing, and administrative entity of the executive branch of the government.[248] It is tasked to plan, develop, and promote the national Information and Communications Technology development agenda.[249] The DICT is assigned the crucial role of selecting and adopting technology standards for the government, thus it was given the power to create guidelines on partnerships between public and private entities, allowing the DICT to control relations between fintech companies and the government in the integration of fintech services.[250] The choices and actions of DICT affect public procurement and can mold the fintech market through public endorsement and network effects that will be made available to those that comply with the adopted standards.[251] As a result, this can influence what standard will be imposed upon other players whether they choose to operate in the private sector or deal with the government instead.[252]

In 2020, DICT partnered with various government agencies and private entities in holding the first Philippine Fintech Festival, which gathered global innovation and tech experts, thought leaders, and business executives around the world to discuss the future of banking, industry transformation, and financial inclusion.[253]

5. National Privacy Commission

The National Privacy Commission (NPC) is labelled as the "country's privacy watchdog."[254] It is an independent body mandated to administer and implement the Data Privacy Act of 2012 and to monitor and ensure compliance of the country with international standards set for data protection.[255] Part of the NPC's mission is to ""[e]stablish a regulatory environment that ensures accountability in the processing of personal data and promotes global standards

---

[248] *Mandate, Powers and Functions*, DICT, *available at* https://dict.gov.ph/about-us/our-mandate/.

[249] *Id.*

[250] Bañez, *supra* note 199, at 31.

[251] *Id.* at 30.

[252] *Id.* at 31.

[253] *1ST PH fintech festival set in May 2020*, DICT, Feb. 12, 2020, *available at* https://dict.gov.ph/1ST-PH-FINTECH-FESTIVAL-SET-IN-MAY-2020/.

[254] *About us*, NPC, available at https://privacy.gov.ph/about-us/#mv.

[255] *Id.*

for data privacy and protection"[256] and "[b]uild a culture of privacy, through people empowerment, that enables and upholds the right to privacy and supports free flow of information."[257]

In the previous years, the NPC has been active in targeting organizations which are obliged to apply the highest level of responsibility in protecting the data of its users. In several instances, the agency launched an investigation into "whether telcos exercised due diligence and accountability in transacting with data aggregators linked to the sending of texts offering spurious jobs and investment schemes to millions of Filipinos."[258] It also sent orders to the certain payment channels where victims are directed to deposit their investments, as the accounts in these payment channels were the victims were defrauded to deposit were later rendered inaccessible.[259]

With the number of text spams and phishing incidents still on the rise, the NPC has encouraged telcos to "continue blocking these data aggregators, as well as the numbers, domains and internet protocol addresses that enable the smishing and text spams."[260] Upon NPC's instructions, various companies have strengthened their awareness campaigns and telco players have committed to cooperate fully with the NPC to reinforce the government's fight against data security breaches.[261]

V. CONSTITUTIONAL CHALLENGES IN THE PHILIPPINE FINTECH INDUSTRY

A. The Right to Privacy

The right to privacy is a fundamental right,[262] but interestingly, this right is not expressly written in the 1987 Constitution. However, the recognition of

---

[256] *Id.*

[257] *Id.*

[258] *NPC probes telcos, bank and payment platform on smishing; inter-agency body formed to go after scammers, NPC*, Dec. 1, 2021, available at https://privacy.gov.ph/npc-probes-telcos-bank-and-payment-platform-on-smishing-inter-agency-body-formed-to-go-after-scammers/.

[259] *Id.*

[260] *Id.*

[261] *Id.*

[262] Sanchez v. Darroca, G.R. No. 242257 (Resolution), June 15, 2021.

the right to privacy is embedded in our legal system.[263] In fact, the Supreme Court oftentimes quotes Justice Brandeis[264] in describing the right to privacy as "the most comprehensive of rights and the right most valued by civilized men."[265]

The case of *Morfe v. Mutuc*[266] recognized that the right to privacy is entrenched in the Constitution's due process clause, stating that "the concept of liberty would be emasculated if it does not likewise compel respect for his personality as a unique individual whose claim to privacy and interference demands respect." [267] No less than the supreme law of the land provides the explicit limitations on unwarranted State intrusion into personal affairs[268] through the Bill of Rights, particularly the provisions that guarantees every person's right to due process,[269] to be secure against unreasonable searches and seizures,[270] and to the privacy of their communication and correspondence.[271]

The idea of privacy has undergone significant changes over time, largely influenced by advancements in technology.[272] In his speech entitled *The Common Right to Privacy*,[273] former Chief Justice Reynato S. Puno explained the three strands of the right to privacy, which are: (1) locational or situational privacy; (2) informational privacy; and (3) decisional privacy.[274]

In ascertaining whether there is a violation of the right to privacy, courts use the "reasonable expectation of privacy" test.[275] This is a two-part test which determines: (1) whether a person has a reasonable expectation of privacy; and (2)

---

[263] Phil. Stock Exchange, Inc. v. Sec. of Finance, G.R. No. 213860, July 5, 2022.

[264] *See* Olmstead v. United States, 277 U.S. 438, 478 (1928). *Note that* in this case, Justice Brandeis, along with Justice Holmes, dissented.

[265] Morfe v. Mutuc, G.R. No. L-20387, Jan. 31, 1968.

[266] *Id.*

[267] *Id.*

[268] Phil. Stock Exchange, Inc. v. Sec. of Finance, G.R. No. 213860, July 5, 2022.

[269] CONST. art. III, § 1.

[270] CONST. art. III, § 2.

[271] CONST. art. III, § 3 (1).

[272] Vivares v. St. Theresa's College, G.R. No. 202666, 744 PHIL 451-480, Sept. 29, 2014.

[273] Delivered before the Forum on The Writ of *Habeas Data* and Human Rights, sponsored by the National Union of Peoples' Lawyers on March 12, 2008 at the Innotech Seminar Hall, Commonwealth Ave., Quezon City, *available at* http://sc.judiciary.gov.ph/speech/03-12-08-speech.pdf.

[274] Locational privacy refers to the privacy that is felt in physical space, such as that which may be violated by trespass and unwarranted search and seizure. Informational privacy is usually defined as the right of individuals to control information about themselves. Decisional privacy is usually defined as the right of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy, *see* Vivares v. St. Theresa's College, G.R. No. 202666, Sept. 29, 2014.

[275] Sps. Hing v. Choachuy, Sr., G.R. No. 179736, June 26, 2013, *citing* Ople v. Torres, G.R. No. 127685, July 23, 1998.

whether the expectation has been violated.[276] Hence, the reasonableness of a person's expectation of privacy must be determined on a case-to-case basis since it depends on the factual circumstances surrounding the case.[277] A concrete example of what does not constitute a violation of the right to data privacy is illustrated in *Kilusang Mayo Uno v. Director-General*,[278]where therein respondents assailed Executive Order No. 420 for infringing the citizens' right to privacy due to the collection and recording of personal identification data for a unified ID system. There, the Supreme Court elucidated that the right to privacy does not bar the adoption of reasonable ID systems by government entities.[279]

In the age of digital finance, what requires specific attention is the right to informational privacy, which is defined as "the right of individuals to control information about themselves."[280]

B. The Right Against Unreasonable Searches and Seizures

Unlike the right to privacy, the protection and guarantee of the people's fundamental right against unreasonable searches and seizures is expressly stated under Article III, Section 2 of the 1987 Constitution,[281] *viz*:

> **SECTION 2**. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he [or she] may produce, and particularly describing the place to be searched and the persons or things to be seized.

---

[276] *Id.*
[277] *Id.*
[278] G.R. No. 16779, Apr. 19, 2006.
[279] Kilusang Mayo Uno v. Director-General, G.R. No. 16779, Apr. 19, 2006.
[280] Vivares v. St. Theresa's College, G.R. No. 202666, Sept. 29, 2014.
[281] Abiang y Cabonce v. People, G.R. No. 265117, Nov. 13, 2023.

As explained by the Supreme Court in *People v. Gabiosa, Sr.,*[282] Article III, Section 2 is one of the provisions in the Bill of Rights preserving the citizens' right to privacy, as it protects every citizen's right against unreasonable searches and seizures.[283] In essence, it preserves the right of the people "to be let alone" vis-à-vis the far-reaching and encompassing powers of the State and ensures protection of the individual from arbitrary searches and arrests initiated and perpetrated by the State.[284] Consequently, any evidence obtained in violation of this rule shall be inadmissible for any purpose in any proceeding.[285]

C. Recent Cases in the Fintech Industry in Southeast Asia

1. Cases Involving the Right to Privacy

Several studies concur that major data breaches in SEA countries evidence the region's weaknesses in the areas of cybersecurity and data protection.[286] According to the Allianz Risk Barometer 2020,[287] cyber incidents – including data breaches – rank as the most serious business risk globally for the first time in history.[288] This is a significant occurrence, because just seven years ago, the same threat held a distant 15th position in the top menaces list for companies around the world.[289] In particular, state-sponsored cyberattacks targeting financial institutions are becoming more frequent, sophisticated, and destructive.[290] In 2017, the G20, which is the collection of twenty of the world's largest

---

[282] G.R. No. 248395, Jan. 29, 2020.

[283] People v. Gabiosa, Sr., G.R. No. 248395, Jan. 29, 2020.

[284] *Id.*

[285] CONST. art. III, § 3 (1).

[286] Cristina Lago, *The biggest data breaches in Southeast Asia*, CSO ONLINE, Jan. 18, 2020, *available at* https://www.csoonline.com/article/569109/the-biggest-data-breaches-in-southeast-asia.html.

[287] *Allianz Risk Barometer 2020: Cyber top peril for companies globally for the first time,* ALLIANZ GROUP, Jan. 14, 2020, *available at* https://www.allianz.com/en/press/news/studies/200114_Allianz-risk-barometer-2020.html.

[288] Id.

[289] Lago, *supra* note 286.

[290] *Timeline of Cyber Incidents Involving Financial Institutions*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, *available at* https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

economies,[291] warned that cyberattacks could "undermine the security and confidence and endanger financial stability."[292]

The SEA region is indeed a mirror of the global trend that has witnessed a growing awareness of cyber threats in recent years.[293] Incidents are growing more detrimental, focusing increasingly on major corporations with intricate attacks and substantial extortion demands.[294] Specifically, a typical ransomware demand would have been in the tens of thousands of dollars five years ago, but at present, the amount can reach in the millions.[295]

In 2022, researchers reported on the banking trojan Fakecalls, which has the ability to 'talk' to victims and pretend to be an employee of the bank.[296] Fakecalls mimics the mobile apps of popular Korean-based banks.[297] In addition to its spyware toolkit, the trojan requests permissions to exfiltrate sensitive data such as live audio and video streams to a remote server in order to gain payment data and other confidential information from the victim.[298]

Earlier in the same year, India-based loans app CashMama reported a data breach in which customer data and other sensitive information were invasively collected and stored was exposed.[299] Another incident entails the North Korean threat actor, Lazarus, which has been operating for more than 10 years and is behind infamous cyber incidents such as the attack on Sony Pictures in 2014 and the spread of the WannaCry ransomware in 2017.[300] In contrast to other state actors, Lazarus demonstrates strong financial incentives, striving to bolster the

---

[291] *What Does the G20 Do?*, COUNCIL ON FOREIGN RELATIONS, *available at* https://www.cfr.org/backgrounder/what-does-g20-do. *Note that* the Group of Twenty ("G20") is an informal gathering of many of the world's largest economies, is the premier global forum for discussing economic issues. It meets regularly to coordinate global policy on trade, health, climate, and other issues.

[292] *Id.*

[293] Lago, *supra* note 286.

[294] *Id.*

[295] *Id.*

[296] *Supra* note at 290.

[297] Ravie Lakshmanan, *FakeCalls Vishing Malware Targets South Korean Users via Popular Financial Apps*, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2023, *available at* https://cyberir.mit.edu/?q=fakecalls-vishing-malware-targets-south-korean-users-popular-financial-apps.

[298] *Id.*

[299] Bharat Sharma, *Thousands Of Indians Exposed In Data Breach Affecting Money Lending App CashMama*, INDIA TIMES.COM, Apr. 6, 2022, *available at* https://www.indiatimes.com/technology/news/thousands-of-indians-exposed-in-data-breach-affecting-money-lending-app-cashmama-566211.html.

[300] *The Lazarus group: North Korean scourge for +10 years, Responsible for some of the largest cyberattacks worldwide*, NCC GROUP, June 30, 2022, *available at* https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/.

struggling North Korean economy.[301] Because of government support and instigation, the actors behind Lazarus face no risk of prosecution in their home country.[302]

In 2021, around 790 banking customers of Singaporean bank OCBC were targeted in a phishing scam resulting in a loss of at least SGD 13.7 million.[303] Once victims clicked on the link provided and typed in their credentials, attackers were able to gain access to victim's bank accounts and drain it of its entire funds.[304] Meanwhile, Taiwan's financial sector was hit by a months-long cyber espionage campaign attributed to Chinese state-sponsored group APT 10.[305] The attackers executed malicious codes on local systems and installed a virus, enabling them to sustain continuous remote access to the infected system.[306]

In the Philippines, GCash, the country's leading fintech corporation,[307] has also led the numerous data privacy breaches of its customers. In 2023, phishing attacks led to unauthorized transactions involving several GCash accounts.[308] According to the NPC, some of the attacks were perpetuated through online gambling websites[309] as a result of a meticulous phishing scheme.[310] A more recurring issue concerning the e-wallet firm is the sudden losing of cash by the customers from their respective GCash accounts.[311] Complainants averred that they were not alerted by text messages containing

---

[301] *Id.*

[302] *Id.*

[303] Vanessa Chelvan, *OCBC says S$13.7 million lost in phishing scams, up from S$8.5 million*, CHANNEL NEWS ASIA, Jan 30, 2022, *available at* https://www.channelnewsasia.com/singapore/ocbc-phishing-scam-more-losses-victims-repor-ted-2469086.

[304] *Id.*

[305] Betty Hou & Jamie Tarabay, *Taiwan Calls on US Support to Defend Banks Against Hacking*, BLOOMBERG, Dec. 12, 2023, *available at* https://www.bloomberg.com/news/articles/2023-12-11/taiwan-calls-on-us-support-to-defend-ba-nks-against-cyberattacks.

[306] *Id.*

[307] *GCash is top fintech brand in Philippines' Top 100 Brands 2021*, BUSINESS WORLD ONLINE, Sep. 6, 2021, *available at* https://www.bworldonline.com/spotlight/2021/09/06/393871/gcash-is-top-fintech-brand-in-philippines-top-100-brands-2021/.

[308] Raymond Dela Cruz, *NPC confirms GCash incident caused by phishing attacks*, PHIL. NEWS AGENCY, May 24, 2023, *available at* https://www.pna.gov.ph/articles/1202151.

[309] *Id. Note that* in a statement, Privacy Commissioner John Henry Naga said "unknown threat actors" took advantage of GCash users through online gambling websites such as "Philwin" and "tapwin1.com."

[310] *Id.*

[311] Sundy Locus, *30 complain of losing cash from GCash accounts, e-wallet firm coordinating with authorities*, GMA NETWORK, Mar. 9, 2023, *available at* https://www.gmanetwork.com/news/topstories/metro/863255/30-complain-of-losing-cash-from-gcash-accounts-e-wallet-firm-coordinating-with-authorities/story/.

one-time passwords—a requirement before cash transfers through the e-wallet could be made.[312]

There are also incidents of selling verified GCash e-Wallet accounts inside a supermarket.[313] Authorities confirmed that GCash accounts were sold to victims for use in online casinos and Philippine offshore gaming operators (POGOs) operated by Taiwanese and Chinese nationals.[314]

Another Fintech corporation that caused waves in the industry is Lyka, a popular app in the Philippines owned by a Hong Kong-based company that "allowed people to earn Lyka GEMs or gift cards in electronic mode for posting, sharing, and liking content."[315] In turn, these GEMs could may be utilized to purchase goods.[316] The app's fame is attributed to celebrities, models and social media "influencers" who regularly post glamor shots of them enjoying the services of resorts and upscale restaurants and paying for these services with Lyka GEMs, which have an exchange rate of PHP 1 per GEM. [317] However, the BSP ordered the popular social media-based platform to cease its services in the Philippines for being an unregistered payment system operator.[318] A non-government organization composed of computer professionals[319] earlier warned the public about the potential dangers of using Lyka, citing security and privacy risks,[320] which may lead to members finding their personal data sold to other companies, based on the language of Lyka's opt-in agreement.[321]

Despite the rampant security breaches that involve fintech corporations, there were no cases elevated to the Supreme Court to date. However, Philippine

---

[312] *Id.*

[313] *Online seller of verified Gcash accounts arrested anew for cybercrime cases*, PNP, July 5, 2022, *available at* https://acg.pnp.gov.ph/main/press-releases/460-online-seller-of-verified-gcash-accounts-arrested-anew-for-cybercrime-cases.html.

[314] Mark Villeza, *NBI nabs 4 suspects in GCash scam*, PHILSTAR.COM, Mar. 28, 2023*, available at* https://www.philstar.com/nation/2023/03/28/2254986/nbi-nabs-4-suspects-gcash-scam.

[315] Rivas, *supra* note at 226.

[316] *Id.*

[317] Daxim Lucas, *Unregistered, celebrity-backed 'Lyka' told to cease operations by BSP*, INQUIRER.NET, July 23, 2021, *available at* https://business.inquirer.net/327693/unregistered-celebrity-backed-lyka-told-to-cease-operations-by-bsp.

[318] *Id.*

[319] *Who We Are*, CP-UNION.COM*, available at* https://cp-union.com/.

[320] Victor Barreiro Jr., *Computer Professionals' Union warns against using Lyka app*, RAPPLER.COM, Feb. 17, 2021, *available at* https://www.rappler.com/technology/apps/computer-professionals-union-warns-against-lyka-app/.

[321] Lucas, *supra* note 317.

courts are no strangers to cases involving violations of the right to data privacy involving other types of entities. In the case of *Abines v. Duque III*,[322] which involves a petition filed by 74 children, represented by their parents, against government officials involved in the Dengvaxia vaccination program in the Philippines, there was a prayer to release the master list of the children inoculated with the vaccines.[323] However, the Supreme Court held that doing so runs afoul of prevailing data privacy laws. as the disclosure of information concerning these individuals is proscribed absent proof of consent from the minor data subject. Such an act could constitute an unwarranted invasion of personal privacy. The Court emphasized that reasonable and appropriate security measures must be in place for the protection of personal data of Filipinos, who should be able to trust that their information will be protected and used only for the purpose by which they are collected.[324]

In *Re: Disturbing Social Media Posts of Lawyers/Law Professors*,[325] the Supreme Court ruled that "at best, the right to privacy has limited application to online activities of lawyers." Citing *Belo-Henares v. Atty. Guevarra*,[326] it was explained that there is no assurance that posts on Facebook, or any social media platform for that matter, can be placed within the confines of privacy due to the nature of social media itself, which is to promote openness and connection to other people, even those outside your "friends," through several tools to interact and share in any conceivable way.[327]

2. Cases Involving the Right against Unreasonable Searches and Seizures

In the cases discussed in the preceding section, it is common that the fintech corporation involved cooperates with government agencies regulating its practices. However, there is a fine line between surrendering information in compliance with rules and regulation and subjecting the customer's data to unreasonable search and seizure.

---

[322] Abines v. Duque III, G.R. No. 235891, Sept. 20, 2022.

[323] *Id.*

[324] *Id.*

[325] Re: Disturbing Social Media Posts of Lawyers/Law Professors, A.M. No. 21-06-20-SC, Apr. 11, 2023.

[326] Belo-Henares v. Guevarra, 801 PHIL 570-589, A.C. No. 11394, Dec. 1, 2016.

[327] Re: Disturbing Social Media Posts of Lawyers/Law Professors, A.M. No. 21-06-20-SC, Apr. 11, 2023., *citing* Belo-Henares v. Guevarra, 801 PHIL 570-589, A.C. No. 11394, Dec. 1, 2016.

In the occasions where there are data privacy breaches, the NPC has held clarificatory meetings with Gcash, where the former raised its concerns, and the latter provided additional information and proof for the conduct of an independent assessment.[328] In the midst of the anomalous fund transfers in 2021, GCash examined the logs of the actions of the fraudster and discovered that a link was sent out to several users.[329] According to the investigation, those who clicked on it would receive a request to link a device.[330] From thereon, the fraudster will be able to phish information from customers and all the user's activities will then be visible to the fraudster.[331] Government agencies, including the NPC and the BSP, have since initiated their own investigation into the incidents while simultaneously seeking data from the affected fintech giant.[332]

In instances filed with the Philippine National Police Anti-Cybercrime Group (PNP-ACG), GCash said it coordinated with the authorities to track down the activities of the scammer. [333] In addition, agents of the National Bureau of Investigation (NBI) arrested suspects allegedly engaged in a GCash scam during separate operations, again through the help of GCash.[334]

As a result of these operations, suspects were arrested and held in custody. In majority of the cases, the alleged perpetrators were charged with violations R.A. No. 8484 or Access Devices Regulation Act of 1998 and R.A. No. 10175 or the Cybercrime Prevention Act of 2012.[335]

The collaboration between fintech companies and governmental entities can indeed offer advantages in detecting and addressing law violations effectively. However, this cooperative effort also presents a significant concern regarding the potential infringement upon the privacy rights of ordinary users. In the process of aiding investigations, fintechs may be required to disclose user data to government authorities. This transfer of personal and sensitive information raises the risk of subjecting individuals to unwarranted intrusions into their privacy. There exists a possibility that such disclosures could result in

---

328 Dela Cruz, *supra* note 308.

329 Lance Yu, *Fraudster behind anomalous GCash fund transfers, says exec*, RAPPLER.COM, May 10, 2023, *available at* https://www.rappler.com/business/fraudster-behind-anomalous-gcash-fund-transfers/.

330 *Id.*

331 *Id.*

332 *Id.*

333 Locus, *supra* note 311.

334 Villeza, *supra* note 314.

335 Locus, *supra* note 311.

arbitrary searches and seizures of sensitive personal data without adequate safeguards in place.

Under these circumstances, individuals may find themselves exposed to undue scrutiny and privacy violations, with their personal data vulnerable to misuse or exploitation by governmental agencies. This now raises concerns about the protection of civil liberties. Without robust safeguards in place to ensure that access to user data is necessary and subject to appropriate oversight, there is a risk of abuse of power and infringement upon individuals' rights.

VI. THE FUTURE OF THE FINTECH INDUSTRY IN SOUTHEAST ASIA

The fintech industry in SEA is fiercely competitive and seems to have reached a point of market saturation.[336] Numerous new and established e-wallet providers struggle to attract fresh users, as dominant digital wallet platforms in each SEA nation have already captured significant market shares.[337] This has led to the presence of around 800 redundant e-wallets across the SEA region.[338]

Given the recent increase in travel resulting from the relaxation of border restrictions, digital payment firms must extend their focus beyond domestic boundaries. Numerous SEA countries have been launching standardized QR codes for bilateral cross-border payments, such Indonesia and Thailand, Singapore and Thailand, and Singapore and Indonesia.[339] SEA governments are also investing in the region's cross-border payment infrastructure, which digital payment providers can leverage for regionalization.[340] In relation to this, ShopeePay recently announced a partnership with 2C2P to enable ShopeePay as a payment option for 2C2P's extensive merchant network across Malaysia, Indonesia, Singapore, Thailand, and the Philippines.[341]

The future of fintech innovations remains uncertain, particularly exacerbated by the chaos caused by the pandemic. Fintech companies, along with their clientele, have suffered financial setbacks; some have resorted to

---

[336] Deloitte Southeast Asia Innovation Team, *supra* note at 60.
[337] *Id.*
[338] *Id*
[339] *Id.*
[340] *Id.*
[341] *Id.*

downsizing or placing staff on furlough, while others grapple with challenges in securing investor funding.[342] Nevertheless, the demand for fintech solutions may be at an all-time high, as businesses and banking consumers increasingly turn to technology to manage their financial affairs.[343]

However, in spite of the prevailing economic unpredictability, the broader and enduring trends shaping the future of fintech appear relatively intact.[344] Consolidation, partnerships and continued collaborations between legacy banks and fintechs appear imminent in the future.[345] Furthermore, consumers are likely to witness the sustained rise of companies promoting innovative services, such as blockchain, cryptocurrency, artificial intelligence, and peer-to-peer transactions, which grab attention with their cutting-edge offerings.[346]

Fintech has become extensively integrated into everyday services to the point of being ubiquitous. Consumers, businesses, and various financial institutions are increasingly leveraging innovative combinations of software, hardware, and data to innovate and provide both novel and traditional financial offerings.[347] Fintech has become deeply intertwined with the framework of our society, and its impact is poised to expand even further in the times ahead.[348]

VII. RECOMMENDATIONS TO ADDRESS THE DIGITAL DILEMMA

A. Improving laws and regulations to protect the constitutional rights of Filipinos

1. Passage of existing bills protecting consumer rights in digital transactions into law

The dawn of digitalization in the financial industry is not lost in our legislators, as there exists the recognition that the Philippines must eventually catch up to the rising standards not only with regard to the adoption of modern financial management tools, but also the protection of data privacy.

---

342 Walden, *supra* note at 5.
343 *Id.*
344 *Id.*
345 *Id.*
346 *Id.*
347 *Id.*
348 *Id.*

In recent years, several bills were drafted to address the digital dilemma shrouding our financial landscape. One such bill is "seeking to promote the adoption of digital payments for financial transactions of the government and all merchants."[349] The bill, which is already approved by the House Committee on Banks and Financial Intermediaries, is proposed to be called the "Use of Digital Payments Act."[350] As a product of the long and laborious deliberations of the members of the House of Representatives, this bill is already a consolidation of House Bills (HBs) 275, 358, 2946, 3737, 4344, and 5073.[351]

One of the objectives of this bill is to make management more efficient for merchants. Its proponents posit that the use of digital payments systems will lessen the need for manual labor and lower the risk of theft from employees. Moreover, the government will also be highly benefited using the said systems as it will "minimiz[e] both disease transmission and possible opportunities for corruption."[352] The bill mandates all national government agencies, government-owned and controlled corporations, and local government units "to utilize safe and efficient digital payment in the collection of taxes, fees, tolls, imposts and other revenues and in the payment of goods, services and other disbursements. To this end, these government entitles may be allowed to include in their respective budgets amounts that will cover transaction fees that they may shoulder."[353] To accomplish this, the various government entities covered "may engage the services of established digital payment system providers."[354]

Another set of house bills which acquired approval at the committee level is what is proposed to be the "Use of Electronic Money Act of 2022."[355] The

---

[349] *Bills on Digital Payments, Use of Electronic Money, Amendment of FIST Act of 2021 hurdle committee level,* CONGRESS.GOV.PH, Feb. 14, 2023, *available at* https://www.congress.gov.ph/-photojournal/zoom.php?photoid=4481.

[350] Filane Cervantes, *House panel pushes for bill on use of digital payments*, PHIL. NEWS AGENCY, Feb. 15, 2023, *available at* https://www.pna.gov.ph/articles/1195231.

[351] *Id.*

[352] *Id.* Davao City Rep. Paolo Duterte, author of House Bill 3737, said the bill seeks to promote the universal use of safe and efficient digital payments in financial transactions of the government and the general public because "[b]y allowing the digital platform of payment as a pre-requisite for the approval or renewal of their business permits, merchants are now mandated to further digital transactions in their every operation. Meanwhile, the government is also duty-bound to utilize safe and efficient electronic or digital means of receiving payment for taxes, fees, tolls, imposts, and other revenues and for the payment of goods, services, and other disbursements."

[353] H. No. 275, 19th Cong., 1st Sess., § 5, ¶ 1 (2022). Use of Digital Payments Act.

[354] § 5, ¶ 2.

[355] *Supra* note at 349.

said bill is a consolidation of HBs 2224 and 2748.[356] This garnered support from various government agencies, particularly the National Economic and Development Authority, as the bill will "accelerat[e] digital transformation in the government in the practice of good governance and improved bureaucratic efficiency espoused in the Philippine Development Plan 2023-2028."[357] Furthermore, this bill requires all concerned agencies to "establish the necessary security features and guidelines as may be needed to prevent phishing and digital fraud,"[358] and emphasizes that "[t]he right to privacy of the consumer shall be of utmost importance."[359] Another important provision of this bill is the mandatory issuance of paper or electronic invoices or receipts for all sales, which shall have the same legal effect of a physical-invoice or receipt.[360]

In sum, legislators have been taking steps to further modernization in the Philippine society, although it is unknown why none of these have reached passage into law. However, it is important to note that despite the huge potential contained in these proposed bills when it comes to promoting and strengthening the use of fintech in various transactions of the government and the public, they are not the much-needed improvement in our data privacy laws. Still, they would be a huge leap forward in matching the global pace of shifting from physical to digital modes of payments.

2. Amendment of the Data Privacy Act of 2012 to adhere to the GDPR

In general, both the GDPR and the Philippines' Data Privacy Act of 2012 (DPA) establish similar approaches in terms of data subjects' rights, principles of accountability, and obligations relating to data security, breach notifications, and the protection of privacy.[361] Moreover, the DPA provides the NPC with similar responsibilities, as well as corrective and investigative powers, as the data

---

[356] *Id.*

[357] Cervantes, *supra* note at 350. The proposed bills are "aligned with the strategies of promoting a safe and efficient national payments system, part of the consolidated draft of the e-Governance Bill, which is a priority measure of President Ferdinand R. Marcos Jr. included in the common legislative agenda of the Legislative Executive Development Advisory Council."

[358] H. No. 278, 19th Cong., 1st Sess., § 9 (2022). e-Money Act of 2022.

[359] *Id.*

[360] H. No. 278, 19th Cong., 1st Sess., § 10 (2022).

[361] *Comparing privacy laws: GDPR v. Data Privacy Act and IRRs*, ONETRUST DATAGUIDANCE, *available at* https://www.dataguidance.com/sites/default/files/gdpr_v_data_privacy_act_and_irrs_0.pdf.

protection authorities under the GDPR.[362] However, the DPA and the GDPR differ in some respects, as presented in the table below:

	Data Privacy Act of 2012[363]	**GDPR**
Biometric Data	None.	*Art. 4 (14).* 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
Publicly Available Information	*Sec. 4 (e).* The act excludes from scope information necessary in order to carry out the functions of public authority, which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.	*Art. 14 (5) (b).* The processing of publicly available information may be permitted for certain archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, **insofar as providing notice is likely to render impossible or seriously impair the achievement of the objectives of that processing.** xxx
Lawfulness, Fairness and Transparency	*Sec. 11 (b).* Personal data shall be processed fairly and lawfully.	*Art. 5 (1) (a).* Personal data shall be processed lawfully, fairly and in a **transparent** manner in relation to the data subject.

[362] *Id.*

[363] Rep. Act No. 10173 (2012).

Access and Correction	*Sec. 16 (8) (d).* The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal data controller correct it immediately and accordingly unless the request is vexatious or otherwise unreasonable.	*Art. 15 (1).* **The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and to access the personal data and information about the processing**, including what categories of data are processed, the recipients of the data, and rights to erasure and rectification of the personal data, the right to lodge a complaint with a DPA, the source of the data, whether the data was subject to automated profiling.
Transfer of Personal Data to Another Person or country	*Sec. 21 (a).* The controller shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.	*Whereas (101).* When a controller sends data to another party to be processed, they are a processor and therefore must be bound by contract with the controller to protect the personal data. **Personal data may only be transferred to third countries where the EU has considered the laws to provide adequate protection or where protected by binding corporate rules, approved model clauses, binding agreements combined with an approved code of conduct or approved certification.**

Right to Erasure	None.	*Art. 17 (1)*. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based xxx and where there is no other legal ground for the processing; (c) the data subject objects to the processing xxx and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing xxx; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services xxx.

To address the existing challenges in data privacy existing with the use of fintech products, it is recommended that the Philippine government adopt the

terms of the GDPR that are not present in the DPA to strengthen the protection that the State provides to its constituents.

First, Congress should include biometric data in the definition of personal data that is protected by our data privacy laws. Biometrics work by "connecting proof-of-identity to our bodies and patterns of behavior" as an effective authentication solution.[364] Fintechs have long used biometrics as part of their KYC procedure and as a method of logging in to apps. Even the government is utilizing this technology, as the Philippine Statistics Authority (PSA) recently pilot-tested biometric authentication through the PhilSys.[365] The activity enabled identity verification through scanning of the fingerprint through biometric authentication devices for the real-time matching process of information to the PhilSys Registry.[366]

Second, the law must contain a qualifier regarding the non-protection of publicly available information. As stated in the GDPR, exclusion from protection of the law will only occur when "providing notice is likely to render impossible or seriously impair the achievement of the objectives of that processing."[367]

Third, transparency must be imbued in the processing of personal data, on top of lawfulness and fairness. This will provide confidence to the individuals whose data is subject to processing.

Fourth, the law should include the right of the individual to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and to access the personal data and information about the processing. Currently under the DPA, the right to access is limited to the right to dispute the inaccuracy or error in the personal data and have the personal data controller correct it immediately. There is already knowledge by the individual that his/her data is subject to processing. However, in cases of doubt and fear,

---

[364] *Biometrics in the Philippines: Here's Everything You Need to Know*, IOT PHILS., *available at* https://www.iotphils.com/biometrics-philippines/#:~:text=Biometrics%20is%20an%20essential%20way,business%20-environments%20in%20the%20Philippines.

[365] PhilSys Registry Office, *PSA pilots identity verification through biometrics via PhilSys; results show 'close to 100 percent successful'*, PHIL. IDENTIFICATION SYSTEM, Nov. 22, 2023, *available at* https://philsys.gov.ph/psa-pilots-identity-verification-through-biometrics-via-philsys-results-show-close-to-100-percent-successful/.

[366] *Id.*

[367] GDPR (2018), art. 14, ¶ 5 (b).

the individual must have the option to confirm if his/her data is indeed being processed.

Fifth, Congress should consider limiting the transfer of personal data to countries with laws that provide adequate protection to privacy. The Philippines' data protection rules do not categorically prohibit the transfer of personal data to foreign countries, which will make the data transferred vulnerable to attack. If personal data is only allowed to be transferred to countries which passed strong data protection laws, individuals can be rest assured of the safety of their personal data.

Sixth, the government should afford the individuals the right to erasure, or the right to be forgotten. This is one of the major pillars of the GDPR that is missing in existing Philippine laws. The ultimate protection that the State can give a constituent is to allow the erasure of personal data when acquired illegally or used for purposes that the data subject did not consent to. With the right to erasure, the ordinary citizen will be equipped with the power to remove any personal data that he/she does not consent to be distributed at all.

In sum, it is evident that amendments to the DPA are necessary so that policymakers can ensure that the law remains robust and effective in safeguarding the rights of individuals while also promoting innovation and economic growth. Moreover, by staying abreast of international best practices and emerging technological trends, the Philippines can position itself as a leader in data protection and privacy regulation within the ASEAN region and beyond. Ultimately, a forward-thinking approach to amending the DPA will not only enhance trust and confidence in the digital economy but also uphold the fundamental rights of Filipino citizens in an increasingly interconnected world.

B. Striking a Balance between Innovation and Regulation

1. *Equalizing the value of data privacy and law enforcement*

a. Cooperation between government agencies and the private sector

In balancing the value of data privacy and law enforcement, the government must navigate a complex landscape where individual rights intersect

with societal security by collaborating closely with the private sector. Such cooperation is crucial in leveraging the expertise and resources of both parties to develop comprehensive solutions that address the intricacies of the digital scene. Regulatory bodies should engage with fintech companies to establish clear guidelines and standards for data privacy protection while ensuring that law enforcement agencies have access to the necessary tools and information to combat crime and ensure public safety.

An example of this collaboration is a memorandum of agreement (MOA) which the SEC and Gcash signed to join forces in going after perpetrators involved in online fraud, e-scams, and other cybercrimes.[368] Under the agreement, GCash will "assist and cooperate with the SEC in investigating financial fraud crimes by providing relevant information and data in accordance with prevailing laws, rules, and regulations."[369] In particular, the Enforcement and Investor Protection Department (EIPD) of the SEC stated that victims of these cybercrimes commonly use online money transfer services, such as e-wallets, for their transactions.[370] In this regard, the MOA entered into allows efficient cooperation between EIPD and GCash wherein "the EIPD can request vital information from GCash to build better cases in its fight against fraud."[371]

Additionally, the agreement reinforces GCash's dedication to safeguarding its customer' funds and data.[372] Having user security as its utmost priority, the fintech giant wants to grant its users the peace of mind and confidence to transact in the digital space by continuously working with the government in combating scams, fraud, and other cybercrimes.[373]

Aside from agreements, there is also active participation by Gcash in the investigations of fraudulent activities involving its app. In the mess involving unauthorized deductions in its users' account balances, GCash assisted the government's crackdown on online scammers.[374] It had helped anti-cybercrime

---

[368] *SEC and GCash sign agreement to combat scams and fraud*, PHIL. DAILY INQUIRER, Oct. 3, 2023, *available at* https://globalnation.inquirer.net/220154/sec-and-gcash-sign-agreement-to-combat-scams-and-fraud.

[369] *Id.*

[370] *Id.*

[371] *Id.*

[372] *Id.*

[373] *Id.*

[374] Beatrice Pinlac, *GCash 'steps up' ties with authorities to crack down on online scams*, PHIL. DAILY INQUIRER, May 11, 2023, *available at* https://newsinfo.inquirer.net/1767954/gcash-steps-up-ties-with-authorities-to-crackdown-on-online-scams.

agents arrest an online seller who allegedly "stole the victim's money after failing to deliver the purchased item" and blocked more than 900,000 accounts believed to be fraudulent.[375]

As the e-wallet with the largest user base in the country, GCash is serious in upholding its trust and security mandate by building close coordination and partnerships with law enforcement authorities, namely the PNP-ACG and the NBI.[376]

b. Effective education for fintech users

In the recent years, GCash has been leveraging the latest innovation in trust technology to build the safest digital ecosystem for its users while doubling down on empowering customers to protect their accounts through education.[377] One of the more recent and "believable" scams is called "spoofing scam," where perpetrators use illegal software to make their text scams appear like they came from legitimate sources such as banks, e-commerce companies, and other big, trusted companies.[378] Since they appear "legit," unsuspecting targets may fall victim and unknowingly click the link and leak sensitive personal and financial information to fraudsters.[379]

To prevent this from happening to its customers, Gcash launched the #GCheckMuna campaign empower customers to protect themselves and become more vigilant in the face of fraud.[380] The e-wallet firm cautions its users that their Send Money Confirmations are now sent to the GCash App inbox.[381] It also advises the public to stay vigilant that if someone contacts them claiming

---

[375] *Id.*

[376] *GCash, NBI, PNP Joint Effort Blocks 900,000 Fraudulent Accounts*, GLOBE.COM, May 4, 2022, *available at* https://www.globe.com.ph/about-us/newsroom/consumer/gcash-nbi-pnp-block-fraudulent-accounts#gref.

[377] James Loyola, *SEC, GCash team up to fight online fraud,* MANILA BULLETIN, Sep. 28, 2023, *available at* https://mb.com.ph/2023/9/28/sec-g-cash-team-up-to-fight-online-fraud.

[378] *PNP, GCash crack down on spoofing scam, warns public of modus*, Sep. 16, 2023, SUNSTAR, *available at* https://www.sunstar.com.ph/bacolod/business/pnp-gcash-crack-down-on-spoofing-scam-warns-public-of-modus#go-ogle_vignette.

[379] *Id.*

[380] *3 Reasons Why You Should Send Money Through GCash,* GCASH.COM, Jul. 29, 2022, *available at* https://www.gcash.com/three-reasons-why-you-should-send-money-through-gcash#:~:text=Aside%20from%20-barri-ng%20over%20900%2C000,in%20the%20face%20of%20fraud.&text=Tip%201%3A%20Never%20share%20your,%2Dtime%20password%20(OTP).

[381] *See supra* note at 378.

to have accidentally transferred money to their GCash account and requests it to be returned, they must carefully review their transaction history to confirm whether this is legitimate or an attempt to deceive and steal from them.[382]

Gcash, as well as other fintech companies, understands the support of customers is necessary in battling cybercrimes, therefore everyone should be vigilant against online scams.[383]

2. Enhancing government tools to prevent unreasonable searches and seizures

The collaboration between fintech companies and government agencies can play a vital role in combating financial crime and ensuring regulatory compliance. Still, it must be balanced with robust privacy protections, transparent oversight mechanisms, and respect for the rule of law.

This can be done by Congress through legislation that explicitly safeguards individuals' privacy rights and restricts government agencies' ability to conduct arbitrary searches and seizures of personal data. This could include enacting more comprehensive data protection laws, updating existing privacy statutes to encompass digital data, and establishing clear legal standards for government access to personal information.

Another approach involves the augmentation of judicial oversight of government surveillance activities by empowering independent courts to review and authorize requests for access to personal data, ensuring that warrants are issued based on sufficient evidence and are subject to rigorous scrutiny.

3. Increasing the penalty for cybercriminals and other law violators

Higher penalties can deter both fintech companies and users alike from engaging in illegal behavior. The fear of significant financial repercussions can discourage them from violating existing laws. It can help promote compliance with laws and regulations, protect consumers and competitors, and uphold the integrity of the marketplace.

---

[382] *Id.*

[383] *See supra* note at 376.

Under the GDPR, penalties for noncompliance have soared, and large tech companies have been subjected to substantial fines.[384] The total reported GDPR fines from May 2018 to January 2020 the total reported GDPR fines were 139 million dollars.[385] However, this amount more than doubled to 332 million dollars by January 2021.[386] For especially severe violations,[387] the administrative fines can be up to 20 million euros,[388] or in the case of an undertaking,[389] up to 4% of their total global turnover of the preceding fiscal year, whichever is higher.[390] Nevertheless, even the catalogue of less severe violations of GDPR sets forth fines[391] of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher.[392] Various institutions are recognizing that GDPR penalties are serious and therefore exerting efforts to avoid noncompliance fines.[393]

In Singapore, a bill has been proposed to increase the maximum penalty for each breach of a technology risk management requirement to 1 million dollars.[394] According to Singapore's Minister of State for Trade and Industry, such step is being undertaken to "underscore the critical importance of technology risk management to [financial institution]s' operations and the sound functioning of the financial system" and was "derived after considering existing penalty regimes of other jurisdictions and Singapore government agencies."[395]

The Singapore Personal Data Protection Commission has also been resilient in its enforcement of the Singapore PDPA.[396] In August 2019, five

---

[384] Gabe Gumbs, *The biggest GDPR penalties for noncompliance*, SPIRION.COM, Dec. 1, 2022, *available at* https://www.spirion.com/blog/gdpr-fines-increase.

[385] *Id.*

[386] *Id.*

[387] *GDPR Fines / Penalties, available at* https://gdpr-info.eu/issues/fines-penalties/.

[388] GDPR (2018), art. 83*,* ¶ 6.

[389] *See supra* note at 387. According to case law of the European Court of Justice, "the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed". An undertaking can therefore not only consist of one individual company in the sense of a legal person, but also out of several natural persons or corporate entities.

[390] GDPR (2018), art. 83*,* ¶ 6.

[391] *Supra* note at 387.

[392] GDPR (2018), art. 83*,* ¶ 4.

[393] Gumbs, *supra* note at 384.

[394] Prisca Ang, *Financial institutions to face higher penalty for cyber attacks, disruptions under new Bill*, STRAITS TIMES, Apr. 5, 2022, *available at* https://www.straitstimes.com/singapore/politics/financial-institutions-to-face-higher-penalty-for-cyber-attacks-disruptions-under-new-bill.

[395] *Id.*

[396] Tan & Azman, *supra* note at 141.

companies that breached data privacy laws by failing to secure the personal details of their customers and employees were fined for a total of SGD 117,000.[397] Among the five, the biggest fine imposed amounted to SGD 54,000 for failure to appoint a data protection officer, develop and implement data protection policies and practices, and protect customers' personal data.[398]

In the Philippines, the penalties for cyberattacks, disruptions, and non-compliance with regulations should also be increased to ensure that they reflect or are commensurate with the extensive damages and effects that are caused by such acts. Any increase in penalties should be accompanied by granting oversight agencies the power to impose measures that will assist them in monitoring compliance, detecting disruptions, and safeguarding stakeholders from the effects of breaches.

VIII. CONCLUSION

True to its claims, fintech is indeed an industry disruptor—it has transformed the world in more ways than one. The finance industry has been redefined from manual transactions performed in physical banks to a couple of taps in a mobile phone.

As a whole, fintech can play a significant role in promoting liberty and prosperity under the rule of law in the Philippines. Fintech helps bring banking and financial services to the unbanked and underbanked populations in the country, fostering economic liberty. As fintech allows more doors to be opened for small businesses, more jobs are being created, which in turn contributes to societal growth and success. Furthermore, fintech stimulates financial literacy, and a financially literate population is more likely to make sound economic decisions, leading to personal and national prosperity.

The transformative world of fintech has always been viewed as the answer—however, it can also be the problem. As discussed in this paper, there is an intricate relationship between fintech and the potential for data privacy breaches. While fintech has undoubtedly revolutionized financial services, its

---

[397] *Id.*
[398] *Id.*

reliance on vast amounts of user data raises significant concerns regarding data privacy and security.

Despite these challenges, the pros of engaging in fintech still outweigh the cons. Consequently, the Philippines must enhance data privacy protection and cybersecurity in order to foster an environment conducive to innovation and growth. The GDPR, labelled as the toughest privacy and security law in the world, is a good reference point in strengthening our own data privacy laws. While there is some effort in creating new laws to specifically address privacy concerns in the current fintech setup, there is very little progress. It can be argued that thorough research is necessary in order to formulate the perfect piece of legislation, but prolonging the enactment of these laws specifically catered to the data protection of fintech users will only increase the risks of security breaches. The growth of the fintech industry is exponential, and its corresponding data collection will progress the same way. Therefore, our legislators are highly encouraged to hasten the passage of proposed bills into law, as it will be highly advantageous to both the government and its constituents alike. By promoting a regulatory framework that upholds the rule of law, this author hopes to create a secure and thriving fintech ecosystem that safeguards liberties while nurturing economic prosperity.

In conclusion, the discourse on data privacy rights within the realm of fintech highlights the crucial balance between innovation and safeguarding personal information. As technology advances and fintech solutions become increasingly ingrained in daily transactions, it is vital for regulatory structures to adapt, ensuring that privacy rights are respected without impeding innovation. Ultimately, striking this delicate balance is key to building trust, advocating for responsible data handling, and leveraging fintech's potential to foster comprehensive and sustainable economic development.