หลักความยุติธรรมในการประมวลผลข้อมูลเครดิตทางเลือก ภายใต้กรอบการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

Fairness Principle in the Processing of Alternative Credit Data under the Thai Personal Data Protection Framework

เกรียงศักดิ์ อารีย์จิตเกษม
นักศึกษาดุษฎีบัณฑิต หลักสูตรปรัชญาดุษฎีบัณฑิต สาขากฎหมายเศรษฐกิจ,
มหาวิทยาลัยการเงินและเศรษฐศาสตร์เซี่ยงไฮ้ นครเซี่ยงไฮ้ สาธารณรัฐประชาชนจีน 200433

Kriengsak Areejitkasame
Ph.D. Candidate, Ph.D. in Economic Law, School of Law,
Shanghai University of Finance and Economics, Shanghai, 200433, China
E-mail : kriengsakareed@hotmail.com

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาความเป็นมาและแนวคิดทางกฎหมายของหลักความยุติธรรมในการคุ้มครองข้อมูลส่วนบุคคล (2) วิเคราะห์เงื่อนไขและองค์ประกอบในกฎหมายที่กำหนดความยุติธรรมในการประมวลผลข้อมูลเครดิตทางเลือก (3) ประเมินว่ากรอบการคุ้มครองข้อมูลส่วนบุคคลของไทยได้ใช้หลักความยุติธรรมในการประมวลผลข้อมูลเครดิตทางเลือกอย่างเหมาะสมหรือไม่ โดยใช้วิธีดำเนินการวิจัยเชิงคุณภาพและศึกษาเปรียบเทียบกับกรอบกฎหมาย มาตรการ และกรณีศึกษาของต่างประเทศ ผลการศึกษาพบว่า (1) แนวคิดเรื่องความยุติธรรมเป็นแนวคิดที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคลและสัมพันธ์กับสิทธิมนุษยชนขั้นพื้นฐาน (2) เทคโนโลยีและแนวปฏิบัติในปัจจุบันเกี่ยวกับการประมวลผลข้อมูลเครดิตทางเลือกนำมาซึ่งความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลจากการเลือกปฏิบัติโดยใช้ข้อมูลอ่อนไหวและโดยเครื่องจักร (3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้กำหนดหลักความยุติธรรมในกรณีของการประมวลผลข้อมูลเครดิตทางเลือก งานศึกษานี้จึงเสนอให้กำหนดหลักความยุติธรรมในกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจนเพื่อให้เจ้าของข้อมูลได้รับการคุ้มครองจากเลือกปฏิบัติในการประมวลผลข้อมูลเครดิตทางเลือก

คำสำคัญ : หลักความยุติธรรม การไม่เลือกปฏิบัติ การประมวลผลข้อมูลเครดิตทางเลือก

26 มีนาคม 2566/ 5 พฤษภาคม 2566/ 8 พฤษภาคม 2566
26 March 2023/ 5 May 2523/ 8 May 2523

Abstract

The purpose of this research article is to (1) study and review the origin, legal concept and practice of fairness principle in the protection of personal data, (2) examine the criteria and elements in law that determine fairness as applied to the processing of alternative credit data, and (3) analyze and evaluate whether the Thai personal data protection framework properly provides the data subject with fairness in the processing of alternative credit data by employing a qualitative research method and making a comparative analysis with foreign laws, frameworks, measures, and relevant cases. This study found that (1) fairness is an essential and multifaceted concept of personal data protection and fundamental human rights; (2) the current technology and practice regarding the processing of alternative credit data brings the risk of discrimination based on sensitive data and by machine; (3) the Thai Personal Data Protection Act (PDPA) 2019 (B.E. 2562) has not yet established fairness principle in the case of alternative credit data processing. This study therefore proposes that the relevant Thai authorities should establish fairness principle in the personal data protection law to ensure that the data subject's decision is immune from unfair treatment and discrimination.

Keywords : Fairness principle, Non-discrimination, Processing of Alternative Credit Data

Introduction

Fairness is one of the key principles of information privacy law that is essential for the protection of alternative credit data. Alternative credit data in this study refers to any non-traditional data that a lender uses for the assessment of the borrower's creditworthiness or the potentiality and willingness to pay back loans, including such data as utility payment, mobile usage, geolocation, social network analysis, etc. Most alternative credit data contain sensitive personal data that requires careful treatment and safeguards against unauthorized or improper uses which can undermine the data subject's fundamental rights and freedom, such as the right to non-discrimination.

Fairness is a core principle mentioned and found in international data protection measures, laws, and financial laws, including the EU and the US. In terms of law, there should be protection against non-discrimination with the following requirements: 1) protection of fundamental rights and freedoms in relation to the processing of personal data, 2) lawfulness, fairness and transparency, 3) special category data, 4) solely automated decisions.[1] However, there is no explicit principle of fairness in the Thai data protection laws and regulations.

---

[1] Binns, R., & Kirkham, R., "How could equality and data protection law shape AI fairness for people with disabilities?." (2021) 14:3 *ACM Transactions on Accessible Computing* (TACCESS) 1, 1-32.

Limited literature indicated a clear role of fairness in personal data protection law, and particularly evaluated the legal criteria and elements of fairness in the processing of alternative credit data under the Thai legislation. Existing foreign literature focused on assessing the legal framework for protecting fairness from the processing and use of alternative credit data, including assessing that US laws protecting fairness as non-discrimination from the use of credit scoring.[2] Many literature works emphasized policy suggestion, guidance, and framework on data protection and privacy for alternative credit data, which encompassed fairness in personal data processing.[3]

Meanwhile, the existing Thai literature mainly focused on legal problems related to credit information under the credit information business law. A study, assessing the protection of credit information under the Credit Information Business Act (CIBA) B.E. 2545 (2002), found that the legal credit information scope mainly in the credit card repayment history is too limited, and proposed to expand the scope of credit information under the law to cover various types of financial data, in order to effectively reflect upon applicants' financial status and behaviors. The other study found a misuse of credit information, for example, when applying for a job, suggesting that Thailand should adopt the US and the UK's approach to legislation on this issue.[4] Literature evaluating Thai legal measures for protecting personal data in financial and commercial banking industry did not research on the case of the processing of alternative credit data, but mainly focused on general principles of law, and the definition of sensitive data and non-sensitive data.[5]

Therefore, this study attempts to examine the legal criteria and elements that determine fairness under the Thai personal data protection law in relation to the processing of alternative credit data. This study also aims to propose modications to the legal concept of fairness and introduce amendments to the Thai personal data protection law in order to properly provide fairness in the processing of alternative credit data.

---

[2] Hurley, M., & Adebayo, J., "Credit scoring in the era of big data." (2016) 18 *Yale Journal of Law & Technology* 148, 148-216.

[3] See, e.g. World Bank and Consultative Group to Assist the Poor (CGAP), *Data Protection and Privacy for Alternative Data, GPFI-FCPL Sub-Group Discussion Paper Draft May 4, 2018* (15 Dec 2022) The Global Partnership for Financial Inclusion <https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf>.; World Bank and Global Partnership for Financial Inclusion, *G20 High-Level Principles for Digital Financial Inclusion* (15 Jan 2023) The Global Partnership for Financial Inclusion <https://www.gpfi.org/sites/gpfi/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf>.; Grady, R. C., Montes, H., Fredesvinda F., & Traversa, M., *Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (English)* (United States: The World Bank, 2018).

[4] Srichola, S. & Tipayanee, P., "Legal Issues Related to Credit Information on the Use of Credit Information for Other Purposes." (2016) 4:3 *DPU Graduate Studies Journal* 215, 215-226.

[5] Khaosanit, D., *Legal measures in private data protection : case study in finance and banking of commercial bank.*. (15 December 2021) Thesis <http://libdoc.dpu.ac.th/thesis/Dawan.Kha.pdf>.

Research Objectives

(1) to study and review the origin, legal concept and practice of fairness principle in the protection of personal data,

(2) to examine the criteria and elements in law that determine fairness as applied to the processing of alternative credit data, and

(3) to analyze and evaluate whether the Thai personal data protection framework properly provides the data subject with fairness in the processing of alternative credit data

Research Methodology

By employing qualitative research, regarding whether the existing Thai personal data protection legislation ensures fairness in the processing of alternative credit data, this study examined legal criteria and elements that determine fairness under the PDPA, the CIBA, and international data protection frameworks, measures, and laws. This study also made an analysis and evaluation of the existing Thai legislation by employing a comparative law research method to identify similarities and differences in the aspect of fairness in the processing of alternative credit data. This evaluation and comparative results were further combined and analyzed to propose modications to the relevant legal concept and also make recommendations for amending the Thai personal data protection legislation.

Research Findings

1. The Legal Denition and Concept of Fairness in Personal Data Protection

Fairness in the protection of personal data can be interpreted in various ways, but this study focuses on fairness as non-discrimination.[6] Discrimination is dened under international law as any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.[7] In the legal context, provisions on fairness or non-discrimination are embedded within the key human rights treaties of the United Nations Legislation.[8]

---

[6] Malgieri, G. “The concept of fairness in the GDPR: a linguistic and contextual interpretation.” (Paper presented at the Conference on fairness,accountability, and transparency, New York, United States, 27-30 January 2020) 154-166.

[7] RightsCon. Toronto, *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems* (16 May 2018) Systems <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/>.

[8] United Nations Legislation, *(a) Universal Declaration of Human Rights, 1948, (b) International Covenant for Civil and Political Rights, 1966, (c) International Covenant on Economic, Social and Cultural Rights, 1966, (d) Convention on the Elimination of All forms of Racial Discrimination, 1966, (e) Convention on the Elimination of All forms of Discrimination Against Women, 1979* (15 Jan 2023) Ohchr <http://www.ohchr.org>.

Individual shall be fairly treated and prevented from discriminatory practices. The use of highly sensitive data to be analyzed by machines or algorithms without human review or inability to explain analytical logic may lead to problems of potential discrimination or exclusion. The data subject should be given various opportunities in society as equals without opinions or prejudices, especially those that come from sensitive information that should be protected, such as gender, race, political views. This study also applies this notion to the case of automated decision-making that brings privacy challenges of inappropriate decision or judgement of individuals.

2. Key Attributes and Risks that Undermine Fairness in the Processing of Alternative Credit Data

2.1 Key Attributes of the Processing of Alternative Credit Data relating to Fairness

Service providers can use big data to build detailed personal proles of an individual, including his or her behavior (e.g., preferences, activities and movements) which can be used for commercial offers.[9] In digital nancial services, big data has been built, for instance, to gain an insight into individual behavioral prole in retail banking and customer's creditworthiness in credit scoring. Analytics and the ability to exploit the big data technologies, advanced statistical models, and predictive analytics in support of real-time decision making across business channels and operations become competitive edges for the nancial rms embracing big data.

Financial rms with big data capability can better understand and adequately analyze the client's risk proles, potentially leading to a more customized and reasonable pricing to each client. For example, when a decent and credible client starts applying for a loan without sufcient proof of income or credit, such as a salary or bank statement, this client can be potentially charged a higher price on the loan. With a data-driven ntech can simply detect the good characteristic and credibility of this client, resulting in signicantly lower interest rate on loan and greater expansion of credit.

Inferences and predictions can be used to make automated decisions (or to provide inputs to human decisions) or for targeted advertising. There are several reasons that accurate default prediction and personalize credit pricing are benecial for both lenders and borrowers.[10] When a lender can accurately predict default, they can determine a cutoff for extending a loan or price risk accordingly, reducing a loss for lenders.[11] The accurate prediction of default may mean that certain customers do not receive

---

[9] Terry, N. P., "Protecting patient privacy in the age of big data." (2012) 81:2 *UMKC Law Review* 385, 385-416.

[10] Gillis, T. B., *False dreams of algorithmic fairness: The case of credit pricing* (Cambridge: Harvard University Press, 2020) 37-40.

[11] See e.g., Phillips, R., "Optimizing prices for consumer credit." (2013) 12:4 *Journal of Revenue and Pricing Management* 360, 360-377.; Staten, M., *"Risk-Based Pricing in Consumer Lending."* (2015) *11.1 Journal of Law, Economics & Policy* 33, 33-58.

loans, however, this may be benecial to consumers if we consider that default and foreclosure are very costly for consumers.[12] The accurate pricing of credit also promotes an expansion of access to credit. The more accurate a lender's prediction, the more they are able to distinguish borrowers with different levels of risk since the lenders can distinguish between the risk of different borrowers.[13]

2.2 The Risks to Fairness in the Processing of Alternative Credit Data

2.2.1 Discrimination Based on Protected Characteristics

The processing of alternative credit data may also lead to the issues of predatory lending, unfair access to credit, and nancial exclusion. Using alternative credit data makes it possible to understand the behavior, preferences and creditworthiness of the borrower. Conversely, the lender may use such information or analysis in the form of predatory lending for certain group of borrowers.[14] Predatory lending includes exchange of value or loan pricing that exceeds the risk of the borrower, the release of unaffordable loan based on the borrower's asset rather than the borrower's ability to repay loan, the repeated renance of a loan to increase interest rates, or deceiving the borrowers of the true nature of the loan obligation or products.[15] Where the lender uses borrower insights obtained from alternative credit data, this may result in the lender granting loans or setting loan terms discriminatory or based on protected or sensitive factors for commercial interest without considering the impact on fair access to credit by all types of borrowers. Moreover, the disproportionate allocation of loan to certain groups of people in the society will cause the other group of creditworthy borrowers to have additional unnecessary burden from unfair judgement or unethical practice that results in nancial exclusion, where such borrowers lack access to credit or other nancial services as they are unfairly deemed to have high risk.

2.2.2 Discrimination by Machine

The increasing use of proling and automated decision-making systems raises concerns about potential discrimination and unfair treatment. When used on a large scale, the results of big data analytics may well feed on each other, magnifying social and economic inequalities.[16] In the most extreme

---

[12] Gathergood, J., Guttman-Kenney, B., & Hunt, S., "How do payday loans affect borrowers? Evidence from the UK market." (2019) 32:2 *The Review of Financial Studies 496, 496-523.*

[13] See Supra Note 10, (Gillis, 2020).

[14] See Supra Note 2, (Hurley & Adebayo, 2016).

[15] FDIC's, *"Supervisory Policy on Predatory Lending"* (15 February 2023) financial-institution-letters <https://www.fdic.gov/news/financial-institution-letters/2007/fil07006a.html>.

[16] O'neil, C., *Weapons of math destruction: How big data increases inequality and threatens democracy* (New York: Crown Publishers, 2016) 272.

case, big data methods may result in data determinism, which means that individuals are judged based on probabilistic knowledge (correlations and inferences) of what they might do, rather than what they actually have done.[17] Furthermore, individuals are treated as passive objects of algorithmic evaluation and decision tools and are unable to present their values and positions, and, additionally, the use of proling and automated decisions may be caused by prejudice and a lack of openness.[18]

Price discrimination or personalized pricing can be dened as differentiating the price for identical products or services based on the data controller's information on a potential customer.[19] Price discrimination can occur in a way that nancial institutions make use of the collected data to charge different prices to different individuals depending on the information they analyze. A study in 2015 found that using algorithms, most US insurers quoted car insurance prices based on credit scores rather than actual driving history. In some cities, such as Florida, drivers with very good driving records but low credit scores paid $1,552 more for car insurance compared to drivers with high credit scores for drunk driving.[20]

Moreover, an individual's creditworthiness may be evaluated based not only on their characteristics, but those of their social network. In 2015, Facebook secured a patent that enables ltering of loan applications depending on whether the average credit rating of a loan applicant's friends exceeds a preset minimum credit score.[21] This may risk discrimination, and even nancial exclusion, if an applicant's friends are mostly low-income members regardless of the real quality of the applicant's credit.[22] These big data technologies are likely to prefer wealthier individuals to get access to nancial services, while impeding nancial access for minority groups that lacked access based on historical data, which is the so called "automating inequality".[23] Increasing studies raise concern that failing to address bias

---

[17] Broeders, D., Schrijvers, E., van der Sloot, B., Van Brakel, R., de Hoog, J., & Ballin, E. H., "Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data." (2017) 33:3 *Computer Law & Security Review* 309, 309-323.

[18] Hänold, S, "Profiling and Automated Decision-Making: Legal Implications and Shortcomings." In Marcelo Corrales, Mark Fenwick, & Nikolaus Forgó (ed), *Robotics, AI and the Future of Law* (Singapore: Springer, 2018) 123, 123-153.

[19] Borgesius, F. Z., & Poort, J., "Online price discrimination and EU data privacy law." (2017) 40:3 J. *Consumer Pol'y* 347, 348.

[20] See Supra Note 16, (O'Neill, 2016).

[21] MacMillan, Rory. "Big Data, Machine Learning, Consumer Protection and Privacy." Paper presented at the 47th Research Conference on Communication, Information and Internet Policy, American University, Washington College of Law, Washington, D.C., 26 July 2019) 9.

[22] Zim, J., *The Use of Social Data Raises Issues for Consumer Lending* (28 April 2016) issues <https://business-law- review.law.miami.edu/social-data-raises-issues-consumer-lending/>.

[23] Eubanks, V., *Automating inequality: How high-tech tools profile, police, and punish the poor* (New York: St. Martin's Press, 2018) 212.

in big data credit platforms may cause harms to individuals.[24] For instance, Amazon's 2016 redlining case that Amazon discriminated against people using Prime delivery only in communities with a majority of white people by offering Amazon Prime's free same-day delivery service recently revealed the exclusion of predominantly black ZIP codes.[25]

3. Legislation relating to Fairness in the Processing of Alternative Credit Data in Thailand

3.1 Personal Data Protection Act B.E. 2562 (2019)

Unfair processing in this study can be referred to as unfair treatment or discrimination occurred in the use of personal data, in particular the collection or processing of personal sensitive data in a way that has an unreasonable effect on the data subject. Hence, the law should protect and contain provisions from collecting or accessing sensitive personal data and analyzing, using, including transferring it to other parties so as not to unfairly affect the data subject. There should be provisions for the use of automated decision-making and proling that protect data from being processed or used unjustied or that would adversely affect the data subject or be discriminated against by the systems or analytic models that are used.

The PDPA prevents the collection of sensitive personal data, which is personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the personal data protection committee.[26] Under the PDPA, any collection of sensitive personal data is prohibited, except that the data controller obtains explicit consent from the data subject or it is information that is disclosed to the public with the explicit consent of the data subject.[27] Explicit consent herein further claries that a request for consent shall be explicitly made in a written statement, or via electronic means, unless it cannot be done by its nature.[28]

---

[24] Johnson, Kristin, Frank Pasquale, and Jennifer Chapman. "Artificial intelligence, machine learning, and bias in finance: toward responsible innovation." (2019) 88:2 *Fordham L. Rev.* 499, 501.

[25] Ingold, D., & Soper, S., *Amazon Doesn't Consider the Race of Its Customers. Should It?,* BLOOMBERGB (21 April 2016) graphics <https://www.bloomberg.com/graphics/2016-amazon-same-day/>; Letzter, R., *Amazon Just Showed Us That "Unbiased' Algorithms Can Be Inadvertently Racist, BUS. INSIDER* (21 April 2016) how-algorithms-can-be-racist <http://www.businessinsider.com/how-algorithms-can-be-racist-2016-4>.

[26] Section 26., *Personal Data Protection Act 2019.*

[27] Section 26 of the PDPA prescribes other exceptions for the collection of sensitive personal data. For instance, prevent a danger to life, body or health of the person, where the data subject is incapable of giving consent; carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or trade union purposes; it is necessary for compliance with a law to achieve the certain purposes.

[28] Section 19, para 2., *Personal Data Protection Act 2019.*

3.2 Credit Information Business Act B.E. 2545 (2002)

Regarding the protection of sensitive data, in addition to the provision under the PDPA, the CIBA also protects certain types of sensitive data that can be processed as alternative credit data by the member service providers. This type of data is referred to as prohibited information in the CIBA. Prohibited information is dened as personal data that does not relate to the request for credit or affects the feeling or may cause damage or obviously affected the rights and freedom of the data subject, including physical handicaps, genetics, information of a person in the process of criminal investigation or criminal proceedings, and other information that are announced by the credit information protection committee. With respect to the provisions relating to prohibited information, the CIBA does not allow credit information company, data controller or data processor to gather and record prohibited information without any exceptions.

Since the denition of personal data that is used for credit information is divided into traditional credit data and alternative credit data, the protection of personal data is therefore separated under the CIBA and the PDPA. Traditional credit data is governed under the CIBA, and non-traditional or alternative credit data is regulated under the PDPA. However, key denitions and provisions under the two laws are not coherent. For example, the denitions of sensitive data and prohibited data and the prohibitions or provisions of such data collection are inconsistent between the two laws. Furthermore, neither the PDPA nor the CIBA have specic additional requirements that can be applied in the case of automated decision-making or proling.

4. Comparative Analysis of Thai Laws and the International Measures, Frameworks, and Laws

4.1 Safeguards of Sensitive Data Processing

Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guideline) broadly states that in implementing the Guideline, member countries should ensure that there is no unfair discrimination against data subjects.[29] This provision aims to protect the data subject against unfair discrimination on such factors as nationality and domicile, sex, race, belief, or trade union afliation.[30] Meanwhile, recital 71 of the General Data Protection Regulation (GDPR) states that "in order to ensure fair and transparent processing in respect of the data subject, the controller should use appropriate mathematical

[29] Art. 19 (i.)., *OECD Privacy Guidelines 2013.*

[30] Ibid, Annex, Art. 19 (i.)., *Guidelines governing the protection of privacy and transborder flows of personal data.*

or statistical procedures for the proling, implement technical and organizational measures appropriate to" prevent "potential risks" for the interests and rights of the data subject, such as "discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect".

The Council of Europe (CoE) Convention 108+ and the GDPR prohibits processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[31] By the same token, the PDPA also prescribes sensitive personal data as personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as announced by the personal data protection committee.[32] The categories of sensitive data under the GDPR and PDPA are consistent and show no signicant difference.

Article 22(4) of GDPR restricts automated decision-making based on protected characteristics of personal data except the data subject has given explicit consent and there exist suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In this case it is evident that if a data controller wishes to use sensitive data for automated decision-making including proling, explicit consent must be obtained from the data subject and appropriate safeguards must be provided regarding the data subject's rights, freedoms and legitimate interests. However, this provision does not explicitly prohibit the discrimination of the data subject from the use of sensitive data. Therefore, even if the data subject has given consent, discrimination may occur by automated decision-making or machines.

4.2 Protection on Lending Discrimination

While the PDPA and the CIBA do not have any specic provision or requirement on the protection against unfair lending or lending discrimination, the specic legislation that can be applied to the case of lending has been shown in the US. Under the US's Equal Credit Opportunity Act (ECOA), nancial institutions are required to give credit equally to creditworthy customers, taking

[31] CoE Convention 108+ 2018, Article 6; General Data Protection Regulation 2018, Art. 9.

[32] Section 26., *Personal Data Protection Act 2019.*

into account sex or marital status, and not discriminate against any credit applicant with respect to any aspect of a credit transaction on the basis of race, color, religion, national origin, sex or marital status, or age, or because all or part of the applicant's income is from any public assistance program, or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act.[33] In addition, the ECOA requires the creditors to provide information about the reasons for taking adverse action against applicants. Adverse actions include denial of a loan, terminating the current credit account, changing unfavorable loan terms, and refusing to increase credit limit.[34] Information on such reasons must be specic and indicate the principal reason(s) of the adverse action.[35] The Fair Credit Reporting Act (FCRA) also requires lenders to disclose information if decisions are made, in whole or in part, based on information from sources other than client information, and to disclose credit scores used for taking adverse action, along with any accompanying information, including the key four to ve factors that adversely affected the client's credit score.

The ECOA and the Fair Housing Act (FHA), a federal law prohibiting discrimination by direct providers of housing, such as landlords and real estate companies as well as other entities, state that there are three types of lending discrimination: disparate treatment, comparative disparate treatment, and disparate impact. First, disparate treatment exists when there is evidence that a lender explicitly considered prohibited characteristics, such as race or color, religion, national origin, sex, marital status, age, handicap. For instance, if a lender offers a credit card limit differently for applicants at the different age ranges, this is considered violating the ECOA by discriminating applicants on age. Second, comparative disparate treatment occurs when a lender treats a credit applicant differently based on any prohibited factors. For example, when a lender found negative information on a female applicant applying for a personal loan, a lender calls the female to discuss and nally grant loan. However, when there is another male applying for a similar loan, the lender also found negative information on the male prole, but the lender rejected the male applicant without discussing any possible solution. This is considered comparative disparate treatment. Third, disparate impact refers to the use of apparently neutral criteria or policy that nevertheless result in disparate treatment of prospective borrowers, including excluding or burdening certain applicants on prohibited factors, without a legitimate business need. For instance, a lender follows a lending policy that imposes a home loan limit at a very high level that disproportionately excludes potential minority applicants owing to their level of income or the house value in their area.

---

[33] 15 USC Chapter 41, Subchapter IV: *Equal Credit Opportunity*, §1691(a).

[34] 12 CFR § 1002 *Equal Credit Opportunity Act* (Regulation B) 2(c).

[35] Ibid, § 1002.9(b)(2).

4.3 Rights and Requirements regarding Automated Decision-Making and Proling

4.3.1 Right not to be subject to solely automated decisions, including proling, which have a legal or similarly signicant effect on them

Under the CoE Convention 108+, the data subject has the right not to be subject to a decision signicantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.[36] Under the GDPR, data subjects must not be subject to automated decisions which produce legal effects. Special protection is required if such decisions are likely to have a signicant impact on the lives of individuals, such as, creditworthiness, job recruitment, performance at work, or the analysis of conduct.[37] Nevertheless, the GDPR allows automated decision-making in case it is necessary to conclude a contract between the data controller and data subject, or in case the data subject gives explicit consent.[38]

4.3.2 Right to express the point of view and to contest the decision

The data controller is required to implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, which at least include the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.[39]

4.3.3 Data Protection Impact Assessment

In case of data processing that can produce result in a high risk to the data subject the data controller shall make Data Protection Impact Assessment (DPIA). Such high-risk data processing includes automated decision-making, evaluation or scoring and processing of sensitive data. In the DPIA, data controller has to describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to the data subject; and identify measures to mitigate those risks. The DPIA process is essential for the data controller to systematically understand risky data processing and be able to identify and minimize potential risks to individuals' rights and freedoms. The PDPA does not specify any requirement on DPIA. Nevertheless, Section 37 (1) of the PDPA requires one of the duties of the data controller to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.

---

[36] Article 9 (a.) – Rights of the data subject, *CoE Convention 108+ 2018.*

[37] Recital 71, Art. 4 (4) and Art. 22, *General Data Protection Regulation 2018.*

[38] Ibid, Art. 22 (2).

[39] Ibid, Art. 22 (3).

Table 1 below summarizes the result of comparative analysis of the fairness criteria and elements in the Thai laws and international frameworks, measures, and laws in terms of the coverage of sensitive data, safeguards of sensitive data processing, and requirements on machine-based credit decisions, including automated decision-making. Such result shows that the Thai law has advantages in terms of the denition and requirements for sensitive data processing. However, the law does not provide explicit legal measures or rights related to automated credit decisions in comparison with those prescribed in the international measures, laws, and framework. In the following part, this study further discusses the relevant cases and authorities' decisions relating to the legal criteria and elements of fairness.

Fairness Criteria and Elements	**Thai Law**	**OECD and APEC Framework**	**CoE 108+ Convention And the GDPR**	**US Law**
Coverage of Sensitive Data	Personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data[41], or of any data which may affect the data subject in the same manner[42]	Such factors as nationality and domicile, sex, race, belief, or trade union affiliation[43]	Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation[44]	Race, color, religion, national origin, sex or marital status, or age, or because all or part of the applicant's income is from any public assistance program, or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act[45]

[40] Ibid, Art. 35.

[41] Section 26, para 4 of the PDPA defines biometric data as the personal data arising from the use of technics or technology related to the physical or behavioral dominance of person, which can be used to identify such person apart from other persons, such as the facial recognition data, iris recognition data or fingerprint recognition data.

[42] Section 26, para 1., *Personal Data Protection Act 2019.*

[43] Art. 19 (i.)., *OECD Privacy Guidelines 2013.*

[44] Article 6., *CoE Convention 108+ 2018; Art. 9., General Data Protection Regulation 2018.*

[45] 15 USC Chapter 41, Subchapter IV: Equal Credit Opportunity, §1691(a).

Fairness Criteria and Elements	Thai Law	OECD and APEC Framework	CoE 108+ Convention And the GDPR	US Law
Safeguards of Sensitive Data Processing	Prevent the collection of sensitive personal data, except that the data controller obtains explicit consent from the data subject or the information is publicly disclosed with the data subject's consent	Protect the data subject against unfair discrimination on such factors	• Establish principle of fair processing, including discriminatory effects on natural persons based on sensitive data • Prohibit processing of sensitive data	Not discriminate against any credit applicant with respect to any aspect of a credit transaction on the protected bases
Requirements on Machine-based Credit Decisions	No specific provision or requirement	No specific provision or requirement	• Restrict automated decision-making based on sensitive data except the data subject has given explicit consent and there exist suitable measures to safeguard the data subject's rights and freedoms and legitimate interests • Right not to be subject to solely automated decisions which have a legal or similarly significant effect on them • Right to obtain human intervention on the part of the controller • Right to express his or her point of view and to contest the decision • Require to make Data Protection Impact Assessment[46]	• Provide information about the reasons for taking adverse action against applicants[47] • Disclose information if decisions are made based on sources other than client information • Disclose credit scores used for taking adverse action, and any information, including the key four to five factors that adversely affected the client's credit score

Table 1: Summary of the Comparative Analysis of the Legal Criteria and Elements of Fairness in the Thai Data Protection Laws and Selected International Data Protection Measures, Laws, and Frameworks

[46] According to the GDPR, Article 35, to make a Data Protection Impact Assessment, data controller has to describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance.

[47] According to the US's ECOA, adverse action includes denial of a loan, terminating the current credit account, changing unfavorable loan terms, and refusing to increase credit limit.

4.4 Cases

4.4.1 Chief Official Ethics Commission:[48] sensitive data from inferences

The fact of this Lithuanian case in 2018 presents that the Chief Official Ethics Commission, which received public funds, legally required individuals to provide a declaration of privacy interests, that was later published on the website of the Lithuanian Supreme Commission for Service Ethics. The issue is whether or not the content of a published declaration affects the right to privacy of the declarant and other persons included in the declaration, such as co-habitant, partners or spouses. This is because such information may reveal family relationships or sexual orientation, including other special categories of data which require specific legal bases for processing and special safeguards.

In 2022, the Court of Justice of the European Union (CJEU) held that any situation in which an entity can make inferences about the special category data by making an intellectual operation involving comparison or deduction or cross-referencing on personal data is considered processing of special category data, even if such data is directly not disclosed as special category data. It is evident that sensitive data in this case includes indirect inference or deduction from the disclosed data. Therefore, if the data controller discloses general personal data, but those data can be inferred that the data subject possesses certain qualities, such as sexual orientation, race, political opinions. Data controllers must therefore be careful and need to determine the extent to which data may be disclosed to third parties or may require additional consent from the data subject and impose appropriate safeguards on such inferable data.

This case highlights the importance of interpretation and coverage of sensitive data. Another type of non-sensitive data may be able to infer or indicate sensitive data. For instance, in case of the disclosure of the name and surname of the co-habitant of the data subject's residence, gender can be inferred from the name of the cohabitant, and also this may imply sextual orientation of the data subject. Therefore, the data controller should not interpret sensitive data requirements solely on the character or type of data, but also consider the circumstances and the context in which such personal information is used. If the collected non-sensitive data can be used to infer any sensitive data, the data subject's consent must be obtained and appropriate safeguards for human rights shall be in place.

4.4.2 Senseonics INC: [49] obtaining bundled consent to process sensitive data

In this case, the Italian Data Protection Supervisory Authority found that a US company, Senseonics INC, had provided an application for diabetic patients, after downloading the app,

---

[48] CJEU C-184/20, *OT v Vyriausioji tarnybines etikos komisija, ECLI:EU:C:2022:601.*

[49] Edpb, *Italian SA fines US company offering diabetes app* (9 February 2023) italian-sa-fines-us-company-offering-diabetes-app <https://edpb.Europa.eu/news/national-news/2022/italian-sa-fines-us-company-offering-diabetes-app_en>.

the data subject was required to accept the terms and conditions of the use of service and privacy policy in one single click. This prevented the data subject from giving consent separately to the processing of health-related information. The authority held that the company's requirement for acceptance of privacy policy was violating the lawfulness and transparency principle and the consent requirement according to Article 5(1) (a), 6, 7 and 9 of the GDPR. From this case it can be seen that even though the data controller requests the data subject's consent to collect and process sensitive data, but the consent has to be separated from the standard privacy policy that ties with the terms of use of the service.

4.4.3 *Portuguese National Statistics Institute:*[50] lack of lawfulness in the processing of sensitive data

In this case it concerns the lawfulness of sensitive data processing for statistics purposes. A national census survey organized by Portuguese National Statistics Institute required citizens to complete identification of all members in the same residence, including answering mandatory questions revealing religion and health data. The Portuguese Supervisory Authority held that such data processing lacked lawfulness for sensitive data processing according to the Article 9(1) of the GDPR, which prohibits the processing of sensitive data, including religious beliefs and health data, and that the questions about religion and health shall be flagged as optional, instead of mandatory. This case illustrates the difference between the lawful bases of the GDPR and the PDPA. The GDPR does not include the data processing for statistics purposes in the lawful bases. Meanwhile, the PDPA includes processing of data for the purpose of statistics to be lawful and exempt from consent requirement; nevertheless, such data processing needs to have suitable measures to safeguard the data subject's rights and freedoms.[51]

4.4.4 Texas Department of Housing and Community Affairs v. Inclusive Communities Project, Inc. (2015):[52] a disparate-impact claim that relies on a statistical disparity

In this case, Inclusive Communities Project, Inc., a Texas-based nonprofit company that helped low-income family in acquiring affordable housing, brought a disparate-impact claim under the FHA, alleging the Texas Department of Housing and Community Affairs that its officers disproportionately allocated too many tax credits to housing in predominantly black people inner-city areas and too few tax credits in predominantly white people suburban area according to statistical evidence. The court held that the

---

[50] Edpb, *The Portuguese Supervisory Authority fines the Portuguese National Statistics Institute (INE) 4.3 million EUR, December 19, 2022.* (9 February 2023) portuguese-supervisory-authority-fines-portuguese-national-statistics <https://edpb.europa.eu/news/national-news/2022/Portuguese-supervisory-authority-fines-portuguese-national-statistics_en>.

[51] Section 24 (1), *Personal Data Protection Act 2019.*

[52] *Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc.* - 135 S. Ct. 2507 (2015).

disparate-impact claims were cognizable under the FHA since it is unlawful to refuse to sell or rent or deny, a housing to a person because of race, or to discriminate against any person in making housing transactions based on race or other protected factors. This case represents lending discrimination by disparate impact since the lending policy of the Texas Department of Housing and Community Affairs disproportionately favored certain group of borrowers and burdened the other group of borrowers based on race, which is one of the protected characteristics under the FHA.

4.4.5 *United States v. Synchrony Bank, f/k/a GE Capital Retail Bank (D. Utah) (2014):*[53] discrimination against Spanish credit card clients by using neutral proxies for national origin programmed into a credit algorithm

GE Capital Retail Bank (GE Capital) offered promotions for its credit card customers who defaulted on payment to settle the balances. The promotion set certain criteria of the qualified customers, including balanced amount, amount and times of payment overdues. However, GE Capital excluded borrowers with "Spanish-preferred" indicators on their accounts or with mailing addresses in Puerto Rico from the credit card debt-repayment programs. In other words, it did not provide this offer to customers who preferred to communicate in Spanish or those who lived in Puerto Rico even though the customer was qualified to receive such promotions. As a result, the Spanish customer was unfairly rejected to gain benefit from the balance settlement promotions. The Consumer Financial Protection Bureau (CFPB) held that this act is in violation of the ECOA's provisions on discrimination since the ECOA does not allow discrimination in any aspect of a credit transaction on the basis of protected characteristics, such as race or national origin.

5. Limitations of the Thai Legal Personal Data Protection Legislation

In enhancing fairness in the processing of alternative credit data, the PDPA mainly prescribes provisions prohibiting collecting sensitive data without prior explicit consent from the data subject. However, the PDPA does not have any requirements or safeguards against the case where the processing of alternative credit data may result in unfair treatment, lending discrimination, inference of sensitive data from non-sensitive data. Additionally, the PDPA does not provide protection in which the credit scoring model may create proxies with protected characteristics from non-sensitive data, or learning algorithms that may use database that contain human bias from historical data.

---

[53] Consumerfinance, *CFPB Orders GE Capital to Pay $225 Million in Consumer Relief for Deceptive and Discriminatory Credit Card Practices,* (9 February 2023) cfpb-orders-ge-capital-to-pay <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-ge-capital-to-pay-225-million-in-consumer-relief-for-deceptive-and-discriminatory-credit-card-practices/>.

The PDPA also does not require the data controller to provide information to the client in case of automated decision-making on lending, nor does it grant the right to object to processing or challenge such automated decision. While the GDPR clearly states that the data subject has such rights regarding automated decision-making and profiling. Furthermore, there is no transparency requirement on the use of automated decision-making or profiling, including explanation on the result and the logic of the model used for automated decision. Moreover, there is no specific prohibition on using sensitive data that may lead to discriminatory credit result by credit models. In regards to providing an explanation or reason for refusing a loan, the US law, including the ECOA and the FHA clearly prescribe the provisions on providing the borrower with the specific explanation on the lender's adverse actions covering the following: refusal of credit, reduction of credit limit or changes in borrowing conditions such as raising interest rates.

In addition, the elements relating to fairness under the CIBA significantly differs from that of the PDPA in the matter of coverage of data processing activities, the protection of prohibited information or sensitive data, the right to explanation on the refusal of credit, the use of credit information for credit scoring model. As for the data subject's rights, the CIBA also does not specify the rights regarding automated decision-making, such as the right not to be subject to an automated decision.

Conclusion and Discussion

The concept of fairness is one of the key principles in the protection of personal data and other fundamental human rights. Fairness in information privacy is often referred to as safeguard of sensitive data, fair treatment, fair processing, and non-discrimination. In alternative credit data processing, there are many cases where lenders may take the collected sensitive data or obtain such data from the analysis or inferences to be used in lending decisions. In addition, lenders may use credit scoring models or automated lending decisions without human review. Both cases pose a significant risk that the borrower may be treated unfairly by using sensitive data or producing potential discriminatory outcomes. It is imperative that the regulator apply fairness principle to the protection of alternative credit data.

From the comparative analysis and assessment of the personal data protection legal framework related to alternative credit data in Thailand, it was evident that the Thai personal data protection law still lacks requirements relating to fairness principle, especially fairness as non-discrimination. For instance, the requirements for the protection of sensitive data under the PDPA and the CIBA are inconsistent. Furthermore, Thai law does not provide for individual rights regarding automated decision making, such as the use of automated credit decision or scoring model as required in the EU law. Thus, the data subject cannot choose

whether or not the controller can process personal data under such automated means, or challenge or object to the machine decision that may be discriminatory or inaccurate. Moreover, the law does not require the data controller to provide any explanation particularly on the logic of the credit model and result, as well as information on the reason for credit refusal as explicitly prescribed in the case of the US law.

Although the Thai and international data protection legislation restricts the controller from processing of sensitive data without explicit consent, giving consent should not imply that the data subject gives away certain fundamental rights. The adoption of big data technologies and practice on the processing of alternative credit data, including data collection and advanced analytics may cause potential discrimination, exclusion, or restriction to individual choices or decisions. In terms of collection and processing of sensitive data, with the current capacity of big data analytics, it is possible to infer sensitive data from non-sensitive data. The machine may generate new sensitive variables from superficially non-sensitive data, and the database used in learning algorithms may contain human bias, allowing the result to discriminate or exclusion from protected characteristics.[54]

Recommendation

In order to properly protect the data subject against unfair treatment, exclusion or discriminatory outcomes from the processing activities of alternative credit data, as well as to ensure that the data subject's choice or decision is immune from unfair judgment or treatment, to the relevant Thai authorities, this study highly recommends that:

(1) fairness as non-discrimination should be explicitly established as one of data processing principles under the PDPA; and

(2) the PDPA should be amended to provide safeguards against discrimination based on protected characteristics, inferences of sensitive data from non-sensitive data, and specific rights related to automated decision-making (e.g. right not to be subject to automated decisions, to obtain human intervention, or to express the point of view and contest the decision), and require the data controller to provide the data subject with transparent information on the use of automated credit decision-making and reasons for refusing a loan.

---

[54] See Supra Note 24, (Johnson et al., 2016), 510.

บรรณานุกรม

Binns, R., & Kirkham, R., "How could equality and data protection law shape AI fairness for people with disabilities?." (2021) 14:3 *ACM Transactions on Accessible Computing* (TACCESS).

Borgesius, F. Z., & Poort, J., "Online price discrimination and EU data privacy law." (2017) 40:3 *J. Consumer Pol'y.*

Broeders, D., Schrijvers, E., van der Sloot, B., Van Brakel, R., de Hoog, J., & Ballin, E. H., "Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data." (2017) 33:3 *Computer Law & Security Review.*

Consumerfinance, *CFPB Orders GE Capital to Pay $225 Million in Consumer Relief for Deceptive and Discriminatory Credit Card Practices,* (9 February 2023) cfpb-orders-ge-capital-to-pay <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-ge-capital-to-pay-225-million-in-consumer-relief-for-deceptive-and-discriminatory-credit-card-practices/>.

FDIC's, *"Supervisory Policy on Predatory Lending."*(15 February 2023) financial-institution-letters <https://www.fdic.gov/news/financial-institution-letters/2007/fil07006a.html>.

Gathergood, J., Guttman-Kenney, B., & Hunt, S., "How do payday loans affect borrowers? Evidence from the UK market." (2019) 32:2 *The Review of Financial Studies.*

Edpb, *Italian SA fines US company offering diabetes app* (9 February 2023) *italian-sa-fines-us-company-offering-diabetes-app <https://edpb.Europa.eu/news/national-news/2022/italian-sa-fines-us-company-offering-diabetes-app_en>.*

Edpb, *The Portuguese Supervisory Authority fines the Portuguese National Statistics Institute (INE) 4.3 million EUR, December 19, 2022.* (9 February 2023) portuguese-supervisory-authority-fines-portuguese-national-statistics <https://edpb.europa.eu/news/national-news/2022/Portuguese-supervisory-authority-fines-portuguese-national-statistics_en>.

Eubanks, V., *Automating inequality: How high-tech tools profile, police, and punish the poor* (New York: St. Martin's Press, 2018).

Gillis, T. B. *False dreams of algorithmic fairness: The case of credit pricing* (Cambridge; Harvard University Press, 2020).

Hänold, S, "Profiling and Automated Decision-Making: Legal Implications and Shortcomings." In Marcelo Corrales, Mark Fenwick, & Nikolaus Forgó (ed), *Robotics, AI and the Future of Law (Singapore: Springer,* 2018).

Hurley, M., & Adebayo, J., "Credit scoring in the era of big data." (2016) 18 *Yale Journal of Law & Technology.*

Ingold, D., & Soper, S., *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERGB (21 April 2016) graphics <https://www.bloomberg.com/graphics/2016-amazon-same-day/>.

Johnson, Kristin, Frank Pasquale, and Jennifer Chapman. *"Artificial intelligence, machine learning, and bias in finance: toward responsible innovation."* (2019) 88:2 *Fordham L. Rev.*

Khaosanit, D., *Legal measures in private data protection : case study in finance and banking of commercial bank.* (15 December 2021) Thesis <http://libdoc.dpu.ac.th/thesis/Dawan.Kha.pdf>.

Letzter, R., *Amazon Just Showed Us That "Unbiased' Algorithms Can Be Inadvertently Racist, BUS. INSIDER* (21 April 2016) how-algorithms-can-be-racist <http://www.businessinsider.com/how-algorithms-can-be-racist-2016-4>.

MacMillan, Rory. "Big Data, Machine Learning, Consumer Protection and Privacy." Paper presented at the 47th Research Conference on Communication, Information and Internet Policy, American University, Washington College of Law, Washington, D.C., 26 July 2019).

Malgieri, G. "The concept of fairness in the GDPR: a linguistic and contextual interpretation." (Paper presented at the Conference on fairness, accountability, and transparency, New York, United States, 27-30 January 2020).

O'neil, C., *Weapons of math destruction: How big data increases inequality and threatens democracy* (New York: Crown Publishers, 2016).

Phillips, R., "Optimizing prices for consumer credit." (2013) 12:4 *Journal of Revenue and Pricing Management.*

RightsCon. Toronto, *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems* (16 May 2018) Systems< https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/>.

Srichola, S. & Tipayanee, P., "Legal Issues Related to Credit Information on the Use of Credit Information for Other Purposes." (2016) 4:3 *DPU Graduate Studies Journal.*

Staten, M., "Risk-Based Pricing in Consumer Lending." (2015) 11.1 *Journal of Law, Economics & Policy.*
Terry, N. P., "Protecting patient privacy in the age of big data." (2012) 81:2 *UMKC Law Review.*

United Nations Legislation, *(a) Universal Declaration of Human Rights, 1948, (b) International Covenant for Civil and Political Rights, 1966, (c) International Covenant on Economic, Social and Cultural Rights, 1966, (d) Convention on the Elimination of All forms of Racial Discrimination, 1966, (e) Convention on the Elimination of All forms of Discrimination Against Women, 1979* (15 Jan 2023) Ohchr <http://www.ohchr.org>.

World Bank and Consultative Group to Assist the Poor (CGAP), *Data Protection and Privacy for Alternative Data, GPFI-FCPL Sub-Group Discussion Paper Draft May 4, 2018* (15 Dec 2022) The Global Partnership for Financial Inclusion<https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf>.

World Bank Group, *Good Practices for Financial Consumer Protection, 2017 Edition* (United States: The World Bank, 2017).

World Bank and Global Partnership for Financial Inclusion, *G20 High-Level Principles for Digital Financial Inclusion* (15 Jan 2023) The Global Partnership for Financial Inclusion <https://www.gpfi.org/sites/gpfi/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf>.

Grady, R. C., Montes, H., Fredesvinda F., & Traversa, M., *Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (English)* (United States:The World Bank, 2018).

Zim, J., *The Use of Social Data Raises Issues for Consumer Lending* (28 April 2016) issues <https://business-law- review.law.miami.edu/social-data-raises-issues-consumer-lending/>.