International Journal of Law, Humanities & Social Science©
Volume 3, Issue 3 (April 2019), P.P.23-37, ISSN: 2521-0793

PRIVACY LAWS IN THE CONTEXT OF FINTECH INDUSTRY IN MAURITIUS: A COMPARATIVE STUDY

Ambareen Beebeejaun[1]

[1](*Lecturer, Faculty of Law and Management, University of Mauritius Reduit, Mauritius)*

Abstract: *Financial technology also known as FinTech is experiencing a phenomenal growth across the globe. Consequently, given the numerous opportunities provided by the FinTech sector, Mauritius has been since the year 2016 been engaged in various endeavours to promote the development of this industry. Nevertheless, the implementation of internet technology and digitalisation of the financial services sectors such as online payment, wealth management, insurance, virtual currency or peer-to-peer lending are likely to cause significant regulatory issues. Hence, it is against this background that the study intends to assess the legal framework with the view of determining whether the existing laws of Mauritius are effective in addressing the challenges that emerge from the rapid growth of FinTech. The research will focus only on data protection as a matter of regulatory concern. The method used for the research is in essence comprised of the black letter approach whereby analysis is made on the laws of Mauritius to assess their effectiveness in tackling new challenges posed by the FinTech sector in relation to data protection. In line with that, the related laws of some other jurisdictions will be examined with a view to seeking recommendations that may be of use to Mauritius stakeholders. Finally, the doctrinal approach will be used so as to critically analyse studies carried out by eminent scholars on the legal issues of FinTech. The paper aims at responding to the research objective set out above. In particular, it is recommended that an amendment to Mauritius laws is necessary in order to create a legal framework that will be more conducive to protect various stakeholders concerned in the FinTech sector. Principally, the Mauritius Data Protection Act 2017 and the regulatory framework will need to be revised in order to promote Mauritius as a sound and attractive investment and business centre. In addition, common consensus agrees that FinTech entails the risk of cybercrimes and money laundering. As such, future scope of research can be focused on the effectiveness of cybercrimes laws as well as anti-money laundering laws in Mauritius in addressing the aforementioned challenges further to the emergence of the FinTech industry in the country. This study is amongst the first research conducted that assesses the efficiency of data protection laws in the context of the FinTech industry.*

Keywords: Fintech, Online Technology, Financial Technology, Mauritius
Research Area: Privacy Law
Paper Type: Research Paper

1. INTRODUCTION

Rapid technological development has resulted in an unprecedented evolution of the financial technology (**FinTech**) industry including innovation in mobile payments, blockchain, digital currencies, distributed ledger technology, peer-to-peer lending and

marketplace lending (Milanesi, 2018). FinTech has, in turn, created various business models as well as consumer needs which affect various aspects of the economy including payment systems, the banking industry and financial regulations (Salmony, 2014). Consequently, in order to fill the gaps of the traditional financial markets emanating from the digitalised FinTech sector, new electronic services are being established to provide consumers with ease of use, high transaction speed and a wide choice of service providers (Truong, 2016). For instance, Gonzalez (2004) states that the FinTech industry has experienced a phenomenal growth following the introduction of the World Wide Web, the online payment gateway PayPal and the digital currency BitCoin.

Contrary to the conventional banking system, most FinTech innovation is largely driven by non-banking institutions such as venture capital-backed FinTech startups, emerging companies and non-traditional providers such as Oracle and Apple. As a result of the boom of the FinTech industry, studies conducted by Pejkovska (2018), Bourdon (2017) and Truong (2016) demonstrate that FinTech has favoured customers in providing a more client-centric and interactive approach to financial and banking services. FinTech also enables a better understanding of client's needs which helps in designing new personalised products and services. In addition, FinTech enables the use of digital tools that helps to collect and integrate structured and unstructured data which are used to enhance value creation, risk management and decision-making process of the service provider. Also, by widening data networks, a broader segment of the global population is having access to liquidity as well as banking and financial services from the emergence of the FinTech sector.

However, despite the fact that entities involved in the FinTech are engaged in the provision of financial and/or banking services, they usually operate in an unregulated or relatively lightly regulated environment (Milanesi, 2018). Hence, the rise of the FinTech sector has drawn the attention of the banking and financial regulators. Notwithstanding the numerous benefits drawn from FinTech, studies conducted by (Arner, 2018) and Ng (2018) demonstrate that development in FinTech brings a number of risks and complications in terms of privacy, consumer protection, transparency and cybersecurity. As such, the focus of regulators across the globe is geared towards creating an environment that is conducive to financial innovation whilst at the same time, protecting markets, customers and investors. It is therefore vital to align existing laws and regulations with the new trend of the digital economy to address both the opportunities and challenged presented by FinTech. Thus, it is against this background that this study intends to assess the legal framework of Mauritius, a country that has been engaged in various endeavours to promote the FinTech industry, with the view of determining whether the existing laws are effective in addressing the challenges that emerge from the rapid growth of FinTech. The research will focus only on data protection as a matter of regulatory concern.

The method used for the research is in essence comprised of the black letter approach whereby analysis is made on the laws of Mauritius to assess their effectiveness in tackling new challenges posed by the FinTech sector. In line with that, the related laws of some other jurisdictions will be examined with a view to seeking recommendations that may be of use to

Mauritius stakeholders. Finally, the doctrinal approach will be used so as to critically analyse studies carried out by eminent scholars on the legal issues of FinTech.

The research paper is structured as follows: the first part has introduced the concept of FinTech and has provided a brief description of the benefits and the associated risks of FinTech. The research objectives and research methodology have also been elaborated on in this part. The second part of the paper will analyse the evolution of the FinTech and will review some existing literature on the challenges and threats of this sector. The third part of the paper will examine the European Union (**EU**) laws with respect to data protection. The fourth part of the research will discuss the development in the data protection laws in Mauritius and will assess the effectiveness of related laws to accommodate the new trend brought by the FinTech sector. The final part will conclude the paper and bring in some recommendations for Mauritius stakeholders based on the comparative study conducted in order to revise Mauritius laws to create a win-win situation for FinTech businesses, customers and regulators.

3 THE FINTECH MARKET AND CHALLENGES

2.1 The Emergence of FinTech

The world has witnessed an ever-increasing number of people using new technology for their financial transactions such as online banking, smartphone payment, online trading platform amongst others. It is therefore imperative to be aware of the origin of FinTech. Truong (2016) states that FinTech is originated from the invention of the printing press that allowed countries to print paper currency notes. Furthermore, in 1866, the invention of the telegraph and the successful installation of the first cable line trans-Atlantic was a huge contribution to the globalisation of the financial system. The Telegraph was used in 1918 which operated the Fedwire Funds Service to transfer money between banks. Since then, the system of money transfers continued to evolve until the early 1970s (Zerucha, 2016).

In 1950, the Diners Club invented the credit card which is one of the most utilised FinTech product. This invention has paved the way for the development of other technology products such as the Automated Teller Machines (ATMs) in 1960. During the same year, the first electronic online platform Quoton was created to support brokers and announce the pricing of the stock market. In 1966, the global Telex network was developed to create a framework for the long-term emergence of FinTech. Thereafter, the Clearing House Interbank Payment System has contributed towards the implementation of an online payment system and in 1970, the first electronic stock trading market became operational.

Consequently, all the banks, financial headquarters, trading centres and offices were using the new technologies. Yet, the use of such technologies was not common to those outside the industry. It is only when the E-Trade Model was developed in 1982 that the public has started to understand the importance and necessity of new technology. In addition, the FinTech sector has boomed mainly because of the invest in internet technology in the 1990s. This has led to the emergence of the e-commerce model, online stock-brokerage services as well as online banking. In addition, FinTech has brought along a new dimension to the global financial sector further to the invention of PayPal, eBay or other financial

support applications through smartphones that allow online purchases and payments without the need to physically travel to banks or ATMs.

Financial institutions are increasingly seeking opportunities to adopt FinTech in order to improve their own efficiency, reduce their operating costs and offer a wider range of products or services. To support this statement, the Global FinTech Report issued by Pricewaterhouse Coopers (PwC) (2017) has found that 82% of financial institutions expect to increase their partnerships with FinTech firms within the following five years. While this sector is client-oriented and has numerous benefits, FinTech is not without risks.

2.2 Challenges of FinTech

A number of plausible reasons exist which justifies people's willingness to resort to FinTech methods such as the adoption of blockchain, cryptocurrencies, alternative payment solutions and FinTech investments as well as banking services. For instance, Pejkovska (2018) argues that using blockchain and cryptocurrencies reduces the costs associated with financial services. Common consensus also agrees that the idea of a digitalised financial system that is free from intermediation is appealing since past records show that financial intermediaries are sometimes not trustworthy and are too ambitious to take up risky projects that they could not handle (Goyal and Joshi, 2012).

Nevertheless, the FinTech industry is not free from risks and threats which may have a negative impact on the economy of a country if not adequately addressed. The adverse effects of FinTech may be felt due to the lack of appropriate legal and regulatory framework because practically all the rules and regulations are tailored to the operations of the traditional financial services or banking transactions. In this respect, FinTech companies are not legally recognised and are free to operate as they please even if the business activity is not within legal limits. For instance, a study conducted by Athey et al. (2016) showed that the Bitcoin has already been used as a means of payment to purchase drugs and illegal weapon on dark-web platforms. Due to the anonymous features of Bitcoin, neither the culprits could be identified nor the origin and destination of the transactions could be traced. The nature of FinTech, therefore, makes it easier for people to commit financial crimes such as money laundering. Consequently, such actions may reduce the general public's trust in the regulatory sector of a country and may even tarnish the reputation of the country.

Amongst the major threats of FinTech are the violation of cybersecurity and data privacy. Ng (2018) states that a common source of weakness of FinTech transactions is that the computerised interfaces between and amongst the parties to the same transaction are not the same. This is because the two or more systems have not been designed at the same time and by the same developers which in turn pose compatibility issues and risks to security. Consequently, when connecting the distinct systems, software engineers do not have access to how the other system works and vice versa, making it harder to thoroughly detect all potential sources of vulnerability. This provides a leeway for hackers and cybercriminals. In addition, the proliferation of connected devices and the growth of cloud computing technologies have increased the number of potential entry points for hackers. A study conducted by Barber (2016) found that in the UK during the year 2016, the country lost 2.5

Million Pounds Sterling due to online crimes involving banking, credit accounts while 1 Million Pounds Sterling involved other types of fraud such as online shopping. The study further demonstrated that one in 10 adults has been a victim of a cybercrime. In addition, when a FinTech company becomes a victim of a cybercrime, it faces serious consequences such as loss of revenue and damage of the entity's reputation.

Coupled with the risks of cybercrime, the evolution of FinTech also pose a significant threat to data privacy. Online transactions require the collection of large amounts of data about customers including personal information and financial records. This can be risky if the appropriate safeguards are not put in place. Prescott and Larose (2016) explain how a FinTech start-up under the name of Dwolla was found guilty of infringement of data privacy in the US. Dwolla assured their clients that their data was safe but when a cyber attack corrupted their online system, the company had put at stake the financial and private information of its clients. The US Consumer Financial Protection Bureau then issued a security enforcement action against Dwolla because it found that the company's representations to its consumers about its cybersecurity misleading. As part of the sanctions, Dwolla had to pay fines, take the necessary steps to improve its data security and make accurate representations to customers. Hence, the consequences of a breach of data may have long-lasting effects such as reputational damage.

Another increasing trend that has been observed is that FinTech firms are starting to collect alternative data that is, gathering information on a customer's online spending behaviour and social media patterns to trace their digital footprint. This data is in turn stored and used for devising business strategies to determine a customer's risk profile. This begs the question as to whether customers are aware that their online behavioural data is being harvested, or if they have the ability to give or withdraw consent at any time. In such cases, legal questions arise with respect to data ownership and if the information can be shared with third parties. It is, therefore, necessary for FinTech firms to establish comprehensive and adequate privacy terms to provide assurance to customers that data privacy laws are not being infringed.

In addition to the above-mentioned risks, Ng (2018) has identified the regulatory challenges of FinTech. In other words, regulators are finding themselves to adopt new tools to have an oversight of this new industry and to control the operations of FinTech firms without however jeopardising innovation in technology. In addition, there is a need for regulators to understand the technical functioning and sophisticated nature of the FinTech sector to help them design adequate protection policies. Likewise, amendments to the Know-Your-Client (KYC) and compliance procedures have to be tailored to accommodate the digitalised nature of FinTech. For example, countries such as the UK has introduced regulatory technology to use new technologies to facilitate the delivery of regulatory requirements.

In the context of Mauritius, Oozeer (2017) states that the law is unclear with regard to the supervision and regulation of FinTech operators. In Mauritius, the two main supervisory bodies are the Financial Services Commission (**FSC**) and the Bank of Mauritius (**BOM**). While the FSC is the regulator for businesses that operate in the non-banking financial sector

and in the global business sector, the BOM regulates and supervises financial banking institutions. In the absence of specific law on this subject, the nature of FinTech makes it difficult to say with certainty which of the two regulators would assume the supervisory role over FinTech entities. However, as Dillon (2017) stated that the FinTech industry in Africa and in Mauritius is still at an infant stage. Therefore, it is preferable that the country does not adopt a prescriptive approach to regulation to give FinTech operators sufficient time to focus on their own businesses rather than to follow rigid rules and regulations. From this perspective, the Mauritius government has introduced the regulatory sandbox regime in the Investment Promotion Act of Mauritius in 2016, a licence that is issued by the Economic Development Board to help firms develop their products in a safe and lighter regulatory environment.

4 DATA PROTECTION LEGAL PROVISIONS IN EUROPE

4.1 The GDPR

The high adoption rate of information technology by people has led to an explosion of data. This is because new technologies enable greater storage capacity at a reduced cost and consequently, updated resources are being introduced to use more and more data. For example, in an attempt to create information and harness knowledge, online service providers are making use of a new technological trend being big data. That trend works with an inferred probability rather than focusing on accurate and precise data. For instance, Google uses the PageRank algorithm for its search engine to display the most relevant results based on probability. Apart from big data, banks, trading or investment entities are making use of data provided by customers for other purposes. In other words, with the explosion of data, it means that there is much data to work with (Reijers, 2016). This helps in designing statistical models to find patterns and correlations in data. With that information, companies are able to develop better business models.

However, the above explanation on the use of data by FinTech entities demonstrates that such systems have vulnerabilities and therefore requires control to stabilise the system. Consequently, in an attempt to align data protection laws with the current technological trend, the EU has come up with the introduction of the General Data Protection Regulation (**GDPR**) and the Payment Services Directive 2 (**PSD2**).

With the view of harmonising data privacy laws across Europe, the EU parliament approved the GDPR on 14 April 2016. It was enforced on 25 May 2018 and all concerned entities have to comply with the GDPR failure of which will attract fines and penalties. The GDPR replaces the 1995 EU Data Protection Directive 95/46/EC and imposes strict new rules on controlling and processing personally identifiable information. Compared to the 1995 EU Data Protection Directive, the GDPR is in the form of a regulation rather than a directive. As such, national legislation is needed to translate the directive into domestic law. Apart from the difference in the type of legislation, the GDPR demarcates from the previous EU Data Protective Directive in the following aspects: the scope, a conscious opt-in consent model, the introduction of the data protection officer, a data breach notification and the right to be forgotten. In terms of the scope, the GDPR applies to all entities holding and processing EU resident's personal data regardless of geographic location. Hence, a FinTech organisation

from the United States that processes the personal data of a European citizen falls within the ambit of the GDPR. In addition, to cater for the increased prevalence of personal information further to the introduction of FinTech, the regulation has provided for the conscious opt-in consent. Opt-in, as the name suggests refers to the fact of explicitly choosing to take part in an activity rather than being forced to take part. The regulation, therefore, requires customers to explicitly authorise companies to process their data instead of giving an implied consent by remaining passive.

The GDPR has also made it compulsory for the entities concerned to appoint a Data Protection Officer (**DPO**). More precisely, an organisation will have to appoint a DPO if it carries out bulk processing of special categories of data or monitoring of individuals such as behaviour tracking or is a public authority. Although the DPO is appointed by the organisation, he/she is an independent officer from the company and is not governed by the executive board but rather by the competent national authority of the respective country.

Furthermore, due to the rising number of data breaches, the GDPR has incorporated provisions on notification requirements for data breaches. That is, companies have the legal obligation to inform customers and the national data protection regulatory body cases of breach of data. This dissemination will help customers to know what went wrong and thus, they have the ability to act on it. For example, customers can change their passwords to prevent further unauthorised access. Moreover, notifying the regulator will enable the latter to either choose to impose sanctions or to incorporate the lessons learnt from the incident and take the appropriate remedial actions such as updating policies and guidelines.

Additionally, to reinforce information privacy rights, the GDPR provides customers with the right to be forgotten. Consequently, customers are entitled to request for the erasure of personal data to companies that hold such data. This right has been legislated further to a ruling held by the EU Court of Justice in the case of *Google Spain v. AEPD and Gonzalez*. In the case, Gonzalez was asked to Google Spain to remove data relating to him from the search engine because the data was no longer relevant. However, Google Spain did not want to entertain the request on the grounds that Google was not within the scope of the EU Data Protection Directive of 1995. The EU Court of Justice considered the duties and obligations of the operator of a search engine and highlighted Article 7(f) of the EU Data Protection Directive which stated that it is vital to strike a balance between the processing of data and respecting the rights and interests of the data subject being Gonzalez in the case. The outcome of the judgement was that an internet search engine must consider requests from individuals to remove links concerning themselves where such information appears to be inadequate, irrelevant or excessive in the current time. Hence, the right to be forgotten that is included in the GDPR was inspired by this court's ruling.

4.2 The PSD2

In 2002, the EU had faced severe political pressure to establish a more efficient European payment system. Given the fact that expenses on European payments were increasing, European banks decided to develop a European wide sole market under the name of Single European Payments Area (**SEPA**) with the aim of reducing costs for both

international and national payments. The PSD1 was, therefore, introduced to regulate the SEPA and each EU member state had to develop the PSD1 into their national laws. The PSD1 provided the legal rules applicable to all payment services in the SEPA countries and included a framework for supervising all parties delivering payment services. However, over the years, some issues cropped up with PSD1 such as the directive covered only European countries. As a result, payments made to and from countries outside the EU were still slow and expensive compared to pan-European payments. Also, PSD1 entitled EU member states to promote or discourage customers from certain payment methods. This created inconsistencies in the system in the case where one country promoted direct debit transfers whilst another country encouraged credit card transfers. Furthermore, the emergence of online trading and FinTech have given rise to new types of third-party service providers that are not covered by the PSD1. Additionally, an impact study of the PSD1 was made in 2013 revealed that the terms of services that are applicable to payment services under PSD1 could be considered as silent consent. This would allow companies to use customer's data for any purpose without having the obligation to inform the respective customers.

Hence, to address the above-mentioned shortcomings of PSD1 and to accommodate new changes brought by the digital world, PSD2 was introduced and formalised in 2015. EU member states were required to change their domestic legislation to align with the new directive and they were given a two-year period to carry out the amendments. One of the main highlights of PSD2 is the regulation of access to financial accounts of customers through the use of a third party either for acquiring payment information or for payment initiation. A third party service provider is one who is not directly controlled by either the seller or a customer in a business transaction (Law Insider, 2018). Examples are PayPal or Google Analytics who are used by online sellers because they save time and money, reduce risk and complexity and increase the ease of use and reliability of the seller's logistics. In this regard, PSD2 extends the scope of its application in relation to payment services to include new non-banking operators as compared to only banking institutions as provided for under PSD1. However, during business dealings, these parties have access to a wide pool of personal data pertaining to all the parties to the transaction. As such, with the view to reinforce the protection of personal data, PSD2 provides that customers can do business with only two types of third party service providers which are as follows:

i. providers that can access customer account data with the customer's consent (also known as account information service providers), or

ii. providers that can initiate payments on behalf of the customer with the customer's consent (also known as payment initiation service providers).

Furthermore, the European Banking Authority (**EBA**) has been appointed as the competent authority on a European level for third-party service providers. Hence, by legally providing for third parties service providers with whom customers can deal and by placing such service providers under the scrutiny and supervision of the EBA, the payment system of the EU is more regulated. In addition, Article 23 of PSD2 empowers the EBA with the legal capacity to intervene and impose penalty or punishment on entities in breach of PSD2 to prevent future incidents from occurring. Also, the new PSD2 obliges banks to cooperate

when the third party service provider requires client's banking information to effectuate a transaction once the customer has given his consent (Article 67 and 94 of PSD2). In that respect, the new directive elaborates on the circumstances in which access to such type of information is allowed and sets out the rights and obligations of both parties, being the third party service provider and the bank.

In matters concerning data protection, the PSD2 states that the processing of personal data by a third party service provider has to be carried out with the applicable data protection directive of EU. In particular, the consent of customers is required to process personal information and the service provider needs to have a clear and precise purpose for collecting and using the data. However, the PSD2 provides a specific exemption when it comes to fraud monitoring. More precisely, PSD2 enables the processing of data for the purpose of reducing fraud without the need to inform customers or obtaining their consent.

Another challenge threatening data privacy is the increased prevalence of cybercriminals. The establishment of service providers on the online platform that has the ability to deal with personal data stored by payment institutions to process payments, provide a new target for criminals to focus on. Hackers take advantage of any shortcoming in the online platform that allows access to personal information. For example, they may leverage the advertisement campaign of a service provider to initiate a spread of phishing emails and try to persuade customers to submit their personal details, and in turn, the cybercriminals will commit fraud from such information. In order to reinforce the security system of the service providers, PSD2 has placed a strong emphasis on customer authentication. In particular, Article 97 of PSD2 defines solid customer authentication as two-factor authentication. That is, either a third party service provider should arrange authentication itself for its services or is allowed to use the authentication method of the banks, redirecting the customer to the bank for authentication. Further regulatory technical standards are being developed by EBA to help service providers and banks to put in place control instruments on customer authentication.

5 MAURITIUS LEGAL FRAMEWORK ON DATA PROTECTION

In Mauritius, data protection and information privacy are regulated by the Data Protection Act of 2017, Act No. 20 of 2017 (**DPA**). The DPA was enacted in 2017 to repeal the previous DPA of 2004 in order to provide for new legal provisions strengthening the control and personal autonomy of data subjects over personal data in line with current relevant international standards. The new DPA came into effect on 15 January 2018.

The DPA of 2004 was no longer appropriate to the digital context, a booming sector in Mauritius (Virahsawmy and Boodhonee, 2018). Consequently, the DPA was enacted to align with the GDPR since the GDPR is relevant for Mauritius due to its extra-territorial applicability. In principle, the GDPR applies to every data controller, data processor and data subject regardless of its location that processes EU citizen's and resident's personal data. In addition, one of the particular characteristics of the GDPR is that EU citizen's personal data will not be transferable to a country that does not have similar regulation as the GDPR. For example, the GDPR will apply to both an EU university and a Mauritian university that collects the personal data of an EU citizen or resident wishing to enrol for a course. Hence,

without aligning data protection laws that are similar to the GDPR, the Mauritius university will not be able to collect data of the EU citizen or resident.

The DPA is structured in nine parts ranging from:

a) Preliminary section – which sets out the definitions of the terms used in the DPA and it also elaborates on the scope of application of the said act.

b) Data Protection Office – provides for the establishment of the data protection office in Mauritius that acts as a regulator for matters concerning data protection and privacy in Mauritius. This section also described the functions and powers of the commissioner of the data protection office.

c) Registration of controllers and processors – provides for application procedures for a person to be allowed to process personal data and the particulars of the registration certificate.

d) Obligations on controllers and processors – regulates the use of personal data by controllers and processors, the requirement to implement technical and organisational measures such as the appropriate data security, record keeping of all processing operations, notification procedures in case of breach of personal data, duty to destroy personal data, categories of personal data amongst others.

e) Processing operations likely to present risk – sets out provisions on data protection impact assessment and the need to obtain the authorisation of the data protection commissioner to process data where high risks are involved and to provide for a framework to mitigate the risks involved.

f) Transfer of personal data outside Mauritius – provides for the procedures for a data controller or processor to transfer data to another country under certain specific circumstances.

g) Rights of data subjects – elaborates on the rights of persons who can be identified and whose data are being stored and processed.

h) Other offences and penalties – provides for penalties if a data controller or processor has unlawfully and without excuse disclosed personal data in a manner that is contrary to the DPA.

i) Miscellaneous – sets out some other provisions relating to the affairs of the data protection office namely on the annual report, compliance audit, the power to issue codes of practice and guidelines of the data protection commissioner, certification, confidentiality and oath.

Given the increasing number of cross-border transactions conducted in or through Mauritius, the Mauritius legislator has reformed the legal regime of data protection further to the enactment of the new DPA. For instance, compared to the DPA of 2004, new rights have been conferred on data subjects. The latter now have the right to request a copy of their personal data which is being processed by a data controller free to charge and in an intelligible form. Another protective measure extended to data subjects is the possibility to request data controllers who have made the personal data of the data subjects public to take reasonable steps to erase information concerning the data subject. In addition, the new DPA affords greater protection to minors. In essence, it is now mandatory to obtain the consent of the parent or guardian of a child under the age of 16 before processing the child's personal data. Also, a data subject has the right to withdraw consent at any time for the processing of

his or her personal data and this will not affect the legality of the processing based on consent before the withdrawal.

Simultaneously, the new DPA has imposed additional obligations on data controllers. For example, under the previous DPA of 2004, there was no legal requirement to ensure whether the appropriate safeguards are in place when personal data is being transferred to another country. However, the DPA of 2017 now imposes a responsibility on data controllers to provide evidence that the country to which personal data is being transferred, has adequate protection to protect the information. Furthermore, a data controller has the duty to report any case of breach of personal data to the data protection commissioner within 72 hours of becoming aware of the breach. Another innovation brought by the DPA 2017 is the duty to conduct data protection impact assessment. In particular, if processing operations are likely to result in high risks to the rights and freedoms of data subjects by virtue of their scope, nature, purposes and context, every controller or processor has to, prior to the processing, assess the impact of the envisaged risks. Thereafter, the data controllers will need to establish the appropriate measures to address such risks.

In addition to new provisions on rights and obligations, the new DPA 2017 has also laid emphasis on data security. Modern concepts such as "pseudonymisation" and "encryption" have been included in the said act with the view of providing more security to data subjects. "Encryption" is defined in the DPA as the process of transforming data into coded form while "pseudonymization" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual. Thus, in devising the methods of processing data and during the process, a data controller or processor has to do the following:

i. establish security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss of, and destruction of the data in his control, and

ii. ensure an appropriate level of security for the harm that may result from unauthorised access to, alteration of, disclosure of, accidental loss of, and destruction of the data in his control and the nature of the data concerned.

In doing so, section 31(2) of the DPA 2017 provides that the data controller or processor may resort to the following security and organisational measures that include:

(a) the pseudonymisation and encryption of personal data,
(b) the ability to ensure ongoing confidentiality, integrity and availability,
(c) the resilience of processing systems and services,
(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
(e) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Further to the reform of the data protection laws, it has been observed that the Mauritius legislator has taken laudable steps to align the DPA with the GDPR. Yet, the strict

penalty provisions under the GDPR have not been replicated in the DPA of 2017. Under the GDPR, a data controller convicted for a breach of GDPR may be fined an amount equivalent to the higher of 4% of its worldwide annual revenue or EUR 20 Million whereas under the DPA, the maximum penalty is approximately EUR 5,000 (MUR 200,000) and a term of imprisonment not exceeding 5 years.

Additionally, the reform has not considered the security safeguards for the protection of personal data when making payments on an online platform. The emergence of the FinTech sector implies extensive use of internet technology for money transfers that involve the following parties: the customer, the seller, the third party service provider and the bank. Granting access to third party service providers to financial information of customers may be risky since such parties may not always require the consent of customers given that these parties are classified as "data controllers". A data controller is defined in section 2 of the DPA as a person or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to that processing. While section 28(1)(a) of the DPA states that no data controller can process personal data if the data subject has not given his or her consent, section 28(1)(b) of the same act carves out the need to obtain consent where processing is required in numerous circumstances, amongst which are:

i. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; and

ii. for the legitimate interests pursued by the data controller or by a third party who whom the data are disclosed.

In essence, if a customer wishes to carry out a payment transaction with a third party service provider, the latter needs to access to the customer's personal information relating to their payment account in order to perform the contract, that is, initiating the payment. As such, there is no need to obtain customer's consent for the associated data processing operations. Viewed from another perspective, processing payment is likely to result in a high risk to the rights and freedoms of data subject by virtue of the nature, scope, context and purpose of such type of transaction. Yet, third-party service providers are using personal information of customers to process payment without obtaining express consent from the latter. This loophole in the DPA needs to be addressed on an urgent basis given the rapid growth of FinTech in Mauritius. Additionally, third-party service providers operate through an online system and if the appropriate cybersecurity mechanisms are not in place, the platform will attract cybercriminals who will in turn gain access to the personal data of customers and may even act on their behalf. Hence, the appropriate safeguards have to be established to ensure a customer's identity are not usurped.

6 CONCLUSION

The FinTech industry is experiencing a boom across the globe. Despite the numerous benefits derived from this sector such as a reduction in the cost of trading and the provision of a quick payment solution, the FinTech industry is not free from challenges. This study has focused on data protection and privacy issues arising from FinTech. It has been observed that without an appropriate legal framework and appropriate safeguards established, firms

engaged in FinTech are at risk for data privacy infringement. Besides that, customers are being victims of cyber attacks and usurpation of identity due to unauthorised access to their personal details. To tackle these issues, the EU has updated its legal and regulatory regime with the aim of harmonising data protection laws in Europe. This study has discussed the GDPR and the PSD2 as innovative legislation to accommodate the digital economic transaction. The scope, application and legal provisions of each of GDPR and PSD2 have been examined in this paper.

On a national level, in its quest to promote Mauritius as a FinTech hub for Africa, the Mauritius government is actively working with key stakeholders including industry experts, technology vendors and regulators. In this respect, one amongst the various initiatives has been the recent reform of data protection laws in Mauritius with the enactment of the DPA in 2017. The said act has been aligned with the provisions of the GDPR due to the extra-territorial applicability of the said regulation. The main changes brought to the new DPA have been discussed and analysed. However, it has been seen that the DPA has not aligned the penalties provision to that of GDPR. In particular, the DPA imposes less lenient sanctions on data controllers and processors than the GDPR. Furthermore, due to the carve-out provisions under which the consent of data subject is not required, the DPA allows third-party service providers to gain access to personal data of individuals without obtaining explicit consent from the latter even when the processing of operations appears to be risky. Consequently, the aforementioned challenges have to be addressed urgently to boost all stakeholder's confidence in the FinTech sector.

6. RECOMMENDATIONS

Based on the comparative study conducted for this research, some recommendations to accommodate the legal framework for data protection laws that is conducive to the FinTech industry are hereby suggested:

- the penalties provided for under the DPA needs to be made more strict to prevent the illegal use of personal data, for instance, the related DPA provision can be aligned with those of GDPR;
- the provision the PSD2 requiring banks to obtain express consent from customers before releasing information to third party service providers has to be provided for in the DPA when making payments and to that effect, the carve-out provision exempting the need for consent of data subject has to be limited;
- article 97 of the PSD2 which provides for a two-factor customer identification to be established by the third party service provider needs to be replicated in the DPA;
- Mauritius laws need to explicitly provide for the types of third-party service providers customers can deal with and then the names of service providers have to be recorded in a public register; and
- third-party service providers should be regulated by an appropriate authority in Mauritius in order to monitor and supervise the payment system in the country.

The above-mentioned recommendations are inspired only from new developments made by the EU in the context of data protection law and are thus non-exhaustive. This study has considered only one challenge of the FinTech sector amongst many other associated risks. Further scope of research may be conducted may be undertaken on the risks of money laundering and on finding ways to accommodate the changing trend brought by FinTech.

REFERENCES

Arner, D. W. 2018. "FinTech and RegTech: Opportunities and Challenges" [Online]. Available at http://www.law.hku.hk/aiifl/wp-content/uploads/ppt/JFR-Arner_Douglas_ppt.pdf [Accessed on 1 November 2018].

Athey, S., Parashkevov, I., Sarukkai, V. and Xia, J. 2016. "Bitcoin pricing, adoption and usage: Theory and evidence" [Online]. Available at https://siepr.stanford.edu/sites/default/files/publications/17-033_1.pdf [Accessed on 1 November 2018].

Barber, L. 2016. "Banking fraud is the biggest cybercrime in UK" [Online]. Available at http://www.cityam.com/245946/banking-fraud-biggest-cyber-crime-britain [Accessed on 1 November 2018].

Bourdon, C. 2017. "Analysis of the FinTech ecosystem: what regulatory and corporate responses could foster the innovation whilst not threatening the financial stability and the consumer's interest?" [Online]. Available at http://arno.uvt.nl/show.cgi?fid=143635 [Accessed on 1 November 2018].

Dillon, A. 2017. "Unlocking capital between Africa and Asia". *Mauritius International Financial Centre*. Vol. April 2017, Issue 5.

European Commission. 2013. "Study on the impact of directive 2007/64/ec" [Online]. Available at http://ec.europa.eu/internal_market/payments/docs/framework/130724_study-impact-psd_en.pdf [Accessed on 2 November 2018].

Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez [2014] Case C-131/12.

Goyal, K. and Joshi, V. 2012. "Indian Banking Industry: Challenges and Opportunities". *International Journal of Business Research and Management*. Vol. 3, Issue 2.

Law Insider. 2018. "Definition of third party service provider" [Online]. Available at https://www.lawinsider.com/dictionary/third-party-service-provider [Accessed on 4 November 2018].

Milanesi, D. 2018. "The rise of FinTech innovation and the future of the banking and financial system: A comparative analysis of the fintech legislation and regulatory frameworks in the US, Europe and the UK" [Online]. Available at https://law.stanford.edu/projects/the-rise-of-financial-technology-fintech-innovation-and-the-future-of-the-banking-and-financial-system-a-comparative-analysis-of-the-fintech-legislative-and-regulatory-frameworks-in-the-united-stat/ [Accessed on 1 November 2018].

Ng, C. 2018. "Regulating FinTech: Addressing challenges in Cybersecurity and Data Privacy" [Online]. Available at https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy [Accessed on 1 November 2018].

Pejkovska, M. 2018. "Potential negative effects of Fintech on the financial services sector" [Online]. Available at https://www.theseus.fi/bitstream/handle/10024/148416/Maja_Pejkovska_Theseus.pdf?sequence=1&isAllowed=y [Accessed on 1 November 2018].

Prescott, N. and Larose, C. 2016. "FinTech companies face big privacy challenges in 2016" [Online]. Available at https://blog.vcexperts.com/2016/08/09/fintech-companies-face-big-privacy-challenges-in-2016/ [Accessed on 1 November 2018].

PwC. 2017. "FinTech and Financial Services are coming together" [Online]. Available at https://www.pwc.com/jg/en/publications/fintech-growing-influence-financial-services.html [Accessed on 1 November 2018].

Reijers, J. 2016. "Payment Service Directive 2" [Online].

Available at https://www.ru.nl/publish/pages/769526/z_jos_reijers.pdf [Accessed on 2 November 2018.

Salmony, M. 2014. "Access to accounts: Why banks should embrace an open future". *Journal of Payments Strategy and Systems*. Vol. 8, Issue 2.

Truong, O. 2016. "How FinTech Industry is changing the world" [Online]. Available at https://www.theseus.fi/bitstream/handle/10024/123633/TRUONG_OANH.pdf?sequence=1 [Accessed on 1 November 2018].

Virahsawmy, M. and Boodhonee, V. 2018. "Mauritius updates its data protection legislation to be in line with GDPR" [Online]. Available at http://www.mondaq.com/x/686402/data+protection/Mauritius+updates+its+Data+Protection+legislation [Accessed on 2 November 2018].

Zerucha, T. 2016. "The history of fintech. Bankless Times" [Online]. Available at https://www.banklesstimes.com/2016/06/27/the-history-of-fintech/ [Accessed on 1 November 2018].