FINANCIAL REGULATORS AND THE NEED FOR DATA PRIVACY AND PROTECTION- ISSUES, OPPORTUNITIES AND CHALLENGES

Written by ***Hemant Garg***

Officer Grade A, International Financial Services Centers Authority, Gift City, Gujarat, India

ABSTRACT

To date, India does not have a data protection legislation that unlike its European counterpart, US, UK or UAE, where dedicated legislations are in force. India is also not a party to any convention on the protection of personal data except the Universal Declaration of Human Rights (UDHR) and The International Covenant on Civil and Political Rights (ICCPR), which recognises the Right to Privacy. With the increased digitalization and the consequent risk of data breaches across borders, the policymakers in India are constantly in the process of drafting water-tight legislation and policies to ensure adequate data protection and to prevent the breach of personal data. The recent developments such as the development of Cert-Fin and the IFSCA, Gandhinagar are in the process of inception but to what extent will they be able to safeguard the associated risks is a territory yet to be explored. This paper is an attempt to primarily focus on legislations in India and their comparison with the legislation abroad with a special reference to the financial regulators. Further, the Author tries to critically analyse the effectiveness of such legislations and proposed frameworks that the financial regulators came up with, followed by suggestions and recommendations which might serve as guidance in future.

Keywords: Cyber security, Financial Regulator, Cert-Fin, Personal Data, Information Technology Act

INTRODUCTION

In an era of rapid technological advancement that is paving the way for increased digitalisation, the territorial boundaries of nations across the globe have become virtual and practically insignificant. Various jurisdictions have resorted to digital means of routing financial transactions for their ease and efficiency, and with the cross-border investment regimes, the amount of transmission of financial data along with its processing and exchange is voluminous. While digitalisation paves the way for increased globalization, it is pertinent to note that data is the most risk-prone and a much-valued resource today, more than ever. The word is that oil is replaced as the most valuable resource on the earth by data[i], and therefore, the loss or breach of personal data can have severe consequences, especially in the financial context. Some of these consequences include credit card violations, server hackings and identity theft. While data breaches take place in almost all sectors, the financial sector is the most prone to such cyber-attacks as it is responsible for safeguarding large amounts of valuable personal data. The Financial sector is also recognised as one of the most critical sectors by various jurisdictions such as the European Union (EU), United States (US), United Kingdom (UK), India, among others, in their response against various incidents of data breaches and violations. Various jurisdictions are enacting data protection regimes that provide for the information that has to be protected and the consequences of the breaches thereof. On the contrary, India does not have a data protection legislation that specifically deals with the issue, unlike its European counterparts where EU General Data Protection Regulation[ii], US, UK or UAE where similar or equivalent regimes are in force. Reliance is also placed upon the fact that India is not a party to any convention on the protection of personal data except the Universal Declaration of Human Rights (UDHR) and The International Covenant on Civil and Political Rights (ICCPR), which recognises the Right to Privacy.[iii] The significant legislation which deals with the subject of data protection in India are IT Act, 2000 and Aadhar Act, 2016. Initially, the IT Act, 2000 principally did not take data protection and general privacy into consideration but pursuant to the IT Amendment Act[iv], Section 43A and Section 72A were introduced, which provide for penalties if a personal data breach takes place due to the negligence of a body corporate. IT (Reasonable Securities Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were also notified which govern data privacy. Similarly, the Aadhar Act, 2016[v] mandates that the entities in the regulated sectors are obligated to maintain the confidentiality of the personal information processed by them. It is not only the financial industries but also the industries across diverse sectors, running the risk of cyber-attacks. A recent example

includes the ransomware attack on the American Company called Colonial Pipeline Company which affected its computerised equipment that manages the pipeline that originates in Houston, Texas, causing a days-long disruption in the fuel supply to the majority of the US. Despite the fact that the breach affected its information technology systems, the Company had to immediately halt all pipeline operations to avoid further harm and also paid the hackers $4.4 million in bitcoin with the assistance of the FBI[vi]. Similarly, CNA Financial Corp., based in Chicago which is one of the largest insurance companies in the United States, discovered a breach in March this year. According to reports, the ransomware attack compromised the data of approximately 75,000 individuals. This information could have included the names, health benefit information, and Social Security numbers of current and former employees, contract workers, and their dependents of the company and according to some media reports the Company agreed to pay a whooping amount of $40 million to gain back the access to its network[vii].

With the increased digitalization and the consequent risk of data breaches across borders, the policymakers are constantly in the process of drafting water-tight legislation and policies to ensure data protection.

WHAT IS THE INDIAN SCENARIO?

The principal legislation dealing with Data Protection in India is the IT Act, 2000. Sections 43A and 72A introduced vide an amendment deals with the compensation in cases of a data breach on account of the negligence of the body corporate processing the personal data and also extends to the liabilities of financial institutions. Section 43A applies to a body corporate[viii] and, The Reserve Bank of India is a body corporate as defined under The Reserve Bank of India Act, 1934[ix]. The Information Technology *(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)* Rules 2011 notified under this Section 43A provides that *'Reasonable Security Practices and Procedures need to be maintained by each body corporate'* in compliance with the said section. Apart from these legislations governing the regulators, it must also be noted that financial regulators In India such as RBI and SEBI have also introduced their own guidelines to ensure cyber security in the economic space.

India's banking and finance regulator, the Reserve Bank of India ('RBI'), issued a series of comprehensive guidelines on *'Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds'* in 2011[x] to prepare Indian banks against emerging risks in the internet age. This was followed up by a mandate for comprehensive internal cybersecurity frameworks in the year 2016 titled *"Cyber Security Framework in Banks*, dated June 2 2016[xi]. By way of the 2016 guidelines, RBI emphasized upon the banks and financial institutions on adapting a robust cyber security/resilience framework to ensure adequate cyber security is in place against any threats. RBI further directed the banks to formulate a cybersecurity policy in order to combat cyber threats and seamless identification of the data that has to be protected. The circular also mandates the creation of a Security Operations Centre (SOC) for the purpose of continuous surveillance and mandates the financial institutions to develop a comprehensive data loss prevention strategy. RBI also issued *"Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services"* on November 9, 2017[xii]. These guidelines govern the risks associated with third party transmission of financial data. For example, Non-Banking Financial Institutions (NBFCs) might outsource activities that they undertake in due course of business to a third party. In that process, there is a transmission of huge amounts of data with the recipient party, which can expose the NBFCs to various risks and thus, the directions by the RBI requires the NBFCs to ensure protection of the confidentiality of the customer information. It mandates that the data provided to recipient party should only be on a "need to know" basis. The security practices adopted by the recipient parties also need to be assessed regularly, and in case any data leak takes place, then the NBFCs will have to report such leaks to the RBI immediately.

The RBI also introduced a Data Localisation Policy[xiii]. Data Localisation is a process in which the data relating to the citizens of a country are stored within the territorial boundaries of a country. The purpose of such restraint is to restrict the surveillance risks and/or data breaches from other countries. The circular mandating the application of this policy on all the authorized Payment System Operators (PSOs) was issued by the Reserve Bank of India on April 6, 2018. According to the policy, payment can be processed outside India, but after the payment is completed, the processed data on the foreign servers has to be deleted, and the data has to be brought back to India in not less than 24 hours from the processing of payment and the data has to be stored in India only. If the PSOs share the payment system data with overseas regulators, then prior approval from the Reserve Bank of India is required. If a transaction

involves a foreign entity and a domestic entity, then such cross-border transaction data can be stored in a foreign system, but the data relating to the domestic entity has to be stored in India only. The FAQs also addressed queries relating to the type of data that has to be stored in India, which includes but is not limited to customer particulars, customer account details, payment credentials etc.

Followed by RBI, the Securities and Exchange Board of India (SEBI) also devised a cyber-security policy framework titled *"Cybersecurity and Cyber Resilience Framework for Stock Brokers/Depository Participants and Mutual Fund/Asset Management Companies"*[xiv]. The said framework, among other issues, emphasised an urgent need to install strong encryption methods to be used by financial institutions for protecting sensitive personal data. It also recommends the adoption of the process of Data Masking by the institutions. Data Masking involves the modification of sensitive data in such a manner that it is of no use for anyone other than the authorized personnel. It also suggests that passwords and security pins should not be stored in plain text and further emphasizes that specific personnel should be identified to take care of these sensitive data, and discusses the effective transmission of sensitive information over digital and virtual networks.

While these and other frameworks have existed on paper for a long period of time, they have only recently been subjected to closer examination. This is unsurprising given the increasing disruption caused by cyber-attacks both directed at India and global phenomena such as Petya/NotPetya and WannaCry. Notably, in 2016, an attack on Indian banks resulted in the theft of over 3 million debit card numbers[xv]. The Government's response has included a proposal to establish an independent cyber-security agency dedicated exclusively to the financial sector, the Computer Emergency Response Team ('CERT-Fin'). The proposal was included in the Government's 2018 Budget and was recently approved by a Ministry of Finance working group[xvi]. CERT- Fin's responsibilities, according to the working group, would include passive functions such as threat intelligence sharing, vulnerability assessment, and analysis, as well as active functions such as 'bringing down rogue sites' and developing standards for data protection, encryption, and access rights[xvii].

The latest in line is the development of International Financial Services Centre Authority (IFSCA) which is a unified authority governing India's International Financial Services Centre (IFSC) for the development and regulation of financial products, financial services, and financial institutions. At the moment, IFSC is India's first international financial services

centre. Prior to the establishment of IFSCA, the IFSC business was regulated by the domestic financial regulators, namely the RBI, SEBI, PFRDA, and IRDAI[xviii]. On July 28, 2021, the Consultation Paper on the proposed International Financial Services Centre Authority (Capital Market Intermediaries) Regulations 2021[xix] was published, and public comment was invited. These regulations seek to establish a comprehensive regulatory framework for capital market intermediaries. Under these regulations, the registered capital markets shall be required to have robust cyber security and cyber resilience framework, with IFSCA issuing fresh requirements and reviewing the older ones for such framework on a periodic basis. This proposal is the latest in a series of moves by the Government to establish specialised agencies charged with addressing various facets of the cybersecurity conundrum.

WHAT ARE THE LEADING JURISDICTIONS UP TO?

EU General Data Protection Regulation:

The two most significant and far-reaching pieces of non-sectoral legislation affecting financial institutions in EU are the Directives on Network and Information Systems Security (NIS Directive) and the General Data Protection Regulation (GDPR), both of which were enacted in 2016. Among other things, the NIS Directive identifies the financial sector as one of seven critical infrastructure sectors for which EU member states must ensure an adequate level of technical and organisational security through specific critical infrastructure legislation. This includes a mandatory incident response regime for financial institutions[xx]. The GDPR, on the other hand, is one of the most-awaited and celebrated privacy regulations in the European Union, which seek to create a uniform framework handling personal information across the member states in the European Union. Financial institutions processing the data of European citizens are required to comply with the GDPR. The compliance requirements under GDPR are also applicable to financial institutions outside the jurisdiction of the European Union that, process the personal information of European Citizens. The non-compliance of GDPR attracts huge fines, and the larger institutions will be required to bear larger penalties.[xxi]

The United Kingdom:

The United Kingdom enacted the Data Protection Act, 2018 (DPA 2018), which is parallel with the GDPR. The Financial Conduct Authority (FCA) and the Bank of England are the lead

financial service regulators in the UK. It is important for the financial institutions under the regulation of the aforesaid authorities to comply with DPA 2018, and another legislation called Privacy and Electronic Communications Regulations 2003. It is significant to note that while The United Kingdom has left the EU, even then, the transmission of personal data takes place across the European jurisdictions, and thus, it was important for the DPA 2018 to be in line with the GDPR.

Monetary Authority of Singapore:

The Personal Data Protection Act, 2012 is the Principal Data Protection Regime in Singapore. It is pertinent to note that Singapore did not have specific legislation on the subject, but several sector-specific legislation or self-regulatory did exist which emphasised on Personal Data Protection.[xxii] The Compliance burden has increased as the sector-specific frameworks will continue to operate concurrently alongside the Personal Data Protection Act. The finance sector is the most prone to cyber-attacks, and thus, it is one of the most regulated sectors. The Monetary Authority of Singapore had issued Technology Risk Management Guidelines in 2013, which have been recently revised[xxiii]. In order for the financial institutions to be able to cope up with the worsening environment of cyber-threats, the revised guidelines aim to broadly classify the roles and responsibilities of the Board of Directors and its Senior Management so that they are able to handle the related tasks with utmost competency. The guidelines also aim to introduce stringent assessment for the third-party vendors before they get access to the Financial Institution's IT System. It also focuses on improving cyber surveillance by way of system and software development.

HKMA Hong Kong:

The Personal Data (Privacy) Ordinance (PDPO)[xxiv] is the main legislation in Hong Kong that protects the privacy of Individuals. It is pertinent to note that a circular titled "Consumer Data Protection" was issued by the HKMA in 2008[xxv] even before the implementation of PDPO. However, the changing technology and the increased cyber-attacks in the financial sector led to amendments in the previously issued circular. The revised circular mandates that the processed data should be classified on the basis of different levels of security risk involved for the determination of the protection required. It also suggests the financial institutions develop security frameworks and policies that should be in line with the relevant supervisory guidance

issued by HKMA from time to time. The institutions are also mandated to conduct periodic audits on the adequacy and the compliance status of their controls on consumer data protection.

United States:

To ensure the stability of the Nation's banking system, federal banking regulators (the Office of the Comptroller of the Currency, the Federal Reserve, and the Federal Deposit Insurance Corporation) are required to promulgate safety and soundness standards for all federally insured depository institutions. Several of these standards address cybersecurity concerns, such as data security, data breaches, and the destruction or theft of business records. The Office of the Comptroller of the Currency (OCC) is the chartering authority and primary federal regulator of national banks and federal savings associations, and it imposes cybersecurity requirements on the institutions it regulates and their service providers through general authority granted by organic legislation. The OCC was established by Congress to charter and supervise national banks. Federal securities regulators (the Securities and Exchange Commission and the Commodity Futures Trading Commission) have also asserted authority over various aspects of cybersecurity in securities markets and their participants. This includes requiring publicly traded financial and non-financial companies to file annual and quarterly reports that include material information for investors, which may include information about cybersecurity risks or breaches[xxvi].

RECOMMENDATIONS AND SUGGESTIONS

There are several fundamental discrepancies rooted in data privacy and the associated risks in the context of financial regulators in the Indian scenario. By now, it is clear that the concept of privacy as a fundamental right is a fairly new concept in the Indian concept, and the testimony of the same is the law laid down in *K.S. Puttaswamy and Anr. vs The Union of India*[xxvii] confers the Right to Privacy as a fundamental right. The judgment was only delivered in 2017 however, before that, there seems to be little or no trace of the concept of privacy being associated as a fundamental right. Contrarily, in jurisdictions like US or UK, the concept of privacy existed much earlier. The first data privacy dedicated legislation was enacted in the UK in the year 1984 while the USA witnessed privacy revolutions as early as during the Second World War. This delay in the inception of the concept of privacy explains the shortcomings and the lack of efficiency in current regimes.

Urgent need for independent legislation:

To date, the data privacy and cyber security as a collaborative concept is governed by the IT Act, 2000 and India doesn't have a dedicated Data Privacy legislation. While the Personal Data Protection Bill, 2019, has already been tabled in the Indian parliament, it is still under scrutiny by the Joint Parliamentary Committee along with the experts and stakeholders. According to a report by Vidhi Centre for Legal Policy, a think-tank closely working with the Indian Government, it takes almost a period of 261 days for a parliamentary law to come into force and receive all necessary approvals[xxviii]. The legislators should understand the need for independent data privacy legislation and accord quicker approval or work upon suggestions to effectively implement the already delayed Data Privacy Law.

Need for one Unified Authority:

India's approach to cybersecurity regulation and policy formulation is characterised by a proliferation of agencies and frameworks combined with lax enforcement. A typically regulated entity in the financial sector is under a mandate to comply with not only the various instructions of the sectoral regulator (e.g., RBI or SEBI), but also with the horizontally applicable framework of the Information Technology Act 2000 (as revised) and the various rules thereunder containing obligations relating to data protection, security, and breach notifications, with the directions of the nodal cybersecurity agency CERT-In, and with Ministry of Electronics and Information Technology ('MEITY') and others, wherever required. This multiplicity of regulatory and policymaking bodies with each having its mandatory compliance requirements not only creates a complex environment for financial sector businesses, increased compliance costs and overheads that hinder the innovation in rapidly emerging sectors but is also likely to create a weak cyber-security policy.

Priority to Cyber security and policy objectives:

Cyber security has gradually become a priority for Indian legislators as a result of repeated security breaches within existing information systems, and a policy agenda focused on rapidly increasing digitization and internet access. While the emphasis on developing cyber security institutions has increased exponentially, there is no long-term budgetary allocation for cyber security[xxix], and the majority of stakeholders believe that the current budgetary allocation is insufficient. There is an urgent need to revisit the budgetary allocations towards Cyber security and related policy work and dedicate a long terms budget specifically towards the subject area.

Need for a more transparent regime:

To date, no sectoral regulator (financial or otherwise) has publicly announced effective enforcement action in relation to cybersecurity obligations or has made effective any stringent penal action under the applicable law. The Cyber Appellate Tribunal, the nodal appellate body for causes of action arising under the IT Act, has been defunct since 2011. All data breach reports which are submitted to CERT-In are kept confidential and never come out in the public domain. Similarly, the NCIIPC also operates in secret and is overseen by the Indian intelligence community. Without transparency in decision-making and enforcement or an independent audit, it seems impossible to assess these bodies' efficacy. Creating additional agencies without enforcing existing frameworks is counterintuitive in this context.

CONCLUSION

Despite a significant historical gap in terms of access to technology and resources available to protect cyberspace, India has increasingly emphasised cyber security as a critical policy concern over the last two decades. Although various issues such as the absence of a unified code and authority working towards cyber security and data privacy are addressed in the proposed Personal Data Protection Bill, 2019, the truest test of the same will only commence when the Bill is enforced and comes into real-world practice.

ENDNOTES

[i] The Economist, ' The world's most valuable resource is no longer oil, but data' (*The Economist*, May 6, 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 19 October 2021

[ii] EU General Data Protection Regulation 2016/679

[iii] SFLC.IN, 'Right to Privacy under UDHR and ICCPR' (*Privacybytes*, October 24, 2017) <https://privacy.sflc.in/universal/ > accessed 21 October 2021

[iv] Information Technology (Amendment) Act, 2008

[v] The Aadhar (Targeted delivery of financial and other subsidies, benefits and services) Act, 2016

[vi] Sean Michael Kerner, 'Colonial Pipeline Hack explained: Everything you need to know' (Whatis.com, July 7, 2021) <https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> accessed on 24 October 2021

[vii] Kartikay Mehrotra and William Turton, 'CAN Financial paid $40 million in Ransom After March Cyberattack' (Bloomberg, May 21, 2021) <https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack > accessed on 24 October 2021

[viii] Linklaters and Talwar Thakore and Associates, 'Data Protected-India' (March 2020) <https://www.linklaters.com/en/insights/data-protected/data-protected---india> accessed on 18 October 2021.

[ix] RBI Act, 1934

[x] Reserve Bank of India, *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Reports and Recommendations* (January, 2011) <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf >

[xi] Reserve Bank of India, *Cyber Security Framework in Banks* (June 2, 2016) <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0 >

[xii] Reserve Bank of India, *Directions on Managing Risks and Code of Conduct in outsourcing Financial Services by NBFCs* (November 9, 2017)< https://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11160 >

[xiii] Reserve Bank of India, *Storage of Payment System Data* (April 6, 2018) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244>

[xiv] Securities and Exchange Board of India, *Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories* (July 6, 2015) <https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html >

[xv]Saloni Shukla and Pratik Bhakta, '3.2 million debit cards compromised; SBI, HDFC Bank, YES Bank and Axis worst hit' (*The Economic Times*, October 20, 2016) https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms, accessed 21 October 2021

[xvi] Ministry of Finance, Department of Economic Affairs, *Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector* (June 30, 2017) <https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf>

[xvii] Tarun Krishnakumar, 'Cyber Insecurity: Regulating the Indian Financial Sector' (*University of Oxford, Faculty of Law*, August 21, 2017) <https://www.law.ox.ac.uk/business-law-blog/blog/2017/08/cyber-insecurity-regulating-indian-financial-sector> accessed on 23 October 2021

[xviii] International Financial Services Centre Authority, About IFSCA, <https://ifsca.gov.in/Pages/Contents/AboutIFSCA> accessed on 21 October 2021

[xix] International Financial Services Centre Authority, *Consultation Paper on Proposed IFSCA (Capital Market Intermediaries) Regulations*, 2021< https://ifsca.gov.in/Viewer/ReportandPublication/14>

[xx] Philipp S. Kruger, 'The European Union, Cybersecurity, and the Financial Sector: A Primer', (*Carnegie Endowment for International Peace*, March 16, 2021) <https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055> accessed on 21 October 2021

[xxi] GDPR for Finance, 'Finance and GDPR: What you need to know' <https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/tech-solutions-library/security/gdpr-finance-wp.pdf > accessed 23 October 2021

[xxii]OneTrust DataGuidance, Singapore- Data Protection Overview (*OneTrust DataGuidance*, April 2021) <https://www.dataguidance.com/notes/singapore-data-protection-overview> accessed on 21 October 2021

[xxiii] Stephanie Magnus, Ken Chia, Eunice Tan, Ying Yi Liew and Alex Toh, Singapore: MAS revises Technology Risk Management Guidelines (*Baker McKenzie*, February 16, 2021) <https://www.globalcompliancenews.com/2021/02/16/singapore-mas-revises-technology-risk-management-guidelines280121/#page=1> accessed on 19 October 2021

[xxiv] Hong Kong Monetary Authority, *Personal Data (Privacy) Ordinance Guideline no. 3.7.2* (December 10, 2018) <https://www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/guidelines/1996/12/guide_372b/>

[xxv]Hong Kong Monetary Authority, *Customer Data Protection* (October 14, 2014) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf>

[xxvi] Congressional Research Service, *Financial Services and Cybersecurity: The Federal Role*, (March 23, 2016) <https://crsreports.congress.gov/product/pdf/R/R44429 >

[xxvii] *K.S. Puttaswamy and Anr. vs. Union of India and Ors* [2017] AIR 2017 SC 4161

[xxviii] Devanik Saha, ' 261 days: The time it takes laws approved by Parliament to be enforced' (*Hindustan Times*, February 7, 2017) <https://www.hindustantimes.com/india-news/261-days-the-time-it-takes-laws-approved-by-parliament-to-be-enforced/story-eZm70hsqRFCTSD84Gisa7K.html> accessed on 23 October 2021

[xxix] Remarko Sengupta, 'Will digital India get a cyber-security allocation?' (*Factor Daily*, January 31, 2017)<https://archive.factordaily.com/budget-2017-will-digital-india-get-cyber-security-allocation/ > accessed on 21 October 2021