BLOCKSUITS

COMPLIANCE OF BLOCKCHAIN WITH THE PERSONAL DATA PROTECTION BILL, 2019

BlockSuits
www.blocksuits.com

Shivani Agarwal
Samaksh Khanna

January 24, 2020

Introduction

Right to privacy enjoys the status of fundamental rights in India in the light of *KS Puttaswamy* v. *Union of India* judgment. In furtherance of the same, there has been ample discussion on enforcing a data protection law in India akin to General Data Protection Regulation ("**GDPR**"). A report was submitted by the committee of Justice B.N. Srikrishna and Data Protection Bill, 2018 was drafted which was later revised and introduced again with significant changes as Data Protection Bill, 2019 ("**Data Protection Bill**") which has been again sent for a revision. India already has a set of much fewer comprehensive rules to regulate data protection, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI**").

Considering the recent formulation of start-ups providing blockchain services and further exploration of the technology, it is essential to discuss if blockchain can be made compliant with the data protection laws that already exist and might be passed and enforced in near future. The Report of the Committee to propose specific actions to be taken in relation to Virtual Currencies dated February 28, 2019 published by the Department of Economic Affairs entails various plausible usages of blockchain, for example, digital KYC verification, mortgage loan applications etc. It is essential to understand the effect of the data protection laws on the entities using blockchain to store data of its customers for various purposed.

Following are the issues raised with respect to blockchain while discussing its compatibility with Data Protection Bill and SPDI:

ISSUE 1

While Rule 5(4) of SPDI states that the data collected by a body corporate or a person shall not be retained longer than the purpose for which it has been collected, the Data protection Bill more specifically incorporates (i) right to erasure once the purpose for which the data was collected has been served; and (ii) right to be forgotten from the continuing disclosures. However, erasing data on blockchain is extremely difficult, if not impossible. Each block of the blockchain contains the hash of the previous block as well, in order to ensure no tempering with the blockchain. Therefore, in order to tamper with information on one block, the entire blockchain shall have to be tampered with or even deleted.

Discussion and Solution

Currently, SPDI does not specifically give a statutory right to erasure or right to be forgotten to data principals. However, the Data Protection Bill states that a person shall have right to erasure under Section 18 and also right to be forgotten under Section 20, in the following instances:

1. The purpose for which data was collected has been served;
2. The data principle withdraws his consent; or
3. Disclosure of personal information was made contrary to the provision of Data Protection Bill or any other law for the time being in force.

The data principal has been given a statutory right to withdraw his consent from continuing disclosure at his own will. However, if entities were to obtain an irrevocable consent of its customers for retention of the data even after the purpose for which the data was collected has been served, it may be possible for blockchain to overcome the challenge of right to erasure and right to be forgotten. It is pertinent to note however, that it a well settled law that statutory rights cannot be waived off. Therefore, it remains to be seen how effective such an undertaking from the customers would be.

Moreover, it is extremely difficult to retract data off of a blockchain because all the data is stored by various nodes for the purpose to render the data tamper proof, however, this requires end number of verification processes and tracking of each data set that has been uploaded by such a node. The entire idea of a blockchain is to keep the process decentralized and hence to retract any information off it would make the blockchain meaningless.
It is pertinent to note that even though the hashes provided in the blockchain is almost tamper proof, it is not impossible. The data may be changed through hashes by altering the original proof of work, as provided in the bitcoin blockchain white paper.

According to the Vajra, white paper, NPCI's blockchain network, any data which is stored on a permissioned blockchain may be compressed if it is not being utilized according to a time stamp, and if any inspection of such data is required then it may be de-compressed accordingly. This is an innovative method to store the data, which is no longer required by 'data fiduciaries', and allocate the data in a separate partition and can be said to be partly compliant with Section 9 of the Data Protection Bill, which states "*The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing*".

A 'built-in consent' mechanism should be adopted by a permissioned blockchain with respect to any personal data that may be stored on a blockchain. A 'built-in' consent mechanism is akin to 'I agree' checkbox that is available on most websites. Section 7(d) of the Data Protection Bill stipulates that the data principal shall be notified about a procedure to withdraw consent, in effect to remove such data for which consent has been withdrawn. An inbuilt consent mechanism inside a blockchain is could be helpful in order to be compliant with the data protection laws.

However, blockchain technology may indeed be used to verify data and protect any personal data. Data 'versioning' may be done in a blockchain to protect any personal data. 'Versioning' is a procedure through which a unique code or a unique identity is provided to every software to be in time and be aware of any updates that are being linked to the same and they also correspond to new developments in such software. Hence, when consent is being withdrawn then such unique identities and code may be used to identify the version for which the consent has been withdrawn and then be removed from the blockchain, again, maintaining that the removal of data from the blockchain is an extremely strenuous process. As all historical data will be logged with all the consents verifying the same, it will be easier to identify if any dispute arises in a court of law. Hence, the questioning of altering the consent to fit into another period or a dispute regarding for which particular cause the consent was provided becomes easily immutable. Hence, a blockchain may be modified to be complaint

under Section 7 of the Data protection Bill. As provided under section 9 of the Data Protection Bill:
” *The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing*“.

Hence, while determining such ‘period’ the above-mentioned method may be utilised. Section 11 lays out detailed attributes related to consent and the same can be followed if an inbuilt consent mechanism software is added to the blockchain. This can only be done by making certain alterations to the blockchain system.

If the usage of the blockchain is for the purposes like keeping a record of land titles or storing arbitral awards, it would be not be necessary to obtain any consent and therefore, the issue of non-compliance with Section 18 and Section 20 of the Data Protection Bill and Rule 5(4) of the SPDI would not arise because the said information must be available in public domain and cannot be withdrawn.

ISSUE 2

Who can be held responsible for the data on blockchain since it is a decentralized mechanism of storing data where there are many nodes who might even be located in different parts of the world. As per the Data Protection Bill, just like GDPR, the liability is on the data fiduciaries and the data processors. However, in case of blockchain, it would be difficult to hold any one person or an entity as a data fiduciaries or data processors.

Discussion and Solution

The structure of the blockchain needs to be carefully examined to determine what entity falls as under the definition of a data processor and data controller. Generally, blockchain can be either ‘public and permissionless’ or ‘private and permissioned’. Public and permissionless networks are available to everyone for exploring blocks. In other words, anyone can download the distributed ledger on their system and the blockchains is accessible to everyone. However, this is not the case with ‘private and permission’ blockchain. ‘Private and permissioned’ blockchain is restricted to an entity or a person or a group of persons and therefore, only accessible them. In a ‘private and permissioned’ network, only a few nodes have the key to add blocks to the blockchain whereas in a ‘public and permissionless’, any one can join the network of the nodes and add blocks to the blockchain. Bitcoin blockchain is an example of public permissionless blockchain. There exists a variety of data controllers in the helm of the blockchain system, hence understanding and tracing each data controller to retract information or identifying a ‘data fiduciary’ is a hefty task.

In the case of ‘private and permissioned’ blockchain, the accountable party can be the entity for which the data is being collected, therefore, bringing in the application of ‘vicarious liability’. The company which is processing such data can be qualified to be the data controller. Where there are 2 (two) or more companies sharing the blockchain network, as stated under GDPR, the data processors should be identified as joint controllers ab initio.

Further, in a public and permissionless blockchain, the question arises whether data miners shall be brought under the purview of the Data Protection Bill while identifying data controllers, as they are the ones that verify the data on the blockchain and also levy a small fee for the same. However, it shall be noted that data miners do not decide the purpose of data processing and cannot be said to be data controllers. Data miners merely serve as maintenance of the blockchain server and cannot be identified as data controllers as they do not decide the purpose of adding such data to the blockchain.

A strong argument arises whether or not users can be said to be data controllers and held liable for any dispute. In todays age, many users determine the use of their own personal data and accordingly store it in networks. However, there has been ample debate regarding whether data subjects or users may be identified as data controllers, especially when the data is being processed by a company. If the data is stored in a permissioned blockchain, it may be viewed to be done for a professional or even commercial use, however, any data stored on a permissionless blockchain would be open to an infinite number of people.

In the light of the above stated, it can be concluded that it will be easily to grant accountability in the case of a private and permissioned blockchain, the liability of stakeholders under a public and permissionless network shall depend on the way in which data is being stored and the entities who the data might help.

ISSUE 3

Technology in most cases surfaces the issue of territorial jurisdiction. In a case, where the public blockchain is spread worldwide, as in the case of bitcoins, and the data of people from worldwide is stored or processed on it, which territory shall have the rightful jurisdiction over it. The blockchain is a decentralised global ledger and thus the origin may not determine jurisdiction. The issue shall pertain specifically with respect to the public and permissionless blockchain.

Discussion and Solution

As per Section 2 of the Data Protection Bill, where data fiduciaries or data processors are not located in India, the Data Protection Bill shall apply to those cases where it relates to profiling of data principles within the territory of India. Subject to Section 33(1) of the Data Protection Bill, the sensitive personal data may be transferred outside India, however, must still be stored in India. Just like the internet, blockchain is a global system, the access to which is allowed to everyone anywhere. The data is stored on various servers and is easily accessible to everyone.

Further, the Data Protection Act requires that in order to process sensitive personal data outside India, an explicit permission must be obtained from the data principle. Any data which is stored on a blockchain may also be accessed outside India, and hence an express permission for the same may not be a default.

However, it should be noted that any entity which is providing services to data principles located in India through the use of a blockchain would fall within the territorial scope of the Data Protection Bill.

ISSUE 4

Can it be said that the data stored on the blockchain is completely anonymous and validates the process of de-identification provided in the Data Protection Bill.

Discussion and solution

De-identification is defined as, as per Section 3(13) of the Data Protection Bill, " *the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal*. " Any data stored on a blockchain is compliant of this definition as it carries a unique code or an identity mark which does not directly classify or identify the data principal. However, the question also arises that whether the data stored on a blockchain is completely anonymised. The DLT function of the blockchain uses encryption and hashing. The blockchain is a confidential ledger and may not said to be a completely anonymous one. Hence, for example, the bitcoin blockchain is hashed by miners, therefore, it cannot be said to be regulated by the Data Protection Bill. The identity of such data miner may not be visible on the blockchain.