Consumer Grievance Redressal

Background

The Personal Data Protection Bill 2019 (PDPB)[1] empowers data principals (users) to make complaints to data fiduciaries (service providers) in case of any contravention of the bill, which has caused or likely to cause harm to the data principals. It also mandates service providers to have a procedure and an effective mechanism in place to redress such grievances of users, in an efficient and speedy manner (within 30 days of receipt of complaint). Users have also been given a right to approach the Data Protection Authority (DPA), in case they are not satisfied with the relief provided to them by a service provider, pursuant to a complaint.[2]

Furthermore, in case of a personal data breach[3] at the end of a service provider, the bill provides discretion to the DPA, for directing service providers to inform its users about the same, based on an assessment by DPA of the severity of harm likely to be caused to them.[4] It also stipulates security safeguards to be undertaken by the service providers based on associated risk and the likelihood of harm from the processing of data.[5]

Shortcomings of these Provisions

Limitations on Seeking Redressal: No time limit has been prescribed at the level of the DPA as well as the Appellate Tribunal to dispose of any complaints made by users, which may deter them from pursuing their complaints in case of delays in getting their grievances redressed. At the same time, the bill does not provide for a direct remedy to data principals against service providers in case of offences [6] which limits their avenues for seeking redressal.

Information Regarding Data Breach: By giving sole discretion to the DPA in assessing cases when the users are to be notified of the breach by the service providers, PDPB limits users' information regarding the potential threats to the security of their data. Additionally, there are no specific standards prescribed to assess the 'severity of harm' creating an ambiguity as it may lead to differing interpretations from time to time.

Mechanisms to Seek Remedy: The procedure for seeking remedy must be accessible and understandable to the data principals. CUTS' user perception survey on privacy and data protection[8] had pointed out,

that only few users who experienced a personal data breach or a privacy violation, went on to complain about it. Users were also found to be unaware regarding the avenues of registering their grievances.

Limitation on Right to Seek

Compensation: Compensation provision in the PDPB, only gives users' right to claim compensation if they have suffered harm.[9] It limits their rights, as first they will have to make an assessment of the harm suffered and, on that basis, make a claim for compensation. This puts a burden on them to have a complete understanding of harm as prescribed under the PDPB. Further, it does not give any clarification regarding the components of the definition of harm which restricts the understanding of users in assessing harm.

Recommendations

Right to Seek Judicial Remedy: PDPB must empower the court to take cognizance of complaints made by users under Section 83(2), which is now only limited to complaints made by DPA. Provision for such a right to seek remedy has already been emphasised upon by the Supreme Court in the *Puttaswamy* judgment[10] wherein the court stated that limiting such rights might make the remedy seeking mechanism sterile. Additionally, the bill should take on from the best practices from European Unions (EUs) General Data Protection Regulation (GDPR) and the Asia Pacific Economic Co-operation (APEC) Privacy Framework, both of which provide for data principals to seek an adequate judicial remedy. Informed by the Consumer Protection Act 2019, a timeline for not more than sixty days may be provided for resolutions of complaints at the level of both DPA[11] and the Appellate Tribunal.[12]

Notification of Breach (Section 23): PDPB should have a provision for users to be notified directly of the data breach by service providers in case of likelihood of harm[13] without undue delay, along with this they should be given recommendations for measures that could be taken to prevent harm. This would help data principals to remain informed and handle their data adequately. Further, it will make service providers more accountable and transparent, which is beneficial for ensuring the trust of users and enhance cyber-security.[14] This practice is also followed in the EU's GDPR and China's Cyber Security Law.[15]

A Mechanism to Seek Remedy: In order to increase the effectiveness of grievance redressal mechanism, the PDPB under Section 50 (Codes of Practice) should prescribe service providers to develop mechanisms for alternate grievance redress options. This could be done through setting up Consumer Service Cells on the lines of CUTS' initiative of *Grahak Sahayta Kendra,*[16] which could act as mediator or conciliator in resolving the complaints. At the same time, consumers

should be provided with an easily accessible mechanism to lodge complaints and be updated about the same through the toll free numbers, online portals (website of the DPA), emails or in person.

Compensation: PDPB should not limit users' right to claim compensation by making it contingent on the harm suffered by them, rather violation itself should be a ground to claim compensation under Section 64. Further, the bill should also provide for more clarification on definitional components of harm so that users are better able to assess the cases of violations that have caused them any harm.

---

1 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2 S. 32 of the bill

3 S. 3(29) of the bill states: "personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal

4 S. 25(5) of the bill

5 S. 24 of the bill

6 S.83(2) of the bill

8 https://cutsccier.org/pdf/survey_analysis-dataprivacy.pdf

9 S.64 of the Bill

10 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012(para 357)

11 S.54 of the bill

12 S. 72 of the bill

13 Chinese Cyber Security Law 2017

14 L. Ablon et al., *Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information. RAND Corporation* (RAND Corporation, 2016).

15 GDPR, Article 34 "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

16 Consumer Care Centre (Grahak Sahayta Kendra) | CUTS Centre for Consumer Action, Research & Training (CART)," https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/