लेजिसलेटिव ब्रीफ

पर्सनल डेटा प्रोटेक्शन बिल, 2019

पर्सनल डेटा प्रोटेक्शन बिल, 2019 को 11 दिसंबर, 2019 को लोकसभा में पेश किया गया। इसके बाद इसे विस्तृत समीक्षा के लिए ज्वाइंट पार्लियामेंटरी कमिटी को सौंप दिया गया।

हाल के ब्रीफ्स:

औद्योगिक संबंधों, सामाजिक सुरक्षा तथा व्यवसायगत सुरक्षा पर तीन श्रम संहिताएं, 2020
21 सितंबर, 2020

बैंकिंग रेगुलेशन (संशोधन) बिल, 2020
14 सितंबर, 2020

अनुराग वैष्णव
anurag@prsindia.org

मनीष कानडजे
manish@prsindia.org

5 अक्टूबर, 2020

बिल की मुख्य विशेषताएं

- बिल व्यक्तियों (डेटा प्रिंसिपल्स) के पर्सनल डेटा की प्राइवेसी की सुरक्षा के लिए फ्रेमवर्क प्रदान करता है जिन्हें एंटिटीज़ (डेटा फिड्यूशरीज़) प्रोसेस करते हैं।
- डेटा प्रिंसिपल की सहमति लेने के बाद ही विशिष्ट उद्देश्य के लिए प्रोसेसिंग की जा सकती है। लेकिन मेडिकल इमरजेंसी के मामले में या लाभ या सेवाएं प्रदान करने के लिए राज्य द्वारा प्रोसेसिंग करने के लिए इस सहमति की जरूरत नहीं है।
- बिल डेटा प्रिंसिपल को कुछ अधिकार देता है। वह अपने डेटा को सही करवा सकता है, इस बात की पुष्टि कर सकता है कि उसके पर्सनल डेटा को प्रोसेस किया गया है और उसके लगातार खुलासे पर प्रतिबंध लगाने की मांग कर सकता है।
- बिल अपने कई प्रावधानों से छूट देता है, जब डेटा को राष्ट्रीय सुरक्षा के हित में, या किसी अपराध को रोकने, उसकी जांच या अभियोजन के लिए प्रोसेस गया हो।
- संवेदनशील पर्सनल डेटा, जैसे वित्तीय या स्वास्थ्य संबंधी डेटा को विदेश ट्रांसफर किया जा सकता है, लेकिन उसे देश में भी स्टोर किया जाना चाहिए।
- डेटा फिड्यूशरीज़ की निगरानी और उन्हें रेगुलेट करने के लिए बिल राष्ट्रीय स्तर पर डेटा प्रोटेक्शन अथॉरिटी (डीपीए) का गठन करता है।

प्रमुख मुद्दे और विश्लेषण

- अपराधों को रोकने, उनका पता लगाने, जांच और अभियोजन के लिए पर्सनल डेटा की प्रोसेसिंग को बिल के प्रावधानों से छूट दी गई है। इस छूट का दायरा बहुत व्यापक हो सकता है।
- राज्य को सेवा प्रदान करने के लिए डेटा प्रोसेसिंग हेतु व्यक्ति की सहमति की जरूरत नहीं। इस प्रकार कमर्शियल सेवाओं के मामले में सार्वजनिक क्षेत्र की संस्थाओं (जोकि सरकार का अंग हैं) और निजी कंपनियों के साथ अलग-अलग किस्म का व्यवहार किया जा रहा है।
- संवेदनशील पर्सनल डेटा के अनिवार्य स्थानीय स्टोरेज के कुछ फायदे हैं जैसे कानून प्रवर्तन एजेंसियां आसानी से और जल्दी डेटा को एक्सेस कर सकेंगी। हालांकि इससे डेटा फिड्यूशरी को इंफ्रास्ट्रक्चर पर अतिरिक्त खर्च करना होगा।
- फिड्यूशरीज़ को डीपीए को उस डेटा ब्रीच की जानकारी देनी होगी जिससे डेटा प्रिंसिपल को नुकसान हो सकता है। संभव है कि इस प्रावधान के चलते बाजार में छवि खराब होने के डर से फिड्यूशरीज़ ब्रीच की पूरी जानकारी न दें।
- एडजुडिकेटिंग अधिकारी के लिए कानूनी पृष्ठभूमि का होना अनिवार्य नहीं है। इस अधिकारी को 'राइट टू बी फॉरगॉटन' से संबंधित मामलों पर फैसला देना है और संभव है कि उसके पास संवैधानिक कानून का अपेक्षित ज्ञान नहीं हो।

भाग क : बिल की मुख्य विशेषताएं

संदर्भ

व्यक्तिगत डेटा वह डेटा होता है जोकि पहचान की विशेषताओं, लक्षणों या गुणों से संबंधित होता है और जिसे किसी व्यक्ति की पहचान के लिए इस्तेमाल किया जा सकता है।[1] हाल के वर्षों में यह पाया गया कि विभिन्न संस्थाएं (बिजनेस और सरकारी, दोनों) निर्णय लेने के लिए पर्सनल डेटा का बड़ी मात्रा में इस्तेमाल कर रही हैं।[2] डेटा प्रोटेक्शन वह प्रक्रिया होती है जोकि नीतियों और कार्य प्रणाली के जरिए पर्सनल डेटा के उपयोग की रक्षा करती है ताकि किसी व्यक्ति की प्राइवेसी में कम से कम दखल हो।

अगस्त 2017 में सर्वोच्च न्यायालय ने कहा था कि निजता का अधिकार (राइट टू प्राइवेसी) भारतीय नागरिकों का मूलभूत अधिकार है।[3] अदालत ने यह भी कहा था कि इनफॉरमेशनल प्राइवेसी या पर्सनल डेटा और तथ्यों की प्राइवेसी निजता के अधिकार के लिए अनिवार्य है। हालांकि ऐसा कोई कानून नहीं है जोकि भारतीय नागरिकों के निजता के अधिकार की सुरक्षा करने के लिए व्यापक रूपरेखा प्रदान करे। वर्तमान में भारत में नागरिकों के पर्सनल डेटा या इनफॉरमेशन के उपयोग को इनफॉरमेशन टेक्नोलॉजी (आईटी) एक्ट, 2000 के अंतर्गत अधिसूचित नियमों द्वारा रेगुलेट किया जाता है।[4] इन नियमों में डेटा प्रोसेस करने वाली संस्थाओं के डेटा कलेक्शन, इनफॉरमेशन के खुलासे और ट्रांसफर के लिए सुरक्षात्मक उपायों को निर्दिष्ट किया गया है।

भारत में डेटा प्रोटेक्शन और डिजिटल अर्थव्यवस्था से संबंधित मुद्दों पर अध्ययन के लिए एक्सपर्ट कमिटी (चेयरपर्सन: जस्टिस बी. एन. श्रीकृष्ण) गठित की गई थी जिसने जुलाई 2018 में अपनी रिपोर्ट सौंपी।[5] कमिटी ने कहा था कि आईटी नियम (2011) डिजिटल अर्थव्यवस्था के विकास के साथ कदम नहीं मिला पाए हैं। उदाहरण के लिए (i) नियमों के अंतर्गत संवेदनशील पर्सनल डेटा की परिभाषा संकुचित है, और (ii) उसके कुछ प्रावधानों का कॉन्ट्रैक्ट द्वारा उल्लंघन किया जा सकता है।

अपनी रिपोर्ट के साथ एक्सपर्ट कमिटी ने ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल का सुझाव दिया जोकि पर्सनल डेटा का इस्तेमाल करने वाली संस्थाओं के लिए डेटा प्रोसेसिंग के नियमों को निर्दिष्ट करता है। इसके अतिरिक्त कमिटी ने एक रेगुलेटरी निकाय की स्थापना का भी सुझाव दिया ताकि कानून का अनुपालन सुनिश्चित हो। पर्सनल डेटा प्रोटेक्शन बिल, 2019 एक्सपर्ट कमिटी के सुझावों और विभिन्न हितधारकों से प्राप्त प्रस्तावों पर आधारित है।[6] 2019 का बिल निम्नलिखित का प्रयास करता है: (i) पर्सनल डेटा के संबंध में व्यक्तियों की प्राइवेसी की रक्षा करना, (ii) ऐसे पर्सनल डेटा की प्रोसेसिंग के लिए रूपरेखा बनाना, और (iii) इन उद्देश्यों के लिए डेटा प्रोटेक्शन अथॉरिटी का गठन।

मुख्य विशेषताएं

- **परिभाषा:** व्यक्तिगत डेटा वह डेटा होता है जोकि पहचान की विशेषताओं, लक्षणों या गुणों से संबंधित होता है और जिसे किसी व्यक्ति की पहचान के लिए इस्तेमाल किया जा सकता है। बिल कुछ पर्सनल डेटा को संवेदनशील पर्सनल डेटा के तौर पर वर्गीकृत करता है। इसमें वित्तीय डेटा, बायोमैट्रिक डेटा, जातिगत, धार्मिक या राजनीतिक विश्वास या निर्दिष्ट डेटा की कोई दूसरी श्रेणी शामिल है। बिल कहता है कि डेटा फिड्यूशरी वह संस्था या व्यक्ति है जोकि पर्सनल डेटा की प्रोसेसिंग का माध्यम और उद्देश्य तय करता है, और डेटा प्रिंसिपल वे व्यक्ति होते हैं जिनसे डेटा संबंधित होता है। बिल निम्नलिखित द्वारा पर्सनल डेटा की प्रोसेसिंग को गवर्न करता है: (i) सरकार, (ii) भारतीय कंपनियां, और (iii) भारत में व्यक्तियों के व्यक्तिगत डेटा से डील करने वाली विदेशी कंपनियां।
- **पर्सनल डेटा की प्रोसेसिंग का आधार:** बिल के अंतर्गत व्यक्तियों की सहमति मिलने पर ही किसी संस्थान को डेटा प्रोसेसिंग की अनुमति दी गई है। हालांकि कुछ मामलों में व्यक्ति की सहमति के बिना भी डेटा प्रोसेसिंग की अनुमति दी जा सकती है। इनमें निम्नलिखित शामिल हैं: (i) अगर व्यक्तियों को सुविधाएं प्रदान करने के लिए यह राज्य द्वारा अपेक्षित है, (ii) कानूनी प्रक्रिया, (iii) मेडिकल इमरेंसी की स्थिति में।
- **डेटा फिड्यूशरीज़ की बाध्यताएं:** डेटा फिड्यूशरी सिर्फ विशिष्ट उद्देश्य के लिए प्रोसेसिंग कर सकता है। इसके अतिरिक्त डेटा फिड्यूशरी कलेक्शन और स्टोरेज की सीमा के अधीन होगा। इसका यह अर्थ है कि विशिष्ट उद्देश्य के लिए जितने डेटा की जरूरत होगी, सिर्फ उतना ही डेटा जमा किया जा सकता है और सिर्फ उतने समय के लिए स्टोर किया जाएगा जितने समय के लिए उसे स्टोर करना जरूरी है। इसके अतिरिक्त सभी डेटा फिड्यूशरीज़ को कुछ पारदर्शी और उत्तरदायित्वपूर्ण उपाय करने होंगे, उदाहरण के लिए: (i) सुरक्षात्मक उपाय करना (जैसे डेटा एन्क्रिप्शन और डेटा के दुरुपयोग को रोकना), और (ii) व्यक्तियों की शिकायतों को दूर करने के लिए शिकायत निवारण प्रणाली तैयार करना।
- **सोशल मीडिया इंटरमीडियरीज़:** बिल सोशल मीडिया इंटरमीडियरीज़ की परिभाषा में उन इंटरमीडियरीज़ को शामिल करता है जोकि यूजर्स के बीच ऑनलाइन ट्रांजैक्शन को संभव बनाते हैं और सूचनाओं को साझा करने की अनुमति देते हैं। उन सभी इंटरमीडियरीज़, जिनके यूजर्स अधिसूचित सीमा से अधिक हैं और जिनका असर निर्वाचित लोकतंत्र या लोक व्यवस्था पर पड़ सकता है, को भारत के यूजर्स के लिए स्वैच्छिक यूजर सत्यापन प्रणाली प्रदान करनी होगी।
- **व्यक्ति के अधिकार:** बिल व्यक्तियों (या डेटा प्रिंसिपल) के कुछ अधिकारों को निर्धारित करता है। इन अधिकारों में निम्नलिखित शामिल हैं: (i) फिड्यूशरी से इस बात की पुष्टि करने का अधिकार कि उसके पर्सनल डेटा को प्रोसेस किया गया है, (ii) गलत, अधूरे या आउट-ऑफ-डेट पर्सनल डेटा में संशोधन की मांग करना, (iii) उस पर्सनल डेटा को मिटाने की मांग करना, जो अब उस उद्देश्य के लिए जरूरी नहीं, जिसके लिए उसे प्रोसेस किया गया था, और (iv) फिड्यूशरी द्वारा उनके पर्सनल डेटा का खुलासा करते रहने पर प्रतिबंध, अगर वह जरूरी नहीं है या सहमति वापस ले ली गई है।
- **डेटा प्रोटेक्शन अथॉरिटी:** बिल डेटा प्रोटेक्शन अथॉरिटी की स्थापना करता है जोकि: (i) लोगों के हितों की रक्षा करने के लिए कदम उठा सकती है, (ii) पर्सनल डेटा के दुरुपयोग को रोक सकती है, और (iii) बिल का अनुपालन सुनिश्चित कर सकती है। इस अथॉरिटी

में एक चेयरपर्सन और छह सदस्य होंगे, जिन्हें डेटा प्रोटेक्शन, इनफॉरमेशन टेक्नोलॉजी या पब्लिक एडमिनिस्ट्रेशन के क्षेत्र में कम से कम 10 वर्ष का अनुभव हो।

- **शिकायत निवारण:** बिल के अंतर्गत डेटा प्रिंसिपल एक्ट के उस प्रावधान का उल्लंघन होने पर शिकायत कर सकता है जिनसे उसे नुकसान हुआ हो, या नुकसान की आशंका हो। डेटा फिड्यूशरी को ऐसी शिकायत को जल्द हल करना होगा (30 दिनों में)। अगर डेटा प्रिंसिपल शिकायत निवारण के तरीके से संतुष्ट नहीं है तो वह डीपीए में शिकायत दर्ज करा सकता है।
- डीपीए शिकायत के आधार पर जांच शुरू कर सकता है और सजा या मुआवजे का प्रावधान कर सकता है। अगर डेटा प्रिंसिपल या डेटा फिड्यूशरी इस फैसले से संतुष्ट नहीं तो वे अपीलीय ट्रिब्यूनल में अपील कर सकते हैं। ट्रिब्यूनल के आदेशों के खिलाफ सर्वोच्च न्यायालय में अपील की जाएगी।
- **भारत से बाहर डेटा का ट्रांसफर:** व्यक्ति द्वारा स्पष्ट सहमति मिलने और विशेष अतिरिक्त शर्तों पर संवेदनशील पर्सनल डेटा को भारत से बाहर ट्रांसफर किया जा सकता है। हालांकि ऐसे संवेदनशील पर्सनल डेटा की एक प्रति को भारत में भी स्टोर होना चाहिए। जिस संवेदनशील डेटा को सरकार महत्वपूर्ण डेटा के तौर पर अधिसूचित करेगी, उसे केवल भारत में ही प्रोसेस किया जा सकता है।
- **छूट:** केंद्र सरकार अपनी किसी एजेंसी को बिल के कुछ प्रावधानों के अनुपालन से छूट दे सकती है: (i) देश की सुरक्षा, लोक व्यवस्था, संप्रभुता और एकता तथा विदेशी राज्यों से मित्रवत संबंध के मद्देनजर, या (ii) उपरोक्त मामलों से संबंधित किसी भी संज्ञेय अपराध (यानी वॉरंट के बिना गिरफ्तारी) के उकसावे को रोकने के लिए। पर्सनल डेटा की प्रोसेसिंग को कुछ विशेष उद्देश्यों के लिए बिल के प्रावधानों से छूट दी जा सकती है, जैसे: (i) किसी अपराध को रोकना, उसकी जांच, या अभियोजन, या (ii) व्यक्तिगत या घरेलू उद्देश्य या (iii) पत्रकारीय और अनुसंधान उद्देश्य। हालांकि यह प्रोसेसिंग विशिष्ट, स्पष्ट और कानूनी उद्देश्य के लिए होनी चाहिए।
- **अपराध और सजा**: बिल के प्रावधानों का उल्लंघन करते हुए पर्सनल डेटा को प्रोसेस या ट्रांसफर करने पर फिड्यूशरी को अपने वार्षिक टर्नओवर का 4% जुर्माना भरना होगा जोकि न्यूनतम 15 करोड़ रुपए के अधीन है। अगर डेटा ऑडिट नहीं किया जाता तो फिड्यूशरी के अपने वार्षिक टर्नओवर का 2% जुर्माना भरना होगा जोकि न्यूनतम पांच करोड़ रुपए के अधीन है। बिना सहमति के डी-आईडेंटिफाइड पर्सनल डेटा का री-आइडेंटिफिकेशन और प्रोसेसिंग (जहां आइडेंटिफायर्स को हटा दिया जाता है) करने पर तीन साल तक की कैद भुगतनी होगी या जुर्माना भरना होगा, या दोनों सजा भुगतनी होगी। अदालत सिर्फ डीपीए की शिकायत पर ही किसी अपराध को संज्ञान में लेगी।
- **सरकार के साथ नॉन-पर्सनल डेटा और बेनाम पर्सनल डेटा की शेयरिंग:** केंद्र सरकार डेटा फिड्यूशरी को निम्नलिखित प्रदान करने का निर्देश दे सकती है: (i) सेवाओं के बेहतर लक्ष्यीकरण के लिए नॉन पर्सनल डेटा, और (ii) बेनाम पर्सनल डेटा (जहां व्यक्तिगत रूप से डेटा की पहचान करना संभव नहीं)।

भाग ख: प्रमुख मुद्दे और विश्लेषण

पर्सनल डेटा की प्रोसेसिंग से नुकसान संभव, लेकिन कुछ लाभ भी

एक्सपर्ट कमिटी (2017) के व्हाइट पेपर में कहा गया था कि व्यक्तियों के पर्सनल डेटा को जमा करने और उसका विश्लेषण करने के कई फायदे हैं।[7] उदाहरण के लिए: (i) कई व्यक्तियों के हेल्थकेयर डेटा, जैसे अस्पताल में विजिट का विवरण, का इस्तेमाल करके हेल्थकेयर प्रोवाइडर निदान का अनुमान लगा सकता है और इलाज का सुझाव दे सकता है, (ii) व्यक्तियों के लोकेशन डेटा को यातायात की निगरानी करने और ड्राइविंग की स्थितियों में सुधार करने के लिए इस्तेमाल किया जा सकता है, (iii) फ्रॉड की पहचान करने के लिए फाइनांशियल ट्रांजैक्शन डेटा का इस्तेमाल किया जा सकता है। कंपनियां पर्सनल डेटा की मदद से अपने ग्राहकों को बेहतर सेवाएं प्रदान कर सकती हैं। उदाहरण के लिए मोबाइल एप्लिकेशन आधारित टैक्सी सेवा यूजर की पिछली ट्रिप के पर्सनल डेटा का इस्तेमाल करके पर्सनलाइज्ड बुकिंग सुझाव दे सकती है। पर्सनल डेटा की प्रोसेसिंग से भारत जैसे विकासशील देश में बाजार में नए अवसरों का सृजन हो सकता है।

इसी बीच यह भी जरूरी है कि डिजिटल अर्थव्यवस्था को बढ़ावा देने और पर्सनल डेटा के संरक्षण के बीच संतुलन कायम किया जाए। मार्च 2020 तक भारत में 687 मिलियन लोग इंटरनेट इस्तेमाल करते हैं, जबकि पांच साल पहले यह आंकड़ा लगभग 200 मिलियन का था।[8] यह बढ़ोतरी इतनी तेजी से हुई कि यूजर्स यह समझने का अनुभव और विशेषज्ञता हासिल नहीं कर पाए कि उनके पर्सनल डेटा का कितना दुरुपयोग किया जा सकता है। पर्सनल डेटा के इस्तेमाल पर रेगुलेशन और प्रतिबंध न होने से यूजर्स को भेदभाव और नुकसान का शिकार होना पड़ सकता है। आम तौर पर उनका अपने डेटा पर सीमित नियंत्रण होता है।[8] वे डेटा कलेक्शन की हद या उसके उद्देश्यों से नावाकिफ हो सकते हैं। व्यक्तियों को नुकसान पहुंचाने के अलावा ऐसे मामलों का असर निर्वाचित लोकतंत्र या लोक व्यवस्था पर पड़ सकता है। उदाहरण के लिए 2018 में पाया गया था कि 87 मिलियन फेसबुक यूजर्स (5 मिलियन भारतीयों सहित) के पर्सनल डेटा को थर्ड पार्टी एप्लिकेशन के जरिए निजी कंपनी कैंब्रिज एनालिटिका के साथ साझा किया गया था। अमेरिका में 2016 के राष्ट्रपति चुनाव के दौरान लक्षित विज्ञापन दिखाने के लिए व्यक्तियों की प्रोफाइलिंग में इस डेटा का इस्तेमाल किया गया था। इस संभावित दुरुपयोग को ध्यान में रखते हुए यह जरूरी हो जाता है कि पर्सनल डेटा की सुरक्षा के लिए एक रूपरेखा तैयार की जाए।

इसी के मद्देनजर बिल डेटा फिड्यूशरीज़ पर प्रतिबंध लगाता है, जिसका उद्देश्य पर्सनल डेटा को प्रोसेस करना है जैसे विशिष्ट उद्देश्य के लिए प्रोसेसिंग, डेटा कलेक्शन और डेटा रिटेंशन की सीमा, और सहमति की जरूरत। हालांकि वह सैंडबॉक्स के रूप में इनोवेशन को बढ़ावा देने के लिए कुछ छूट भी प्रदान करता है। इसके अतिरिक्त क्रेडिट स्कोरिंग और सर्च इंजन्स के संचालन जैसे उद्देश्यों के लिए सहमति की शर्त से छूट दी गई है।

अपराधों को रोकने और उनका पता लगाने के लिए प्रोसेसिंग को बिल के अंतर्गत व्यापक छूट

बिल: क्लॉज 36(क), 3(20)

बिल के अंतर्गत फिड्यूशरीज़ कई बाध्यताओं के अधीन हैं, जैसे (i) डेटा कलेक्शन के उद्देश्य को स्पष्ट करना, (ii) यह सुनिश्चित करना कि प्रोसेस किया गया डेटा पूरा है और भ्रामक नहीं, और (iii) यह सुनिश्चित करना कि डेटा अपेक्षित अवधि के बाद रीटेन नहीं किया गया है। इसके अतिरिक्त फिड्यूशरीज़ को डीपीए को पर्सनल डेटा ब्रीच की जानकारी देनी होगी जिससे डेटा प्रिंसिपल को नुकसान हो सकता है। हालांकि किसी अपराध को रोकने, उनका पता लगाने, और जांच करने तथा अभियोजन के लिए पर्सनल डेटा को प्रोसेस करने पर फिड्यूशरीज़ को इन सभी शर्तों से छूट दी गई है, सिर्फ एक शर्त यह है कि यह प्रोसेसिंग विशिष्ट, स्पष्ट और कानूनी उद्देश्य से होनी चाहिए। इसका अर्थ यह है कि फिड्यूशरी उस उद्देश्य के लिए जरूरी डेटा से अधिक डेटा जमा कर सकता है और उसे जरूरत से अधिक लंबी अवधि के लिए रख सकता है। इसके अतिरिक्त व्यक्तियों का उनके डेटा पर कोई अधिकार नहीं होगा। यह तर्क दिया जा सकता है कि अपराधों को रोकने या उनकी जांच हेतु प्रोसेसिंग करने के लिए डेटा प्रिंसिपल की सहमति नहीं ली जा सकती। हालांकि यह अस्पष्ट नहीं कि बाकी की बाध्यातएं क्यों लागू नहीं होंगी।

इसके अतिरिक्त बिल पर्याप्त सुरक्षात्मक उपायों के बिना यह छूट देता है। उदाहरण के लिए भारतीय टेलीग्राफ एक्ट, 1885 के अंतर्गत भारतीय टेलीग्राफ नियम, 1951 में राष्ट्रीय सुरक्षा जैसे उद्देश्यों के लिए टेलीफोन कॉल्स के इंटरसेप्शन की अनुमति है। हालांकि नियमों के अंतर्गत छूट का आदेश सिर्फ केंद्र या राज्य सरकार के गृह सचिव द्वारा दिया जा सकता है।[9] इसके अतिरिक्त इंटरसेप्ट किए गए रिकॉर्ड्स को छह महीने के भीतर नष्ट करना होता है, जब तक कि कार्य संबंधी उद्देश्य के लिए उनकी जरूरत न हो।[10] ऐसे सुरक्षात्मक उपाय बिल में नहीं हैं।

एक्सपर्ट कमिटी (2018) ने कहा था कि किसी कानून के उल्लंघन को रोकना, उसका पता लगाना, जांच और अभियोजन राज्य के अनिवार्य कार्य हैं।[5] उसने सुझाव दिया था कि इन गतिविधियों को बिल के कुछ प्रावधानों से छूट मिलनी चाहिए। हालांकि ये छूट उन हितों के अनुपात में होनी चाहिए जिन्हें प्राप्त किया जाना है। लेकिन सवाल यह है कि फिड्यूशरी को इस उद्देश्य के लिए बिल के अधिकतर प्रावधानों से छूट देना, वह भी बिना किसी सुरक्षात्मक उपाय के, क्या अपेक्षित उद्देश्य के अनुपात में है?

एक समान सेवाएं देने वाली सरकारी और निजी कंपनियों के साथ अलग-अलग व्यवहार

बिल: क्लॉज 12(क)

बिल राज्य सहित सभी फिड्यूशरीज़ को डेटा प्रिंसिपल की सहमति के बिना पर्सनल डेटा को प्रोसेस करने से प्रतिबंधित करता है। हालांकि कुछ मामलों में व्यक्ति की सहमति के बिना भी पर्सनल डेटा की प्रोसेसिंग की जा सकती है। इनमें निम्नलिखित शामिल हैं: (i) अगर डेटा प्रिंसिपल को सेवा या लाभ प्रदान करने के लिए यह राज्य द्वारा अपेक्षित है, (ii) डेटा प्रिंसिपल को लाइसेंस या परमिट जारी करना, (iii) कानूनी प्रक्रिया, या (iv) मेडिकल इमरेंसी की स्थिति में। यह स्पष्ट नहीं है कि सेवा या लाभ देने के लिए राज्य को डेटा प्रिंसिपल की सहमति की जरूरत क्यों नहीं है।

इस सिलसिले में एक्सपर्ट कमिटी (2018) ने कहा था कि अगर राज्य सेवा या लाभ का एकमात्र प्रदाता हो तो व्यक्ति और राज्य के बीच शक्तियों का असंतुलन होता है।[5] इसका यह अर्थ है कि अगर डेटा प्रिंसिपल को लाभ या सेवा चाहिए तो उसके पास सहमति से इनकार करने का विकल्प नहीं होता। ऐसी स्थिति में सहमति की शर्त का विचार बेमायने है। इसलिए राज्य को सेवा या कल्याण लाभ प्रदान करने के लिए सहमति के बिना पर्सनल डेटा प्रोसेस करने की अनुमति होनी चाहिए।

हालांकि यह अस्पष्ट है कि राज्य द्वारा प्रदान की जाने वाली सभी सेवाओं के लिए यह छूट क्यों दी गई है (जिसमें कमर्शियल सेवाएं भी शामिल हैं)। उदाहरण के लिए संसद के कानून द्वारा बनी एक बीमा कंपनी भारतीय संविधान के अनुच्छेद 12 के अंतर्गत राज्य की परिभाषा के दायरे में आती है। बिल के अंतर्गत कंपनी सहमति हासिल किए बिना अपने ग्राहकों के पर्सनल डेटा को प्रोसेस कर सकती है। हालांकि निजी क्षेत्र की उसकी प्रतिद्वंद्वी कंपनियों को ग्राहकों के डेटा को प्रोसेस करने से पहले उनकी सहमति लेनी होगी। इसलिए इस प्रावधान के परिणामस्वरूप एक समान सेवाएं देने वाली सरकारी और निजी कंपनियों के साथ अलग-अलग किस्म का व्यवहार होता है।

ब्रीच की इच्छानुसार रिपोर्टिंग से हितों का टकराव हो सकता है

बिल: क्लॉज 25(1)

बिल के अंतर्गत डेटा फिड्यूशरी को किसी पर्सनल डेटा ब्रीच की जानकारी डीपीए को तभी देनी होगी, जब उस ब्रीच से डेटा प्रिंसिपल को नुकसान होने की आशंका हो। बिल के अनुसार, डेटा ब्रीच का अर्थ है, पर्सनल डेटा का अनाधिकृत या दुर्घटनावश खुलासा, हेरफेर या पहुंच न होना। बिल के अनुसार, नुकसान का अर्थ है, वित्तीय नुकसान, साख का नुकसान होना, या सेवा न मिलना। अब, डेटा ब्रीच की सूचना डीपीए को देने की जरूरत है या नहीं, अगर यह तय करने का अधिकार डेटा फिड्यूशरी को दिया जाता है तो इससे हितों का टकराव हो सकता है।

इस पर एक्सपर्ट कमिटी (2018) ने कहा था कि हर एक डेटा ब्रीच का असर एक बराबर नहीं होता।[5] अपेक्षाकृत कम असर वाले ब्रीच की सूचना से बचने के लिए सिर्फ ऐसे ब्रीच की जानकारी डीपीए को दी जानी चाहिए जिससे डेटा प्रिंसिपल को नुकसान हो सकता है। ऐसी चुनींदा सूचनाओं से यह सुनिश्चित होगा कि डीपीए को कम असर वाले ब्रीच की सूचनाओं का भार नहीं सहना पड़ेगा। हालांकि इसमें फिड्यूशरीज़ का आर्थिक हित छिपा हो सकता है कि वह बाजार में अपनी साख बनाए रखने के लिए डेटा ब्रीच के असर को कम करके दिखाए। उदाहरण के लिए जून 2019 में यह खबर आई थी कि एक अमेरिकी मल्टीनेशनल कंपनी ने पर्सनल डेटा ब्रीच की सूचना नहीं दी और कहा कि सिर्फ डेमोन्स्ट्रेशन डेटा लीक हुआ था।[11] उल्लेखनीय है कि डीपीए पर्सनल डेटा ब्रीच इत्यादि के मामले में फिड्यूशरी का डेटा ऑडिट कर सकती है।[12] इसलिए ऐसे मामलों की सूचना देने से फिड्यूशरी के डेटा ट्रस्ट स्कोर पर असर पड़ सकता है।

इसके अतिरिक्त यह कहा जा सकता है कि डेटा प्रिंसिपल ऐसे फिड्यूशरी पर भरोसा कर सकता है जिसके साथ डेटा ब्रीच के कम मामले हों क्योंकि ऐसे फिड्यूशरी को दूसरों की तुलना में सुरक्षित माना जा सकता है। ऐसी स्थिति में फिड्यूशरी द्वारा इच्छानुसार डेटा ब्रीच की सूचना देने से व्यक्ति उस सूचना से वंचित रह सकता है जिसके आधार पर वह भविष्य में किसी फिड्यूशरी को चुन सकता है, और उस पर अपने डेटा के लिए भरोसा कर सकता है।

बिल के अंतर्गत शिकायत निवारण

शिकायत तभी की जा सकती है जब डेटा प्रिंसिपल को नुकसान की कोई आशंका हो

बिल: क्लॉज 32(2)

बिल के अंतर्गत डेटा प्रिंसिपल एक्ट के प्रावधानों का उल्लंघन होने पर डेटा फिड्यूशरी को इसकी शिकायत कर सकता है लेकिन इसकी शर्त यह है कि इस उल्लंघन से उसे कोई नुकसान हुआ हो या नुकसान की आशंका हो। अगर डेटा प्रिंसिपल शिकायत निवारण के तरीके से संतुष्ट नहीं है तो वह डीपीए को शिकायत कर सकता है। यह सवाल किया जा सकता है कि डेटा प्रिंसिपल के अधिकारों का उल्लंघन होने पर या एक्ट के किसी उल्लंघन पर शिकायत क्यों नहीं दर्ज कराई जा सकती। उदाहरण के लिए अगर डेटा फिड्यूशरी कमर्शियल फायदे के लिए सहमति के बिना यूजर के पर्सनल डेटा की माइनिंग करता है तो जरूरी नहीं कि यूजर को इससे नुकसान हो। हालांकि ऐसे मामलों में शिकायत दर्ज कराने के लिए यूजर को यह प्रदर्शित करना होगा कि इससे उसे नुकसान की आशंका है।

'राइट टू बी फॉरगॉटन' के अधिकार के उपयोग के लिए एडजुडिकेटिंग अधिकारी के पास जरूरी विशेषज्ञता नहीं हो सकती

बिल: क्लॉज 20(1), 20(2), 20(3), 62(3)

बिल प्रावधान करता है कि डेटा प्रिंसिपल को अपने पर्सनल डेटा पर अधिकार हैं। राइट टू बी फॉरगॉटन के अंतर्गत डेटा प्रिंसिपल पर्सनल डेटा के निरंतर खुलासे पर प्रतिबंध लगा सकता है, अगर उस उद्देश्य के लिए डेटा की जरूरत न रह गई हो या सहमति वापस ले ली गई हो। इस अधिकार का उपयोग सिर्फ तभी किया जा सकता है, जब डीपीए द्वारा नियुक्त एडजुडिकेटिंग अधिकारी कोई आदेश जारी करता हो (डेटा प्रोटेक्शन, कानून या इनफॉरमेशन टेक्नोलॉजी के क्षेत्र का विशेषज्ञ)। अधिकारी तय करेगा कि क्या इस अधिकार का उपयोग किसी व्यक्ति की बोलने और अभिव्यक्ति की स्वतंत्रता के अधिकार या सूचना के अधिकार का उल्लंघन करता है। सवाल यह है कि क्या एडजुडिकेटिंग अधिकारी यह फैसला करने के लिए पर्याप्त सक्षम है। ऐसे मामलों की व्याख्या आम तौर पर उच्च न्यायालय द्वारा की जाती है, चूंकि इनमें संवैधानिक अधिकारों से संबंधित सवाल जुड़े होते हैं। हालांकि बिल एक एडजुडिकेटिंग अधिकारी की नियुक्ति की अनुमति देता है जोकि डेटा प्रोटेक्शन या इनफॉरमेशन टेक्नोलॉजी के क्षेत्र का तो विशेषज्ञ हो सकता है लेकिन कानून का नहीं। इसलिए उस अधिकारी में 'राइट टू बी फॉरगॉटन' के उपयोग से संबंधित मामलों पर फैसला लेना की विशेषज्ञता नहीं हो सकती है।

देश में संवेदनशील पर्सनल डेटा का स्टोरेज

स्थानीय स्तर पर संवेदनशील पर्सनल डेटा को स्टोर करने के फायदे और नुकसान

बिल: क्लॉज 33(1)

बिल कहता है कि व्यक्तियों के संवेदनशील पर्सनल डेटा (जैसे स्वास्थ्य डेटा या वित्तीय डेटा) को विदेश भेजा जा सकता है लेकिन भारत में उसकी एक कॉपी स्टोर की जानी चाहिए। केंद्र सरकार के पास यह अधिकार है कि वह डीपीए और क्षेत्रगत रेगुलेटर की सलाह से अन्य श्रेणियों के डेटा को संवेदनशील पर्सनल डेटा के तौर पर वर्गीकृत करे। एक्सपर्ट कमिटी (2018) ने यह कहा था कि संवेदनशील पर्सनल डेटा के स्थानीय स्टोरेज के कई फायदे हैं जैसे: (i) जांच के लिए कानून प्रवर्तन एजेंसियों की डेटा तक आसान और जल्द पहुंच, (ii) देश में डिजिटल इंफ्रास्ट्रक्टर और डेटा प्रोसेसिंग के इकोसिस्टम का निर्माण, और (iii) भारतीय नागरिकों पर विदेशी चौकसी को रोकना।[5] उसने सुझाव दिया था कि सभी पर्सनल डेटा की सर्विंग कॉपी को भारत में स्टोर किया जाना चाहिए।

हालांकि कमिटी ने यह भी कहा था कि संवेदनशील पर्सनल डेटा के स्टोरेज के अपने नुकसान भी हैं। अक्सर घरेलू कंपनियां विदेशी इंफ्रास्ट्रक्चर जैसे डेटा स्टोर करने के लिए क्लाउड कंप्यूटिंग का इस्तेमाल करती हैं। इसलिए अनिवार्य स्थानीय स्टोरेज से डेटा फिड्यूशरी का खर्चा बढ़ सकता है। इसके अतिरिक्त भारत में डेटा प्रोसेसिंग पर लगने वाली अतिरिक्त लागत के कारण कुछ डेटा फिड्यूशरी भारत में निवेश करने को हतोत्साहित हो सकते हैं। संवेदनशील पर्सनल डेटा के स्थानीय स्टोरेज की शर्त से डेटा संवेदनशील और गैर संवेदनशील पर्सनल डेटा में बांटा जाएगा और फिड्यूशरीज़ पर अनुपालन का अतिरिक्त भार आएगा।

दूसरे देशों से अलग अपराधों के लिए कैद सहित दूसरी सजाएं

बिल: क्लॉज 82

बिल के अंतर्गत डेटा फिड्यूशरी या डेटा प्रोसेसर की सहमति के बिना डी-आइडेंटिफाइड पर्सनल डेटा की री-आइडेंटिफिकेशन करने पर तीन साल तक की कैद भुगतनी होगी या जुर्माना भरना होगा, या दोनों सजा भुगतनी होगी। बिल के अनुसार, पर्सनल डेटा के डी-आइडेंटिफिकेशन का अर्थ है, डेटा से आइडेंटिफायर्स को हटाना या छिपाना, ताकि डेटा प्रिंसिपल को सीधे तौर पर चिन्हित न किया जा सके। री-आइडेंटिफिकेशन का मतलब है, इस पूरी प्रक्रिया को उलटा करना। बिल के अन्य सभी उल्लंघनों (जिनमें बिना सहमति के व्यक्ति के पर्सनल डेटा को हासिल करना, उसे ट्रांसफर करना या बेचना शामिल है) पर मौद्रिक सजा है, लेकिन डी-आइडेंटिफाइड पर्सनल डेटा की री-आइडेंटिफिकेशन करने पर जेल की सजा हो सकती है। उल्लेखनीय है कि कनाडा के प्राइवेसी एक्ट और यूरोपीय संघ में जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) में किसी अपराध या उल्लंघन पर जेल की सजा नहीं है।[2,13]

अंतरराष्ट्रीय डेटा प्रोटेक्शन कानूनों से बिल की तुलना

बिल के अनेक प्रावधान अंतरराष्ट्रीय डेटा प्रोटेक्शन कानूनों से फर्क हैं। इसके सोशल मीडिया इंटरमीडियरीज़ और नॉन पर्सनल डेटा से संबंधित प्रावधान यूरोपीय संघ, ऑस्ट्रेलिया और कनाडा के कानूनों से फर्क हैं क्योंकि अन्य क्षेत्राधिकारों में यह मौजूद नहीं हैं। इन क्षेत्राधिकारों के डेटा प्रोटेक्शन कानूनों में संवेदनशील पर्सनल डेटा की परिभाषा में वित्तीय डेटा शामिल नहीं हैं। इसके अतिरिक्त अधिकतर क्षेत्राधिकारों में कानून के उल्लंघन पर जेल की सजा नहीं है। यूरोपीय संघ के जीडीपीआर में यूजर को कुछ अतिरिक्त अधिकार दिए गए हैं जोकि भारत के प्रस्तावित कानून में मौजूद नहीं हैं। उदाहरण के लिए 'राइट टू ऑब्जेक्ट' जिसके अंतर्गत यूजर को अपने डेटा की

प्रोफाइलिंग या डायरेक्ट मार्केटिंग उद्देश्य के लिए उसकी प्रोसेसिंग पर आपत्ति जताने का अधिकार है। तालिका 1 में बिल के कुछ प्रावधानों को प्रस्तुत किया गया है जोकि अंतरराष्ट्रीय कानूनों से फर्क हैं।

तालिका 1: डेटा प्रोटेक्शन और प्राइवेसी कानूनों की अंतरराष्ट्रीय तुलना

देश	यूरोपीय संघ	ऑस्ट्रेलिया	कनाडा	भारत (प्रस्तावित बिल)
संवेदनशील पर्सनल डेटा	▪ वित्तीय डेटा, पासवर्ड शामिल नहीं	▪ वित्तीय डेटा, पासवर्ड शामिल नहीं	▪ अलग से परिभाषित नहीं	▪ वित्तीय डेटा, स्वास्थ्य डेटा शामिल, पासवर्ड शामिल नहीं
डेटा का स्थानीय स्टोरेज	▪ अनिवार्य नहीं	▪ अनिवार्य नहीं ▪ क्षेत्र विशिष्ट अनिवार्यता, जैसे स्वास्थ्य डेटा के लिए	▪ अनिवार्य नहीं	▪ संवेदनशील पर्सनल डेटा की स्थानीय कॉपी अनिवार्य, महत्वपूर्ण पर्सनल डेटा का विशिष्ट स्थानीय स्टोरेज अनिवार्य
डेटा का सीमा पार ट्रांसफर	▪ अनुमति है, अगर प्राप्तकर्ता देश के पास डेटा प्रोटेक्शन के पर्याप्त स्टैंडर्ड्स हैं (यूरोपीय आयोग द्वारा विश्लेषित)	▪ अनुमति है, अगर प्रोसेसिंग करने वाली कंपनी ने यह सुनिश्चित करने के लिए कदम उठाए हैं कि प्राप्तकर्ता देश के प्राइवेसी के सिद्धांतों का उल्लंघन नहीं करेगा	▪ अनुमति है, अगर प्रोसेसिंग करने वाली कंपनी ने सुरक्षा के तुलनात्मक स्तर को सुनिश्चित करने के लिए कॉन्ट्रैक्चुअल या दूसरे उपाय किए हैं	▪ अनुमति है (कुछ डेटा के लिए), अगर रेगुलेटर ने मंजूरी दी है या सरकार ने निर्दिष्ट किया है
छूट	▪ सार्वजनिक और राष्ट्रीय सुरक्षा, रक्षा, न्यायिक प्रक्रिया, घरेलू, पत्रकारीय, शोध और रोजगार उद्देश्यों के लिए	▪ रक्षा और खूफिया एजेसियों, संघीय अदालतों, राजनीतिक पार्टियों, छोटे व्यवसाय, पत्रकारीय और रोजगार उद्देश्यों के लिए	▪ पूरी तरह छूट नहीं ▪ जैसे पत्रकारीय उद्देश्य के लिए सहमति मांगने से खास छूट मिल सकती है	▪ संप्रभुता और एकता, राष्ट्रीय सुरक्षा, मित्रवत संबंध, लोक व्यवस्था, अपराधों को रोकने और अभियोजन, शोध और पत्रकारीय उद्देश्य, सैंडबॉक्स
सजा	▪ 20 मिलियन EUR तक, या पिछले वर्ष के विश्व्यापी वार्षिक टर्नओवर का 4%, जो भी अधिक हो ▪ जेल नहीं	▪ 2.1 मिलियन AUD तक ▪ जेल नहीं, इमरजेंसी के दौरान हासिल की गई सूचना का खुलासा करने के अतिरिक्त किसी अन्य अपराध के लिए जेल नहीं	▪ 1,00,000 CAD तक ▪ जेल नहीं	▪ 15 करोड़ रुपए तक या पिछले वर्ष के विश्वव्यापी वार्षिक टर्नओवर का 4% ▪ डी-आइडेंटिफाइड पर्सनल डेटा की री-आइडेंटिफिकेशन करने पर कैद (अधिकतम 3 वर्ष)

Sources: European Union – The General Data Protection Regulation, 2016; Australia – The Privacy Act, 1988; Canada – The Privacy Act, 1985; The Personal Information Protection and Electronic Documents Act, 2000; The Personal Data Protection Bill, 2019; PRS.

1. Section 3(28), The Personal Data Protection Bill, 2019.
2. The General Data Protection Regulation 2016, European Union.
3. Justice K. S. Puttaswamy Vs. Union of India, Supreme Court, Writ Petition (Civil) 494 of 2012, August 24, 2017.
4. Information Technology (Reasonable security practices and sensitive personal data or information) Rules, 2011.
5. "A Free and Fair Digital Economy", Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, July 2018.
6. Statement of Objects and Reasons, The Personal Data Protection Bill, 2019.
7. "White Paper of the Committee of Experts on a Data Protection Framework for India", November 2017.
8. "Draft Empowerment and Protection Architecture", NITI Aayog, August 2020.
9. PUCL Vs. Union of India, Writ Petition (Civil) 256 of 1991, Supreme Court, December 18, 1996.
10. Rule 419(A), The Indian Telegraph Rules, 1951.
11. "Cybersecurity giant Symantec plays down unreported breach of test data", The Guardian, June 13, 2019.
12. Section 29, The Personal Data Protection Bill, 2019.
13. The Personal Information Protection and Electronic Documents Act, 2000, Canada; The Privacy Act, 1985, Canada.