लेजिसलेटिव ब्रीफ

ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022

ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022 को इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय ने 18 नवंबर, 2022 को सार्वजनिक टिप्पणियों के लिए जारी किया था।

साकेत सूर्य
saket@prsindia.org

ओमिर कुमार
omir@prsindia.org

30 दिसंबर, 2022

बिल की मुख्य विशेषताएं

- बिल भारत के भीतर डिजिटल पर्सनल डेटा की प्रोसेसिंग पर लागू होगा जहां यह डेटा ऑनलाइन जमा किया जाता है या ऑफलाइन जमा करने के बाद उसका डिजिटलीकरण होता है। यह भारत के बाहर होने वाली प्रोसेसिंग पर भी लागू होगा, अगर यह प्रोसेसिंग भारत में वस्तुओं या सेवाओं को पेश करने के लिए या व्यक्तियों की प्रोफाइलिंग करने के लिए की जा रही है।
- पर्सनल डेटा को सिर्फ वैध उद्देश्यों के लिए प्रोसेस किया जा सकता है, जिसके लिए व्यक्ति ने अपनी सहमति दी है। कुछ मामलों में यह माना जा सकता है कि सहमति दे दी गई है (डीम्ड)।
- डेटा फिड्यूशरीज़ पर बाध्यता होगी कि वह डेटा की सटीकता को बनाए रखें, डेटा को सुरक्षित रखें और उद्देश्य पूरा होने पर डेटा को डिलीट कर दें।
- बिल व्यक्तियों को कुछ अधिकार देता है जिसमें सूचना हासिल करने, डेटा में संशोधन करने और उसे मिटाने, तथा शिकायत निवारण का अधिकार शामिल है।
- केंद्र सरकारी एजेंसियों को निर्दिष्ट आधार पर बिल के प्रावधानों का पालन करने से छूट दे सकता है जैसे राज्य की सुरक्षा, सार्वजनिक व्यवस्था और अपराधों का निवारण।
- केंद्र सरकार भारतीय डेटा प्रोटेक्शन बोर्ड की स्थापना करेगी। यह बोर्ड बिल के प्रावधानों के उल्लंघन संबंधी मामलों पर फैसला सुनाएगा।

प्रमुख मुद्दे और विश्लेषण

- अगर राज्य को राष्ट्रीय सुरक्षा जैसे कुछ कारणों के आधार पर डेटा प्रोसेसिंग के प्रावधानों से छूट मिलेगी तो डेटा कलेक्शन, प्रोसेसिंग और उसका रीटेंशन जरूरत से कहीं ज्यादा हो सकता है। इससे प्राइवेसी के मौलिक अधिकार का उल्लंघन हो सकता है।
- बिल बैंकिंग या टेलीकॉम सेवा जैसे एक से कमर्शियल काम करने वाली निजी और सरकारी संस्थाओं के साथ सहमति और स्टोरेज की सीमा को लेकर, अलग-अलग बर्ताव करता है। इससे निजी क्षेत्र के सेवा प्रदाताओं के समानता के अधिकार का उल्लंघन हो सकता है।
- केंद्र सरकार भारतीय डेटा प्रोटेक्शन बोर्ड के संयोजन, और नियुक्तियों के तरीके और कार्यकाल को निर्दिष्ट करेगी। इससे बोर्ड के स्वतंत्र कामकाज पर सवाल खड़े होते हैं।
- बिल डेटा प्रिंसिपल को 'राइट टू बी फॉरगॉटन' और डेटा पोर्टेबिलिटी का अधिकार नहीं देता।
- बिल डेटा फिड्यूशरीज़ से यह अपेक्षा करता है कि वह किसी बच्चे के पर्सनल डेटा की प्रोसेसिंग से पहले उसके कानूनी अभिभावक से सत्यापन योग्य सहमति हासिल करेगा। इस प्रावधान के अनुपालन के लिए डेटा फिड्यूशरी को हर उस व्यक्ति की आयु का सत्यापन करना होगा, जो उसकी सेवा हासिल करने के लिए साइन अप करता है। इसका डिजिटल स्पेस में एनॉनिमिटी पर विपरीत असर हो सकता है।

भाग क : बिल की मुख्य विशेषताएं

संदर्भ

पर्सनल डेटा ऐसी इनफॉरमेशन होती है जिसका संबंध किसी चिन्हित या चिन्हित होने योग्य व्यक्ति से होता है। बिजनेस और सरकारी संस्थाएं वस्तुओं और सेवाओं की डिलिवरी के लिए पर्सनल डेटा को प्रोसेस करती हैं। पर्सनल डेटा की प्रोसेसिंग से व्यक्तियों की प्राथमिकताओं को समझने में मदद मिलती है जोकि कस्टमाइजेशन, टार्गेटेड एडवर्टाइजिंग और सुझावों को विकसित करने के लिए उपयोगी हो सकता है। पर्सनल डेटा की प्रोसेसिंग से कानून प्रवर्तन में भी मदद मिल सकती है। अगर प्रोसेसिंग अनियंत्रित तरीके से की जाएगी तो इसका व्यक्तियों की प्राइवेसी पर प्रतिकूल असर हो सकता है। प्राइवेसी को मौलिक अधिकार के रूप में मान्यता दी गई है।[1] यह व्यक्तियों को कई तरह के नुकसान पहुंचा सकता है, जैसे वित्तीय नुकसान, प्रतिष्ठा का नुकसान और प्रोफाइलिंग।

वर्तमान में भारत में डेटा प्रोटेक्शन पर अलग से कोई कानून नहीं है। पर्सनल डेटा के उपयोग को इनफॉरमेशन टेक्नोलॉजी (आईटी) एक्ट, 2000 के तहत रेगुलेट किया जाता है।[2,3] यह गौर किया गया कि यह फ्रेमवर्क पर्सनल डेटा की सुरक्षा को सुनिश्चित करने के लिए पर्याप्त नहीं है।[1] 2017 में केंद्र सरकार ने जस्टिस बी.एन.श्रीकृष्ण की अध्यक्षता में डेटा प्रोटेक्शन पर एक्सपर्ट कमिटी का गठन किया था ताकि देश में डेटा प्रोटेक्शन से संबंधित मुद्दों की समीक्षा की जा सके। 2018 में कमिटी ने रिपोर्ट सौंपी।[4] कमिटी के सुझावों के आधार पर दिसंबर 2019 में लोकसभा में पर्सनल डेटा प्रोटेक्शन बिल, 2019 पेश किया गया।[5] बिल को ज्वाइंट पार्लियामेंटरी कमिटी के पास भेजा गया जिसने दिसंबर 2021 में अपनी रिपोर्ट सौंपी।[2] अगस्त 2022 में बिल को संसद में वापस ले लिया गया। नवंबर 2022 में इलेक्ट्रॉनिक और इनफॉरमेशन टेक्नोलॉजी मंत्रालय ने ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022 को सार्वजनिक टिप्पणियों के लिए जारी किया।[6]

मुख्य विशेषताएं

- **एप्लिकेबिलिटी**: बिल भारत में डिजिटल पर्सनल डेटा की प्रोसेसिंग पर लागू होगा, जहां यह डेटा: (i) ऑनलाइन जमा होता है, या (ii) ऑफलाइन जमा होता है और उसका डिजिटलीकरण किया जाता है। यह भारत के बाहर पर्सनल डेटा प्रोसेसिंग पर भी लागू होगा, अगर यह प्रोसेसिंग भारत में वस्तुओं या सेवाओं को पेश करने या व्यक्तियों की प्रोफाइलिंग करने के लिए की जा रही है। पर्सनल डेटा का अर्थ है, किसी भी व्यक्ति का ऐसा डेटा जिससे वह पहचाना जाता है या उससे संबंधित है। प्रोसेसिंग का अर्थ है, डिजिटल पर्सनल डेटा पर होने वाला ऑटोमेटेड ऑपरेशन या सेट ऑफ ऑपरेशंस। इसमें कलेक्शन, स्टोरेज, उपयोग और शेयरिंग शामिल है।
- **सहमति**: पर्सनल डेटा को सिर्फ वैध उद्देश्य के लिए प्रोसेस किया जा सकता है, जिसके बारे में व्यक्ति ने अपनी सहमति दी हो। सहमति लेने से पहले नोटिस दिया जाना चाहिए। नोटिस में जमा किए जाने वाले पर्सनल डेटा का विवरण और प्रोसेसिंग के उद्देश्य होने चाहिए। किसी भी समय सहमति वापस ली जा सकती है। कुछ स्थितियों में यह माना जाएगा कि सहमति दे दी गई है, जब निम्नलिखित के लिए प्रोसेसिंग जरूरी हो: (i) कानून के तहत किया जाने वाला कार्य, (ii) राज्य द्वारा सेवा या लाभ का प्रावधान, (iii) मेडिकल इमरजेंसी, (iv) रोजगार संबंधी उद्देश्य, और (v) निर्दिष्ट सार्वजनिक हित के उद्देश्य, जैसे राष्ट्रीय सुरक्षा, धोखाधड़ी को रोकना और इनफॉरमेशन की सिक्योरिटी। 18 वर्ष से कम आयु के लोगों के लिए, कानूनी अभिभावक द्वारा सहमति दी जाएगी।
- **डेटा प्रिंसिपल के अधिकार और कर्तव्य**: जिस व्यक्ति के डेटा को प्रोसेस किया जाता है (डेटा प्रिंसिपल), उसके निम्नलिखित अधिकार हैं: (i) प्रोसेसिंग के बारे में इनफॉरमेशन हासिल करना, (ii) पर्सनल डेटा में संशोधन और उसे मिटाने की मांग करना, (iii) मृत्यु या अक्षमता की स्थिति में इन अधिकारों के उपयोग के लिए किसी दूसरे व्यक्ति को नामजद करना, और (iv) शिकायत निवारण। डेटा प्रिंसिपल के कुछ कर्तव्य भी होंगे, जैसे: (i) उन्हें झूठी या ओछी शिकायत नहीं दर्ज करानी चाहिए, (ii) उन्हें झूठे विवरण पेश नहीं करने चाहिए, इनफॉरमेश को छिपाना नहीं चाहिए या निर्दिष्ट मामलों में किसी दूसरे व्यक्ति का रूप नही धरना चाहिए। कर्तव्यों का उल्लंघन 10,000 रुपए तक के जुर्माने के साथ दंडनीय होगा।
- **डेटा फिड्यूशरी की बाध्यताएं**: प्रोसेसिंग के उद्देश्य और साधनों का निर्धारण करने वाली संस्था को डेटा फिड्यूशरी कहा जाता है। उन्हें निम्नलिखित करना होगा: (i) उन्हें डेटा की सटीकता और उसकी पूर्णता को सुनिश्चित करने के लिए उपयुक्त प्रयास करने होंगे, (ii) डेटा ब्रीच को रोकने के लिए उपयुक्त सिक्योरिटी सेफगार्ड बनाना होगा और ब्रीच की स्थिति में भारतीय डेटा प्रोटेक्शन बोर्ड और प्रभावित व्यक्तियों को इसकी सूचना देनी होगी, और (iii) जैसे ही उद्देश्य पूरा हो जाता है और कानूनी या व्यापारिक उद्देश्यों के लिए रिटेंशन जरूरी नहीं होता तो पर्सनल डेटा को रीटेन करना रोकना होगा (स्टोरेज लिमिटेशन)। स्टोरेज लिमिटेशन की शर्त सरकारी संस्थाओं की प्रोसेसिंग पर लागू नहीं होगी।
- **भारत के बाहर पर्सनल डेटा का ट्रांसफर**: डेटा फिड्यूशरी पर्सनल डेटा को किन देशों को ट्रांसफर कर सकता है, इस संबंध में केंद्र सरकार अधिसूचना जारी करेगी। ये ट्रांसफर निर्दिष्ट नियमों और शर्तों के अधीन होंगे।
- **छूट**: डेटा प्रिंसिपल के अधिकार और डेटा फिड्यूशरी की बाध्यताएं (डेटा सिक्योरिटी के अलावा) कुछ विशिष्ट मामलों में लागू नहीं होंगे। इन मामलों में अपराध का निवारण और जांच, और कानूनी अधिकारों या दावों का प्रवर्तन शामिल है। केंद्र सरकार अधिसूचना के जरिए कुछ गतिविधियों को बिल के प्रावधानों से छूट दे सकती है। इनमें निम्नलिखित शामिल हैं: (i) राज्य की सुरक्षा और सार्वजनिक व्यवस्था के हित में सरकारी संस्थाओं द्वारा प्रोसेसिंग, और (ii) रिसर्च, आर्काइविंग या स्टैटिसटिक्स के उद्देश्य से।
- **भारतीय डेटा प्रोटेक्शन बोर्ड**: केंद्र सरकार भारतीय डेटा प्रोटेक्शन बोर्ड की स्थापना करेगी। बोर्ड के मुख्य कार्यों में निम्नलिखित शामिल हैं: (i) अनुपालन की निगरानी और अर्थ दंड लगाना, (ii) डेटा ब्रीच की स्थिति में डेटा फिड्यूशरी को जरूरी उपाय करने का निर्देश देना, और (iii) प्रभावित व्यक्तियों की शिकायतों की सुनवाई करना। केंद्र सरकार निम्नलिखित निर्दिष्ट करेगी: (i) बोर्ड का संयोजन, (ii) चयन प्रक्रिया, (iii) नियुक्ति और सेवा के नियम और शर्तें, और (iv) हटाने का तरीका।
- **सजा**: बिल की अनुसूची में विभिन्न अपराधों के लिए अर्थदंड का प्रावधान है, जैसे (i) बच्चों से संबंधित शर्तों को पूरा न करने पर 150 करोड़ रुपए तक, और (ii) डेटा ब्रीच को रोकने के लिए सिक्योरिटी संबंधी उपाय न करने पर 250 करोड़ रुपए तक। बोर्ड जांच करने के बाद अर्थदंड लगाएगा।

भाग ख: प्रमुख मुद्दे और विश्लेषण

राज्य को छूट देने से प्राइवेसी पर प्रतिकूल प्रभाव पड़ सकता है

बिल: क्लॉज 2 (18), 8 और 18

राज्य द्वारा पर्सनल डेटा प्रोसेसिंग को बिल के कई प्रावधानों से छूट दी गई है। संविधान के अनुच्छेद 12 के अनुसार, राज्य में निम्नलिखित शामिल हैं: (i) केंद्र सरकार, (ii) राज्य सरकार, (iii) स्थानीय निकाय, और (iv) सरकारी प्राधिकरण और उसके द्वारा गठित कंपनियां। हम इन छूटों से संबंधित मुद्दों पर यहां चर्चा कर रहे हैं।

बिल से राज्य द्वारा अनियंत्रित तरीके से डेटा प्रोसेसिंग हो सकती है जोकि प्राइवेसी के अधिकार का उल्लंघन हो सकता है

सर्वोच्च न्यायालय (2017) ने कहा था कि प्राइवेसी के अधिकार में किसी भी प्रकार का दखल, उस दखल की जरूरत के अनुपात में होना चाहिए।[1] इस छूट से डेटा कलेक्शन, प्रोसेसिंग और रिटेंशन उस जरूरत के समाप्त होने के बाद भी होता रहेगा। यह आनुपातिक नहीं हो सकता, और प्राइवेसी के मौलिक अधिकार का उल्लंघन हो सकता है।

बिल केंद्र सरकार को यह अधिकार देता है कि वह राज्य की सुरक्षा और सार्वजनिक व्यवस्था को बहाल रखने जैसे उद्देश्यों से, बिल के किसी या सभी प्रावधानों से सरकारी एजेंसियों की प्रोसेसिंग को छूट दे सकती है। कुछ मामलों, जैसे अपराधों के निवारण, जांच और प्रॉसीक्यूशन के लिए प्रोसेसिंग, में डेटा प्रिंसिपल के अधिकार और डेटा फिड्यूशरी की बाध्यताएं लागू नहीं होंगी (सिर्फ डेटा सिक्योरिटी को छोड़कर)। बिल के तहत सरकारी एजेंसियों के लिए यह जरूरी नहीं कि प्रोसेसिंग के उद्देश्य के पूरा होने के बाद वे पर्सनल डेटा को डिलीट कर देंगी। उपरिलिखित छूट का इस्तेमाल करके, राष्ट्रीय सुरक्षा के आधार पर सरकारी एजेंसी नागरिकों का डेटा जमा कर सकती है, ताकि निगरानी के लिए 360 डिग्री प्रोफाइल बनाया जा सके। वह इस उद्देश्य से सरकारी एजेंसियों द्वारा रखा गया डेटा इस्तेमाल कर सकती है। इससे सवाल उठता है कि क्या ये छूट आनुपातिकता की कसौटी पर खरी उतरेंगी।

राष्ट्रीय सुरक्षा जैसे आधार पर कम्यूनिकेशन के इंटरसेप्शन पर, *पीयूसीएल बनाम भारत संघ* (1996) मामले में सर्वोच्च न्यायालय ने कुछ सुरक्षात्मक उपायों को अनिवार्य किया था, जिसमें निम्न शामिल हैं: (i) आवश्यकता स्थापित करना, (ii) उद्देश्य की लिमिटेशन, और (iii) स्टोरेज की लिमिटेशन।[7,8] यह बिल के तहत डेटा फिड्यूशरी की बाध्यताओं के समान है, जिसके एप्लिकेशन को छूट दी गई है। श्रीकृष्ण कमिटी (2018) ने कहा था कि राष्ट्रीय सुरक्षा तथा अपराधों के निवारण और प्रॉसीक्यूशन जैसे आधारों पर प्रोसेसिंग के मामले में, निष्पक्ष और उपयुक्त प्रोसेसिंग और सुरक्षात्मक उपायों के अतिरिक्त दूसरी बाध्यताएं लागू नहीं होनी चाहिए। उसने कहा था कि स्टोरेज लिमिटेशन और पर्पज स्पेसिफिकेशन, अगर लागू होते हैं, को अलग कानून के जरिए लागू किया जाए। भारत में ऐसी कानूनी संरचना मौजूद नहीं है।

युनाइटेड किंगडम में 2018 में डेटा प्रोटेक्शन कानून लागू किया गया था, और वह राष्ट्रीय सुरक्षा और रक्षा के लिए ऐसी ही छूट का प्रावधान करता है।[9] हालांकि इंटेलिजेंस और कानून प्रवर्तन संबंधी गतिविधियों के लिए सरकारी एजेंसियों द्वारा पर्सनल डेटासेट्स की बल्क प्रोसेसिंग को इनवेस्टिगेटरी पावर्स एक्ट, 2016 के तहत रेगुलेट किया जाता है।[10] सेक्रेटरी ऑफ स्टेट (यानी गृह मंत्री) इस कार्रवाई के लिए वॉरंट जारी करता है जिसके लिए ज्यूडीशियल कमीश्नर की पूर्व अनुमति जरूरी होती है। ऐसी कार्रवाई के लिए जरूरत और अनुपातिकता स्थापित की जानी चाहिए। वॉरंट की अवधि के बाद डेटा रिटेंशन पर नियंत्रण है। यह कानून संसदीय निगरानी का भी प्रावधान करता है।

झूठे तथ्यों के प्रसार को रोकने के लिए सहमति के बिना प्रोसेसिंग

बिल निर्दिष्ट करता है कि "झूठे तथ्यों के प्रसार को रोकना" उन सार्वजनिक हित के उद्देश्यों में से एक उद्देश्य है, जिसके लिए सहमति हासिल की गई मानी जाएगी। इससे सवाल उठता है कि इस आधार की क्या जरूरत है। यह तर्क दिया जा सकता है कि इस प्रसार के कारण किसी नुकसान या प्रतिकूल असर को पहले ही अपराध के लिए उकसाने से रोकने, सार्वजनिक व्यवस्था और राज्य की सुरक्षा जैसे आधारों के तहत कवर किया गया है। झूठे तथ्यों को सिर्फ बताना या प्रसारित करना किसी कानून के तहत अपराध नहीं हो सकता। सर्वोच्च न्यायालय (2015) ने कहा है कि संविधान के तहत स्पीच को सिर्फ उन्हीं आधारों पर सीमित किया जा सकता है, जब वह उकसाने के स्तर तक पहुंच जाती है।[11] स्पीच के अन्य सभी प्रकार, भले वे अपमानजनक या अलोकप्रिय हों, संविधान के तहत संरक्षित हैं।[11]

क्या सहमति की शर्त तब भी लागू होनी चाहिए जब सरकारी एजेंसी कमर्शियल सेवा प्रदान करती है

बिल में प्रावधान है कि राज्य और उसकी एजेंसियों द्वारा लाभ और सेवा प्रदान करने की स्थिति में, डेटा प्रोसेसिंग के लिए सहमति हासिल की गई मानी जाएगी। सहमति की शर्त व्यक्तियों को डेटा कलेक्शन और प्रोसेसिंग की सीमा पर नियंत्रण प्रदान करती है। सरकार और उसके स्वामित्व वाली सार्वजनिक क्षेत्र की इकाइयां लोगों को विभिन्न सेवाएं प्रदान करती हैं, जैसे स्वास्थ्य, बैंकिंग, टेलीकॉम और बिजली। इस प्रकार सरकारी स्वास्थ्य विभाग और कंपनियां, जैसे एसबीआई, बीएसएनएल और राज्य डिस्कॉम्स को, डेटा की प्रोसेसिंग के लिए लोगों की सहमति लेने की जरूरत नहीं है। सवाल यह है कि क्या यह उपयुक्त है। श्रीकृष्ण कमिटी (2018) ने कहा था कि अगर राज्य सेवा या लाभ का अकेला प्रदाता है, तो व्यक्ति और राज्य के बीच शक्तियों का असंतुलन है।[4] डेटा प्रिंसिपल के पास सहमति न देने का कोई विकल्प नहीं होता, अगर उसे लाभ या सेवा की जरूरत हो।[4] ऐसी स्थिति में सहमति की आवश्यकता का विचार बेमायने है।[4] हालांकि यह स्पष्ट नहीं है कि यह छूट राज्य द्वारा प्रदान की जाने वाली कमर्शियल सेवा सहित सभी सेवाओं पर क्यों दी गई है।

बिल एक जैसे काम करने वाली सार्वजनिक और निजी संस्थाओं के साथ अलग-अलग व्यवहार करता है

जैसे कि ऊपर कहा गया है, सरकारी कंपनी अपने ग्राहकों का पर्सनल डेटा, उनकी सहमति लिए बिना प्रोसेस कर सकती है, और वह उसे असीमित अवधि के लिए रख कर सकती है। हालांकि निजी क्षेत्र के उसके प्रतिस्पर्धियों को इन शर्तों का पालन करना होगा। इसलिए इन प्रावधानों के परिणामस्वरूप, एक जैसे काम करने वाली सार्वजनिक और निजी संस्थाएं के साथ अलग-अलग व्यवहार होगा। इससे संविधान के अनुच्छेद 14 के तहत संरक्षित समानता के अधिकार का उल्लंघन हो सकता है।

डेटा फिड्यूशरी की बाध्यताओं से छूट का असर

सार्वजनिक हित के उद्देश्यों, जैसे राष्ट्रीय सुरक्षा के लिए सहमति की जरूरत बेमायने है क्योंकि ये कार्रवाइयां गुप्त प्रकृति की होती हैं। हालांकि यह तर्क दिया जा सकता है कि दूसरे सिद्धांत प्राइवेसी की रक्षा के लिए लागू रहने चाहिए। चूंकि ये बाध्यताएं लागू नहीं होतीं, राष्ट्रीय अपराध रिकॉर्ड्स ब्यूरो या यूनीक आइडेंटिफिकेशन अथॉरिटी ऑफ इंडिया के डेटा ब्रीच को बिल की व्यवस्था के तहत रिपोर्ट कराने

की जरूरत नहीं है। एक अपराध की जांच और प्रॉसीक्यूशन के लिए जमा किए गए डेटा को दूसरे उद्देश्यों के लिए इस्तेमाल किया जा सकता है। इसी प्रकार जहां कानूनी अधिकारों या हकदारियों को लागू करने के लिए पर्सनल डेटा को प्रोसेस किया जाता है (जैसे राष्ट्रीय खाद्य सुरक्षा एक्ट, 2013) तो डेटा की सटीकता और पूर्णता सुनिश्चित करने की बाध्यता लागू नहीं होगी। डेटा प्रिंसिपल के अधिकार, जिसमें पर्सनल डेटा में संशोधन का अधिकार और शिकायत निवारण का अधिकार शामिल है, भी लागू नहीं होगा। इस प्रकार, जिन मामलों में गलत डेटा की प्रोसेसिंग के आधार पर कोई व्यक्ति कानूनी अधिकारों से वंचित हो जाता है, वहां बिल उस व्यक्ति को कोई उपाय प्रदान नहीं देता। ऐसे उपाय निर्दिष्ट कानूनों में प्रदान करने पड़ सकते हैं।

बिल भारतीय डेटा प्रोटेक्शन बोर्ड की स्वतंत्रता सुनिश्चित नहीं करता

बिल: क्लॉज 19, 20 और 21 (1)

बिल केंद्र सरकार से भारतीय डेटा प्रोटेक्शन बोर्ड के गठन की अपेक्षा करता है। इसमें प्रावधान है कि बोर्ड स्वतंत्र निकाय के रूप में काम करेगा। इसके संयोजन, सदस्यों की नियुक्ति की शर्तों और उन्हें हटाने के तरीके को केंद्र सरकार द्वारा निर्दिष्ट किया जाएगा। सवाल यह है कि क्या इन विवरणों को मूल कानून में दर्ज होना चाहिए ताकि बोर्ड की स्वतंत्रता सुनिश्चित की जा सके।

बोर्ड के मुख्य कार्यों में निम्नलिखित शामिल हैं: (i) बिल के प्रावधानों के गैर अनुपालन को निर्धारित करना, (ii) अर्थदंड लगाना, और (iii) डेटा ब्रीच की स्थिति में डेटा फिड्यूशरीज़ को जरूरी उपाय करने का निर्देश देना। अक्सर सरकारी संस्थाएं ऐसी जांच का विषय होती हैं क्योंकि वे बड़ी मात्रा में पर्सनल डेटा को प्रोसेस करती हैं। इससे सवाल उठता है कि क्या ऐसे मामलों में बोर्ड स्वतंत्रता से काम कर पाएगा।

पर्सनल डेटा प्रोटेक्शन बिल, 2019 में स्वतंत्र डेटा प्रोटेक्शन अथॉरिटी का प्रावधान था। उसके संयोजन और नियुक्तियों के तरीके और शर्तों को बिल में निर्दिष्ट किया गया था।[12] भारतीय दूरसंचार विनियामक प्राधिकरण और भारतीय प्रतिस्पर्धा आयोग जैसे गुलेटर्स की स्थापना करने वाले कानूनों में भी ऐसे विवरण दिए गए हैं।[13,14] विशेष रूप से वे सेवा के कार्यकाल को सुनिश्चित करते हैं और इनके तहत पदाधिकारियों को सिर्फ किन्हीं आधार पर हटाया जा सकता है, जैसे पद का दुरुपयोग, अपराध के लिए सजा, अस्वस्थ दिमाग और इनसॉल्वेंसी। आरटीआई एक्ट, 2005 के तहत, जबकि केंद्रीय सूचना आयोग के सदस्यों का कार्यकाल केंद्र द्वारा निर्दिष्ट किया जा सकता है, लेकिन अन्य विवरण, जैसे नियुक्तियों का सुझाव देने के लिए चयन समिति, क्वालिफिकेशन और बर्खास्तगी का तरीका एक्ट में निर्दिष्ट किया गया है।[15]

डेटा पोर्टेबिलिटी का अधिकार और राइट टु बी फॉरगॉटन नहीं दिया गया है

बिल में डेटा पोर्टेबिलिटी का अधिकार और राइट टु बी फॉरगॉटन नहीं दिया गया है। 2018 के ड्राफ्ट बिल और संसद में पेश 2019 के बिल में ये अधिकार प्रदान किए गए थे।[16,17] 2019 के बिल की समीक्षा करने वाली ज्वाइंट पार्लियामेंटरी कमिटी ने इन अधिकारों को बरकरार रखने का सुझाव दिया था।[2] यूरोपीय संघ के जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) में भी इन अधिकारों को मान्यता दी गई है।[18] श्रीकृष्ण कमिटी (2018) ने गौर किया था कि किसी भी डेटा प्रोटेक्शन कानून का सबसे अनिवार्य अंग, डेटा प्रिंसिपल के अधिकार होते हैं।[4] ये अधिकार स्वायत्तता, पारदर्शिता और जवाबदेही के सिद्धांत पर आधारित होते हैं जिनसे व्यक्तियों को अपने डेटा पर नियंत्रण मिलता है।[4]

डेटा पोर्टेबिलिटी का अधिकार: डेटा पोर्टेबिलिटी के अधिकार से डेटा प्रिंसिपल अपने डेटा को अपने इस्तेमाल के लिए डेटा फिड्यूशरी से हासिल और ट्रांसफर कर सकता है, वह भी एक स्ट्रक्चर्ड, आम तौर पर इस्तेमाल होने वाले और मशीन रीडेबल फॉरमैट में। इससे डेटा प्रिंसिपल को अपने डेटा पर नियंत्रण मिल जाता है और वह एक फिड्यूशरी से दूसरे फिड्यूशरी को अपने डेटा का माइग्रेशन कर सकता है। एक संभावित चिंता यह हो सकती है कि ऐसी इनफॉरमेशन के एक्सेस से डेटा फिड्यूशरी के ट्रेड सीक्रेट्स का खुलासा हो सकता है।[4] श्रीकृष्ण कमिटी (2018) ने सुझाव दिया था कि जब तक कि यह संभव है कि इस इनफॉरमेशन को देने में किसी ट्रेड सीक्रेट का खुलासा न हो, इस अधिकार की गारंटी होनी चाहिए।[4] ज्वाइंट पार्लियामेंटरी कमिटी ने गौर किया था कि ट्रेड सीक्रेट्स डेटा पोर्टेबिलिटी से इनकार करना का आधार नहीं हो सकते और इसे सिर्फ तकनीकी व्यावहारिकता के आधार पर नकारा जा सकता है।[2]

राइट टु बी फॉरगॉटन: राइट टु बी फॉरगॉटन, यानी भूलने के अधिकार का अर्थ है, इंटरनेट पर व्यक्तियों का पर्सनल डेटा के खुलासे को सीमित करने का अधिकार।[4] श्रीकृष्ण कमिटी (2018) ने गौर किया था कि राइट टु बी फॉरगॉटन एक ऐसा विचार है जोकि अन्यथा सीमारहित डिजिटल क्षेत्र में मेमोरी की सीमा स्थापित करने का प्रयास करता है।[4] हालांकि कमिटी ने यह भी कहा था कि इस अधिकार को प्रतिस्पर्धी अधिकारों और हितों के साथ संतुलन बनाने की जरूरत हो सकती है। इस अधिकार के उपयोग से किसी दूसरे के मुक्त भाषण और अभिव्यक्ति के अधिकार और सूचना प्राप्त करने के अधिकार में दखल पड़ सकती है।[1] उसकी एप्लिकेबिलिटी कुछ कारकों पर निर्भर करती है जैसे डेटा की संवेदनशीलता, लोगों के लिए पर्सनल डेटा की प्रासंगिकता और सार्वजनिक जीवन में डेटा प्रिंसिपल की भूमिका।[1]

बच्चों के लिए अतिरिक्त प्रावधान

बिल: क्लॉज 2 (3) और 10

बच्चों के डेटा की प्रोसेसिंग पर अतिरिक्त बाध्याएं लागू होती हैं। हम इन प्रावधानों पर नीचे चर्चा कर रहे हैं।

माता-पिता की सत्यापन योग्य सहमति से, डिजिटल प्लेटफॉर्म पर प्रत्येक की आयु का सत्यापन करना पड़ सकता है

बिल में अपेक्षित है कि डेटा फिड्यूशरी किसी बच्चे के पर्सनल डेटा को प्रोसेस करने से पहले उसके कानूनी अभिभाव से सत्यापन योग्य सहमति हासिल करे। इस प्रावधान का अनुपालन करने के लिए हर डेटा फिड्यूशरी को उसकी सेवा के लिए साइन अप करने वाले प्रत्येक व्यक्ति की आयु का सत्यापन करना होगा। यह निर्धारित करना जरूरी होगा कि क्या व्यक्ति एक बच्चा है और इस बाद उसके कानूनी अभिभावक से सहमति लेनी होगी। इसका डिजिटल स्पेस में एनॉनिमिटी पर विपरीत असर हो सकता है। वर्तमान में कई डेटा फिड्यूशरी यूजर्स से यह डेक्लेरेशन लेते हैं कि वे सहमति देने की न्यूनतम अपेक्षित आयु से अधिक के हैं। चूंकि इस डेक्लेरेशन के अलावा कोई सत्यापन नहीं किया जाता, इसलिए एक बच्चा झूठा डेक्लेरेशन दे सकता है और सेवा का उपयोग कर सकता है। इस अंतराल को दूर करने के लिए आयु का प्रमाण जरूरी है जो एनॉनिमिटी से समझौता होगा।

बच्चे की परिभाषा अन्य क्षेत्राधिकारों से अलग

बच्चों को होने वाले नुकसान को कम करने के लिए डेटा फिड्यूशरीज़ की कुछ अतिरिक्त बाध्यताएं हैं। जबकि यह एक स्वीकृत सिद्धांत है कि बच्चों के डेटा की प्रोसेसिंग अधिक सुरक्षा के अधीन होनी चाहिए, लेकिन पर्सनल डेटा प्रोसेसिंग हेतु सहमति देने के लिए अलग-अलग क्षेत्राधिकार बच्चे को कैसे परिभाषित करते हैं, इसमें अंतर है। बिल के तहत बच्चे का अर्थ है, 18 वर्ष से कम आयु का कोई व्यक्ति। यूएसए और यूके में 13 वर्ष से अधिक आयु के व्यक्ति पर्सनल डेटा की प्रोसेसिंग के लिए सहमति दे सकते हैं।[19,20] यूरोपीय संघ के जीडीपीआर ने इसे 16 वर्ष की आयु पर निर्धारित किया है, उसके सदस्य देश इसे कम करके, 13 वर्ष तक कर सकते हैं।[21] श्रीकृष्ण कमिटी (2018) ने सुझाव दिया कि बच्चों की सहमति की आयु निर्धारित करते समय कुछ कारकों को ध्यान में रखा जाना चाहिए जैसे 13 वर्ष की न्यूनतम आयु और 18 वर्ष की अधिकतम आयु और व्यावहारिक कार्यान्वयन सुनिश्चित करने के लिए एक एकल सीमा।[4] उसने कहा था कि बच्चों के पूर्ण स्वायत्त विकास के लिहाज से 18 वर्ष की आयु बहुत अधिक हो सकती है।[4] हालांकि मौजूदा कानूनी संरचना के साथ संगति के लिए सहमति की आयु 18 वर्ष होनी चाहिए।[4] भारतीय कॉन्ट्रैक्ट एक्ट, 1972 के तहत किसी कॉन्ट्रैक्ट को साइन करने की न्यूनतम आयु 18 वर्ष है।[22]

'हानि' की परिभाषा

बिल: क्लॉज 2 (10)

बिल डेटा प्रिंसिपल के संबंध में हानि को इस प्रकार परिभाषित करता है, जैसे: (i) कोई शारीरिक हानि, (ii) पहचान को तोड़ना मरोड़ना या उसकी चोरी, (iii) उत्पीड़न, या (iv) कानूनी लाभ में रुकावट या भारी नुकसान का कारण। हम उपरोक्त परिभाषा से संबंधित कुछ मुद्दों पर चर्चा कर रहे हैं।

हानि की परिभाषा संकुचित हो सकती है

पर्सनल डेटा प्रोटेक्शन बिल, 2019 ने निम्नलिखित प्रकार की हानियां को निर्दिष्ट किया था: (i) मानसिक चोट, (ii) प्रतिष्ठा का नुकसान या अपमान, (iii) भेदभावपूर्ण व्यवहार, (iv) ब्लैकमेल या वसूली, (v) ऐसा कोई पर्यवेक्षण या निगरानी जिसकी डेटा प्रिंसिपल द्वारा समुचित रूप से अपेक्षा नहीं की जाती, और (vi) स्पीच, मूवमेंट पर नियंत्रण, या देखे जाने या निगरानी किए जाने के भय से उत्पन्न होने वाली कोई अन्य कार्रवाई।[23] 2022 के ड्राफ्ट बिल में इनमें से कोई शामिल नहीं है। ज्वाइंट पार्लियामेंटरी कमिटी (जेपीसी) ने सुझाव दिया था कि 2019 के बिल में हानियों की सूची में 'मनोवैज्ञानिक तिकड़म जो व्यक्ति की स्वायत्तता को बाधित करे' को शामिल किया जाए।[2] 2022 के ड्राफ्ट बिल में ऐसी हानि का प्रावधान नहीं है। यह अस्पष्ट है कि 2022 के ड्राफ्ट बिल में जिस शब्द 'उत्पीड़न' का इस्तेमाल किया गया है, उसमें उपरिलिखित हानियों के प्रकार शामिल होंगे। जेपीसी ने यह सुझाव दिया था कि केंद्र सरकार को हानियों के अन्य प्रकार को निर्दिष्ट करने का अधिकार दिया जाए।[2] उसने तर्क दिया था कि भविष्य में हानियों के नए प्रकार चिन्हित करने पर विचार किया जा सकता है। बिल में केंद्र सकार को ऐसी शक्तियां नहीं प्रदान की गई हैं।

भारी हानि क्या होती है, इस पर स्पष्टता की कमी

बिल के तहत हानि में कानूनी लाभ में रुकावट या भारी नुकसान का कारण शामिल है। यह अस्पष्ट है कि भारी नुकसान क्या होता है। बिल भारी नुकसान के निर्धारण के संबंध में कोई दिशानिर्देश नहीं देता।

डेटा प्रोटेक्शन कानून के विभिन्न ड्राफ्ट्स के बीच मुख्य अंतर

तालिका 1: डेटा प्रोटेक्शन कानून के विभिन्न ड्राफ्ट्स के बीच तुलना

ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल, 2018	पर्सनल डेटा प्रोटेक्शन बिल, 2019	ज्वाइंट पार्लियामेंटरी कमिटी के सुझाव	ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022
दायरा और एप्लिकेबिलिटी			
▪ पर्सनल डेटा की प्रोसेसिंग: (i) भारत में, (ii) भारत के बाहर अगर वह भारत में, वस्तुओं और सेवाओं को व्यवस्थित तरीके से पेश करने या व्यक्तियों की प्रोफाइलिंग, से जुड़े कारोबार के लिए है।	▪ अनाम (एनॉनिमाइज्ड) पर्सनल डेटा को शामिल करने के लिए 2018 के बिल का दायरा बढ़ाता है।	▪ नॉन-पर्सनल डेटा और अनाम पर्सनल डेटा को शामिल करने के लिए 2018 के बिल के दायरे को बढ़ाता है।	▪ 2018 के बिल की तुलना में, भारत में किए जाने वाले व्यवसाय को हटाता है, इसमें ऑफलाइन पर्सनल डेटा और नॉन-ऑटोमेटेड प्रोसेसिंग शामिल नहीं है।
डेटा ब्रीच को दर्ज करना			
▪ फिड्यूशरी डेटा ब्रीच के बारे में डेटा प्रोटेक्शन अथॉरिटी को बताएगा, जिसके हानि पहुंचाने की आशंका है, अथॉरिटी यह तय करेगी कि डेटा प्रिंसिपल को सूचना देनी है या नहीं।	▪ 2018 के बिल के समान।	▪ डेटा ब्रीच के प्रत्येक मामले की सूचना 72 घंटों के भीतर अथॉरिटी को देनी होगी, चाहे उससे हानि की आशंका हो अथवा न हो।	▪ पर्सनल डेटा ब्रीच के हर मामले की सूचना डेटा प्रोटेक्शन बोर्ड और प्रत्येक प्रभावित डेटा प्रिंसिपल को देनी होगी।
राज्य, सार्वजनिक व्यवस्था, अपराध के निवारण आदि के लिए बिल के प्रावधानों से छूट			
▪ प्रोसेसिंग किसी कानून के तहत अधिकृत होनी चाहिए, और कानून द्वारा स्थापित प्रक्रिया के अनुसार होनी चाहिए, और उसे आवश्यक और आनुपातिक होना चाहिए।	▪ केंद्र सरकार, आदेश द्वारा एजेंसियों को छूट दे सकती है, जहां प्रोसेसिंग जरूरी या उचित हो, और यह कुछ प्रक्रिया, सुरक्षात्मक उपायों और निरीक्षण के अधीन है।	▪ यह जोड़ा गया कि आदेश में एक प्रक्रिया निर्दिष्ट होनी चाहिए जोकि निष्पक्ष, न्यायसंगत और उचित हो।	▪ केंद्र सरकार अधिसूचना के जरिए छूट दे सकती है; किसी प्रक्रिया या सुरक्षात्मक उपाय को निर्दिष्ट करने की आवश्यकता नहीं है।
डेटा पोर्टेबिलिटी का अधिकार और राइट टु बी फॉरगॉटन			

ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल, 2018	पर्सनल डेटा प्रोटेक्शन बिल, 2019	ज्वाइंट पार्लियामेंटरी कमिटी के सुझाव	ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022
▪ डेटा प्रिंसिपल के पास डेटा पोर्टेबिलिटी (इंटरऑपरेबल फॉरमैट में डेटा हासिल करना) का अधिकार और राइट टु बी फॉरगॉटन (इंटरनेट पर पर्सनल डेटा के खुलासे पर नियंत्रण) होगा।	▪ दोनों अधिकारों के लिए प्रावधान था।	▪ दोनों अधिकारों के लिए प्रावधान था।	▪ प्रावधान नहीं है।
रेगुलेटर			
▪ निम्नलिखित की स्थापना करता है: (i) क्षेत्र को रेगुलेट करने के लिए भारतीय डेटा प्रोटेक्शन अथॉरिटी, और (ii) अपीलीय ट्रिब्यूनल।	▪ 2018 के बिल की तरह।	▪ 2018 के बिल की तरह।	▪ भारतीय डेटा प्रोटेक्शन बोर्ड का प्रावधान करता है, जिसका मुख्य कार्य गैर अनुपालन पर फैसले देना है; कोई अपीलीय ट्रिब्यूनल नहीं।
पर्सनल डेटा को भारत से बाहर ट्रांसफर करना			
▪ हर फिड्यूशरी को भारत में पर्सनल डेटा की कम से कम एक सर्विंग कॉपी स्टोर करनी होगी। ▪ अगर सहमति मिल जाती है तो वह भारत के बाहर कुछ अनुमोदित देशों या अथॉरिटी द्वारा मंजूर कॉन्ट्रैक्ट्स के तहत डेटा को ट्रांसफर कर सकता है। ▪ कुछ क्रिटिकल डेटा को भारत में ही प्रोसेस किया जा सकता है।	▪ संवेदनशील पर्सनल डेटा की एक कॉपी भारत में रहनी चाहिए। ▪ कुछ संवेदनशील पर्सनल डेटा को सिर्फ तभी ट्रांसफर किया जा सकता है, जब स्पष्ट सहमति प्रदान कर दी गई हो, दूसरे पर्सनल डेटा पर कोई पाबंदी नहीं है। ▪ क्रिटिकल पर्सनल डेटा पर 2018 के बिल के ही समान।	▪ यह जोड़ा गया कि संवेदनशील पर्सनल डेटा को केंद्र सरकार की पूर्व मंजूरी के बिना, विदेशी एजेंसियों या सरकार के साथ शेयर नहीं किया जाए।	▪ संवेदनशील और क्रिटिकल पर्सनल डेटा के वर्गीकरण को खत्म करता है। ▪ प्रावधान करता है कि पर्सनल डेटा को केंद्र सरकार द्वारा अधिसूचित देशों में ट्रांसफर किया जा सकता है, जोकि निर्दिष्ट शर्तों और नियमों के अधीन होगा।

स्रोत: इलेक्ट्रॉनिक्स और इनफॉरमेशन टेक्नोलॉजी मंत्रालय द्वारा जारी ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल, 2018 और ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2022; लोकसभा में पेश पर्सनल डेटा प्रोटेक्शन बिल, 2019; पर्सनल डेटा प्रोटेक्शन बिल, 2019 पर ज्वाइंट पार्लियामेंटरी कमिटी की रिपोर्ट; पीआरएस।

1. Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.
2. Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021.
3. The Information Technology Act, 2000.
4. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.
5. The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
6. The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
7. Rule 419A, The Indian Telegraph Rules, 1951 issued under Section 7 (2) of the Indian Telegraph Act, 1885.
8. People's Union for Civil Liberties (PUCL) vs Union of India, Supreme Court of India, December 18, 1996.
9. Chapter 3, Data Protection Act, 2018, United Kingdom.
10. Part 6, 7, and 8, Investigatory Powers Act, 2016, United Kingdom.
11. Shreya Singhal vs Union of India, Writ Petition (Criminal) No. 167 Of 2012, Supreme Court of India, March 24, 2015.
12. Chapter IX, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
13. Chapter II: Telecom Regulatory Authority of India, The Telecom Regulatory Authority of India Act, 1997.
14. Chapter III: Competition Commission of India, The Competition Act, 2002.
15 Chapter III: Central Information Commission, The Right to Information Act, 2005.
16. Clause 26, The Personal Data Protection Bill, 2018, as released by Ministry of Electronics and Information Technology.
17. Clause 19, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
18. Article 20, General Data Protection Regulation, European Union.
19. Children's Online Privacy Protection Rule ("COPPA"), Federal Trade Commission, USA, as accessed on December 6, 2022.
20. Guide to Data Protection, Information, Information Commissioner's Office, United Kingdom, as accessed on December 6, 2022.
21. Article 8, General Data Protection Regulation, European Union.
22. Section 11, The Indian Contract Act, 1872.
23. Clause 3(20), The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.