लेजिसलेटिव ब्रीफ

पर्सनल डेटा प्रोटेक्शन (ड्राफ्ट) बिल, 2018

जस्टिस बी.एन. श्रीकृष्ण की अध्यक्षता में विशेषज्ञ कमिटी ने 27 जुलाई, 2018 को इलेक्ट्रॉनिक्स और इनफॉरमेशन टेक्नोलॉजी मंत्रालय को ड्राफ्ट बिल सौंपा था।

हाल के लेजिसलेटिव ब्रीफ्स:

डीएनए टेक्नोलॉजी (प्रयोग और लागू होना) रेगुलेशन बिल, 2018

26 नवंबर, 2018

मानव तस्करी (निवारण, संरक्षण और पुनर्वास) बिल, 2018

30 अक्टूबर, 2018

मंदिरा काला
mandira@prsindia.org

आहिता पॉल
ahita@prsindia.org

21 दिसंबर, 2018

बिल की मुख्य विशेषताएं

- बिल सरकार तथा भारत और विदेश में निगमित निजी एंटिटीज़ (डेटा फिड्यूशरीज़) द्वारा लोगों के पर्सनल डेटा की प्रोसेसिंग को रेगुलेट करता है। व्यक्ति (डेटा प्रिंसिपल) की सहमति, या आपात स्थिति में, या सरकार द्वारा लाभ वितरण हेतु प्रोसेसिंग की अनुमति है।
- अपने डेटा के संबंध में डेटा प्रिंसिपल के अनेक अधिकार हैं जैसे डेटा में संशोधन करना या फिड्यूशरी के पास स्टोर किए गए डेटा को हासिल करना।
- किसी व्यक्ति के डेटा को प्रोसेस करने के दौरान फिड्यूशरी की कुछ बाध्यताएं हैं जैसे उस व्यक्ति को डेटा प्रोसेसिंग की प्रकृति और उसके उद्देश्यों की सूचना देना।
- बिल में डेटा प्रोसेसिंग के कुछ प्रावधानों के अनुपालन से छूट दी गई है जैसे राष्ट्रीय सुरक्षा के हित में, कानूनी बाध्यताओं के लिए या पत्रकारिता के उद्देश्यों के लिए डेटा प्रोसेस करना।
- बिल में अपेक्षा की गई है कि पर्सनल डेटा की एक सर्विंग कॉपी भारत के राज्य क्षेत्र में स्टोर की जाएगी। कुछ महत्वपूर्ण पर्सनल डेटा को सिर्फ देश में स्टोर किया जाएगा।
- डेटा फिड्यूशरीज़ को सुपरवाइज़ और रेगुलेट करने के लिए बिल के अंतर्गत राष्ट्रीय स्तर की एक डेटा प्रोटेक्शन अथॉरिटी (डीपीए) का गठन किया गया है।

प्रमुख मुद्दे और विश्लेषण

- डेटा फिड्यूशरी से यह अपेक्षा की गई है कि अगर डेटा के अतिक्रमण (ब्रीच) से किसी को नुकसान होने की आशंका है तो वह डीपीए को इस अतिक्रमण की सूचना देगा। संभव है कि किसी अतिक्रमण की सूचना देना है अथवा नहीं, इस संबंध में हितों का टकराव हो। चूंकि डीपीए अनेक मानदंडों के आधार पर फिड्यूशरी का रेगुलेशन और मूल्यांकन करती है। इसमें डेटा अतिक्रमण के मामले भी शामिल हैं।
- बिल पत्रकारिता, शोध या कानूनी प्रक्रिया जैसे उद्देश्यों के लिए छूट की अनुमति देता है। यहां यह प्रश्न किया जा सकता है कि क्या इन कारणों से किसी व्यक्ति की निजता के अधिकार का उल्लंघन किया जा सकता है। क्या ये उद्देश्य इतने आवश्यक हैं और निजता के अधिकार के उल्लंघन के अनुपात में हैं।
- सरकार से यह अपेक्षा नहीं की गई है कि लाभ या सेवाएं प्रदान करने के लिए किसी व्यक्ति की सहमति हासिल करे। यह अस्पष्ट है कि यह छूट केवल सरकार की कल्याणकारी सेवाओं तक सीमित क्यों नहीं है, जैसा कि जस्टिस श्रीकृष्ण कमिटी की रिपोर्ट में प्रस्तावित है।
- कानून प्रवर्तन करने वाली संस्थाओं को डेटा आसानी से हासिल हो जाए, इसके लिए बिल में यह अनिवार्य किया गया है कि भारत में पर्सनल डेटा की एक कॉपी को स्टोर किया जाए। कुछ मामलों में यह उद्देश्य हासिल नहीं किया जा सकता, जैसे अगर फिड्यूशरी किसी दूसरे देश में पंजीकृत हो।
- यह प्रश्न किया जा सकता है कि क्या डीपीए कानून का उल्लंघन करने वाले व्यक्तियों को न्यायालय की मंजूरी या आदेश के बिना गिरफ्तार कर सकती है या उन्हें हिरासत में ले सकती हैं।

भाग क : बिल की मुख्य विशेषताएं[1]

संदर्भ

किसी व्यक्ति के पर्सनल डेटा को जमा करने और उसका उपयोग करने के दौरान उसकी निजता का कम से कम उल्लघंन हो, इसके लिए बनी नीतियों और प्रक्रियाओं को डेटा प्रोटेक्शन कहा जाता है। भारत में नागरिकों के पर्सनल डेटा या सूचना के उपयोग को इनफॉरमेशन टेक्नोलॉजी एक्ट, 2000 के सेक्शन 43 ए के अंतर्गत इनफॉरमेशन टेक्नोलॉजी (उपयुक्त सुरक्षा पद्धति एवं प्रक्रियाएं तथा संवेदनशील डेटा या सूचना) नियम द्वारा रेगुलेट किया जाता है।[2] ये नियम स्पष्ट करते हैं कि पर्सनल इनफॉरमेशन वह सूचना होती है जिससे किसी व्यक्ति की पहचान की जा सकती है। इस नियम के अंतर्गत अगर डेटा से संबंधित सुरक्षा मानकों को प्रबंधित करने में किसी प्रकार की लापरवाही होती है तो बॉडी कॉरपोरेट (जोकि डेटा का इस्तेमाल कर रही है) उस व्यक्ति को मुआवजा देने के लिए जिम्मेदार होगी।

पिछले कुछ वर्षों के दौरान तकनीकी विकास के कारण विभिन्न गतिविधियों के जरिए बड़ी मात्रा में डेटा जनरेट किया जा रहा है और विभिन्न कंपनियां डेटा के आधार पर अपने फैसले लेने के लिए बाध्य हैं।[3] सरकारें भी लाभ वितरण के लिए बड़े पैमाने पर डेटा इकट्ठा कर रही हैं और उसका उपयोग कर रही हैं। इसका एक उदाहरण आधार की बायोमीट्रिक पहचान और सत्यापन प्रणाली है जिसके जरिए सरकार एलपीजी सबसिडी जैसे लाभों का लक्षित वितरण सुनिश्चित करती है।

2012 में सर्वोच्च न्यायालय में आधार की संवैधानिक वैधता को चुनौती दी गई थी और कहा गया था कि यह व्यक्ति के निजता के अधिकार का उल्लंघन करता है। इसके बाद अगस्त, 2017 में सर्वोच्च न्यायालय की नौ न्यायाधीशों की खंडपीठ ने फैसला दिया कि निजता का अधिकार भारतीय नागरिकों का मूलभूत अधिकार है।[4] न्यायालय ने कहा कि संविधान द्वारा निजता के अधिकार को अनुच्छेद 21 के अंतर्गत जीवन और व्यक्तिगत स्वतंत्रता के अधिकार के अभिन्न अंग के तौर पर संरक्षण प्राप्त है। न्यायालय ने यह भी कहा कि 'सूचनागत निजता', या पर्सनल डेटा और तथ्यों की निजता, निजता के अधिकार का अनिवार्य पहलू है।

विश्व के अनेक देशों ने सूचनाओं की प्रोसेसिंग के संबंध में व्यक्ति के अधिकारों के संरक्षण के लिए व्यापक रेगुलेटरी फ्रेमवर्क बनाएं हैं।[3] जुलाई 2017 में जस्टिस बी.एन. श्रीकृष्ण की अध्यक्षता में विशेषज्ञ कमिटी की स्थापना की गई थी जिसके निम्नलिखित कार्य थे (i) भारत में डेटा प्रोटेक्शन से संबंधित विभिन्न मुद्दों की जांच करना, (ii) उन्हें लक्षित करने के तरीके सुझाना, और (iii) ड्राफ्ट डेटा प्रोटेक्शन बिल का सुझाव देना।[5] 27 जुलाई, 2018 को इस ड्राफ्ट बिल को इलेक्ट्रॉनिक्स और इनफॉरमेशन टेक्नोलॉजी मंत्रालय को सौंपा गया। बिल पर्सनल डेटा के संबंध में व्यक्ति की स्वायत्तता की रक्षा करने, पर्सनल डेटा का इस्तेमाल करने वाली एंटिटीज़ के लिए डेटा प्रोसेसिंग के नियम निर्दिष्ट करने और डेटा प्रोसेसिंग की गतिविधियों का निरीक्षण करने के लिए रेगुलेटरी संस्था बनाने का प्रयास करता है।

प्रमुख विशेषताएं

- **परिभाषाएं:** बिल स्पष्ट करता है (i) 'पर्सनल डेटा' कोई ऐसी सूचना है जो व्यक्तिगत पहचान प्रदान करती है, (ii) डेटा 'प्रोसेसिंग' एक ऐसा कार्य है जिसमें डेटा को इकट्ठा करना, उसका मैन्यूपुलेशन, शेयरिंग या स्टोरेज शामिल हैं, (iii) 'डेटा प्रिंसिपल' वह व्यक्ति है जिसके पर्सनल डेटा को प्रोसेस किया जाता है, (iv) 'डेटा फिड्यूशरी' वह एंटिटी या व्यक्ति है, जो डेटा प्रोसेसिंग के प्रकार और उद्देश्यों को तय करता है, और (v) 'डेटा प्रोसेसर' वह एंटिटी या व्यक्ति होता है जो फिड्यूशरी की ओर से डेटा को प्रोसेस करता है।
- **किस क्षेत्र में लागू होता है:** बिल (i) सरकार और भारत में निगमित निजी एंटिटीज़, और (ii) विदेश में निगमित एंटिटीज़, अगर वे भारत के राज्यक्षेत्र में डेटा प्रिंसिपल्स के डेटा को नियमित रूप से प्रोसेस करती हैं, द्वारा पर्सनल डेटा की प्रोसेसिंग को प्रबंधित करता है। केंद्र सरकार एक अधिसूचना के जरिए उन भारतीय एंटिटीज़ को छूट दे सकती है जोकि विशेष रूप से भारत के राज्यक्षेत्र से बाहर डेटा प्रिंसिपल्स के डेटा को प्रोसेस करती हों।

  डेटा प्रोसेसिंग के आधार: बिल कहता है कि अगर किसी व्यक्ति ने सहमति दी हो तो फिड्यूशरीज़ डेटा प्रोसेसिंग कर सकते हैं। हालांकि कुछ मामलों में व्यक्ति की सहमति के बिना भी डेटा प्रोसेसिंग की अनुमति दी जा सकती है। यह अनुमति निम्नलिखित आधार पर दी जा सकती है (i) अगर संसद या राज्य विधानमंडल के कार्यों के लिए यह जरूरी है या अगर सरकार द्वारा लोगों को सुविधाएं प्रदान करने के लिए यह अपेक्षित है, (ii) अगर कानून के अंतर्गत या किसी अदालती आदेश के अनुपालन के लिए ऐसा करना जरूरी हो, (iii) मेडिकल इमरजेंसी की स्थिति में जरूरी कदम उठाने के लिए या कानून व्यवस्था भंग होने पर, (iv) रोजगार से संबंधित उद्देश्यों, जैसे भर्ती, के लिए, या (v) किन्हीं दूसरे उपयुक्त उद्देश्यों के लिए जिन्हें अथॉरिटी द्वारा निर्दिष्ट किया जाएगा, जैसे धोखाधड़ी का पता लगाने, ऋण की वसूली करने, क्रेडिट स्कोरिंग और व्हिसिल ब्लोइंग के मामलों में।
- **संवेदनशील पर्सनल डेटा:** बिल के अनुसार, संवेदनशील पर्सनल डेटा वह है जिसमें पासवर्ड्स, फाइनांशियल डेटा, बायोमीट्रिक और जेनेटिक डेटा, जाति, धर्म या राजनैतिक विश्वास शामिल होते हैं। बिल संवेदनशील पर्सनल डेटा की प्रोसेसिंग के लिए अधिक सख्ती की बात करता है जैसे प्रोसेसिंग करने से पहले व्यक्ति की स्पष्ट सहमति लेना।
- **डेटा प्रिंसिपल के अधिकार:** बिल उस डेटा प्रिंसिपल के कुछ अधिकार निर्धारित करता है, जिसके डेटा को प्रोसेस किया जा रहा है। इनमें निम्नलिखित शामिल हैं (i) डेटा फिड्यूशरी के पास अपने पर्सनल डेटा की समरी हासिल करने का अधिकार, (ii) गलत, अधूरे या पुराने पर्सनल डेटा में संशोधन की मांग करने का अधिकार, (iii) कुछ मामलों में किसी दूसरे डेटा फिड्यूशरी को पर्सनल डेटा ट्रांसफर करने का अधिकार, और (iv) 'टू बी फॉरगॉटन' का अधिकार, (यानी एक बार प्रयोग किए जाने के बाद किसी का व्यक्तिगत डेटा मिटा दिया जाए या उस डेटा को अनाम बता दिया जाए) जिसमें डेटा प्रिंसिपल अपने पर्सनल डेटा को प्रतिबंधित कर सकता या यह कह सकता है कि उसके डेटा का अब खुलासा न किया जाए।
- **डेटा फिड्यूशरी के लिए बाध्यताएं:** बिल में उस डेटा फिड्यूशरी की बाध्याएं निर्धारित की गई हैं जो पर्सनल डेटा को प्रोसेस करते हैं। इनमें निम्नलिखित शामिल हैं: (i) डेटा प्रोसेसिंग को उचित और तर्कसंगत तरीके से प्रोसेस करना, (ii) डेटा प्रिंसिपल को डेटा कलेक्शन की प्रकृति और उद्देश्यों, उनके अधिकारों, इत्यादि की सूचना देना, और (iii) सिर्फ उतने डेटा को इकट्ठा करना, जितना किसी विशिष्ट उद्देश्य के लिए जरूरी है और उसे तभी तक स्टोर करना, जब तक कि ऐसा करना जरूरी हो।

- **छूट:** बिल डेटा प्रोसेसिंग की कुछ गतिविधियों को छूट देता है। बिल के अनुसार, निम्नलिखित उद्देश्यों के लिए किसी व्यक्ति के पर्सनल डेटा की प्रोसेसिंग निर्दिष्ट बाध्यताओं के अधीन नहीं होगी और डेटा प्रिंसिपल्स को बिल में निर्दिष्ट अधिकार प्राप्त नहीं होंगे (i) राष्ट्रीय सुरक्षा (कानून के अनुसार) के लिए, (ii) किसी अपराध को रोकने, उसकी जांच करने या प्रॉसीक्यूशन के लिए, (iii) कानूनी कार्यवाही के लिए (iv) व्यक्तिगत या घरेलू उद्देश्यों के लिए, और (v) पत्रकारिता के उद्देश्य के लिए।
- इन उद्देश्यों के लिए डेटा प्रोसेस इन शर्तों पर ही किया जा सकता है (i) पर्सनल डेटा को निष्पक्ष और उचित तरीके से प्रोसेस किया जाए, और (ii) डेटा प्रोसेसिंग के लिए उपयुक्त सुरक्षात्मक उपाय सुनिश्चित किए जाएं।
- शोध के लिए डेटा प्रोसेसिंग को भी उस सीमा तक छूट दी जाती है, जितनी बिल के अंतर्गत गठित डेटा प्रोटेक्शन अथॉरिटी द्वारा निर्दिष्ट की गई है। बीस लाख रुपए से कम के टर्नओवर वाली छोटी एंटिटीज़, जोकि सौ डेटा प्रिंसिपल्स से कम के डेटा को प्रोसेस करती हैं, को भी बिल के अधिकतर प्रावधानों से छूट दी गई है।
- **डेटा प्रोटेक्शन अथॉरिटी:** बिल डेटा प्रोटेक्शन अथॉरिटी (डीपीए) की स्थापना का प्रावधान करता है। डीपीए की निम्नलिखित शक्तियां हैं (i) विभिन्न क्षेत्रों के सभी डेटा फिड्यूशरीज़ के लिए विशिष्ट रेगुलेशंस बनाना, (ii) डेटा फिड्यूशरीज़ का निरीक्षण करना, (iii) बिल के अनुपालन का आकलन करना और प्रवर्तन संबंधी कार्रवाई करना, और (iv) डेटा प्रिंसिपल्स की शिकायतों को प्राप्त करना, उनका प्रबंधन करना और उनका निवारण करना। इस अथॉरिटी में एक चेयरपर्सन और छह सदस्य होंगे जिन्हें डेटा प्रोटेक्शन और इनफॉरमेशन टेक्नोलॉजी के क्षेत्र में कम से कम दस वर्षों का अनुभव हो।
- डीपीए के पास सजा और मुआवजा देने के लिए अलग से एक एडजूडिकेशन विंग होगा। एडजूडिकेटिंग ऑफिसर साइबर और संवैधानिक कानून, और डेटा प्रोटेक्शन जैसे विषयों में कम से कम सात वर्ष के पेशेवर अनुभव प्राप्त विशेषज्ञ होंगे। डीपीए के आदेशों के खिलाफ केंद्र सरकार द्वारा गठित अपीलीय ट्रिब्यूनल में अपील की जा सकती है और ट्रिब्यूनल के खिलाफ सर्वोच्च न्यायालय में अपील की जा सकती है।
- **डेटा का सीमा पारीय स्टोरेज:** बिल के अनुसार, प्रत्येक फिड्यूशरी भारत में स्थित सर्वर या डेटा सेंटर में सभी पर्सनल डेटा की 'सर्विंग कॉपी' रखेगा। केंद्र सरकार उन विशेष श्रेणियों के पर्सनल डेटा को अधिसूचित करके, इस शर्त से छूट दे सकती है, अगर उसे ऐसा जरूरी लगता हो या रणनीतिक हितों के लिए ऐसा करना जरूरी हो। केंद्र सरकार कुछ विशेष श्रेणियों के पर्सनल डेटा को 'महत्वपूर्ण पर्सनल डेटा' के तौर पर अधिसूचित कर सकती है जिन्हें केवल भारत में स्थित सर्वर्स में प्रोसेस किया जाएगा।
- **देश के बाहर डेटा का ट्रांसफर:** पर्सनल डेटा (संवेदनशील पर्सनल डेटा को छोड़कर, जोकि 'महत्वपूर्ण' है) को विशिष्ट स्थितियों में भारत के बाहर ट्रांसफर किया जा सकता है। इनमें ऐसे मामले शामिल हैं जहां (i) केंद्र सरकार यह निर्धारित करती है कि उस विशेष देश में ट्रांसफर की अनुमति है, या (ii) जब डीपीए इस बात को मंजूर करती है कि ट्रांसफर जरूरी स्थितियों में किया जा रहा है।
- **अपराध और सजा:** बिल के अंतर्गत अथॉरिटी कानून का उल्लंघन करने पर फिड्यूशरीज़ को सजा दे सकती है। जिन प्रावधानों का उल्लंघन करने पर सजा का प्रावधान किया गया है, वे निम्नलिखित हैं (i) डेटा प्रोसेसिंग की बाध्यताएं, (ii) डीपीए द्वारा जारी निर्देश, और (iii) सीमा पारीय डेटा स्टोरेज और ट्रांसफर संबंधी शर्तें। उदाहरण के लिए फिड्यूशरी को किसी भी डेटा ब्रीच की सूचना डीपीए को देनी होगी, जिससे प्रिंसिपल को नुकसान पहुंचने की आशंका हो। डीपीए को सूचित न करने पर फिड्यूशरी को पांच करोड़ रुपए या अपने विश्वस्तरीय टर्नओवर का दो प्रतिशत, जो भी अधिक हो, का जुर्माना भरना पड़ सकता है।
- इसके अतिरिक्त पर्सनल और संवेदनशील पर्सनल डेटा को हासिल करने, उसका खुलासा करने, उसे ट्रांसफर करने, बेचने या बेचने की पेशकश करने वाले व्यक्ति को पांच वर्ष तक की सजा भुगतनी पड़ सकती है या तीन लाख रुपए तक का जुर्माना भरना पड़ सकता है।

भाग ख: प्रमुख मुद्दे और विश्लेषण

'निष्पक्ष और उचित' तरीके से डेटा प्रोसेसिंग के लिए कोई दिशानिर्देश नहीं

बिल: सेक्शन 4, 11(2)

बिल के अनुसार, 'डेटा प्रिंसिपल' वह व्यक्ति है जिसका डेटा प्रोसेस किया गया है। 'डेटा फिड्यूशरी' वह सर्विस प्रोवाइडर हो सकता है जो वस्तुएं और सेवाएं प्रदान करने के लिए डेटा को इकट्ठा करता है, उसे स्टोर और इस्तेमाल करता है। डेटा प्रोसेस करते समय फिड्यूशरी यह सुनिश्चित करने के लिए बाध्य है कि डेटा 'निष्पक्ष और उचित तरीके से प्रोसेस किया जाए जोकि व्यक्ति की निजता का सम्मान करे।' इसके अतिरिक्त फिड्यूशरी को डेटा प्रोटेक्शन अथॉरिटी (डीपीए) के सामने यह प्रदर्शित करना होगा कि डेटा निष्पक्ष और उचित तरीके से प्रोसेस किया गया है। इस प्रावधान का उल्लंघन होने पर फिड्यूशरी को अपने विश्वस्तरीय टर्नओवर का चार प्रतिशत जुर्माना भरना पड़ेगा (न्यूनतम 15 करोड़ रुपए के अधीन)।

हालांकि बिल सभी डेटा फिड्यूशरीज़ पर यह बाध्यता निश्चित करता है लेकिन डेटा प्रोसेसिंग के 'निष्पक्ष और उचित तरीके' से संबंधित सिद्धांत या दिशानिर्देश निर्दिष्ट नहीं करता है। मार्गदर्शक सिद्धांत न होने से एक जैसी डेटा प्रोसेसिंग करने वाले फिड्यूशरीज़ अलग-अलग तरह के मानकों को अपनाएंगे और एक उद्योग से जुड़े फिड्यूशरीज़ अलग-अलग तरह के मानकों का विकास और अनुपालन करेंगे। इसके अतिरिक्त किसी दिशानिर्देश के अभाव में फिड्यूशरीज़ से उनका अनुपालन करने की उम्मीद करना अनुचित होगा। उल्लेखनीय है कि इस प्रावधान का अनुपालन न करने से भारी-भरकम मुआवजा भरना पड़ सकता है।

जस्टिस श्रीकृष्ण कमिटी की रिपोर्ट ने सुझाव दिया है कि न्यायालयों और रेगुलेटरी अथॉरिटीज़ को निष्पक्ष तथा उचित प्रोसेसिंग के सिद्धांतों को विकसित करने की अनुमति होनी चाहिए।[5] बदलते समय में तकनीकी प्रगति के साथ तथा विभिन्न डेटा फिड्शरीज़ के बीच ये मानक भिन्न-भिन्न हो सकते हैं।[5]

डेटा ब्रीच की रिपोर्ट का विकल्प देने से हितों का टकराव संभव

बिल: सेक्शन 3(21), 3(30), 32(1), 35(2), 35(5)

बिल के अंतर्गत डीपीए द्वारा डेटा फिड्यूशरीज़ को रेगुलेट किया जाएगा जोकि उनके द्वारा कानून के अनुपालन का आकलन करेगी, उचित कार्रवाई करेगी और सजा तय करेगी। बिल के अनुसार अगर डेटा अतिक्रमण से प्रिंसिपल को किसी तरह के नुकसान की आशंका है (जैसे डेटा

का दुर्घटनावश या अनाधिकृत इस्तेमाल या उसका खुलासा) तो फिड्यूशरी इसकी सूचना डीपीए को देगा। प्रश्न यह है कि क्या फिड्यूशरी के पास इस बात का निर्णय लेने का अधिकार है कि डीपीए को अतिक्रमण की सूचना देने की जरूरत है।

डेटा अतिक्रमण के चुनींदा मामलों की सूचना देने से अथॉरिटी के पास कम महत्व वाले मामले नहीं पहुंचेंगे और फिड्यूशरी पर भी सूचना देने का दबाव नहीं होगा। लेकिन इससे हितों के टकराव की आशंका हो सकती है कि अतिक्रमण के किसी मामले की सूचना दी जाए अथवा नहीं, क्योंकि डीपीए ही फिड्यूशरी को रेगुलेट कर रही है। उसका ऑडिट एक स्कोर के रूप में सारबद्ध किया जाता है जोकि सार्वजनिक होता है और फिड्यूशरी की विश्वसनीयता को प्रभावित करता है। इसके अतिरिक्त डेटा अतिक्रमण के जोखिम को कम महत्व देने में फिड्यूशरीज़ का आर्थिक हित भी हो सकता है, चूंकि ऐसे कई मामले हुए हैं जब अतिक्रमण ने कंपनियों के स्टॉक प्राइज़ेज़ को नकारात्मक रूप से प्रभावित किया है।[6]

कुछ प्रकार की डेटा प्रोसेसिंग को छूट देने से सवाल उठ सकते हैं

बिल: सेक्शन 44, 45, 46, 47, 48

बिल डेटा प्रिंसिपल की सूचना को प्रोसेस करने के लिए सभी डेटा फिड्यूशरीज़ के लिए कुछ बाध्यताएं निर्धारित करता है। फिड्यूशरी को प्रिंसिपल को इसकी सूचना देनी होगी और प्रोसेसिंग से पहले उसकी सहमति हासिल करनी होगी। वे विशिष्ट उद्देश्यों के लिए डेटा का इस्तेमाल कर सकते हैं और केवल तब तक उसे उचित सुरक्षात्मक उपायों के साथ स्टोर कर सकते हैं, जब तक कि उसकी जरूरत है। इसके अतिरिक्त अपने डेटा के संबंध में डेटा प्रिंसिपल को कुछ अधिकार भी हैं, जैसे (i) फिड्यूशरी के पास अपने पर्सनल डेटा की समरी हासिल करने का अधिकार, और (ii) गलत, अधूरे या पुराने डेटा में संशोधन की मांग करने का अधिकार।

हालांकि उपरिलिखित बाध्यताएं और सुरक्षात्मक उपाय तब लागू नहीं होंगे, जब डेटा को निम्नलिखित उद्देश्यों के लिए प्रोसेस किया जाएगा (i) राष्ट्रीय सुरक्षा, (ii) किसी अपराध का निवारण, उसकी जांच और प्रॉसीक्यूशन, (iii) कानून कार्यवाहियां, (iv) व्यक्तिगत या घरेलू उद्देश्य, और (v) शोध और पत्रकारिता संबंधी उद्देश्य। प्रश्न यह है कि क्या बिल में उल्लिखित सभी प्रकार की छूट देना न्यायसंगत है।

पुट्टास्वामी बनाम भारत संघ मामले में सर्वोच्च न्यायालय ने कुछ स्थितियों में किसी व्यक्ति की निजता के अधिकार के संबंध में अपवादों को अनुमति दी थी। इनमें ऐसे मामले शामिल हैं जहां एक बड़े सार्वजनिक उद्देश्य को पूरा करने के लिए किसी व्यक्ति की निजता का उल्लंघन हो। इन अपवादों को कानून का समर्थन प्राप्त होना चाहिए और उस उद्देश्य को हासिल करने के लिए यह जरूरी और उसके अनुपात में होना चाहिए। ऐसा लगता है कि कानून के अनुसार, राष्ट्रीय सुरक्षा संबंधी छूट तर्कसंगत है। लेकिन यह अस्पष्ट है कि कानूनी कार्यवाहियों, या शोध तथा पत्रकारिता संबंधी उद्देश्यों के लिए क्या यह छूट जरूरी है और उसके अनुपात में है। उल्लेखनीय है कि आधार की संवैधानिकता पर फैसला देते समय सर्वोच्च न्यायालय ने कहा था कि सिम कार्ड्स से आधार नंबर को जोड़ने का प्रावधान गैर अनुपातिक है, इसलिए असंवैधानिक है।[7]

बिल निम्नलिखित कानूनी कार्यवाहियों के लिए पर्सनल डेटा के खुलासे की अनुमति देता है (i) कानूनी अधिकार या दावे को लागू करना, (ii) किसी आरोप पर अपनी सफाई देना, और (iii) कानूनी सलाह लेना। प्रश्न किया जा सकता है कि क्या इस छूट के आधार पर न्यायालय के आदेश के बिना व्यक्तिगत सूचना की मांग करना अनुमति योग्य है। यह भी अस्पष्ट है कि *पुट्टास्वामी बनाम भारत संघ* मामले में जो अपवाद पेश किए गए थे, क्या शोध और पत्रकारिता संबंधी उद्देश्य उसमें शामिल किए जा सकते हैं। इन छूटों का वैध उद्देश्य यह है कि पत्रकारिता संबंधी स्वतंत्रता प्राप्त हो या शोध की गुंजाइश छोड़ी जाए। इस छूट को डेटा प्रिंसिपल्स की निजता की सुरक्षा के साथ संतुलन बैठना होगा।

सरकार के कामकाज के लिए डेटा प्रोसेसिंग के लिए सहमति जरूरी नहीं

सरकार द्वारा सेवाओं और लाभों के प्रावधान के लिए सहमति हासिल करने का तर्क अस्पष्ट है

बिल: सेक्शन 13(2), 19

बिल के अंतर्गत डेटा फिड्यूशरीज़ (सरकार सहित) बिना सहमति के किसी व्यक्ति के डेटा को प्रोसेस नहीं कर सकते। हालांकि सरकार कुछ कार्यों के लिए सहमति के बिना भी डेटा को प्रोसेस कर सकती है, जैसे (i) सेवाओं और लाभ के वितरण के लिए, और (ii) सर्टिफिकेशन, लाइसेंस और परमिट जारी करने के लिए। जस्टिस श्रीकृष्ण कमिटी की रिपोर्ट में कहा गया है कि नागरिकों और सरकार के बीच शक्ति का असंतुलन है। इसलिए सरकारी लाभ हासिल करने के लिए सहमति की वैधता पर सवाल खड़े किए जा सकते हैं।[5] इसलिए व्यक्ति की सहमति के बिना भी सरकारी लाभ की प्रकृति वाली किसी भी सेवा के लिए डेटा प्रोसेसिंग की अनुमति होनी चाहिए।

इसके अतिरिक्त रिपोर्ट कहती कि बिना सहमति के डेटा प्रोसेसिंग की अनुमति केवल उन्हीं सरकारी संस्थाओं को दी जानी चाहिए जोकि लाभ वितरण और रेगुलेटरी कार्य से प्रत्यक्ष रूप से जुड़ी हुई हैं।[5] हालांकि रिपोर्ट स्वीकार करती है कि सरकारी संस्थाओं को सहमति के बिना प्रोसेसिंग की छूट देने से इस छूट का दायरा बहुत व्यापक हो जाएगा। इसके बावजूद बिल सभी सरकारी सेवाओं के लिए सहमति के बिना डेटा प्रोसेसिंग की अनुमति देता है।[5] उदाहरण के लिए इसमें सार्वजनिक क्षेत्र के बैंक या सार्वजनिक क्षेत्र की दूरसंचार कंपनियां शामिल हो सकती हैं। जबकि इन क्षेत्रों की निजी संस्थाओं को डेटा प्रोसेसिंग के लिए व्यक्ति की सहमति हासिल करना जरूरी होगा।

विधानमंडल के कार्यों के लिए सहमति के बिना प्रोसेसिंग का उद्देश्य अस्पष्ट है

बिल: सेक्शन 13(1), 19

बिल के अनुसार, संसद या राज्य विधानमंडल के किसी कार्य के लिए बिना सहमति के डेटा प्रोसेसिंग की जा सकती है। यह अस्पष्ट है कि संसद के किस कार्य के लिए बिना सहमति के प्रोसेसिंग करना जरूरी है।

भारत में डेटा की कॉपी को स्टोर करना

बिल: सेक्शन 40, 41(1)

बिल के अनुसार प्रत्येक डेटा फिड्यूशरी को भारत में स्थित सर्वर में सभी पर्सनल और संवेदनशील पर्सनल डेटा की 'सर्विंग कॉपी' रखनी होगी। केंद्र सरकार जरूरत या रणनीतिक हितों के आधार पर पर्सनल डेटा की कुछ श्रेणियों को इस शर्त से छूट दे सकती है। इसके अतिरिक्त सरकार कुछ 'महत्वपूर्ण पर्सनल डेटा' को अधिसूचित कर सकती है जिसे भारत स्थित सर्वर्स में ही प्रोसेस किया जाएगा।

'सर्विंग कॉपी' और 'महत्वपूर्ण पर्सनल डेटा' की परिभाषा नहीं दी गई

यह अस्पष्ट है कि डेटा की 'सर्विंग कॉपी' के क्या अर्थ हैं। वह भारत में स्थित सर्वर में डेटा का लाइव, रियल टाइम रेप्लिकेशन हो सकता है या वह ऐसा बैकअप हो सकता है जिसे समय-समय पर तैयार किया जाए। इस संबंध में निर्देश देना जरूरी है क्योंकि 'सर्विंग कॉपी' की

प्रकृति कैसी है, इसी के आधार पर फिड्यूशरीज़ के लिए लागत, प्रभाव और लागू करने की समय सीमा तय होगी, जोकि सभी के लिए अलग-अलग हो सकती है। इसके अतिरिक्त यह कहा जा सकता है कि कानून में इस संबंध में व्यापक मानदंड निर्दिष्ट होने चाहिए कि कोई डेटा कितना 'महत्वपूर्ण' है। इसी के आधार पर फिड्यूशरीज़ भारत में डेटा स्टोर करने के संबंध में तैयारी करेंगे।

देश के भीतर डेटा की कॉपी का स्थानीय स्टोरेज अस्पष्ट है

जस्टिस श्रीकृष्ण कमिटी की रिपोर्ट में पर्सनल डेटा के स्थानीय स्टोरेज के लाभ को स्वीकार किया गया था।[5] इससे जांच के लिए कानून प्रवर्तन एजेंसियों द्वारा डेटा की प्रोसेसिंग की प्रक्रिया सरल होगी और उसमें तेजी आएगी। इससे विदेश में भारतीय नागरिकों की चौकसी नहीं की जा सकेगी और आर्टिफिशियल इंटेलिजेंस में घरेलू शोध को बढ़ावा मिलेगा।

हालांकि ऐसा जरूरी नहीं है कि कुछ मामलों में कानून का प्रवर्तन तेजी से हो, जैसे उस स्थिति में जब डेटा फिड्यूशरी किसी दूसरे देश में एक एंटिटी के रूप में पंजीकृत हो। ऐसे मामलों में दो देशों के कानूनों में आपसी टकराव के कारण आपसी विधि सहायता संधि (म्युचुअल लीगल एसिस्टेंस ट्रीटीज़) (एमएलएटीज़) लागू होती है।[5] जस्टिस श्रीकृष्ण कमिटी की रिपोर्ट ने कहा था कि एमएलएटी प्रक्रिया में काफी समय लगता है और इसलिए कानून प्रवर्तन में तेजी लाने का उद्देश्य स्थानीय स्तर पर डेटा स्टोर करने से पूरा नहीं हो सकता।[5]

इसके अतिरिक्त कुछ डेटा फिड्यूशरीज़ भारतीय बाजार में निवेश करने से हतोत्साहित हो सकते हैं क्योंकि उन्हें डुप्लीकेट सर्वर लगाने के कारण अतिरिक्त खर्च करना पड़ेगा और इसलिए उपभोक्ताओं को सभी डेटा फिड्यूशरीज़ की सेवाएं चुनने का विकल्प गंवाना पड़ सकता है। कुछ डिटिजल सेवाओं के लिए उपभोक्ताओं को भी अतिरिक्त कीमत चुकानी पड़ सकती है। इसका असर उन छोटे डेटा फिड्यूशरीज़ पर पड़ सकता है जो सस्ती वैकल्पिक स्टोरेज प्रणाली पर निर्भर होते हैं।

उल्लेखनीय है कि यूरोपीय संघ, ऑस्ट्रेलिया और कनाडा के कानूनों के अनुसार देश में डेटा की कॉपी स्टोर करना जरूरी नहीं है।[3] इसके अतिरिक्त ऑस्ट्रेलिया और कनाडा के कानून डेटा यूज़र (फिड्यूशरी) को स्वतंत्र रूप से यह निश्चित करने की अनुमति देते हैं कि क्या डेटा देश से बाहर ट्रांसफर किया जा सकता है।[3] बिल इस फैसले में डीपीए की संलग्नता की शर्त रखता है जोकि यूरोपीय संघ के समान है।

नुकसान की आशंका होने पर ही शिकायत दर्ज कराई जा सकती है

बिल डेटा प्रोसेसिंग पर अनेक प्रतिबंध लगाता है (जैसे विशिष्ट उद्देश्य के लिए जरूरी डेटा को ही इकट्ठा करना, इत्यादि) और अपने डेटा पर डेटा प्रिंसिपल को नियंत्रण का अधिकार देता है। हालांकि डेटा प्रिंसिपल तभी शिकायत दर्ज कर सकता है जब बिल के प्रावधानों का उल्लंघन होने पर उसे नुकसान हो या नुकसान होने की आशंका हो। यह सवाल खड़ा किया जा सकता है कि क्या शिकायत दर्ज कराने के लिए सिर्फ प्रिंसिपल के अधिकारों का अतिक्रमण होना पर्याप्त नहीं है। डेटा प्रिंसिपल को अतिरिक्त रूप से यह प्रदर्शित करना होगा और साबित करना होगा कि गैरकानूनी डेटा प्रोसेसिंग के कारण उन्हें नुकसान हुआ है और यह डेटा प्रिंसिपल पर अतिरिक्त भार डाल सकता है।

बिल: सेक्शन 39(2)

डेटा प्रोटेक्शन अथॉरिटी की शक्तियां और कार्य

डीपीए द्वारा सजा और मुआवजा के आदेश के प्रवर्तन के लिए न्यायालय के आदेश की जरूरत नहीं

बिल डीपीए को यह अधिकार देता है कि कानूनी प्रावधानों का उल्लंघन होने पर डीपीए डेटा फिड्यूशरीज़ को सजा दे सकती है। डीपीए द्वारा नियुक्त रिकवरी ऑफिसर्स के पास डीपीए के सजा और मुआवजे के आदेश को लागू करने की शक्ति होगी। डीपीए के आदेश के अनुसार ऑफिसर्स डेटा फिड्यूशरीज़ के खिलाफ अनेक कार्रवाइयां कर सकते हैं जिनमें निम्नलिखित शामिल हैं (i) चल एवं अचल संपत्ति की कुर्की और बिक्री, और (ii) गिरफ्तारी और जेल में नजरबंदी।

बिल: सेक्शन 78(1), 78(2)

बिल यह विनिर्दिष्ट नहीं करता कि इस कार्रवाई के लिए किसी अदालती आदेश की जरूरत है। दूसरे एक्ट्स रेगुलेटरों, जैसे आरबीआई या इरडा को संपत्ति की कुर्की और बिक्री तथा लोगों की गिरफ्तारी की अनुमति तभी देते हैं जब न्यायालय की मंजूरी मिल जाए। हालांकि प्रतिभूति कानून (संशोधन) एक्ट, 2014 के बाद सेबी एक्ट सेबी के रिकवरी ऑफिसर्स को इस बात की अनुमति देता है कि वे बोर्ड के आदेश के बाद ऐसी कार्रवाई कर सकते हैं।[8]

विशेष डेटा प्रोटेक्शन जागरूकता फंड की स्थापना से हितों का टकराव संभव

बिल विनिर्दिष्ट करता है कि उसके प्रावधानों के उल्लंघन पर पंद्रह करोड़ रुपए या फिड्यूशरी के विश्वस्तरीय वार्षिक टर्नओवर का चार प्रतिशत जुर्माने के तौर पर वसूला जाएगा। इस जुर्माने को डेटा प्रोटेक्शन जागरूकता फंड में जमा किया जाएगा और डीपीए निम्नलिखित के विषय में जागरूकता फैलाने के लिए उसका उपयोग करेगी (i) डेटा एनॉनिमाइजेशन के तरीके, और (ii) डेटा अतिक्रमण पर उचित कार्रवाई करना, इत्यादि। यह अस्पष्ट है कि बिल के अंतर्गत जुर्माने को भारत के समेकित कोष में क्यों जमा नहीं किया जाएगा। विशेष डेटा प्रोटेक्शन जागरूकता कोष अलग से बनाने से, जिसका उपयोग डीपीए द्वारा किया जाएगा, डीपीए द्वारा अधिक जुर्माना लगाने की आशंका हो सकती है और विवादों में मध्यस्थता तथा शिकायत निवारण के दौरान हितों का टकराव हो सकता है। सेबी एक्ट, 1992 जैसे एक्ट्स में यह अनिवार्य किया गया है कि जुर्माने के तौर पर जमा होने वाली राशि को भारत के समेकित कोष में जमा कराया जाएगा।[9] हालांकि पीएफआरडीए एक्ट, 2013 पेंशन फंड के सबस्क्राइबर्स के हितों की रक्षा करने के लिए सबस्क्राइबर एजुकेशन एंड प्रोटेक्शन फंड की स्थापना करता है। इस एक्ट के अंतर्गत एकत्र होने वाला जुर्माना इस फंड में जमा होता है और सिर्फ पीएफआरडीए द्वारा इस्तेमाल किया जाता है।[10]

बिल: सेक्शन 77(2), 77(3)

'राइट टू बी फॉरगॉटन' के संबंध में एडजुडिकेटिंग ऑफिसर के पास विशेषतज्ञता नहीं भी हो सकती है

बिल के अंतर्गत डेटा प्रिंसिपल कुछ अधिकारों का उपयोग कर सकता है, जैसे (i) फिड्यूशरी के पास मौजूद पर्सनल डेटा की समरी हासिल करने का अधिकार, (ii) गलत पर्सनल डेटा में संशोधन की मांग करने का अधिकार, और (iii) 'राइट टू बी फॉरगॉटन' जिसमें डेटा प्रिंसिपल अपने पर्सनल डेटा को प्रतिबंधित कर सकता या यह कह सकता है कि उसके डेटा का अब खुलासा न किया जाए। राइट टू बी फॉरगॉटन के उपयोग के लिए डेटा प्रिंसिपल को डीपीए को लिखित अनुरोध करना होगा।

बिल: सेक्शन 27(1), 27(2), 68(3)

डीपीए का एक एडजुडिकेटिंग ऑफिसर यह तय करेगा कि डेटा प्रिंसिपल के राइट टू बी फॉरगॉटन के उपयोग से क्या किसी व्यक्ति की अभिव्यक्ति की स्वतंत्रता या सूचना के अधिकार का उल्लंघन होता है। सामान्य तौर पर न्यायलयों द्वारा ऐसे मामलों की व्याख्या की जाती है। एक तरफ एडजुडिकेटिंग ऑफिसर की योग्यता का मानदंड संवैधानिक कानून में उसका ज्ञान और विशेषज्ञता है, यह ऑफिसर दूसरे क्षेत्रों,

जैसे डेटा प्रोटेक्शन का भी विशेषज्ञ हो सकता है। ऐसी स्थिति में उस ऑफिसर के पास अभिव्यक्ति की स्वतंत्रता के संभावित उल्लंघन के संवैधानिक मुद्दे पर फैसला लेने की विशेषज्ञता नहीं भी हो सकती है।

डेटा प्रोटेक्शन और निजता से संबंधित अंतरराष्ट्रीय कानूनों से बिल की तुलना

बिल में ऐसे अनेक प्रावधान हैं जोकि यूरोपीय संघ, ऑस्ट्रेलिया और कनाडा में डेटा संरक्षण और निजता के कानूनों से अलग हैं। तालिका 1 ऐसे कुछ प्रावधानों का उल्लेख कर रही है जोकि भिन्न हैं।

तालिका 1: डेटा प्रोटेक्शन और निजता के कानूनों की अंतरराष्ट्रीय तुलना

देश	यूरोपीय संघ	ऑस्ट्रेलिया	कनाडा	भारत (प्रस्तावित ड्राफ्ट बिल)
एंटिटीज़ का कवरेज	▪ निजी और सरकारी एंटिटीज़ के लिए एक कानून	▪ निजी और सरकारी एंटिटीज़ के लिए एक कानून	▪ निजी और संघीय सरकार की एंटिटीज़ के लिए अलग-अलग कानून	▪ निजी और सरकारी एंटिटीज़ के लिए एक कानून
संवेदनशील पर्सनल डेटा	▪ फाइनांशियल डेटा, पासवर्ड्स शामिल नहीं	▪ फाइनांशियल डेटा, पासवर्ड्स शामिल नहीं	▪ अलग से स्पष्ट नहीं, कोई भी डेटा संदर्भ के आधार पर संवेदनशील हो सकता है	▪ फाइनांशियल डेटा, पासवर्ड्स शामिल
किसी देश में डेटा का स्टोरेज और शेयरिंग				
डेटा का स्थानीय स्टोरेज	▪ अनिवार्य नहीं	▪ अनिवार्य नहीं ▪ क्षेत्र आधारित अनिवार्यताएं, जैसे स्वास्थ्य संबंधी डेटा	▪ अनिवार्य नहीं	▪ कॉपी रखने की अनिवार्यता, महत्वपूर्ण पर्सनल डेटा सिर्फ देश में स्टोर
डेटा का सीमा पारीय ट्रांसफर	▪ अनुमति है, अगर यूरोपीय कमीशन तय करता है कि डेटा प्राप्त करने वाले देश में डेटा संरक्षण के पर्याप्त मानदंड हैं	▪ अनुमति है, अगर प्रोसेसिंग करने वाली एंटिटी यह सुनिश्चित करने के लिए कदम उठाएं कि प्राप्तकर्ता देश के निजता के सिद्धांतों का अतिक्रमण नहीं करता	▪ अनुमति है, अगर प्रोसेसिंग एंटिटी संरक्षण के तुलनात्मक स्तर को सुनिश्चित करने के लिए अनुबंधीय या दूसरे तरीके इस्तेमाल करती है	▪ (कुछ डेटा की) अनुमति है, अगर रेगुलेटर द्वारा मंजूर हो या सरकार द्वारा विनिर्दिष्ट हो
रेगुलेशन और प्रवर्तन				
डेटा अतिक्रमण की सूचना	▪ संभावित हानिकारक अतिक्रमण की सूचना रेगुलेट को देनी होगी ▪ व्यक्ति को सूचना देने की आवश्यकता नहीं, अगर प्रोसेसिंग एंटिटी ने उपयुक्त सुधारात्मक उपाय किए या उसे इसके लिए अतिरिक्त परिश्रम करना पड़े	▪ संभावित हानिकारक अतिक्रमण की सूचना रेगुलेटर और प्रभावित व्यक्तियों को देनी होगी	▪ संभावित हानिकारक अतिक्रमण की सूचना रेगुलेटर और प्रभावित व्यक्तियों को देनी होगी *(संशोधन अब लागू नहीं)*	▪ संभावित हानिकारक अतिक्रमण की सूचना रेगुलेटर को देनी होगी ▪ रेगुलेटर गंभीरता या व्यक्ति की कार्रवाई की जरूरत के आधार पर तय करेगा कि क्या व्यक्ति को सूचना देनी है
आपराधिक सजा	▪ कोई आपराधिक सजा नहीं	▪ कोई आपराधिक सजा नहीं	▪ कोई आपराधिक सजा नहीं	▪ कुछ अपराधों के लिए पांच वर्ष तक की सजा

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; India - The Personal Data Protection (Draft) Bill, 2018; PRS

1. This Brief has been written on the basis of the Personal Data Protection (Draft) Bill, as presented to the Ministry of Electronics and Information Technology, by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, on July 27, 2018.
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
3. Data protection and privacy statutes in various countries: European Union – The General Data Protection Regulation, 2016; Australia – The Privacy Act, 1988; Canada – The Personal Information Protection and Electronic Documents Act, 2000; The Privacy Act, 1985.
4. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors, W.P. (C) No. 494 of 2012, August 24, 2017.
5. "A Free and Fair Digital Economy", Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna.
6. In September 2017, Equifax stock prices fell by 18% after they announced a data breach affecting 143 million people.
7. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors, W.P. (C) No. 494 of 2012, September 26, 2018.
8. Clause 21, The Securities Laws (Amendment) Act, 2014.
9. Section 15JA, The Securities and Exchange Board of India Act, 1992.
10. Section 29, The Pension Fund Regulatory and Development Authority Act, 2013.