डेटा स्थानीयकरण से संबंधित मुद्दे

लेखक-ऋषभ बेली (अध्येता, नेशनल इंस्टीट्यूट ऑफ पब्लिक फाइनेंस एंड पॉलिसी, नई दिल्ली)

यह आलेख सामान्य अध्ययन प्रश्न पत्र-III (आंतरिक सुरक्षा, साइबर क्राइम) से संबंधित है।

द हिन्दू

25 फरवरी, 2020

"संशोधित व्यक्तिगत डेटा संरक्षण विधेयक में स्थानीय डेटा संग्रहण पर विवादास्पद खंडों की फिर से जाँच की आवश्यकता है।"

लोकसभा के शीतकालीन सत्र में पेश किए गए कई महत्त्वपूर्ण कानूनों में से एक व्यक्तिगत डेटा संरक्षण (PDP) विधेयक, 2019 था। विधेयक को एक संयुक्त संसदीय समिति को प्रेषित किया गया था, जो वर्तमान में सार्वजनिक परामर्श की प्रक्रिया से जुड़ी हुई है।

मसौदा कानून एक व्यापक कानून है, जो व्यक्तियों को इस बात पर अधिक नियंत्रण देने का प्रयास करता है कि उनका व्यक्तिगत डेटा कैसे एकत्र, संग्रहित और उसका उपयोग किया जाए। एक बार पारित होने के बाद, विधेयक वर्तमान भारतीय गोपनीयता कानून में कई सुधारों की बात करता है, जिसे अपर्याप्त और अनुचित रूप से लागू किया गया है।

हालाँकि, पीडीपी विधेयक भी दोषरहित नहीं है। इसे विभिन्न आधारों पर आलोचना का सामना करना पड़ा है, जिसमें राज्य के लिए बनाए गए अपवाद, राज्य निगरानी पर लगाए गए सीमित जाँच और प्रस्तावित डेटा संरक्षण प्राधिकरण की संरचनाओं और प्रक्रियाओं में विभिन्न कमियां शामिल हैं।

व्यक्तिगत डेटा संरक्षण बिल 2019

संक्षिप्त पृष्ठभूमि

- अगस्त 2017 में, सुप्रीम कोर्ट की 9 न्यायाधीशों वाली पीठ ने ' पुट्टूस्वामी केस ' में निजता को भारतीय नागरिकों का मौलिक अधिकार घोषित किया था। न्यायालय ने यह भी कहा कि 'सूचनात्मक गोपनीयता' या व्यक्तिगत डेटा और तथ्यों की गोपनीयता, निजता के अधिकार का एक अनिवार्य पहलू है।
- विदित है कि व्यक्तिगत डेटा संरक्षण विधेयक, 2018 (Personal Data Protection Bill, 2018), सुप्रीम कोर्ट के पूर्व न्यायाधीश बी. एन. श्रीकृष्णा की अध्यक्षता में एक उच्च-स्तरीय विशेषज्ञ समूह द्वारा तैयार किया गया था, परंतु अंतर मंत्रालयी वार्ताओं के कारण उस समय संसद से यह प्रस्ताव पारित नहीं हो सका था।
- यह डेटा साझाकरण में "सहमति" की नैतिकता को बनाए रखने और गोपनीयता मानदंडों का उल्लंघन करने वालो को दंडित करने के लिए, गोपनीयता ढाँचे को विकसित करने का पहला कदम है।

ड्राफ्ट बिल में डेटा स्थानीयकरण

कानून के अधिक विवादास्पद मुद्दों में से एक "डेटा स्थानीयकरण" से संबंधित प्रावधान हैं। यह वाक्यांश, जो डेटा के सीमा पार हस्तांतरण पर किसी भी प्रतिबंध का उल्लेख कर सकता है (उदाहरण के लिए, स्थानांतरण के लिए अनुमति लेने की आवश्यकता, डेटा के विदेशी हस्तांतरण के लिए करों का अधिरोपण आदि) काफी हद तक देश के भीतर डेटा को रखने की आवश्यकता को संदर्भित करता है।

पीडीपी बिल भारत के बाहर व्यक्तिगत डेटा के हस्तांतरण को सक्षम बनाता है, जिसमें संवेदनशील व्यक्तिगत डेटा की उप-श्रेणी देश में एक प्रतिलिपि के रूप में होगी। हालाँकि, डेटा प्रोसेसिंग/इकट्ठा करने वाली इकाइयाँ महत्त्वपूर्ण व्यक्तिगत डेटा (एक श्रेणी जिसे सरकार बाद के चरण में अधिसूचित कर सकती है) को देश के बाहर स्थानांतरित करने से राकेगी।

इन प्रावधानों को मसौदा विधेयक के पुराने संस्करण से बदल दिया गया है, जिसे 2018 में न्यायमूर्ति श्रीकृष्ण समिति द्वारा जारी किया गया था। 2018 के मसौदे में और अधिक कड़े उपाय लागू किए गए थे जिनके लिए देश में (विभिन्न स्थितियों के अधीन) व्यक्तिगत और संवेदनशील व्यक्तिगत डेटा दोनों को प्रतिबिंबित किया जाना आवश्यक है।

विधेयक के 2019 संस्करण में प्रावधानों को उदार बनाने का यह कदम निस्संदेह स्वागतयोग्य है, खासकर व्यवसायों और उपयोगकर्ताओं के लिए। उदारीकृत आवश्यकताएँ व्यवसाय के लिए लागतों को सीमित करेंगी और साथ ही यह भी सुनिश्चित करेंगी कि उपयोगकर्ताओं को अपने डेटा को संग्रहीत करने के लिए अधिक लचीलापन प्राप्त हो सके।

प्रथम दृष्टया, 2019 के मसौदे में बदलाव इस मुद्दे के लिए अधिक आनुपातिक दृष्टिकोण को दर्शाता है, ऐसा इसलिए क्योंकि वे डेटा की संवेदनशीलता पर आधारित सीमा पार से डेटा ट्रांसफर के लिए एक थकाऊ प्रणाली को लागू करते हैं। यह 2017 के पुट्टस्वामी मामले में सुप्रीम कोर्ट के फैसले के अनुसार लगता है, जहाँ कोर्ट ने स्पष्ट कर दिया था कि निजता के मौलिक अधिकार में हस्तक्षेप केवल तभी स्वीकार्य होगा जब अन्य बातों के साथ-साथ यह आवश्यक और समानुपातिक हो।

हालाँकि, करीब से जाँच करने पर यह प्रतीत होता है कि संशोधित कानून वास्तव में आनुपातिकता की कसौटी पर खरा नहीं उतर सका है।

स्थानीयकरण का उद्देश्य

मोटे तौर पर डेटा स्थानीयकरण मानदंडों को लागू करने के पक्ष में व्यापक रूप से तीन तर्क दिए गए हैं: जिसमें पहला है संप्रभुता और सरकारी कार्य; जो भारतीय डेटा को राष्ट्रीय हित (आर्थिक और रणनीतिक रूप से) के लिए उपयोग किए जाने वाले संसाधन के रूप में पहचान करने की आवश्यकता और भारतीय कानून तथा राज्य कार्यों के प्रवर्तन को सक्षम करने की आवश्यकता का उल्लेख करता है।

दूसरा तर्क है कि एआई इकोसिस्टम में स्थानीय बुनियादी ढाँचा, रोजगार और योगदान देने के मामले में स्थानीय उद्योग को आर्थिक लाभ होगा। अंत में, नागरिक स्वतंत्रता के संरक्षण के बारे में यह तर्क है कि डेटा की स्थानीय मेजबानी भारतीय कानून को डेटा पर लागू कर के अपनी गोपनीयता और सुरक्षा को बढ़ाएगी और उपयोगकर्ता स्थानीय उपचार तक पहुँच बनाने में सक्षम हो सकेंगे।

उपयोगकर्ता की गोपनीयता की रक्षा?

नेशनल इंस्टीट्यूट ऑफ पब्लिक फाइनेंस एंड पॉलिसी द्वारा प्रकाशित 2018 वर्किंग पेपर में, हमने (लेखक) इस धारणा में गिरावट पर ध्यान दिलाया कि डेटा स्थानीयकरण से बेहतर गोपनीयता सुरक्षा को बढ़ावा मिलेगा। हमने पाया कि डेटा की सुरक्षा को तकनीकी उपायों, कौशल, साइबर सुरक्षा प्रोटोकॉल आदि द्वारा निर्धारित किया जाता है।

स्थानीयकरण से नागरिकों पर निगरानी आसान हो सकती है। हालाँकि, यह भारतीय नागरिकों द्वारा विदेशी खुफिया सहित डेटा तक किसी भी तरह की अनधिकृत पहुँच के खिलाफ निजता के अधिकार के बेहतर प्रयोग को भी सक्षम कर सकता है।

कुल मिलाकर, डेटा को सुरक्षा प्रदान करना डेटा सुरक्षा व्यवस्था की प्रभावशीलता पर निर्भर करेगी।

इसके अलावा, पीडीपी विधेयक का अतिरिक्त क्षेत्रीय अनुप्रयोग यह भी सुनिश्चित करता है कि देश के बाहर डेटा स्थानांतरित होने पर भी कानून के तहत् डेटा सुरक्षा दायित्वों का अस्तित्व बना रहे।

यदि गोपनीयता सुरक्षा वास्तविक विचार है, तो व्यक्तियों को अपने डेटा को किसी भी स्थान पर संग्रहीत करने के लिए सक्षम बनाना होगा। पीडीपी विधेयक में पहले उल्लिखित समस्याओं को देखते हुए, यह तर्कपूर्ण है कि यूरोपीय संघ या कैलिफोर्निया में संग्रहीत और संसाधित किए जाने पर भारतीयों का डेटा अधिक सुरक्षित रहेगा (इन दोनों के पास मजबूत डेटा संरक्षण कानून और उन्नत तकनीकी पारिस्थितिकी तंत्र हैं)।

इन परिस्थितियों में, संयुक्त संसदीय समिति के लिए यह महत्त्वपूर्ण हो जाता है कि वर्तमान में कानून में स्थानीयकरण के प्रावधानों का अधिक गहन मूल्यांकन करने के लिए विधेयक की जाँच की जाए। संयुक्त संसदीय समिति को आदर्श रूप से पीडीपी विधेयक में निहित (अपेक्षाकृत उदार) उपायों की आवश्यकता, उद्देश्य और व्यावहारिकता की पहचान करनी चाहिए।

विशेषताएँ

- संवेदनशील व्यक्तिगत डेटा को केवल व्यक्ति की स्पष्ट सहमति के साथ संसाधित किया जा सकता है और यह सहमति सूचित, स्पष्ट एवं विशिष्ट होनी आवश्यक है। यह डेटा केवल डेटा संरक्षण प्राधिकरण की अनुमति से विदेशों में भेजा जा सकता है।
- विधेयक के प्रावधानों का पालन नहीं करने पर विधेयक 5 करोड़ या 2% टर्नओवर (जो भी अधिक हो) दंड का प्रावधान भी करता है।
- सरकार नागरिकों को बेहतर सेवाएँ प्रदान करने के लिए गैर-व्यक्तिगत डेटा तक पहुँच प्राप्त करने के लिए एक प्रत्ययी (संस्था या व्यक्ति) को निर्देशित करने का हक प्रदान करता है।
- कुछ परिस्थितियों में, व्यक्ति की सहमति के बिना डेटा के प्रसंस्करण की अनुमति दी जा सकती है, इनमें- (I) संसद या राज्य विधायिका के किसी कार्य के लिए (II) किसी न्यायालय के फैसले का अनुपालन के लिए (III) एक चिकित्सा आपातकाल का जवाब देने या सार्वजनिक व्यवस्था के टूटने से निपटने के लिए (IV) रोजगार से संबंधित प्रयोजन के लिए (V) डेटा संरक्षण अधिनियम द्वारा निर्दिष्ट उचित उद्देश्य के लिए।
- 'राष्ट्रीय सुरक्षा' के हित में, कुछ सरकारी एजेंसियों के पास अपराधों से संबंधित किसी भी जाँच के लिए व्यक्तिगत डेटा तक पहुँच हो सकती है।
- केंद्र सरकार के द्वारा महत्त्वपूर्ण व्यक्तिगत डेटा (Critical Personal Data) को अधिसूचित करने का भी प्रावधान किया गया है, यह महत्त्वपूर्ण व्यक्तिगत डेटा तब केवल भारत में स्थित एक सर्वर या डेटा सेंटर में संसाधित किया जाएगा।

इसके अलावा, स्थानीयकरण-संबंधी मानदंडों को लाभदायक बनाने के लिए, चाहे वह नागरिक अधिकारों की रक्षा के लिए हो या कानून प्रवर्तन की डेटा तक पहुँच सुनिश्चित करने के लिए हो या स्थानीय अर्थव्यवस्था के विकास को सक्षम करने के लिए हो, नीतिगत स्तर पर व्यापक सोच को विकसित करना पड़ेगा। उदाहरण के लिए, निगरानी संबंधी कानूनों में सुधार करना, अधिक विस्तृत और अद्यतित पारस्परिक कानूनी सहायता संधियों में शामिल होना, पर्याप्त डिजिटल बुनियादी ढाँचे के विकास को सक्षम करना और उचित डेटा-साझाकरण नीतियाँ बनाना, जो गोपनीयता और अन्य पक्ष के अधिकारों को संरक्षित करते हैं।

चिंता के विषय

- डेटा के स्थानीयकरण (Localisation) से भारत को ऐसी सेवाओं के लिए एक असुगम बाजार बना दिया जाएगा, जो स्थानीयकरण की वित्तीय लागत की भरपाई नहीं कर सकती।
- यह भारतीय स्टार्ट-अप्स या सेवा उद्योग को विश्व स्तर पर विस्तार करने से रोक सकता है। क्योंकि कुछ डिजिटल सेवाओं के लिए उपभोक्ताओं से अतिरिक्त लागत वसूल की जा सकती है।
- हाल ही में, मैसेजिंग प्लेटफॉर्म व्हाट्सएप ने कहा कि, कुछ भारतीय पत्रकार और अधिकार कार्यकर्ता उन लोगों में शामिल थे, जिनकी जासूसी एक इजरायली कंपनी की प्रौद्योगिकी द्वारा की जा रही थी। इजरायल की इस कंपनी के अनुसार वह दुनिया भर की 'सरकारी एजेंसियों' के लिए काम करती है।
- Google ने अपने 500 भारत के उपभोक्ताओं सहित दुनिया के 12,000 उपयोगकर्ताओं को अलर्ट किया था कि उनके खिलाफ "सरकार समर्थित" फिशिंग (phishing) के प्रयास किये जा रहे हैं। भारत सरकार ने अभी भी इन घटनाओं के बारे में कोई स्पष्टीकरण नहीं दिया है ।
- डाटा प्रत्ययी (Data Fiduciary): "डेटा फिड्यूसरी" एक सेवा प्रदाता हो सकता है जो सामान और सेवाएँ प्रदान करने के दौरान डेटा एकत्र या, संग्रहीत और उपयोग करता है। डेटा को संसाधित करते समय, यह सुनिश्चित करने के लिए कि फिड्यूसरी बाध्य है कि डेटा को 'निष्पक्ष और उचित तरीके से संसाधित किया जाना है जो व्यक्ति की गोपनीयता का सम्मान करता है।'
- विधेयक में कहा गया है कि प्रत्येक डेटा फिड्यूसरी भारत में एक सर्वर में सभी व्यक्तिगत और संवेदनशील व्यक्तिगत डेटा की 'सेवारत प्रतिलिपि (Serving copy)' रखेगा।
- महत्वपूर्ण डेटा फिड्यूसरी: डेटा प्रोटेक्शन अथॉरिटी अपने डेटा प्रोसेसिंग, जैसे डेटा की मात्रा, डेटा की संवेदनशीलता, कंपनी के टर्नओवर के आधार पर कुछ संस्थाओं को महत्वपूर्ण डेटा फिड्यूसरी के रूप में लेबल कर सकती है।
- सरकार कुछ "महत्त्वपूर्ण व्यक्तिगत डेटा (Critical Personal Data)" को अधिसूचित कर सकती है जिसे केवल भारत में स्थित सर्वरों में संसाधित किया जाएगा। हालाँकि, बिल में 'सेवारत प्रति (Serving copy)' और 'महत्त्वपूर्ण व्यक्तिगत डेटा' की परिभाषाएँ नहीं दी गई हैं।
- विधेयक के अनुसार, जहाँ भी सरकार को यह आवश्यक लगता है, वह निर्देश दे सकती है कि इस तरह के व्यक्तिगत डेटा के प्रसंस्करण के संबंध में, इस अधिनियम के सभी या कोई प्रावधान सरकार की किसी भी एजेंसी पर लागू नहीं होंगे।
- स्थानीयकरण भारतीय डेटा को विदेशी खतरों से बचा सकता है।

GS World Committed To Excellence

संभावित प्रश्न (प्रारंभिक परीक्षा)

प्र. व्यक्तिगत डेटा संरक्षण (PDP) विधेयक, 2019 के संदर्भ में, निम्नलिखित कथनों पर विचार कीजिए:

1. यह विधेयक न्यायमूर्ति राजिन्दर सच्चर के 2018 के मसौदे से प्रेरित है।
2. पीडीपी विधेयक केवल भारत के अंदर व्यक्तिगत डेटा के हस्तांतरण को सक्षम बनाता है।
3. इस विधेयक में डेटा स्थानीयकरण से संबंधित प्रावधान भी शामिल हैं।

उपर्युक्त में से कौन-सा/से कथन असत्य है/हैं?

(a) केवल 1 (b) 1 और 2

(c) केवल 3 (d) 1 और 3

Expected Questions (Prelims Exams)

Q. Consider the following statements in the context of the Personal Data Protection (PDP) Bill, 2019.

1. The Bill is inspired by the draft of Justice Rajinder Sachar 2018.
2. The PDP Bill enables the transfer of personal data only within India.
3. The Bill also contains provisions related to data localization.

Which of the above statements is / are incorrect ?

(a) Only 1 (b) 1 and 2

(c) Only 3 (d) 1 and 3

नोट : 24 फरवरी को दिए गए प्रारंभिक परीक्षा (संभावित प्रश्न) का उत्तर 1 (a) होगा।

संभावित प्रश्न (मुख्य परीक्षा)

प्र. डेटा के स्थानीयकरण से क्या अभिप्राय है? आधुनिक विश्व में यह क्यों आवश्यक है? भारत के विशेष संदर्भ में इसके महत्त्व को भी दर्शाएं। (250 शब्द)

What does Data Localization mean? Why is it necessary in the modern world? Also show its importance in the special reference of India. (250 words)

नोट :- अभ्यास के लिए दिया गया मुख्य परीक्षा का प्रश्न आगामी UPSC मुख्य परीक्षा को ध्यान में रख कर बनाया गया है। अतः इस प्रश्न का उत्तर लिखने के लिए आप इस आलेख के साथ-साथ इस टॉपिक से संबंधित अन्य स्रोतों का भी सहयोग ले सकते हैं।