ज्ञानविविधा
कला, मानविकी और सामाजिक विज्ञान की सहकर्मी-समीक्षित, मूल्यांकित, त्रैमासिक शोध पत्रिका

ISSN : 3048-4537(Online)
3049-2327(Print)
IIFS Impact Factor-2.25
Vol.-2; Issue-3 (July-Sept.) 2025
Page No.- 15-24

https://journal.gyanvividha.com

VINOD KUMAR
UGC-NET.

Corresponding Author :

VINOD KUMAR
UGC-NET.

Data Privacy as a Fundamental Right

I. परिचय : पर्यावरण एवं पृष्ठभूमि

वर्तमान युग में अर्थव्यवस्था, शासन और सामाजिक व्यवहार का केंद्रबिंदु डिजिटलीकरण बन चुका है। सूचना एवं संचार प्रौद्योगिकी (ICT) का प्रसार, डेटा-संचालित व्यवसाय मॉडल, और इंटरनेट ऑफ थिंग्स (IoT) ने वैश्विक स्तर पर पारंपरिक कामकाजी प्रणालियों को पूरी तरह से परिवर्तित कर दिया है। एंटरप्राइजेज से लेकर शिक्षा, स्वास्थ्य देखभाल और मनोरंजन तक, सभी क्षेत्रों में डिजिटल प्लेटफ़ॉर्म और क्लाउड-सर्विसेज का व्यापक उपयोग हो रहा है। इस परिवर्तन ने न केवल कार्यप्रणालियों को सुगम बनाया है, बल्कि डेटा की मात्रा और उसकी विविधता में भी अभूतपूर्व वृद्धि की है ।

डिजिटलीकरण की प्रवृत्ति और व्यक्तिगत डेटा का विस्तार

डिजिटलीकरण की तेज़ी ने व्यक्तिगत डेटा की मात्रा में अभूतपूर्व वृद्धि की है। केवल अप्रैल 2025 तक ही, विश्व की लगभग 5.64 अरब जनसंख्या इंटरनेट से जुड़ी हुई थी, जो कुल आबादी का 68.7% से अधिक है । IDC के अनुमानों के अनुसार, वर्ष 2025 तक प्रत्येक व्यक्ति प्रतिदिन औसतन 4,900 से भी अधिक डिजिटल इंटरैक्शन करेगा, अर्थात् लगभग प्रत्येक 18 सेकंड पर एक डेटा जनरेशन होगी । भारत में डिजिटल भुगतान, ई-गवर्नेंस पोर्टल एवं "डिजिटल इंडिया" पहल के कारण डेटा जेनरेशन और भी तीव्र गति से बढ़ी है; केंद्र सरकार की MeitY वार्षिक रिपोर्ट 2021–22 के अनुसार, राज्य-स्तरीय और केंद्र-स्तरीय सभी योजनाओं में डिजिटल चैनलों के माध्यम से होने वाले लेनदेन और रिकॉर्ड संकलन में पिछले पांच वर्षों में कई गुना वृद्धि हुई है।

गोपनीयता के अधिकार का वैश्विक तथा भारतीय संदर्भ

इन सभी प्रगतियों के बीच, व्यक्तिगत गोपनीयता का अधिकार और भी अधिक महत्वपूर्ण हो गया है। **वैश्विक मानवाधिकार संरचनाओं** में,

Universal Declaration of Human Rights का अनुच्छेद 12 स्पष्ट रूप से प्रत्यक्ष या अप्रत्यक्ष हस्तक्षेप से सुरक्षा की गारंटी देता है: "कोई भी व्यक्ति अपने निजी जीवन, परिवार, आवास या पत्राचार में मनमानी दखल से नहीं गुजरना चाहिए" । इसी प्रकार, **International Covenant on Civil and Political Rights** का अनुच्छेद 17 भी इसी रक्षा की व्यवस्था करता है । **भारतीय संवैधानिक परिदृश्य** में, उच्चतम न्यायालय ने **न्यायमूर्ति के.एस. पुत्तस्वामी बनाम भारत संघ (2017)** के निर्णय में अनुच्छेद 21 के अंतर्गत गोपनीयता को व्यक्तिगत स्वतंत्रता का अभिन्न एवं मौलिक अधिकार माना है । इस निर्णय ने भारत में डेटा गोपनीयता की कानूनी नींव रखी, परंतु साथ ही कई नियामक और संवैधानिक अंतराल भी उजागर किए, जिन्हें आगामी संशोधनों से पाटने की आवश्यकता है।

II. पुत्तस्वामी निर्णय का अवलोकन

1. न्यायमूर्ति के.एस. पुत्तस्वामी बनाम भारत संघ (2017) का सार : न्यायमूर्ति के.एस. पुत्तस्वामी (सेवानिवृत्त) एवं अन्य बनाम भारत संघ एवं अन्य, (2017) 10 SCC 1 में सुप्रीम कोर्ट ने नौ-न्यायाधीशीय पीठ द्वारा विचारणीय प्रश्न यह निर्भर करता है कि क्या "गोपनीयता का अधिकार" भारतीय संविधान के भाग III अन्तर्गत मौलिक अधिकार के रूप में मान्यता प्राप्त है। याचिका का मूल आधार-व्यवस्था में अनिवार्य पहचान संख्या को सरकारी तथा निजी संस्थानों से जोड़ने के आदेश के विरुद्ध निजता की रक्षा की माँग था। याचिकाकर्ताओं ने तर्क दिया कि व्यक्तिगत डेटा का इस प्रकार अनियंत्रित उपयोग नागरिकों के निजता अधिकार का हनन है तथा यह अनुच्छेद 21 (जीवन और व्यक्तिगत स्वतंत्रता की रक्षा) का उल्लंघन है ।

2. तथ्यात्मक पृष्ठभूमि एवं याचिकाकर्ताओं के तर्क याचिका दायर की गई थी ताकि आधार नंबर के बहुआयामी और अनियंत्रित उपयोग—जैसे बैंकिंग, शिक्षा, सार्वजनिक वितरण प्रणाली इत्यादि—को चुनौती दी जा सके। याचिकाकर्ताओं ने संविधान के मूल ढाँचे में व्यक्तिस्थ मौलिक अधिकारों का हवाला देते हुए कहा कि आधार प्रणाली नागरिकों की गोपनीयता और व्यक्तिगत स्वायत्तता पर अप्रयुक्त हस्तक्षेप का माध्यम बन चुकी है। उन्होंने कहा कि पहले के निर्णय—खरक सिंह बनाम उत्तर प्रदेश एवं एम.पी. शर्मा बनाम भारत संघ—को पुनर्विचार की आवश्यकता थी, क्योंकि उन निर्णयों में गोपनीयता को मौलिक अधिकार नहीं माना गया था ।

3. संवैधानिक अनुच्छेद 21 एवं गोपनीयता का मौलिक अधिकार मान्यता : पीठ ने सर्वसम्मति से यह माना कि गोपनीयता "जीवन और व्यक्तिगत स्वतंत्रता" का अविभाज्य अंग है और भाग III की अन्य स्वतंत्रताओं के साथ जुड़ा हुआ है। न्यायालय ने स्पष्ट किया कि अनुच्छेद 21 के अंतर्गत "न्यायसंगत, उचित और संवैधान द्वारा स्थापित प्रक्रिया" (procedure established by law) का अभिप्राय केवल "प्रक्रिया" तक सीमित नहीं, बल्कि अंतरराष्ट्रीय मानवाधिकार मानकों के अनुरूप "न्यायसंगत, उचित और अनुपातपूर्ण प्रक्रिया" को भी शामिल करता है ।

4. निर्णय के मुख्य बिंदु

(क) निजता की परिभाषा एवं उसके आयाम: निर्णय में निजता को पाँच प्रमुख आयामों—सूचना गोपनीयता, शारीरिक गोपनीयता, निर्णय गोपनीयता, संपत्ति गोपनीयता एवं संघ गोपनीयता—में वर्गीकृत किया गया है। न्यायालय ने निजता को "इस बात का अधिकार कि हम कब, किसे और कितना स्वयं से संबंधित सूचना का प्रकटीकरण करें" के रूप में परिभाषित किया ।

(ख) राज्य की हस्तक्षेप सीमा एवं संतुलन की कसौटी: अदालत ने यह निर्धारित किया कि किसी भी मौलिक अधिकार में हस्तक्षेप तभी वैध होगा जब वह –

(i) विधि द्वारा स्थापित हो,

(ii) वैध एवं आवश्यक लक्ष्य के लिए हो,

(iii) मध्यस्थता की कसौटी पर खरा उतरे।

इस तीन-चरणीय परीक्षण ने संवैधानिक हस्तक्षेप की सीमाओं को स्पष्ट किया ।

इस प्रकार, पुत्तस्वामी निर्णय ने भारतीय संविधान में गोपनीयता के अधिकार को पक्की संवैधानिक नींव प्रदान की और भविष्य में डेटा-संबंधी नियमों तथा संवैधानिक संशोधनों के लिए मार्गदर्शक सिद्धांत स्थापित किए।

III. निर्णयोपरांत कानूनी अंतराल

1. **आधार अधिनियम पर पुत्तस्वामी का प्रभाव (2018) :** न्यायालय ने 26 सितंबर 2018 को अपने आदेश में स्पष्ट किया कि आधार अधिनियम 2016 के कई प्रावधान—विशेषकर बैंकिंग, शिक्षा, सार्वजनिक वितरण प्रणाली एवं मोबाइल सेवाओं के साथ आधार अनिवार्य करने वाले नियम—संवैधानिक नहीं ठहराए जा सकते, जब तक कि उन्हें "न्यायसंगत, उचित और अनुपातपूर्ण" प्रक्रिया की कसौटी पर नहीं तौला गया । इस निर्णय ने सरकार को निर्देश दिया कि आधार को केवल सेवा की सुलभता एवं लक्ष्य निर्धारण तक सीमित रखा जाए, अन्यथा व्यक्तियों के निजता अधिकार का उल्लंघन होगा।

2. **आधार अधिनियम 2016 के प्रावधानों में संशोधन संबंधी आवश्यकता :** आधार अधिनियम—जिसे बाद में संशोधित भी किया गया—में बायोमेट्रिक डेटा के संग्रह, भंडारण अवधि, पुनःप्रमाणीकरण और प्राधिकरण के दायरे जैसे विषय अस्पष्ट रहे। उदाहरणतः, अधिनियम के अनुच्छेद 7 में बायोमेट्रिक पहचान के विस्तृत प्रावधानों को सीमित करना और अनुच्छेद 29 में डेटा प्रस्तुतिकरण के उपयोग पर पाबन्दियाँ लगाना आवश्यक था। पुत्तस्वामी निर्णय ने इन प्रावधानों को धारा 7(3) व नियम 9(2) के अंतर्गत दुबारा परिभाषित करने एवं "उद्देश्य-सीमितता" लागू करने की सिफारिश की।

3. **गोपनीयता-संबंधी अन्य अधिनियमों में कमी**

सूचना प्रौद्योगिकी अधिनियम, 2000 में संवेदनशील व्यक्तिगत डेटा की रक्षा हेतु केवल धारा 43A (डेटा प्रोटेक्शन ऑफ़िशियल की ज़िम्मेदारी) एवं धारा 72A (गोपनीयता उल्लंघन) शामिल हैं, पर ये प्रावधान भी विस्तृत परिभाषा, प्रभावी प्रवर्तन तंत्र एवं दंडात्मक व्यवस्था के अभाव में अधूरी साबित हुए । परिणामतः, निजता के संवैधानिक अधिकार की रक्षा हेतु समग्र एवं समन्वित कानूनी ढाँचे की कमी स्पष्ट हुई।

4. **डेटा संरक्षण का कोई समग्र कानून न होना**

भारत में अभी तक कोई पूर्ण डेटा संरक्षण अधिनियम पारित नहीं हुआ है। व्यक्तिगत डेटा संरक्षण विधेयक, 2019 को संसद में विस्तारित चर्चा के पश्चात् संयुक्त समिति को भेजा गया, पर वास्तविक रूपरेखा अधूरी रही । इस अभाव ने कॉर्पोरेट्स, सरकारी निकायों और स्टार्ट-अप्स के बीच डेटा सुरक्षा मानकों में असंगति पैदा की तथा "उद्देश्य-सीमितता" और "भंडारण-सीमितता" जैसे मूलभूत सिद्धांतों का अनुपालन सुनिश्चित नहीं हो सका।

5. राष्ट्रीय सुरक्षा व नवोन्मेष के बीच असंतुलन

राष्ट्रीय सुरक्षा हितों के तहत अत्यधिक छूटें देना पुत्तस्वामी निर्णय द्वारा स्थापित अनुपात原则 (proportionality) के सिद्धांत का उल्लंघन कर सकता है। उदाहरण के लिए, राष्ट्रीय साइबर सुरक्षा नीति 2013 में आत्मनिर्भरता बढ़ाने के नाम पर डेटा एक्सेस की व्यापक शक्ति प्रदान कर दी गई है, जिससे नवोन्मेष को बढ़ावा देने के लिए आवश्यक गोपनीयता अवरोधित हो सकते हैं । साथ ही, MeitY की वार्षिक रिपोर्ट 2021–22 में नवोन्मेष के लिए सख्त डेटा साझा नीति की वकालत करते हुए भी नागरिक गोपनीयता पर संतुलित दृष्टिकोण की कमी दिखी है ।

इन अंतरालों को पाटने हेतु समग्र डेटा संरक्षण कानून, स्पष्ट संशोधन, और राष्ट्रीय सुरक्षा व

नवोन्मेष के बीच संतुलन सुनिश्चित करने वाले प्रावधान अनिवार्य हैं।

IV. डेटा संरक्षण समिति रिपोर्ट एवं विधेयक समीक्षा

1. बी.एन. श्रीकृष्ण समिति रिपोर्ट (जुलाई 2018)

न्यायमूर्ति बी.एन. श्रीकृष्ण के नेतृत्व में गठित विशेषज्ञ समिति ने जुलाई 2018 में "White Paper on Data Protection Framework for India" प्रस्तुत किया। समिति ने भारत में डेटा सुरक्षा की मौजूदा चुनौतियों का सर्वांगीण विश्लेषण करते हुए प्रमुख रूप से निम्न मानक एवं अनुशंसाएँ सुझाईं:

- **डेटा श्रेणीकरण**: व्यक्तिगत डेटा को "सामान्य" व "संवेदनशील" में विभाजित कर, अलग-अलग स्तर की सुरक्षा सुनिश्चित करने का प्रस्ताव।
- **डेटा न्यूनतमता एवं उद्देश्य-सीमितता**: केवल आवश्यक डेटा का संग्रह एवं उपयोग, और कार्य पूरा होते ही उसका विनाश।
- **सूचना एवं सहमति**: डेटा विषय को स्पष्ट नोटिस, संग्रह के उद्देश्य व संभावित रिस्पॉन्स देने का अधिकार, तथा मुक्त व सूचित सहमति की व्यवस्था।
- **डेटा सुरक्षा तंत्र**: क्रिप्टोग्राफ़िक साधन, नियमित आंतरिक—बाहरी ऑडिट और डेटा उल्लंघन सूचना प्रणाली।
- **उत्तरदायित्व एवं पारदर्शिता**: डेटा फिड्यूशियरी (Data Fiduciary) को एक जिम्मेदार एवं जवाबदेह इकाई मानते हुए, सार्वजनिक रिपोर्टिंग व ऑडिट की व्यवस्था।
- **स्वायत्त निगरानी प्राधिकरण** : एक स्वतंत्र "Data Protection Authority of India" की स्थापना, जिसे शिकायत सुनने एवं दंडात्मक कार्रवाई का अधिकार।

2. व्यक्तिगत डेटा संरक्षण विधेयक, 2019

पुत्तस्वामी निर्णय के बाद संसद में पेश यह बिल मूलतः उपरोक्त समिति की राय से प्रेरित था। बिल के प्रमुख प्रावधानों में शामिल हैं:

- **अधिकार**: डेटा सब्जेक्ट को पहुँच, सुधार, मिटाने (erasure), सहमति वापसी (revocation) और "भुलाए जाने का अधिकार" (Right to Be Forgotten) प्राप्त होना।
- **कर्तव्य** : डेटा फिड्यूशियरी को सहमति आधारित संग्रह, उद्देश्य-निश्चितता, न्यूनतमता, भंडारण-सीमितता और "प्राइवेसी बाई डिज़ाइन" सिद्धांतों का अनुपालन करना अनिवार्य।
- **दंड प्रावधान**: गोपनीयता उल्लंघन पर ₹15 करोड़ या वैश्विक कारोबार का 4% (जो अधिक हो) जुर्माना, तथा बॉर्डर-क्रॉस ट्रांसफ़र नियमों की अवहेलना पर अतिरिक्त दंड।
- **छूट**: सरकार को "सार्वजनिक आदेश", "राष्ट्रीय सुरक्षा" और "न्यायिक जाँच" जैसे मकसदों के लिए बिल से अस्थायी रूप से अलग रहने का अधिकार।
- **डेटा संरक्षण प्राधिकरण** : एक नियामक निकाय जिसे शिकायत निस्तारण, दिशानिर्देश जरी करने तथा निरिक्षण व सुनवाई का मौलिक अधिकार प्राप्त है।

3. Digital Personal Data Protection बिल, 2023 : 2019 के बिल के असफल प्रयास के पश्चात् 2023 में अंततः नया "Digital Personal Data Protection Act" पारित हुआ। इसके प्रमुख संशोधन एवं तकनीकी नवाचार इस प्रकार हैं :

- **डेटा वर्गीकरण में सरलीकरण**: केवल "डिजिटल व्यक्तिगत डेटा" को कवर करते हुए संवेदनशील और सामान्य डेटा की श्रेणियाँ एकीकृत।
- **स्पष्ट अभिगम्यों का प्रावधान**: डेटा सब्जेक्ट के "अभिगम्य अधिकार" (पहुँच, सुधार, मिटाना, सहमति वापसी) को सुनिश्चित करने हेतु एक वृहद् डिजिटल पोर्टल।

- **Data Protection Board of India**: शिकायत निस्तारण के त्वरित व्यवस्था हेतु एक त्वरित निवारण बोर्ड, जो इलेक्ट्रॉनिक फॉर्म में सुनवाई कर सकता है।
- **प्राइवेसी-फर्स्ट डिज़ाइन**: ऐप्लिकेशन एवं सेवाओं में गोपनीयता-एन्हांसिंग तकनीकों (क्रिप्टो-एनक्रिप्शन, differential privacy) को अनिवार्य मापदंड किया गया।
- **प्रौद्योगिकीय नवाचार**: "नॉलेजबिल्डर" मॉड्यूल के माध्यम से डेटा प्रोसैसिंग का स्वचालित गोपनीयता मूल्यांकन तथा "कंसेंट मैनेजर" ऐप से प्रभावी सहमति प्रबंधन।
- **लचीले दंड प्रावधान**: न्यूनतम ₹50 करोड़ से आरंभ और संगठनों को "नॉन-मानूफैक्चरिंग" (non-compliance) पर तकनीक-विशिष्ट जुर्मानों के विकल्प।

4. संयुक्त समिति की रिपोर्ट (दिसंबर 2021)

लोकसभा सचिवालय द्वारा प्रस्तुत इस रिपोर्ट में संयुक्त संसदीय समिति ने PDP Bill 2019 की समीक्षा करते हुए मुख्यतः निम्न सुझाव दिए:

- **Data Protection Authority की स्वतंत्रता**: बजट, मानव संसाधन और निर्णय-प्रक्रिया में पूर्ण स्वायत्तता सुनिश्चित करने हेतु संवैधानिक दर्जा।
- **सरकारी छूटों का सीमांकन**: "राष्ट्रीय सुरक्षा" व "सार्वजनिक आदेश" छूटों के लिए निश्चित समयसीमा व "सनसेट क्लॉज" (sunset clause) लागू करने की वकालत।
- **क्रॉस-बॉर्डर डेटा ट्रांसफ़र** : केवल उन देशों को मंजूरी जहाँ GDPR-समान डेटा सुरक्षा मानक हों, अन्यथा स्थानीय होस्टिंग अनिवार्य।
- **बच्चों की सुरक्षा**: 18 वर्ष से कम आयु के डेटा पर "अग्रिम अभिभावकीय सहमति" एवं ट्रैकिंग प्रतिबंध।
- **दंडात्मक प्रावधानों में संशोधन**: विलम्बित कार्रवाई पर अतिरिक्त पेनल्टी और त्वरित निवारण प्रक्रिया हेतु अधिकृत "ग्रेवियन्सी रेगुलेटर" की स्थापना।
- **डेटा सुरक्षा प्रभाव आकलन**: संवेदनशील प्रोजेक्ट्स के लिए अनिवार्य DPIA (Data Protection Impact Assessment) एवं नियमित ऑडिटिंग।

V. राष्ट्रीय सुरक्षा एवं नवोन्मेष का संतुलन

1. राष्ट्रीय साइबर सुरक्षा नीति, 2013 : भारत सरकार द्वारा जारी "राष्ट्रीय साइबर सुरक्षा नीति, 2013" का मुख्य उद्देश्य देश की डिजिटल परिसंपत्तियों की सुरक्षा सुनिश्चित करना है। नीति का एक प्रमुख स्तंभ **गोपनीयता एवं डेटा संरक्षण** है, जिसमें कहा गया है कि "सभी सरकारी व निजी सुविधाओं में डेटा की गोपनीयता, अखंडता एवं उपलब्धता को बनाए रखना आवश्यक" है । नीति के प्रावधानों के अनुसार, संवेदनशील सरकारी एवं नागरिक डेटा को एन्क्रिप्शन, पहुँच नियंत्रण, और नियमित सुरक्षा ऑडिट से संरक्षित करना होगा। इसके अलावा, नीति ने **"डिजिटल इंडिया"** पहल के तहत नवोन्मेष के लिए सुरक्षित वातावरण प्रदान करने हेतु **साईबर इकोसिस्टम** को मज़बूत करने पर बल दिया है। हालांकि, नीति ने डेटा-संबंधी विस्तारपूर्वक नियमों के बजाय व्यापक सिद्धांत दिए हैं, जिससे क्रियान्वयन में अस्पष्टता बनी हुई है ।

2. MeitY वार्षिक रिपोर्ट 2021–22 : इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (MeitY) की वार्षिक रिपोर्ट 2021–22 में डेटा सुरक्षा में उन्नत प्रयासों का वर्णन है। रिपोर्ट के अनुसार, **CERT-In** (Indian Computer Emergency Response Team) ने सिक्योरिटी इवेंट्स पर 24×7 निगरानी व्यवस्था स्थापित की है तथा डेटा उल्लंघन की तात्कालिक सूचना एवं प्रतिक्रिया तंत्र को तेज़ किया गया है ।

मंत्रालय ने **एन्क्रिप्शन नीति** को भी अंतिम रूप दिया, जिससे सरकारी डिजिटल परियोजनाओं में एन्क्रिप्शन-अट-रेस्ट और एन्क्रिप्शन-इन-ट्रांज़िट अनिवार्य हुआ। इसके अतिरिक्त, रिपोर्ट ने **कुशल साइबर सुरक्षा पेशेवरों** की कमी, पुराने अवसंरचनात्मक तंत्र तथा विभिन्न मंत्रालयों एवं राज्य निकायों के बीच समन्वयहीनता को मुख्य चुनौतियाँ बताया है।

3. नवोन्मेष को बढ़ावा देने हेतु उपाय : राष्ट्रीय सुरक्षा और नवोन्मेष के लक्ष्य को संतुलित करने के लिए निम्न उपाय प्रभावी सिद्ध हो सकते हैं:

- **इननोवेशन सैंडबॉक्स**: डेटा-संचालित स्टार्ट-अप्स को नियंत्रित एवं सुरक्षित वातावरण में प्रयोग करने की अनुमति देकर नई तकनीकों का परीक्षण।
- **प्राइवेसी-एनहांसिंग टेक्नोलॉजीज** : जैसे differential privacy, homomorphic encryption, जो संवेदनशील डेटा उपयोग की अनुमति देते समय गोपनीयता बरकरार रखें।
- **सार्वजनिक–निजी भागीदारी**: **MeitY** और **Startup India** के माध्यम से अनुसंधान अनुदान, हैकथॉन एवं प्रायोगिक परियोजनाओं के लिए वित्तीय एवं तकनीकी सहायता।

4. निजी क्षेत्र एवं स्टार्ट-अप्स के अनुशंसित गाइडलाइन

निजी क्षेत्र और नवोन्मेषी स्टार्ट-अप्स हेतु कुछ प्रमुख निर्देश निम्नलिखित हैं:

- **Privacy by Design**: डेटा संग्रह और प्रसंस्करण प्रणालियों में गोपनीयता प्रारंभिक स्तर से शामिल करें ।
- **उद्देश्य-सीमितता एवं न्यूनतमता**: केवल आवश्यक डेटा ही संग्रहित करें और उपयोग पूरा होते ही उसे सुरक्षित रूप से मिटा दें।
- **Data Protection Impact Assessment (DPIA)**: संवेदनशील प्रोजेक्ट्स हेतु प्रारंभिक DPIA कराकर संभावित गोपनीयता जोखिमों का आकलन।
- **एन्क्रिप्शन एवं पहुँच नियंत्रण**: डेटा "एट-रेस्ट" व "इन-ट्रांज़िट" दोनों अवस्थाओं में एन्क्रिप्ट करें तथा मल्टी-फैक्टर ऑथेंटिकेशन लागू करें।
- **नियमित ऑडिट एवं उल्लंघन सूचना**: स्वतंत्र सुरक्षा ऑडिट करवाएं और डेटा उल्लंघन पर नियामक प्राधिकरण को समयबद्ध सूचना दें।
- **ISO 27001 एवं GDPR-अनुकूल फ्रेमवर्क**: अंतरराष्ट्रीय मानकों का पालन करके वैश्विक बाजार में प्रतिस्पर्धात्मकता बनाए रखें।

इन उपायों से न केवल राष्ट्रीय सुरक्षा का संरक्षण होगा, बल्कि नवोन्मेष को भी गति मिलेगी, जिससे भारत एक सुरक्षित एवं नवोन्मेषी साइबर इकोसिस्टम का निर्माण कर सकेगा।

VI. अंतर्राष्ट्रीय तुलनात्मक अध्ययन

1. EU का GDPR मॉडल : यूरोपीय संघ का "General Data Protection Regulation" (Regulation (EU) 2016/679) 25 मई 2018 से लागू हुआ। इसके तहत डेटा विषयों को **सहमति**, **पहुँच का अधिकार**, **भुलाए जाने का अधिकार**, और **डेटा पोर्टेबिलिटी** जैसे अधिकार प्राप्त हैं। GDPR में **Data Protection Officer (DPO)** की नियुक्ति अनिवार्य है, तथा संवेदनशील डेटा के लिए **Data Protection Impact Assessment (DPIA)** का संचालन करना पड़ता है। अनुपालन सुनिश्चित करने हेतु प्रत्येक सदस्य-राज्य में **Supervisory Authority** (जैसे फ्रांस में CNIL, जर्मनी में BfDI) होती है, जिन्हें उच्चतम 20 मिलियन यूरो या वैश्विक टर्नओवर का 4% तक जुर्माना लगाने का अधिकार है। इसके अतिरिक्त **Codes of Conduct**, **Certification Mechanisms** और **One-Stop Shop** व्यवस्था के माध्यम से संगठनों को दिशानिर्देश प्रदान किए जाते हैं।

2. संयुक्त राज्य अमेरिका, सिंगापुर एवं ऑस्ट्रेलिया के मॉडलों का संक्षिप्त तुलना

- **संयुक्त राज्य अमेरिका:** यहाँ कोई एक समग्र संघीय कानून नहीं है; इसके बजाय सेक्टोरल अप्रोच है—जैसे **HIPAA** स्वास्थ्य डेटा हेतु, **Gramm-Leach-Bliley Act** वित्तीय डेटा हेतु, तथा **FTC Act** के तहत **Federal Trade Commission** द्वारा उपभोक्ता डेटा उल्लंघनों पर प्रवर्तन होता है। हाल में प्रस्तावित **American Privacy Rights Act** एक राष्ट्रीय मानक स्थापित करने का प्रयास कर रहा है।
- **सिंगापुर: Personal Data Protection Act (PDPA) 2012** व्यावसायिक और सार्वजनिक दोनों क्षेत्रों के लिए बुनियादी डेटा संरक्षण सुनिश्चित करता है। इसमें **सहमति-आधारित संग्रह**, **उद्देश्य-सीमितता**, और **Do Not Call Registry** के नियम शामिल हैं; नियामक प्राधिकरण **PDPC (Personal Data Protection Commission)**है।
- **ऑस्ट्रेलिया: Privacy Act 1988** के तहत 13 **Australian Privacy Principles (APPs)** लागू होते हैं। इनमें **ओपन और ट्रांसपेरेंट डेटा मैनेजमेंट**, **अनामिकता**, **डेटा क्वालिटी**, और **डेटा उल्लंघन सूचना** जैसे प्रावधान शामिल हैं; प्रवर्तन **OAIC (Office of the Australian Information Commissioner)** द्वारा किया जाता है ।

3. सामान्य सिद्धांत एवं संवैधानिक संरचनाएं

सभी मॉडलों में "**उद्देश्य-सीमितता**" और "**न्यूनतमता**" के सिद्धांत प्रमुख हैं। GDPR संवैधानिक स्तर पर उच्च जुर्माना और **One-Stop Shop** के साथ एकीकृत अप्रोच प्रदान करता है, जबकि अमेरिका में **चौथे संशोधन** के तहत मौलिक अधिकार आधारित सीमाएँ और सेक्टोरल अप्रोच प्रचलित है । सिंगापुर और ऑस्ट्रेलिया में स्वतंत्र नियामक निकायों के माध्यम से व्यावहारिक संतुलन रखा गया है। इन तुलनात्मक मॉडलों से स्पष्ट होता है कि एक समग्र, लचीला, और सशक्त डेटा संरक्षण तंत्र कैसे मौलिक अधिकारों की रक्षा, नवोन्मेष को प्रोत्साहन, और राष्ट्रीय सुरक्षा की आवश्यकताओं के बीच संतुलन स्थापित कर सकता है।

VII. मसौदा संवैधानिक संशोधन प्रस्ताव

1. संशोधन का प्रस्तावित ढाँचा : इस संशोधन का उद्देश्य संवैधानिक अनुच्छेद 21 (जीवन एवं व्यक्तिगत स्वतंत्रता की रक्षा) में स्पष्ट रूप से "गोपनीयता" को परिभाषित करना और उसे मौलिक अधिकार का अभिन्न अंग बनाना है। प्रस्तावित संशोधन निम्नानुसार होगा : अनुच्छेद 21 में, 'जीवन' और 'व्यक्तिगत स्वतंत्रता' में 'गोपनीयता' को शामिल किया जाए, जिसे कानून द्वारा स्थापित 'न्यायसंगत, उचित एवं अनुपातपूर्ण प्रक्रिया' के तहत संरक्षित और संतुलित किया जाएगा।

इसमें पारदर्शिता एवं जवाबदेही के सिद्धांतों के साथ-साथ डेटा संरक्षण हेतु आवश्यक संस्थागत व्यवस्था का प्रावधान होगा ।

2. अनुच्छेद 21 में "गोपनीयता" की स्पष्ट परिभाषा एवं व्याख्या : संशोधित अनुच्छेद 21(1) में निम्न-लिखित व्याख्यात्मक उपधारा जोड़ी जाए :

"गोपनीयता" का आशय है स्वयं से संबंधित सूचना, संचार, शारीरिक, मानसिक, आर्थिक एवं संवेदी पहलुओं का संरक्षण, जिसके अंतर्गत–

1. सूचना गोपनीयता (Information Privacy),
2. शारीरिक गोपनीयता (Bodily Privacy),
3. निर्णय गोपनीयता (Decisional Privacy),
4. संघ गोपनीयता (Associational Privacy) एवं
5. स्थानिक गोपनीयता (Locational Privacy) आते हैं।

यह परिभाषा पुत्तस्वामी निर्णय में उद्धृत पाँच आयामों की अवधारणा को संवैधानिक महत्व देती है ।

3. मुख्य धाराएँ

3.1 डेटा संरक्षण प्राधिकरण का निर्माण : संविधान में स्वायत्त **Data Protection Authority of India** (DPAI) की संवैधानिक स्थिति निर्धारित की जाए, जिसके पास निम्न अधिकार हों:

- शिकायत निस्तारण एवं दंडाधिकार,
- दिशानिर्देश जारी करने की क्षमता,
- स्वतंत्र ऑडिट एवं निरीक्षण प्रक्रिया।

यह प्राधिकरण संसदीय नियंत्रण से मुक्त हो एवं बजट, मानव संसाधन में पूर्ण स्वायत्तता प्राप्त करे ।

3.2 नवोन्मेष हेतु "वैध उद्देश्यों" की सीमा तय करना : संवैधानिक संशोधन में "वैध उद्देश्यों" की सूचीबद्ध परिभाषा दी जाए, उदाहरणतः–

- सार्वजनिक स्वास्थ्य एवं कल्याण,
- शिक्षा,
- अनुसंधान एवं नवोन्मेष,
- आर्थिक लेनदेन।

हर उद्देश्य के लिए "मध्यस्थता (proportionality)" की कसौटी लागू होगी, ताकि नवोन्मेष और व्यक्तिस्वतंत्रता में समुचित संतुलन बना रहे ।

3.3 राष्ट्रीय सुरक्षा के लिए विशेष छूट के प्रावधान

राष्ट्रीय सुरक्षा, सार्वजनिक आदेश एवं न्यायिक प्रक्रिया के लिए अस्थायी छूट (sunset clause) लागू हो, जिसमें–

- अस्थायी कड़ी छूटें केवल संसद द्वारा पारित विस्तारित अधिनियम तक सीमित हों,
- छूट की समयावधि एवं पुन:समीक्षा तंत्र संवैधानिक रूप से निर्धारित हो।

  इससे संतुलन बना रहेगा और छूट का दुरुपयोग रोका जा सकेगा ।

4. कार्यान्वयन एवं निगरानी तंत्र

4.1 स्वतंत्र निगरानी बोर्ड एवं जाँच प्रक्रिया : संशोधन में एक **Independent Oversight Board** का प्रावधान हो, जिसमें न्यायाधिकरण, डेटा विशेषज्ञ एवं नागरिक प्रतिनिधि सम्मिलित हों। इस बोर्ड के अंतर्गत–

- नियमित "निष्पक्षता ऑडिट" (Fairness Audit) और "गोपनीयता प्रभाव आकलन" (Privacy Impact Assessment) अनिवार्य हों,
- डेटा उल्लंघन की घटना पर त्वरित सार्वजनिक सूचना एवं मुआवजा तंत्र लागू हो,
- प्रत्येक वर्ष स्वतंत्र "गोपनीयता रिपोर्ट" संसद को प्रस्तुत की जाए।

यह पूरी संरचना न केवल संवैधानिक सुरक्षा को मजबूत बनाएगी, बल्कि नवोन्मेष और राष्ट्रीय सुरक्षा के बीच संतुलन भी सुनिश्चित करेगी, जिससे भारत में एक सशक्त एवं लोकतांत्रिक डेटा संरक्षण तंत्र का निर्माण संभव होगा।

VIII. निष्कर्ष एवं सिफारिशें

इस अध्ययन से स्पष्ट हुआ कि **पुत्तस्वामी निर्णय** ने व्यक्तिगत गोपनीयता को मौलिक अधिकार के रूप में स्थापित करके भारतीय संवैधानिक ढाँचे को समृद्ध किया। तथापि, निर्णय के पश्चात् आधार अधिनियम, सूचना प्रौद्योगिकी अधिनियम तथा अन्य संवैधानिक एवं वैधानिक व्यवस्थाओं में अनेक अंतराल उद्घाटित हुए—जिनमें समग्र डेटा संरक्षण कानून का अभाव, उद्देश्य-सीमितता तथा भंडारण-सीमितता के सिद्धांतों का अस्पष्ट प्रवर्तन, और राष्ट्रीय सुरक्षा एवं नवोन्मेष के बीच संतुलनहीनता प्रमुख हैं।

सिफारिशें:

1. **संवैधानिक समीक्षा एवं संशोधन:** अनुच्छेद 21 में गोपनीयता की स्पष्ट परिभाषा व "उद्देश्य-सीमितता" का संवैधानिक लेवल पर समावेश।
2. **समग्र डेटा संरक्षण कानून:** संवैधानिक दर्जे का **Data Protection Authority** स्थापित कर, पूरे देश में एकरूप मानदंड लागू करना।

3. **अनुपातसंगत सुरक्षा छूट का नियंत्रित प्रयोग:** राष्ट्रीय सुरक्षा हेतु अस्थायी एवं समयबद्ध छूटें ('sunset clauses') एवं नियमित पुनःसमीक्षा तंत्र।
4. **तकनीकी परिवर्तन के अनुकूल निगरानी:** differential privacy, homomorphic encryption जैसे प्राइवेसी-एनहांसिंग तकनीकों को "Privacy by Design" के अंतर्गत अनिवार्य करना।
5. **भविष्य के शोध हेतु दिशा:** डेटा-आधारित नवोन्मेष, आर्टिफिशियल इंटेलिजेंस, एवं बिग डेटा एनालिटिक्स के संदर्भ में गोपनीयता-प्रभाव आकलन (PIA) के क्षेत्र में गहन शोध।

इन कदमों से न केवल संवैधानिक सुरक्षा मज़बूत होगी, बल्कि भारत में सुरक्षित, नवोन्मेषी एवं लोकतांत्रिक डेटा पारिस्थितिकी तंत्र भी सुनिश्चित होगा।

संदर्भ ग्रंथ :

1. **न्यायमूर्ति के.एस. पुत्तस्वामी (सेवानिवृत्त) एवं अन्य बनाम भारत संघ एवं अन्य**, (2017) 10 SCC 1 सुप्रीम कोर्ट का मूल निर्णय (24 अगस्त 2017) – PDF, https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf en.wikipedia.org
2. **न्यायमूर्ति के.एस. पुत्तस्वामी (सेवानिवृत्त) एवं अन्य बनाम भारत संघ एवं अन्य**, आधार अधिनियम पर निर्णय (26 सितम्बर 2018),UIDAI द्वारा प्रकाशित निर्णय – PDF, https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdfuidai.gov .in
3. **प्रस्तावित डेटा संरक्षण समिति रिपोर्ट**, न्यायमूर्ति बी.एन. श्रीकृष्ण समिति, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार, जुलाई 2018, https://www.meity.gov.in/static/uploads/2024/02/10on.pdfmeity.gov.in
4. **व्यक्तिगत डेटा संरक्षण विधेयक, 2019** (हिंदी PDF), PRS India, https://hi.prsindia.org/files/bills_acts/bills_parliament/2019/Hindi%20The%20Personal%20Data%20Protection%20Bill%2C%202019.pdf hi.prsindia.org
5. **डिजिटल व्यक्तिगत डेटा संरक्षण बिल, 2023** (हिंदी), PRS India, https://hi.prsindia.org/billtrack/डिजिटल-पर्सनल-डेटा-प्रोटेक्शन बिल -2023 hi.prsindia.org
6. **Report of the Joint Committee on the Personal Data Protection Bill, 2019** (हिंदी PDF), लोकसभा सचिवालय, 16 दिसंबर 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf eparlib.nic.in
7. **आधार (लक्षित वितरण) अधिनियम, 2016** (अद्यतन हिंदी PDF), UIDAI, https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf uidai.gov.in
8. **UIDAI की कानूनी रूपरेखा** (हिंदी), UIDAI वेबसाइट-https://uidai.gov.in/hi/aboutuidai-hi/legal-framework-hi.htmluidai.gov.in
9. **आधार (नामांकन एवं अद्यतन) विनियम, 2016** (हिंदी PDF), UIDAI,https://uidai.gov.in/images/2_2016_compressed.pdfuidai.gov.in
10. **आधार प्रमाणीकरण नियम, 2020** (हिंदी PDF)UIDAI,https://uidai.gov.in/images/Aadhaar_Authentication_for_Good_Governance_Rules_2020.pdfuidai.gov.in

11. **राष्ट्रीय साइबर सुरक्षा नीति, 2013 (NCSP-2013)** (हिंदी PDF), Gazette of India, https://xn--m1bdba5a7gresc7dsa.xn--11b7cb3a6a.xn--h2brj9c/writereaddata/files/gazette_NCSP_2013.pdf xn--m1bdba5a7gresc7dsa.xn--11b7cb3a6a.xn--h2brj9c
12. **राष्ट्रीय साइबर सुरक्षा नीति, 2013 – विश्लेषण**, Drishti IAS (हिंदी), https://www.drishtiias.com/hindi/mains-practicequestion/question-1848drishtiias. com
13. **राष्ट्रीय साइबर सुरक्षा नीति 2013 पर लोकसभा में पेश रिपोर्ट** (हिंदी PDF), गृह मंत्रालय, https://www.mha.gov.in/MHA1/Par2017/pdfs/par2016-pdfs/ls-010316Hindi/830.pdf mha.gov.in
14. **MeitY वार्षिक रिपोर्ट 2021–22**, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (हिंदी PDF), https://www.meity.gov.in/static/uploads/2024/02/32-1.pdf meity.gov.in
15. **Joint Committee on the Personal Data Protection Bill, 2019 – मौखिक साक्षात्कार (Oral Evidence)**, PRS India, https://prsindia.org/parliamentarycommittees/joint-committee-on-the-personal-data-protection-bill-2019prsindia.org
16. **Personal Data Protection Bill, 2019** (हिंदी), Wikipedia, https://en. Wikipedia.org/wiki/Personal_Data_Protection_Bill%2C_2019 en.wikipedia.org
17. **Digital Personal Data Protection Act, 2023** (हिंदी), Wikipedia,https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act%2C_2023en.wikipedia.org
18. **India's data protection bill: Further work needed in order to ensure true privacy**, Access Now (PDF), https://www.accessnow.org/wp-content/uploads/ 2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf accessnow.org
19. **Data Justice in Digital Social Welfare: A Study of the Rythu Bharosa Scheme**, Silvia Masiero एवं Chakradhar Buddha, https://arxiv.org/abs/2108.09732 arxiv.org
20. **A Technical Look At The Indian Personal Data Protection Bill**, Ram Govind Singh एवं Sushmita Ruj, https://arxiv.org/abs/2005.13812arxiv.org

•