SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

भारत में निजता का अधिकार व डिजिटल व्यक्तिगत डाटा संरक्षण अधिनियम 2023 – एक विश्लेषणात्मक अध्ययन

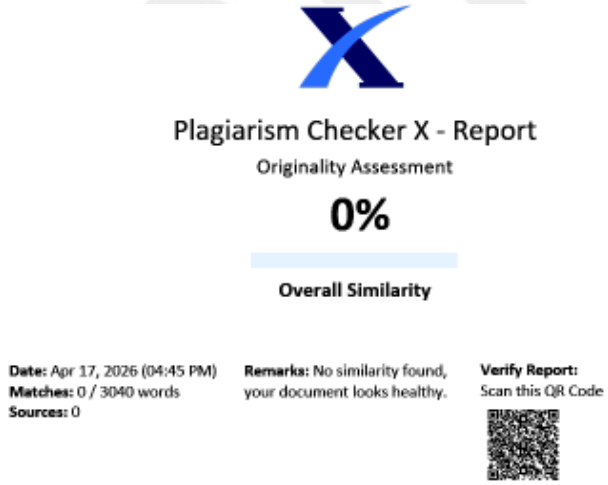
लेखराज, एलएल.एम. (सत्र–2024–25)
शा. जे. योगानंदम छत्तीसगढ़ महाविद्यालय, रायपुर, छत्तीसगढ़, भारत

ORIGINAL ARTICLE

Author
लेखराज
E-mail : lekhrajsahu1960@gmail.com

shodhsamagam1@gmail.com

Received on : 15/02/2026
Revised on : 16/04/2026
Accepted on : 25/04/2026
Overall Similarity : 00% on 17/04/2026



शोध सार

भारत में निजता के अधिकार की लड़ाई काफी लम्बी है। उच्चतम न्यायायलय ने अपने विभिन्न न्यायिक निर्णयों[1] के माध्यम से निजता के अधिकार को मौलिक अधिकार कि श्रेणी में लाने का प्रयास किया है जो वर्ष 2017 में जस्टिस के एस पुट्टास्वामी बनाम भारत संघ के ऐतिहासिक निर्णय से साकार हुआ। दूसरी ओर विश्व एक डिजिटल युग में प्रवेश कर चूका है जिससे भारत भी अछूता न रहा। प्रौद्योगिकी के विकास ने लोगो के दैनिक जीवन को अत्यधिक प्रभावित किया है। समावेशी डिजिटल पहुँच अनुच्छेद 21 के तहत गरिमापूर्ण जीवन के अधिकार का हिस्सा बन चूका है।[2] अनुराधा भसीन के मामले में इन्टरनेट को स्वतंत्र मौलिक अधिकार तो नहीं कहा लेकिन यह माना कि इन्टरनेट के माध्यम से अनुच्छेद 19(1) (a) में अभिव्यक्ति कि स्वतंत्रता और अनुच्छेद 19(1)(g) के तहत व्यापार करने का अधिकार शामिल है। फहीम शिरीन बनाम केरल राज्य 2019 के मामले केरल उच्च न्यायालय ने पहली बार इन्टरनेट को अनुच्छेद 21 के साथ जोड़ा था। यह शोध भारत के सर्वोच्च न्यायालय द्वारा घोषित "निजता के अधिकार"[3] और हाल ही में लागू "डिजिटल व्यक्तिगत डाटा संरक्षण अधिनियम 2023" के बीच के संबंधों का विश्लेषण करता है जहाँ निजता भारतीय संविधान में वर्णित अनुच्छेद 21 के तहत एक मौलिक अधिकार है जो कि सैद्धांतिक आधार है, वहीं DPDP एक्ट 2023 उसे डिजिटल युग में वैधानिक ढांचा प्रदान कर व्यावहारिक रूप देता है। यह शोध दोनों के बीच सामंजस्य और संभावित विरोधाभासों की जांच करता है तथा इनके बीच के विधिक पहलुओं पर प्रकाश डालता है तथा यूएसए और यूरोपीय संघ जैसे देशों में डेटा सुरक्षा से संबंधित कानूनों की तुलना करना और यह देखना कि भारत में डेटा की सुरक्षा कैसे की जा रही।

मुख्य शब्द

निजता का अधिकार, उच्चतम न्यायालय, अभिव्यक्ति कि स्वतंत्रता, डिजिटल व्यक्तिगत डाटा संरक्षण अधिनियम.

परिचय

जस्टिस के.एस. पुट्टास्वामी बनाम भारत संघ मामले में सुप्रीम कोर्ट ने निजता को अनुच्छेद 21 के तहत एक मौलिक अधिकार माना। वर्तमान डिजिटल युग में संवेदनशील डाटा का लीक होना, गोपनीयता का उल्लंघन होना एक आम बात हो चूका है, लोगों की दैनिक जीवन का हिस्सा बन चुके मोबाइल, लैपटॉप, कंप्यूटर, इंटरनेट जैसे आधुनिक तकनिकी विकास ने विश्व में डिजिटल क्रांति ला दी है। ऐसे में डिजिटल डाटा की सुरक्षा के लिए एक सुनियोजित कानून की आवश्यकता प्रासंगिक हो जाती है। परिणाम स्वरुप 2023 में DPDP ACT 2023 पारित हुआ जो व्यक्तिगत डेटा का संरक्षण व बिना स्वतन्त्र अनुमति के डाटा संग्रहित करने पर भारी भरकम जुर्माने का प्रावधान करती है। यह कानून यूरोपीय यूनियन का General Data Protection Regulation की तरह व्यक्तिगत डाटा की सुरक्षा तथा गोपनीयता के लिए बनाया गया है। क्या वास्तव में DPDP ACT 2023 निजता के अधिकार का संरक्षण करती है? और यदि करती है तो इस कानून कि पहुँच आम लोगो तक है या नहीं, त्वरित न्याय कैसे प्रदान किया जाये यह प्रश्नाधीन विषय है, क्योंकि आज भारत डिजिटल युग में प्रवेश कर चूका है और इस बात कि सम्भावना हमेशा बनी रहती है कि डाटा लीक, निजता जैसे संवेदनशील सूचना के प्रसारण बिना किसी पंजीकृत प्लेफार्म के माध्यम से प्रसारित हो रही है। ऐसे में क्या DPDP ACT 2023, आईटी एक्ट 2000 तथा निजता का अधिकार में सामंजस्य स्थापित करने में सफल हुआ है? क्या व्यक्तिगत नैतिक दायित्व को क़ानूनी दायरे में खड़ा किया जा सकता है? कुछ घटनाओं ने भारतीय डेटा संरक्षण और गोपनीयता मानकों पर सवाल उठाया है और आउटसोर्सिंग उद्योग को शर्मिंदा कर दिया है। वैश्वीकरण और भारत में बढ़ती बीपीओ उद्योग के साथ, डेटा की सुरक्षा के लिए कानून की आवश्यकता है। इसके लिए कारण हैं, बीपीओ उद्योग के हर व्यक्तिगत उपभोक्ता को उन कर्मचारियों से भिन्न स्तर की गोपनीयता की उम्मीद होगी जो व्यक्तिगत डेटा संभालते हैं। लेकिन हाल के अतीत में ऐसी स्थिति सामने आई है जहाँ कर्मचारियों या सिस्टम ने ग्राहकों की व्यक्तिगत जानकारी को बिना पूर्व सहमति के तीसरे पक्ष को दे दिया इसलिए, अन्य देश जो भारत को बीपीओ व्यवसाय प्रदान करते हैं, उनसे उम्मीद करते हैं कि भारतीय सरकार और बीपीओ संगठन डेटा संरक्षण के लिए उपाय करें। यह शोध उक्त प्रश्नों का उत्तर खोजने का प्रयास करती है।

निजता का अधिकार

भारतीय संस्कृति और पश्चिमी संस्कृति के बीच का अंतर व्यक्ति की अस्पष्ट अवधारणा से शुरू होता है। पश्चिमी दुनिया व्यक्ति को इस अद्भुत विचार के साथ देखती है, कि वह एक अभेद्य सुरक्षित क्षेत्र में जी रहे है, और उसके पास ''चुनने की स्वतंत्रता'' है। समग्र भारतीय संस्कृति सामूहिकता के सामाजिक–केंद्रित विश्वास को अपनाती है, जहां व्यक्ति की गोपनीयता की प्रधानता खो जाती है, जबकि पश्चिम में व्यक्ति–केंद्रीकरण की ही धारणा को प्रोत्साहित करता है। भारत एक सामूहिक समाज है जहां व्यक्तिवाद या गोपनीयता को उतना महत्व नहीं दिया जाता जितना कि यूके या यूएस में दिया जाता है, जहां व्यक्ति की प्रधानता कम से कम सामूहिकता के महत्व के बराबर होता है। इन दोनों संस्कृतियों से आने वाले व्यक्तियों के मन में डेटा संरक्षण की भिन्न समझ की ओर ले जाता है जबकि पश्चिम से आने वाला व्यक्ति इसे अपनी गोपनीयता से संबंधित मामला मानता है, जो उसके लिए सर्वोपरि है। समाजिक मूल्य केवल अपनी गोपनीयता की चिंता नहीं करती बल्कि समस्त जनमानस की गोपनीयता को भी ध्यान में रखता है। डेटा सुरक्षा को सामान्यतः "गोपनीयता" के साथ जोड़ा जाता है। तकनीकी प्रगति और आर्थिक सुधारों के साथ, अब डेटा के असंगत संचयन और प्रबंधन से सुरक्षा की व्यापक मांग है।[4]

भारत में निजता का अधिकार अनुच्छेद 21 के तहत एक संवैधानिक अधिकार है अर्थात राज्य के विरुद्ध उपलब्ध मौलिक उपचार है यदि राज्य द्वारा किसी व्यक्ति की निजता व गोपनीयता का उल्लंघन करता है तो उसे विधि द्वारा समर्थित व उचित प्रक्रिया के तहत होना चाहिए।

सर्वोच्च न्यायालय ने निजता के उल्लंघन के लिए ''तीन–चरणीय परीक्षण'' (Three-fold Test)[5] निर्धारित किया है।

- **वैधानिकता (Legality)**: राज्य यदि किसी कि निजता में हस्तक्षेप करता है तो उसे विधि द्वारा समर्थित होना चाहिए।
- **आवश्यकता (Necessity)**: हस्तक्षेप का एक वैध उद्देश्य होना चाहिए।
- **आनुपातिकता (Proportionality)**: हस्तक्षेप और उद्देश्य के बीच तार्किक व युक्तियुक्त सम्बन्ध होना चाहिए।

तुलनात्मक अध्ययन

भारत में न्यायमूर्ति बी.एन. श्रीकृष्ण की अध्यक्षता में एक समिति बनाई गई थी। बी.एन. श्रीकृष्ण समिति की रिपोर्ट (White Paper) DPDP एक्ट 2023 के आने से पहले "A Free and Fair Digital Economy: Protecting Privacy, Empowering

Indians" इसे भारत में डेटा संरक्षण कानून का ''ब्लूप्रिंट'' माना जाता है। भारत सरकार द्वारा उक्त रिपोर्ट को आधार मानकर वैयक्तिक डाटा का संरक्षण करने और गोपनीयता व संवेदनशील डाटा लीक को बचाने तथा डिजिटल युग में निजता के अधिकार को यथार्थ रूप देने के उद्देश्य से व्यक्तिगत डाटा संरक्षण अधिनियम 2023 पारित किया गया। जिनकी प्रमुख विशेषताएँ निम्नानुसार हैः

सहमति प्रबंधक (Concent Manager)[6]: डेटा प्रोसेसिंग के लिए स्पष्ट और स्वतंत्र सहमति अनिवार्य है। किसी कम्पनी को आपका डाटा इस्तेमाल करने के लिए स्पष्ट, सूचित व बिना शर्त सहमति लेनी होगी। बताना होगा कि आपका डाटा का उपयोग क्यों और कहा किया जाएगा तथा उपयोगकर्ता के पास अपनी सहमति किसी भी समय वापस लेने का अधिकार होगा। बच्चो कि (18 वर्ष से कम) डाटा प्रोसेस करने के लिए माता –पिता या अभिभावक की सहमति अनिवार्य होगी।

डेटा फिड्यूशरी (Data Fiduciary)[7]: वह संस्था जो डेटा को प्रोसेस करती है। जैसे (गूगल, फेसबुक आदि) डाटा सुरक्षा, डाटा उल्लंघन कि सूचना तथा डाटा उद्देश्य पूरा होने पर डिलीट करने का दायित्व डाटा फिड्यूशरी का होगा।

डेटा प्रिंसिपल (Data Principal)[4]: – वह व्यक्ति जिसका डेटा है।

वैयक्तिक डाटा (Personal Data)[9]: कोई डाटा जिसकी ऐसी डाटा द्वारा या उसके सम्बन्ध में पहचान कि जा सके।

भारतीय डाटा संरक्षण बोर्ड (DPB)[10]: इस कानून के कार्यान्वयन व शिकायत के लिए स्थापित क़ानूनी निकाय। यह बोर्ड एक डिजिटल न्यायालय कि तरह कार्य करेगी। इसके अलावा डाटा सुधार, मिटाने (Erasure) और शिकायत निवारण का अधिकार तथा डेटा उल्लंघन पर रूपये 250 करोड़ तक के जुर्माने का प्रावधान है । DPDP ACT डिजिटल नागरिक के अधिकारों और डिजिटल अर्थव्यवस्था की जरूरतों के बीच संतुलन स्थापित करने की कोशिश करता है।

यूरोपीय यूनियन (EU): जनरल डेटा प्रोटेक्शन रेगुलेशन (GDPR) यूरोपीय संघ (EU) का एक विस्तृत कानून है जो 25 मई 2018 से प्रभावी हुआ। इसका मुख्य उद्देश्य इंटरनेट के युग में नागरिकों को उनके व्यक्तिगत डेटा पर अधिक नियंत्रण देना और व्यवसायों के लिए डेटा सुरक्षा के नियमों को सरल और समान बनाना है।

GDPR के प्रमुख विशेषताएँ[11]

GDPR के अंतर्गत कुछ बुनियादी सिद्धांत और प्रावधान दिए गए हैं जिनका पालन हर उस संस्था को करना होता है जो डेटा प्रोसेस करती हैः

- **स्पष्ट सहमति (Lawful Basis & Consent)**: कंपनियां बिना ठोस कारण के डेटा प्रोसेस नहीं कर सकतीं। उन्हें उपयोगकर्ता से स्पष्ट और सरल भाषा में सहमति लेनी होती है।
- **डेटा का सीमित उपयोग (Purpose Limitation)**: डेटा केवल उसी उद्देश्य के लिए उपयोग किया जा सकता है जिसके लिए सहमति ली गयी है।
- **डेटा न्यूनीकरण (Data Minimçation)**: कंपनियों को केवल उतना ही डेटा इकट्ठा करना चाहिए जितना उनके काम के लिए अनिवार्य हो तथा डेटा सटीक होना चाहिए और गलत डेटा को तुरंत मिटाने या सुधारने की व्यवस्था होनी चाहिए।
- **गोपनीयता और सुरक्षा (Integrity - Confidentiality)**: डेटा को सुरक्षित रखने के लिए एन्क्रिप्शन (Encryption) जैसे तकनीकी उपाय करना अनिवार्य है।
- **'क्षेत्राधिकार का विस्तार (Extra - territorial Applicability)**: यह कानून केवल यूरोप की कंपनियों पर ही नहीं, बल्कि दुनिया की हर उस कंपनी पर लागू होता है जो यूरोपीय नागरिकों का डेटा प्रोसेस करती है या उन्हें सामान/सेवाएं बेचती है।
- **उल्लंघन पर भारी जुर्माना (Heavy Penalties)**: नियमों का उल्लंघन करने पर कंपनियों पर बहुत बड़ा जुर्माना लगाया जा सकता है। यह जुर्माना 20 मिलियन यूरो या कंपनी के वैश्विक वार्षिक टर्नओवर का 4: (जो भी अधिक हो) तक हो सकता है।
- **उपयोगकर्ताओं के अधिकार (Individual Rights)**: GDPR नागरिकों को कई अधिकार देता हैः भूल जाने का अधिकार (Right to be Forgotten), एक्सेस का अधिकार (Right of Access), डेटा पोर्टेबिलिटी (Data Portability),

प्रोसेसिंग पर रोक (Right to Object) उपयोगकर्ता अपने डेटा के मार्केटिंग या अन्य उपयोगों पर रोक लगा सकते हैं।

आलोचनात्मक बिन्दुः चुनौतियाँ और विरोधाभास

भारत में DPDP ACT 2023 एक बड़ी उपलब्धि है, लेकिन कुछ प्रावधान ऐसे है जहाँ इस कानून को आलोचना होती है:

- **सरकारी छूट (Government Exemptions)**: इस अधिनियम की धारा 7 और 17 के तहत केंद्र सरकार को व्यापक छूट दी गई है। राष्ट्रीय सुरक्षा और सार्वजनिक व्यवस्था के नाम पर सरकार डेटा एकत्र कर सकती है, जिससे ''निगरानी राज्य'' (Surveillance State) का खतरा बढ़ जाता है। जो पुट्टास्वामी निर्णय के ''आनुपातिकता'' सिद्धांत के विरुद्ध हो सकती है। राष्ट्रिय हित बताकर किसी व्यक्ति, संस्था या निगम कि निगरानी कि सकती है जो एक लोकतान्त्रिक देश के लिए खतरा का विषय बन सकता है।
- **RTI एक्ट में संशोधनः** DPDP एक्ट ने RTI एक्ट की धारा 8(1)(j) को संशोधित कर दिया है। अब सरकारी अधिकारी ''व्यक्तिगत जानकारी'' का हवाला देकर जानकारी देने से मना कर सकते हैं, जिससे पारदर्शिता कम होने की संभवना को इंकार नहीं किया जा सकता।
- **डेटा प्रोटेक्शन बोर्ड (DPB) की स्वतंत्रताः** बोर्ड के सदस्यों की नियुक्ति और कार्यकाल का नियंत्रण पूरी तरह सरकार के हाथ में है, जिससे इसकी निष्पक्षता पर सवाल उठते हैं।
- **बच्चों का डेटाः** 18 साल से कम उम्र के बच्चों के डेटा के लिए माता–पिता की सहमति अनिवार्य है जो किशोरों की ऑनलाइन गोपनीयता और स्वायत्तता को सीमित कर सकता है।
- **केन्द्रीय नियंत्रणः** DPDP ACT केन्द्रीय अभिकरणों को अधिक शक्ति प्रदान करती है जिससे भारत के संघीय ढांचे पर प्रभाव पड़ने कि सम्भावना से इंकार नहीं किया जा सकता।

इसके अलावा डेटा फिड्यूशरी जैसे संस्था व्यक्तिगत डाटा के प्रोसेस करने के लिए डेटा हेर फेर कर व्यक्तिगत गोपनीयता को प्रभावित कर सकती है। दूरस्थ क्षेत्र में तकनिकी शिक्षा कि कमी व डिजिटल पहुच से दूर होने के कारण स्वतन्त्र सहमति कि बिंदु एक विवादस्पद हो सकता है। डेटा प्रोसेस करने वाली संस्था द्वारा सहमति प्राप्त करने के जिस माध्यम का उपयोग करती है वह तकनिकी व भाषाई निश्चितता पर आधारित होती है।

निष्कर्ष

डिजिटल पर्सनल डाटा प्रोटेक्शन एक्ट भारत के डिजिटल संप्रभुता की दिशा में एक बड़ा कदम है। हालाँकि, यह निजता के अधिकार को एक कानूनी रूप देता है, लेकिन सरकार को दी गई अत्यधिक शक्तियां संवैधानिक मर्यादाओं को चुनौती दे सकती हैं। भविष्य में न्यायिक व्याख्याएं ही यह तय करेंगी कि यह कानून मौलिक अधिकारों की रक्षा में कितना सफल होता है। सरकार को दी गयी बेलगाम शक्तियां और RTI ACT के साथ इसका टकराव इसका सबसे कमजोर पक्ष है इसकी सफलता इस बात पर निर्भर करेगी कि आने वाला डेटा प्रोटेक्शन बोर्ड कितनी स्वायत्तता से कार्य करता है। डेटा संरक्षण क़ानूनों द्वारा प्रदान किए गए अधिकारों और सूचना के अधिकार अधिनियम के तहत उपलब्ध अधिकारों के बीच विरोधाभास होने के बारे में सवाल उठाए जाते हैं, जो नागरिकों को सार्वजनिक जानकारी तक पहुँच का अधिकार प्रदान करता है। इसका उत्तर यह हो सकता है कि डेटा संरक्षण क़ानून दुनिया भर में मौजूद हैं, यहां तक कि उन देशों में भी जिनमें विस्तृत सार्वजनिक जानकारी तक पहुँच कानून बनाए गए हैं। यह प्रमाणित हो चुका है कि ये दोनों प्रकार के कानून साथ–साथ मौजूद होने में सक्षम हैं। विरोधाभासी होने के बजाय, ये एक–दूसरे के विपरीत काम करते हैं और एक–दूसरे को अर्थ देते हैं।

सूचना का अधिकार, RTI अधिनियम के तहत, ऐसी जानकारी से संबंधित है जो सार्वजनिक अधिकारियों के पास उपलब्ध है, जिसमें कार्य, दस्तावेज़, अभिलेख, जानकारी के नमूने आदि शामिल हैं, जिन तक नागरिक को पहुँच का अधिकार है। यह स्वयं ही डेटा, जिसमें व्यक्तिगत जानकारी भी शामिल है, के लिए अंतर्निहित सुरक्षा उपलब्ध कराता है। इस प्रकार, जिस प्रकार किसी व्यक्ति को सार्वजनिक जानकारी तक पहुँच का अधिकार है, उसी प्रकार उसे अपनी व्यक्तिगत जानकारी तक अनधिकृत पहुँच को रोकने का अधिकार भी है। व्यक्तिगत जानकारी जो डेटा सुरक्षा का हिस्सा है। वास्तव में, आरटीआई अधिनियम में ही कई प्रावधान ऐसे हैं जो प्रत्यक्ष या अप्रत्यक्ष रूप से यह सुनिश्चित करते हैं की किसी व्यक्ति से संबंधित निजी जानकारी को अनधिकृत प्रकटीकरण से बचाया जाए।

इस प्रकार, एक स्पष्ट रूप से परिभाषित अलग डेटा सुरक्षा प्रणाली आरटीआई अधिनियम के प्रावधानों के साथ सहक्रियाशील होगी। आरटीआई अधिनियम के तहत, नागरिकों के लिए ऐसे सार्वजनिक कर्मचारियों की व्यक्तिगत जानकारी तक पहुंचने में सार्वजनिक हित का दावा करना संभव हो सकता है और चूंकि कानून इसे स्पष्ट रूप से नहीं बताता है, इसका उपयोग किसी सरकारी कर्मचारी की व्यक्तिगत गोपनीयता में हस्तक्षेप करने के लिए किया जा सकता है। इसलिए, आरटीआई अधिनियम के तहत यह स्पष्ट किया जाना आवश्यक है की सरकारी कर्मचारी की व्यक्तिगत जानकारी जनता के लिए उपलब्ध कराई जा सकती है ताकि डेटा सुरक्षा प्रणाली के साथ किसी भी तरह के संघर्ष से बचा जा सके।[12]

क्रेडिट सत्यापन वह मूल आधार है जिस पर आधुनिक बैंकिंग प्रणाली आधारित है। इस संदर्भ में, बैंक और वित्तीय संस्थान संभावित उधारकर्ताओं की व्यक्तिगत जानकारी तक पहुंचने की क्षमता पर निर्भर करते हैं ताकि यह आकलन कर सकें कि उन्हें ऋण दिया जाना चाहिए या नहीं। डेटा संरक्षण कानून डेटा एकत्र करने को प्रतिबंधित नहीं करते। वे केवल यह नियंत्रित करते हैं कि डेटा किस प्रकार से एकत्र और प्रसंस्कृत किया जाता है। अधिकांश डेटा संरक्षण कानून उन व्यक्तिगत जानकारियों के प्रसंस्करण को उस उद्देश्य तक सीमित करते हैं जिसके लिए उन्हें एकत्र किया गया था। अतरू, जब तक किसी व्यक्ति की क्रेडिट–योग्यता सत्यापित करने के लिए प्रदान की गई व्यक्तिगत जानकारी केवल उसी उद्देश्य के लिए उपयोग की जाती है, तब तक ऐसे डेटा को प्रस्तावित डेटा संरक्षण कानून के अंतर्गत उपयोग करने में कोई समस्या नहीं होगी। इसके अलावा, डेटा विषय को सहमति का विकल्प भी उपलब्ध है। यदि किसी डेटा विषय को ऋण या अन्य चीजों की आवश्यकता है, तो उसे अपने व्यक्तिगत जानकारी तक पहुंच के लिए सहमति देनी होगी।

ऐसे में DPDP ACT 2023 व निजता के अधिकार पर सामंजस्य स्थापित करने नागरिको की गोपनीयता व व्यक्तिगत डाटा संरक्षण का प्रभावी विकल्प के रूप में DPB अर्थात् Data Protection Bord अच्छा और प्रभावी विकल्प हो सकता है। सहमति प्राप्त करने के सरल, स्पस्ट व आसन भाषा का प्रयोग हो ताकि तकनिकी समस्यायों से सहमति पर कोई विवाद न हो।

संदर्भ सूची

1. एम.पी.शर्मा बनाम सतीश चन्द्र 1954, खड़कसिंह बनाम उत्तरप्रदेश राज्य (1964) SCR (1) (332), गोविन्द बनाम मध्यप्रदेश राज्य (AIR 1975 SCR 1378), आर.राजगोपाल बनाम तमिलनाडु राज्य 1994, पीयूसीएल बनाम भारत संघ 1997, जस्टिस के.एस. पुट्टा स्वामी बनाम भारत संघ 2017, आधार कार्ड केश 2018।
2. अमर जैन बनाम भारत संघ (2025) SCR.
3. जस्टिस के.एस .पुट्टूस्वामी एवं अन्य बनाम भारत संघ एवं अन्य 2017 SCR.
4. Richrd A. Sweder & Edmund J. Bourne, Does the Concept fo the Person Vary Cros&Culturally?
5. Justice K.S. Puttsaami and other versus Uinon fo India sc 2017, Data Protection In India - article by Majmudar & Co. available at https:\\www.scribd.com\document/136287003\Data-Protection-in-India, Accessed on 12/02/2025.
6. धारा 2(G) व्यक्तिगत डाटा संरक्षण अधिनियम 2023।
7. धारा 2(I) व्यक्तिगत डाटा संरक्षण अधिनियम 2023।
8. धारा 2(J) व्यक्तिगत डाटा संरक्षण अधिनियम 2023।
9. धारा 2(T) व्यक्तिगत डाटा संरक्षण अधिनियम 2023।
10. धारा 18 व्यक्तिगत डाटा संरक्षण अधिनियम 2023।
11. EUR&LEX (OFFICIAL JOURNAL OF THE EUROPEAN UNION) REGULATION (EU) 2016/679, European Commission & Data Protection: Rules for the protection of personal data inside and outside the EU.
12. Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.

****