

कृत्रिम बुद्धिमत्ता, साइबर सुरक्षा, और डिजिटल शासन के युग में सूचना प्रौद्योगिकी अधिनियम, 2000 का पुनर्मूल्यांकन

डॉ. हिमांशु पांडे*
सुलेखा चौरसिया**
प्रज्ञा सिंह***
डॉ. मनविंदर सिंह पाहवा****

सार

सूचना प्रौद्योगिकी अधिनियम, 2000 (सूचना प्रौद्योगिकी अधिनियम) ने भारत में डिजिटल लेन-देन को समर्थित करने, साइबर अपराधों को नियंत्रित करने और इलेक्ट्रॉनिक शासन (ई-गवर्नेंस) को सुगम बनाने के उद्देश्य से लागू किया गया था। हालांकि, कृत्रिम बुद्धिमत्ता, साइबर सुरक्षा के खतरों और डिजिटल शासन के द्रुत परिवर्तनों के कारण, यह अधिनियम अब कई गतिशील मामलों में अद्यतन नहीं हो रहा है। कृत्रिम बुद्धिमत्ता परमिट साइबर अपराधों, डेटा सुरक्षा उल्लंघनों और स्वतः संचालित निर्णय लेने की तकनीकों ने इस कानून की प्रभावकारिता पर नए प्रश्न उठाए हैं। इस अध्ययन में सूचना प्रौद्योगिकी अधिनियम, 2000 के विश्लेषण पर ध्यान दिया गया है और यह देखा गया है कि यह कितनी प्रचलित डिजिटल चुनौतियों के साथ सामर्थी है। शोध का मुख्य सवाल है कि क्या सूचना प्रौद्योगिकी अधिनियम वर्तमान तकनीकी नवीनताओं के अनुरूप है, क्या इसमें साइबर सुरक्षा के प्रगतिशील उपायों की आवश्यकता है, और भारतीय डिजिटल शासन संरचना को मजबूत बनाने के लिए कौन-कौन से सुधार आवश्यक हैं। इस अध्ययन में सकारात्मक शोध पद्धति का उपयोग किया गया है, जिसमें मामले का अध्ययन, तुलनात्मक कानूनी विश्लेषण और साक्ष्य-आधारित शोध शामिल हैं।

शब्दकोश: सूचना प्रौद्योगिकी, ई-गवर्नेंस, साइबर अपराध, डेटा सुरक्षा, डिजिटल शासन।

प्रस्तावना

सूचना प्रौद्योगिकी अधिनियम, 2000 भारत में डिजिटल लेनदेन, साइबर अपराधों और इलेक्ट्रॉनिक गवर्नेंस को नियंत्रित करने वाला एक महत्वपूर्ण कानून है। यह अधिनियम इंटरनेट और डिजिटल संचार के विकास के साथ उत्पन्न चुनौतियों का समाधान करने के लिए बनाया गया था। वर्तमान में, कृत्रिम बुद्धिमत्ता, साइबर सुरक्षा और डिजिटल गवर्नेंस के संदर्भ में, यह अधिनियम कई नए और जटिल मुद्दों का सामना कर रहा है। साइबर खतरों की बढ़ती जटिलता, डाटा गोपनीयता की चिंताएँ, कृत्रिम बुद्धिमत्ता—आधारित निर्णय लेने की

* प्रोफेसर, महाराष्ट्र नेशनल लॉ यूनिवर्सिटी, नागपुर (एनएलयू, नागपुर), महाराष्ट्र।
** शोधार्थी, वाणिज्य विभाग, डॉ. हरिसिंह गौर सागर विश्वविद्यालय, सागर, म.प्र.।
*** शोधार्थी, वाणिज्य विभाग, डॉ. हरिसिंह गौर सागर विश्वविद्यालय, सागर, म.प्र.।
**** प्रोफेसर, वाणिज्य विभाग, डॉ. हरिसिंह गौर सागर विश्वविद्यालय, सागर, म.प्र.।

नैतिकता और डिजिटल अधिकारों की सुरक्षा जैसे मुद्दे इस कानून के पुनर्मूल्यांकन की आवश्यकता को दर्शाते हैं। इसलिए, वर्तमान तकनीकी परिवर्तनों के अनुरूप सूचना प्रौद्योगिकी अधिनियम को अद्यतन करना आवश्यक है। यह अद्यतन डिजिटल युग की उभरती चुनौतियों का प्रभावी समाधान प्रदान करने और एक सुरक्षित, उत्तरदायी तथा समावेशी साइबर वातावरण सुनिश्चित करने में सहायक होगा। वर्तमान युग डिजिटल क्रांति का युग है, जहाँ संचार, व्यापार, बैंकिंग, शिक्षा और सरकारी कार्यप्रणालियाँ इंटरनेट पर निर्भर हो गई हैं। इस डिजिटल विकास के साथ-साथ साइबर अपराधों और ऑनलाइन धोखाधड़ी की घटनाएँ भी बढ़ी हैं। इन चुनौतियों का समाधान करने और डिजिटल लेन-देन को कानूनी मान्यता देने के उद्देश्य से भारत सरकार ने सूचना प्रौद्योगिकी अधिनियम, 2000 को लागू किया। यह अधिनियम भारत में साइबर कानून का मूलभूत आधार है और डिजिटल के सुरक्षित एवं सुव्यवस्थित बनाने में सहायक है। भारत में सूचना एवं संचार प्रौद्योगिकी के बढ़ते प्रभाव के देखते हुए संयुक्त राष्ट्र महासभा के मॉडल लॉ के आधार पर इस अधिनियम के तैयार किया गया। संसद ने इसे 17 मई 2000 के पारित किया और 17 अक्टूबर 2000 के इसे आधिकारिक रूप से लागू किया गया। कृत्रिम बुद्धिमत्ता आज के डिजिटल युग में तकनीकी नवाचार का एक प्रमुख अंग बन चुकी है। कृत्रिम बुद्धिमत्ता का उपयोग स्वास्थ्य, शिक्षा, वित्त, व्यापार, रक्षा और संचार जैसे क्षेत्र में हो रहा है। हालाँकि, इसके दुरुपयोग की संभावना भी बढ़ गई है, जिससे डेटा सुरक्षा, साइबर अपराध, गोपनीयता उल्लंघन, धोखाधड़ी और साइबर आतंकवाद जैसे खतरे उत्पन्न हो रहे हैं। भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 डिजिटल अपराधों साइबर सुरक्षा से संबंधित प्रमुख कानून है। यह अधिनियम कृत्रिम बुद्धिमत्ता से संबद्ध नहीं है, लेकिन इसके विभिन्न प्रावधानों के कृत्रिम बुद्धिमत्ता से जुड़े कानूनी मामलों में लागू किया जा सकता है।

कृत्रिम बुद्धिमत्ता से संबंधित सूचना प्रौद्योगिकी अधिनियम, 2000 के प्रमुख प्रावधान

- **साइबर अपराध कृत्रिम बुद्धिमत्ता** – जनित अपराध (धारा 43, 66, 66, 66, 66, 66, 66) कृत्रिम बुद्धिमत्ता के बढ़ते उपयोग के कारण साइबर अपराधों की जटिलता भी बढ़ गई है। कई अपराध कृत्रिम बुद्धिमत्ता की सहायता से स्वचालित हो गए हैं, जिससे धोखाधड़ी, हैकिंग, फिशिंग, पहचान की चोरी साइबर आतंकवाद जैसी घटनाएँ बढ़ रही हैं।
 - हैकिंग डेटा उल्लंघन (धारा 66) कृत्रिम बुद्धिमत्ता का उपयोग स्वचालित रूप से कंप्यूटर नेटवर्क या डेटा सिस्टम के हैक करने के लिए किया जा सकता है। उदाहरण कृत्रिम बुद्धिमत्ता –आधारित का उपयोग करके संवेदनशील सरकारी या व्यावसायिक डेटा चुराया जा सकता है। इस धारा के तहत दोषी पाए जाने पर 3 साल की जेल या 5 लाख रुपये तक का जुर्माना लगाया जा सकता है।
 - पहचान की चोरी धोखाधड़ी (धारा 66) कृत्रिम बुद्धिमत्ता –जनित फर्जी दस्तावेज, जीवमितीय डेटा की चोरी और कृत्रिम मीडिया तकनीकका दुरुपयोग कर धोखाधड़ी के अंजाम दिया जा सकता है। उदाहरण– कृत्रिम बुद्धिमत्ता का उपयोग कर बैंकिंग सिस्टम के धोखा देना या किसी व्यक्ति की आवाज और छवि के प्रतिरूपण करके ठगी करना। दोषी पाए जाने पर 3 साल तक की सजा 1 लाख रुपये तक का जुर्माना हो सकता है।
 - साइबर आतंकवाद (धारा 66) कृत्रिम बुद्धिमत्ता का उपयोग स्वचालित साइबर हमलों कृत्रिम मीडिया तकनीकसे आतंकवाद फैलाने के लिए किया जा सकता है। उदाहरण– कृत्रिम बुद्धिमत्ता –निर्मित फर्जी वीडियो या गलत सूचना फैलाकर समाज में दंगे भड़काना। इस धारा के तहत दोषी के आजीवन कारावास की सजा दी जा सकती है।
- **डेटा गोपनीयता – कृत्रिम बुद्धिमत्ता और डेटा संरक्षण (धारा 72, 72)** – कृत्रिम बुद्धिमत्ता बड़े पैमाने पर डेटा एकत्र और विश्लेषण करता है, जिससे डेटा गोपनीयता से संबंधित समस्याएँ उत्पन्न होती हैं।

- अवैध डेटा संग्रहण (धारा 72) यदि कोई व्यक्ति या संगठन कृत्रिम बुद्धिमत्ता —संचालित सिस्टम का उपयोग करके किसी अन्य व्यक्ति की निजी जानकारी प्राप्त करता है और उसे बिना अनुमति के साझा करता है, तो यह अपराध माना जाएगा। उदाहरण—कृत्रिम बुद्धिमत्ता प्रणाली द्वारा नागरिकों की निजी बातचीत या गतिविधियाँ ध्वन्यालेखन कर किसी तीसरे पक्ष को बेचना। दोषी पाए जाने पर 2 साल की जेल या 1 लाख रुपये तक का जुर्माना लगाया जा सकता है।
- व्यक्तिगत डेटा का दुरुपयोग (धारा 72) कृत्रिम बुद्धिमत्ता का उपयोग कर अनधिकृत डेटा विश्लेषण करना और उसे व्यावसायिक लाभ के लिए बेचना गैरकानूनी है। उदाहरण— सोशल मीडिया प्लेटफॉर्म कृत्रिम बुद्धिमत्ता कलन विधिका उपयोग कर यूजर्स की निजी जानकारी विज्ञापन कंपनियों को बेचते हैं। इस धारा के तहत भी 2 साल की जेल या 5 लाख रुपये तक का जुर्माना हो सकता है।
- **इलेक्ट्रॉनिक अनुबंध और कृत्रिम बुद्धिमत्ता** — निर्मित निर्णय (धारा 10) आजकल कई कृत्रिम बुद्धिमत्ता —संचालित चौटबॉट और सॉफ्टवेयर स्वचालित रूप से डिजिटल अनुबंध तैयार कर रहे हैं।
 - धारा 10 के अनुसार, इलेक्ट्रॉनिक अनुबंध कानूनी रूप से वैध हैं। लेकिन यदि कोई कृत्रिम बुद्धिमत्ता आधारित सिस्टम अनुबंध करता है और भविष्य में विवाद उत्पन्न होता है, तो जिम्मेदारी किसकी होगी? कृत्रिम बुद्धिमत्ता निर्माता, उपयोगकर्ता या सॉफ्टवेयर डेवलपर? इस विषय पर कोई स्पष्ट दिशा-निर्देश नहीं हैं, जिससे यह एक जटिल कानूनी मुद्दा बन जाता है।
- कृत्रिम बुद्धिमत्ता और अवैध सामग्री (धारा 69, 69, 79) कृत्रिम बुद्धिमत्ता की मदद से फर्जी खबरें, डीपफेक वीडियो और द्वेषपूर्ण भाषण को तेजी से फैलाया जा सकता है।
 - अवैध डिजिटल सामग्री की निगरानी (धारा 69) सरकार को यह अधिकार प्राप्त है कि वह कृत्रिम बुद्धिमत्ता संचालित प्लेटफॉर्म पर संदिग्ध या राष्ट्र-विरोधी सामग्री की निगरानी कर सके। उदाहरण— कृत्रिम बुद्धिमत्ता का उपयोग कर भडकाऊ या गलत सूचना फैलाना। इस धारा के तहत सरकार इंटरनेट सेवा प्रदाताओं और कृत्रिम बुद्धिमत्ता कंपनियों से डेटा मांग सकती है।
 - **वेबसाइट और कृत्रिम बुद्धिमत्ता** — आधारित सेवाओं पर प्रतिबंध (धारा 69) यदि कोई वेबसाइट या कृत्रिम बुद्धिमत्ता आधारित एप्लिकेशन राष्ट्रीय सुरक्षा के लिए खतरा उत्पन्न करता है, तो सरकार उसे ब्लॉक कर सकती है।
 - **कृत्रिम बुद्धिमत्ता** — संचालित प्लेटफॉर्म की जिम्मेदारी (धारा 79) यदि कोई कृत्रिम बुद्धिमत्ता संचालित सोशल मीडिया प्लेटफॉर्म या वेबसाइट अवैध सामग्री को फैलाने से रोकने में असफल रहती है, तो उसे इसके लिए उत्तरदायी ठहराया जा सकता है। उदाहरण कृत्रिम बुद्धिमत्ता कलन विधि का उपयोग कर अभद्र भाषा को बढ़ावा देना या हिंसा भड़काने वाली सामग्री को तेजी से प्रसारित करना।

सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत कृत्रिम बुद्धिमत्ता उपयोग में कानूनी चुनौतियाँ

- डेटा संरक्षण और गोपनीयता सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 43ए और 72ए संवेदनशील व्यक्तिगत डेटा की सुरक्षा करती है और इसके अनधिकृत प्रकटीकरण के लिए दंड का प्रावधान करती है। कृत्रिम बुद्धिमत्ता प्रणाली बड़े पैमाने पर डेटा एकत्र और संसाधित करती हैं, जिससे सहमति, सुरक्षा और दुरुपयोग को लेकर गंभीर चिंताएँ उत्पन्न होती हैं। कृत्रिम बुद्धिमत्ता के लिए विशिष्ट डेटा संरक्षण कानूनों की अनुपस्थिति कानूनी अनिश्चितताओं को बढ़ाती है।
- साइबर सुरक्षा जोखिम— सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66, 66सी, 66डी और 70 साइबर अपराध जैसे हैकिंग, पहचान की चोरी और धोखाधड़ी को कवर करती है। यहीं, डीपफेक और

स्वचालित फिशिंग जैसे कृत्रिम बुद्धिमत्ता – संचालित साइबर हमले मौजूदा कानूनी ढांचे के लिए नई चुनौतियाँ पेश करते हैं, जिनका प्रभावी रूप से समाधान नहीं हो पा रहा है।

- बौद्धिक संपदा (आईपी) अधिकार— सूचना प्रौद्योगिकी अधिनियम, 2000 में कृत्रिम बुद्धिमत्ता-जनित सामग्री के मालिक और सुरक्षा को सीधे संबोधित नहीं करता है, जिससे कानूनी अस्पष्टता बनी रहती है। प्रश्न उठता है कि कृत्रिम बुद्धिमत्ता द्वारा पैदा की गई सामग्री कॉपीराइट के भीतर आ सकती है या नहीं और कृत्रिम बुद्धिमत्ता –प्रणाली निदानित नवाचारों के पेटेंट कराया जा सकता है।
- कृत्रिम बुद्धिमत्ता निर्णयों के लिए जिम्मेदारी सूचना प्रौद्योगिकी अधिनियम की धारा 79 मध्यस्थों के सुरक्षित अधिकार प्रदान करती हैं, लेकिन सूचना प्रौद्योगिकी – संचालित निर्णयों की जिम्मेदारी के स्पष्ट रूप से परिभाषित नहीं करती। यदि कोई दुर्घटना कृत्रिम बुद्धिमत्ता के कारण होती है, जैसे कि स्वयं संचालित वाहनों की टक्कर या पक्षपातपूर्ण भर्ती प्रक्रिया, तो जवाबदेही निर्धारित करना एक महत्वपूर्ण कानूनी चुनौती बन जाती है।
- पक्षपात और भेदभाव— सूचना प्रौद्योगिकी अधिनियम में कृत्रिम बुद्धिमत्ता पूर्वाग्रह के स्पष्ट रूप से संबोधित नहीं किया गया है, फिर भी कृत्रिम बुद्धिमत्ता कलन विधि कई क्षेत्र जैसे कि भर्ती, ऋण प्रदान करने और कानून प्रवर्तन में पक्षपात के बढ़ावा दे सकते हैं। यह निष्पक्षता के बारे में चिंताएं पैदा करता है और नैतिक और कानूनी समस्याएं उत्पन्न करता है और इसके लिए उचित नियामक निगरानी की आवश्यकता होती है।
- गलत सूचना –सूचना प्रौद्योगिकी अधिनियम की धारा 66डी, 67 और 69ए ऑनलाइन धोखाधड़ी, अश्लील सामग्री और वेबसाइट अवरोधन के संबंधित करते हैं। किन्तु कृत्रिम बुद्धिमत्ता द्वारा संचालित डीपफेक तकनीक गलत सूचना अभियानों से डिजिटल नैतिकता से जुड़े वर्तमान कानूनों की चुनौती मिलती है, जिससे इनके दुरुपयोग को प्रभावी रूप से रोका जाता है।
- नैतिक नियामक अंतराल –सूचना प्रौद्योगिकी अधिनियम कृत्रिम बुद्धिमत्ता के नैतिकता, पारदर्शिता या जवाबदेही पर नियंत्रण नहीं देता है। कृत्रिम बुद्धिमत्ता के बढ़ते उपयोग को देखते हुए, भारत डिजिटल इंडिया अधिनियम और व्यक्तिगत डेटा संरक्षण (पीडीपी) विधेयक पर काम कर रहा है, जो यह चिंताएं दूर करने और कृत्रिम बुद्धिमत्ता शासन के लिए विशिष्ट नियम लागू करने की दिशा में एक महत्वपूर्ण कदम हो सकता है।

साहित्य समीक्षा

- डॉ. अस्वथी प्रकाश ,जी और बी. जननी (2020) ने अपने शोध में बताया है कि सूचना प्रौद्योगिकी अधिनियम, 2000 ने इलेक्ट्रॉनिक लेनदेन, पत्राचार और व्यावसायिक प्रक्रियाओं के भारत में कानूनी मान्यता प्रदान की थी। इसके अतिरिक्त, इस अधिनियम ने भारतीय दंड संहिता, साक्ष्य अधिनियम और बैंकर्स बुक्स साक्ष्य अधिनियम में संशोधन किया था, साथ ही जैसे शब्दों के पुनर्परिभाषित किया था।
- अंकिता गुप्ता (2011) ने अपने शोध में किशोर न्याय (देखभाल और संरक्षण) अधिनियम, 2000 का विश्लेषण किया था। उन्होंने पाया कि 1986, 2000 2006 के अधिनियमों में समय के साथ समाज में हुए परिवर्तनों के समाहित करने की आवश्यकता थी। उन्होंने आयु सीमा और अधिकतम सजा में संशोधन की सिफारिश की थी तथा विधायी छूट की आवश्यकता पर बल दिया था। इसके अलावा, उन्होंने चिकित्सीय न्यायशास्त्र की अवधारणा के लागू करने पर जोर दिया था, जिससे किशोर न्याय प्रणाली के और अधिक प्रभावी बनाया जा सके।
- योगेश कोलेकर (2015) ने सूचना प्रौद्योगिकी अधिनियम, 2000 की समीक्षा की थी और निष्कर्ष निकाला था कि यह अधिनियम संयुक्त राष्ट्र के इलेक्ट्रॉनिक वाणिज्य मॉडल कानून पर आधारित एक प्रमुख विधायी ढांचा था। उन्होंने यह भी उल्लेख किया था कि यह अधिनियम भारत में साइबर अपराध और

इलेक्ट्रॉनिक वाणिज्य से संबंधित मुद्दों के संबोधित करता था और साथ ही आर्थिक विकास और ई-गवर्नेंस के बढ़ावा देने में सहायक था।

- माइकल फिल्बी (2013) ने अपने शोध में वित्तीय सेवा और बाजार अधिनियम, 2000 के तहत अंदरूनी व्यापार के प्रवर्तन का विश्लेषण किया था। उन्होंने बताया था कि वित्तीय सेवा प्राधिकरण के आपराधिक न्याय अधिनियम, 1993 के तहत निरीक्षण, जांच और प्रवर्तन की शक्ति प्राप्त थी।
- हेमाली शाह (2016) ने अपने अध्ययन में सूचना प्रौद्योगिकी अधिनियम, 2000 में संशोधित हस्ताक्षर प्रावधानों पर निष्कर्ष निकाला था कि 2008 के संशोधन ने इसे प्रौद्योगिकी-तटस्थ होने का प्रयास किया था, किंतु यह अधिनियम अभी भी जटिल, अस्पष्ट और कमजोर बना हुआ था। उन्होंने यही उल्लेख किया था कि यह अधिनियम इलेक्ट्रॉनिक हस्ताक्षरों के उपयोग के प्रभावी रूप से नियंत्रित करने में असफल रहा था और अन्य विकासशील देशों जैसे चीन तथा विकसित देशों जैसे ऑस्ट्रेलिया, यूके और सिंगापुर की तुलनात्मक रूप से अधिक विनियमित था।
- निकोलाए स्फेटकु (2024) ने अपनी रिसर्च में मानव और कृत्रिम बुद्धिमत्ता की जटिल यात्रा का विश्लेषण किया था। उन्होंने इसके उत्पत्ति और भविष्य में मानव बुद्धिमत्ता के साथ इसके संभावित मेल पर वार्ता की थी।
- योसेफ बोनापार्टे (2023) ने वित्तीय में कृत्रिम बुद्धिमत्ता के अवसरों की समीक्षा की थी। उनके शोध में यह निष्कर्ष निकाला गया था कि अगले दशक में उत्पन्न राजस्व +2.7 ट्रिलियन तक पहुंच सकता है, जिसमें बाजार हिस्सेदारी सेवा-आधारित प्रौद्योगिकी की होगी। उन्होंने वित्तीय क्षेत्र से संबंधित शेरों के मूल्यांकन मॉडल प्रस्तुत किए थे और इस संभावना पर प्रकाश डाला था कि वित्तीय बाजार बुलबुले में प्रवेश कर सकता है।
- गियुसेपिना (पीना) और डी अगोस्टिनो (2023) ने अपनी शोध में उभरती प्रौद्योगिकियों की कानूनी सेवाओं और डिजिटल परिवर्तन पर प्रभाव का विश्लेषण किया था। उन्होंने बताया था कि तकनीक पहले से ही उन कार्यों के स्वचालित कर रही थी, जिन्हें पारंपरिक रूप से मानव कानूनी पेशेवरों द्वारा किया जाता था, जैसे कि अदालत के फैसलों की भविष्यवाणी करना, अनुबंध तैयार करना और मामलों का सारांश तैयार करना।
- विकिरण मडाला (2023) ने अपने शोध में द्वारा समाज में किए गए बदलावों की समीक्षा की थी। उन्होंने अनुसंधान में देखा था कि विभिन्न क्षेत्र के जैसे कि सरकार, नेटवर्क, संगठनों और व्यक्तियों के प्रभावित कर रहा था। डेटा संग्रह, हाइपर-कस्टमाइजेशन, ग्राहक वफादारी, लागत बचत और दक्षता में वृद्धि के अवसर प्रदान कर रहा था, जिससे वित्तीय संस्थानों और विज्ञापनदाताओं के महत्वपूर्ण लाभ मिल रहा था।
- लिआ विंग (2024) ने अपने उपादान में विवाद समाधान प्रणालियों के बढ़ते एकीकरण पर चर्चा की थी। उन्होंने राष्ट्रीय प्रौद्योगिकी और विवाद समाधान केंद्र के फेलो के विचारों का संकलन किया था, जिन्होंने के संभावित लाभों और जोखिमों पर अपनी प्रतिक्रियाएँ दी थीं। शोध में इस बात पर भी ध्यान दिया गया था कि बढ़ते उपयोग से विवाद समाधान प्रक्रियाओं में महत्वपूर्ण बदलाव आ सकते हैं।
- सतीश गजवाडा (2021) ने अपने शोध के दौरान विकासवादी संगणना के क्षेत्र में बढ़ते रुझानों का अध्ययन किया था। उन्होंने अनुकूलन कलन विधि पर विशेष ध्यान केंद्रित किया था, जो मानव व्यवहार से प्रेरित थे। दिसंबर 2016 में, उन्होंने कृत्रिम मानव अनुकूलन नामक एक नए क्षेत्र के प्रस्तुत किया था, जिसका उद्देश्य इस विषय के लोकप्रिय बनाना और इसके संभावित अवसरों के उजागर करना था। इसके अलावा, उन्होंने कृत्रिम अर्थशास्त्र अनुकूलन नामक एक अन्य नए क्षेत्र का भी प्रस्ताव दिया था। उनके शोध ने इस दिशा में संभावनाओं और अनुसंधान के नए द्वार खोले थे।

शोध अंतर

भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 कृत्रिम बुद्धिमत्ता और संबंधित साइबर सुरक्षा खतरों के प्रबंधन में सीमित है। यह अधिनियम तेजी से विकसित हो रही कृत्रिम बुद्धिमत्ता प्रौद्योगिकियों से उत्पन्न कानूनी और नैतिक चुनौतियों के पूरी तरह से नहीं संभालता, जैसे कि डेटा सुरक्षा, स्वचालित निर्णय-निर्माण, और कृत्रिम बुद्धिमत्ता-आधारित साइबर अपराध। इसके अलावा, कृत्रिम बुद्धिमत्ता-निर्मित निर्णयों की जिम्मेदारी, डेटा गोपनीयता, गलत सूचना के प्रसार के लिए उपयुक्त प्रावधानों की कमी है। इस स्थिति के कारण, एक समग्र भविष्य-आधारित कानूनी ढांचे की आवश्यकता है जो भारत में कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के क्षेत्र में जोखिमों के प्रभावी ढंग से नियंत्रित सुरक्षित कर सके।

शोध उद्देश्य

- इस शोध का मुख्य उद्देश्य सूचना प्रौद्योगिकी अधिनियम, 2000 की प्रभावशीलता का मूल्यांकन करना है खासकर कृत्रिम बुद्धिमत्ता साइबर सुरक्षा के संदर्भ में।
- शोध का दूसरा उद्देश्य साइबर अपराधों और डेटा सुरक्षा उल्लंघनों से निपटने के लिए आवश्यक कानूनों में सुधारों का अध्ययन करना है।
- इस अध्ययन में भारत और अन्य देशों के साइबर सुरक्षा और कृत्रिम बुद्धिमत्ता कानूनों की तुलनात्मक समीक्षा की जाएगी, ताकि कानूनी दृष्टिकोण से अंतर्राष्ट्रीय प्रभावशीलता के समझा जा सके।

तुलनात्मक समीक्षा

भारत यूरोपीय संघ के साइबर सुरक्षा कृत्रिम बुद्धिमत्ता कानूनों की तुलना

भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 प्रमुख साइबर सुरक्षा लागू कानून है जो साइबर अपराधों और ई-कॉमर्स के लिए कानूनी फ्रेमवर्क प्रदान करता है। 2008 के संशोधन में डेटा सुरक्षा और साइबर आतंकवाद के सम्मिलित किया गया है, लेकिन कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के लिए स्पष्ट गाइडेंस का अभाव है। द्वारा, हालाँकि, डिजिटल पर्सनल डेटा सुरक्षा बिल, 2023 प्रस्तावित है, जो डेटा प्रोटेक्शन के मजबूत करने की दिशा में एक महत्वपूर्ण कदम हो सकता है। भारत में कृत्रिम बुद्धिमत्ता डेटा प्रोटेक्शन के लिए अभी तक कोई विशेष कानून नहीं है।

यूरोपीय संघ – यूरोपीय संघ के सामान्य डेटा संरक्षण विनियमन व्यक्तिगत डेटा की रक्षा और गोपनीयता के लिए कड़े नियमों के तहत व्यक्तिगत डेटा की सुरक्षा करेगा। भारत में कंपनियों पर गैर-अनुपालन के लिए भारी जुर्माने का प्रावधान है और कृत्रिम बुद्धिमत्ता और बिग डेटा पर कड़े प्रतिबंध हैं। भारत के तहत व्यक्तिगत डेटा की रक्षा के गहरी प्राथमिकता दी जाती है और इसमें डेटा स्थानांतरण, डेटा प्रोसेसिंग और डेटा विषय के अधिकारों के लिए कड़े नियम हैं। यूरोपीय संघ में कृत्रिम बुद्धिमत्ता के लिए भी दिशा-निर्देश और रेगुलेशन प्रस्तावित हैं, जो कृत्रिम बुद्धिमत्ता के नैतिक और सुरक्षित उपयोग के सुनिश्चित करने के लिए बनाए गए हैं।

- डेटा सुरक्षा— GDPR के अधीन, डेटा सुरक्षा के सख्त नियम प्रभावी होते हैं, जिनकी तुलना भारत के डेटा सुरक्षा कानून से की जाती है, जो अभी इतना कठोर नहीं है। यूरोपीय बाजार में भारतीय कंपनियों के कार्य करने के लिए ळक्क अनुपालन होना आवश्यक है।
- कृत्रिम बुद्धिमत्ता नियंत्रण— यूरोपीय संघ में कृत्रिम बुद्धिमत्ता और बिग डेटा पर कठोर नियंत्रण हैं, जो भारत में कृत्रिम बुद्धिमत्ता और डेटा प्रोटेक्शन के लिए स्पष्ट दिशा-निर्देशों की अनुपस्थिति में हैं।
- कानूनी ढांचा— भारत का सूचना प्रौद्योगिकी अधिनियम 2000 साइबर क्राइम और ई-कॉमर्स के लिए कानूनी ढांचा देता है, जबकि ळक्क डेटा गोपनीयता और सुरक्षा पर अधिक जोर देता है।

- गोपनीयता और अधिकार— GDPR यूरोपीय संघ में डेटा विषय के अधिकारों की उच्च प्राथमिकता देता है, जैसे कि डेटा एक्सेस, सुधार, और मिटाने का अधिकार, जबकि भारतीय कानून में इस तरह के अधिकारों के लिए अभी तक कोई कठोर प्रावधान नहीं है।

भारत संयुक्त राज्य अमेरिका के साइबर सुरक्षा कृत्रिम बुद्धिमत्ता कानूनों की तुलनात्मक समीक्षा

भारत में साइबर सुरक्षा के क्षेत्र में प्रमुख कानून सूचना प्रौद्योगिकी अधिनियम, 2000 है। यह अधिनियम साइबर अपराधों और ई-कॉमर्स के लिए एक कानूनी ढांचा स्थापित करता है। 2008 में किए गए संशोधनों के अंतर्गत डेटा सुरक्षा और साइबर आतंकवाद के शामिल किया गया, लेकिन कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के लिए स्पष्ट दिशा-निर्देशों की कमी बनी हुई है। वर्तमान में, डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023 की प्रस्तावित रूपरेखा है, जो डेटा सुरक्षा के सुदृढ़ करने में एक महत्वपूर्ण कदम माना जा सकता है। भारतीय कानून कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा से संबंधित मुद्दों पर अभी भी विकासशील चरण में हैं, और फिलहाल कोई विशिष्ट कानून लागू नहीं है।

संयुक्त राज्य अमेरिका में, क्लाउड अधिनियम ;सवनक ।बजद्ध सरकार को डेटा तक विधिक पहुंच प्रदान करता है। यह अधिनियम तकनीकी कंपनियों को डेटा साझा करने के लिए बाध्य कर सकता है, जिससे कृत्रिम बुद्धिमत्ता और मशीन लर्निंग के लिए आवश्यक डेटा तक पहुंच सुनिश्चित होती है। इस प्रकार, अमेरिका का दृष्टिकोण डेटा प्रबंधन में अधिक स्पष्टता और नीतिगत दिशा प्रदान करता है, जबकि भारत के कानून इस क्षेत्र में अभी भी विकास की प्रक्रिया में हैं।

भारत और चीन के साइबर सुरक्षा और कृत्रिम बुद्धिमत्ता कानूनों की तुलना

भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 (सूचना प्रौद्योगिकी अधिनियम 2000) मुख्य साइबर सुरक्षा कानून है, जो साइबर अपराधों और ई-कॉमर्स के लिए कानूनी ढांचा प्रदान करता है। 2008 के संशोधन में डेटा सुरक्षा और साइबर आतंकवाद को शामिल किया गया है, लेकिन कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के लिए स्पष्ट दिशा-निर्देशों की कमी है। वर्तमान में डिजिटल पर्सनल डेटा सुरक्षा बिल (DPDP, Bill), 2023 प्रस्तावित है, जो डेटा सुरक्षा को मजबूत करने की दिशा में एक महत्वपूर्ण कदम हो सकता है। भारतीय कानून कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के मामले में अब भी विकसित हो रहे हैं और अभी तक कोई विशेष कानून लागू नहीं हुआ है।

चीन का साइबर सुरक्षा डेटा स्थानीयकरण को अनिवार्य बनाता है, जिसका अर्थ है कि डेटा को चीन में ही संग्रहीत करना होगा। इसके अलावा, चीन में कृत्रिम बुद्धिमत्ता और बिग डेटा पर कड़े सरकारी नियंत्रण होते हैं। इस प्रकार, भारत और चीन का दृष्टिकोण साइबर सुरक्षा और कृत्रिम बुद्धिमत्ता कानूनों में स्पष्ट अंतर दर्शाता है, जहाँ चीन ने कड़े नियमों और नीतियों को अपनाया है जबकि भारत में विकास और सुधार की प्रक्रिया जारी है।

स्वाट विश्लेषण मॉडल

मजबूत पक्ष

- सूचना प्रौद्योगिकी अधिनियम, 2000— यह कानून साइबर अपराध और ई-कॉमर्स के लिए एक कानूनी ढांचा प्रदान करता है। इस अधिनियम ने भारत में साइबर सुरक्षा के क्षेत्र में महत्वपूर्ण योगदान दिया है।
- 2008 का संशोधन— इस संशोधन ने डेटा सुरक्षा और साइबर आतंकवाद को भी शामिल किया, जिससे साइबर सुरक्षा के दायरे में विस्तार हुआ।
- धारा 66 और 69 इन धाराओं ने अवैध ऑनलाइन गतिविधियों और सामग्री को रोकने में महत्वपूर्ण भूमिका निभाई है।
- डिजिटल व्यक्तिगत डेटा सुरक्षा बिल, 2023 यह प्रस्तावित रूपरेखा डेटा सुरक्षा को मजबूत करने की दिशा में एक महत्वपूर्ण कदम हो सकता है।

- डेटा प्रोसेसिंग के लिए सहमति यह बिल डेटा प्रोसेसिंग के लिए सहमति प्राप्त करने की आवश्यकता पर जोर देता है।
- डेटा संरक्षण अधिकारी ;क्वद्धरू क्च की नियुक्ति की आवश्यकता है, जो डेटा सुरक्षा नीतियों को लागू करने और निगरानी करने में मदद करेगा।

कमजोरियां पक्ष

- नुकसानपूर्ण दिशा निर्देशों की कमी— कृत्रिम बुद्धिमत्ता और डेटा प्रोटेक्शन के स्पष्ट दिशा-निर्देशों का अभाव, जो कृत्रिम बुद्धिमत्ता विकास को प्रभावित कर सकता है।
- स्पष्ट नीतियों की अनुपस्थिति— कृत्रिम बुद्धिमत्ता और मशीन लर्निंग के लिए विशेष नीतियों की अनुपस्थिति, जो नवाचार और अनुसंधान को बाधित कर सकती हैं।
- अनुपालन की अनुपस्थिति— डेटा प्रोटेक्शन कानूनों का अनुपालन न करने वाले संगठनों के लिए सख्त नियमों और जुर्मानों की अनुपस्थिति।
- भारतीय कानून कठोर नहीं है, जिससे डेटा सुरक्षा में असमानता हो सकती है।
- डेटा गोपनीयता— डेटा गोपनीयता के मामले में कमजोर प्रावधान।
- अंतरराष्ट्रीय मानकों की अनुपस्थिति — वैश्विक डेटा सुरक्षा मानकों के साथ सामंजस्य नहीं।
- सूचना प्रौद्योगिकी विशेष कानून कृत्रिम बुद्धिमत्ता और डेटा सुरक्षा के लिए विशेष कानून की संभावना, जो इस क्षेत्र में सुधार ला सकते हैं।
- कृत्रिम बुद्धिमत्ता अनुसंधान और विकास में निवेश को बढ़ावा देना।
- डेटा सुरक्षा के मानकों को बढ़ावा देना और वैश्विक स्तर पर प्रतिस्पर्धी बनाना।
- सुरक्षा मानकों का कार्यान्वयन डेटा प्रोटेक्शन को मजबूत करने के लिए, जिससे डेटा सुरक्षा में बेहतरी हो सकती है।
- डेटा सुरक्षा जागरूकता बढ़ाना डेटा सुरक्षा के महत्व का बढ़ाना।
- डेटा सुरक्षा में बेहतरी के साथ नए व्यापारिक अवसरों की उत्पत्ति।

चुनौती पक्ष

- चुनौती अंतरराष्ट्रीय अनुपालन— भारतीय कंपनियों के लिए अंतरराष्ट्रीय बाजारों में अनुपालन की चुनौती।
- व्यापारिक जोखिम अंतरराष्ट्रीय मानकों का पालन न करने पर व्यापारिक नुकसान का सामना करना।
- प्रतिस्पर्धा में कमी वैश्विक प्रतिस्पर्धा में कमी आने की संभावना।
- साइबर हमलों और डेटा सुरक्षा के संदर्भ में कमजोरियों का फायदा उठाने वाले हमलावर।
- साइबर आतंकवाद— साइबर आतंकवाद के बढ़ते खतरों का सामना करना।
- महत्वपूर्ण डेटा की चोरी और दुरुपयोग की संभावना।

अवसर पक्ष

यह बाहरी कारक होते हैं जो शोध को सकारात्मक रूप से प्रभावित कर सकते हैं, जैसे

- क्षेत्र में उभरती प्रवृत्तियाँ या विकास
- अन्य शोधकर्ताओं या संस्थानों के साथ सहयोग के अवसर
- नई तकनीकी या विधात्मक विकास
- अन्वेषण या अनपेक्षित शोध क्षेत्रका विस्तार

मुख्य निष्कर्ष

- सूचना प्रौद्योगिकी अधिनियम, 2000 और कृत्रिम बुद्धिमत्ता यह अधिनियम मुख्य रूप से इलेक्ट्रॉनिक गवर्नेंस, डेटा सुरक्षा, और साइबर अपराध को नियंत्रित करता है, लेकिन इसमें कृत्रिम बुद्धिमत्ता से जुड़ी विशिष्ट चुनौतियों का प्रत्यक्ष समाधान नहीं है। भारत में कृत्रिम बुद्धिमत्ता के विकास और उपयोग के लिए वर्तमान कानून अन्यथा कम हैं, क्योंकि सूचना प्रौद्योगिकी अधिनियम 2000 उस समय बना था जब कृत्रिम बुद्धिमत्ता का विकास प्रारंभिक अवस्था में था।
- कृत्रिम बुद्धिमत्ता से उत्पन्न कानूनी चुनौतियाँ लड़ाईपूर्ण स्थितियों में कार्य करते हुए, कृत्रिम बुद्धिमत्ता आधारित निर्णयों में पारदर्शिता की कमी के कारण उत्तरदायित्व तय करना मुश्किल होता है। कृत्रिम बुद्धिमत्ता द्वारा उत्पन्न की गई सामग्री या स्वायत्त निर्णयों की वजह से नैतिकता और गोपनीयता की समस्याएँ बढ़ती जा रही हैं। डेटा सुरक्षा और व्यक्तिगत जानकारी की सुरक्षा के लिए कड़ी नियमों की आवश्यकता है, जो वर्तमान कानून में पर्याप्त रूप से शामिल नहीं हैं। भारत की स्थिति अन्य देशों की स्थिति से अलग होगी।
- भारत की स्थिति अन्य देशों के साथ-यूरोपीय संघ (EU) का GDPR (General Data Protection Regulation) के द्वारा व्यक्तिगत डेटा की सुरक्षा का मजबूत कानून है, जबकि भारत का डेटा संरक्षण विधेयक अभी प्रक्रियाधीन है। अमेरिका और चीन में कृत्रिम बुद्धिमत्ता नियमन से संबंधित विशेष नीतियाँ विकसित की जा रही हैं, जबकि भारत अभी शुरुआती स्तर पर है। भारत को कृत्रिम बुद्धिमत्ता विनियमन और नैतिक दिशानिर्देशों पर स्पष्ट नीति की आवश्यकता है।

निष्कर्ष

सूचना प्रौद्योगिकी अधिनियम, 2000 भारत में डिजिटल नियमन का मुख्य कानून है, लेकिन यह कृत्रिम बुद्धिमत्ता से निर्मित कानूनी और नैतिक चुनौतियों को प्रभावी ढंग से संबोधित करने के लिए सक्षम नहीं है। कृत्रिम बुद्धिमत्ता के बढ़ते उपयोग के साथ उत्तरदायित्व, पारदर्शिता, न्यायसंगतता, डेटा गोपनीयता और नैतिकता से अनेक नए सवाल सामने आए हैं। अभी तक, भारत में कृत्रिम बुद्धिमत्ता के लिए विशिष्ट कानूनी ढाँचा नहीं है, लेकिन राष्ट्रीय कृत्रिम बुद्धिमत्ता रणनीति और व्यक्तिगत डेटा संरक्षण विधेयक इस दिशा में कुछ सफलता दिखाते हैं। वैश्विक स्तर पर, यूरोपीय संघ का और अन्य देशों की नीतियाँ कृत्रिम बुद्धिमत्ता नियमन में भारत के लिए उपयुक्त संदर्भ हो सकती हैं। भारत को प्रोत्साहित होना चाहिए कि वह कृत्रिम बुद्धिमत्ता के नैतिक, कानूनी और सामाजिक प्रभावों को ध्यान में रखते हुए एक समग्र नियामक ढाँचा विकसित करे, जिससे नवाचार और सुरक्षा के बीच संतुलन बना रहे।

भविष्य की संभावनाएँ और आवश्यक सुधार

- भारत में कृत्रिम बुद्धिमत्ता और सूचना प्रौद्योगिकी कानूनों को अद्यतन करने के लिए कृत्रिम बुद्धिमत्ता नियामक ढाँचे की स्थापना आवश्यक है।
- कृत्रिम बुद्धिमत्ता नैतिकता और पारदर्शिता से संबंधित दिशा-निर्देश बनाए जाने चाहिए ताकि कृत्रिम बुद्धिमत्ता का सुरक्षित और जवाबदेह उपयोग सुनिश्चित किया जा सके।
- सूचना प्रौद्योगिकी अधिनियम, 2000 को संशोधित करने से कृत्रिम बुद्धिमत्ता-जनित कानूनी विवादों का समाधान करने के लिए विशेष प्रावधान जोड़े जाने चाहिए।

संदर्भ ग्रन्थ सूची

1. प्रसाद, ए., — जनानी, बी. (2020). कृत्रिम बुद्धिमत्ता अधिनियम 2000 में किए गए विभिन्न संशोधनों का तुलनात्मक अध्ययन और विश्लेषण, विशेष रूप से 2008 अधिनियम के संदर्भ में।
2. गुप्ता, अ. (2011). नाबालिग न्याय (देखभाल और सुरक्षा) अधिनियम, 2000 — एक आलोचना। SSRN-<https://ssrn.com/abstract=1884927>

3. कोलकर, य. (2015). सूचना प्रौद्योगिकी अधिनियम, 2000 का समीक्षा। एसएसआरएन <https://ssrn.com/abstract=2611827>
4. फिल्बी, म. (2013). वित्तीय सेवाएं और बाजार अधिनियम 2000 के तहत आंतरिक व्यापार की प्रवर्तन। कॉर्पोरेट वकील, 24(11), 2003। <https://ssrn.com/abstract=2087821>
5. शाह, ए., – श्रीवास्तव, ए. (2016). संशोधित भारतीय सूचना प्रौद्योगिकी अधिनियम 2000 में हस्ताक्षर प्रावधान— विधायी अराजकता। कॉमन लॉ वर्ल्ड रिव्यू, 43, 208–230। <https://ssrn.com/abstract=2748441>
6. स्फेटकु, एन. (2024). कृत्रिम बुद्धिमत्ता का नैतिकता। इंटेलिजेंस, प्राकृतिक उत्पत्ति से कृत्रिम सीमाओं तक – मानव बुद्धिमत्ता बनाम कृत्रिम बुद्धिमत्ता, 2024। <https://ssrn.com/abstract=4957094>
- 7- बोनापार्ट, य. (2023). वित्त में कृत्रिम बुद्धिमत्ता—मूल्यांकन और अवसर। एसएसआरएन <https://ssrn.com/abstract=4475689>
8. डशआगोस्टीनो, जी. (2023). अग्रणी कानूनी व्यवधान संपादकीय— कृत्रिम बुद्धिमत्ता के भविष्य के लिए एक दृष्टिकोण। लीडिंग लीगल डिस्प्रेशन— कृत्रिम बुद्धिमत्ता और वकीलों और कानून के लिए एक टूलकिट, 2021।
9. मदाला, आर., कृष्णा, ए. एस., राम्या, पी., सबरीराजन, ए., डोभाल, डी., – सापते, एस. (2023). वित्त और विपणन प्रणाली में कृत्रिम बुद्धिमत्ता आधारित नवीनतम व्यावसायिक अनुसंधान। ICONSTEM 2023, चेन्नई।
10. विंग, एल. (2024). कृत्रिम बुद्धिमत्ता पर टिप्पणियाँ। इंटरनेशनल जर्नल ऑफ ऑनलाइन डिस्प्यूट रेजोल्यूशन, 9(2), 147–176।
11. गजवाडा, एस. (2021). कृत्रिम मानव अनुकूलन क्षेत्रों में अवसरों का सागर। मशीन लर्निंग और कृत्रिम बुद्धिमत्ता पर लेन—देन, 6(3), 24 (2018)। <https://doi.org/10.14738/tmlai.63-4529>

