IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

भारतीय कानूनी प्रणाली में कृत्रिम बुद्धिमत्ता और साइबर सुरक्षाः उभरती चुनौतियाँ और कानूनी ढांचा

गरिमा सिंह
पी.एच.डी शोधार्थी
विधि संकाय
एस.एस.जे.विश्वविद्यालय(अल्मोड़ा)

सार

कृत्रिम बुद्धिमत्ता वैश्विक स्तर पर डिजिटल पारिस्थितिकी तंत्र में क्रांतिकारी बदलाव ला रही है, जिससे न केवल महत्वपूर्ण लाभ प्राप्त हो रहे हैं, बल्कि साइबर सुरक्षा के क्षेत्र में नई कमजोरियाँ भी उत्पन्न हो रही हैं। भारत में कृत्रिम बुद्धिमत्ता को तेजी से अपनाया जा रहा है, जिससे वर्तमान में प्रौद्योगिकी, व्यापार एवम् जीवनचर्या में बदलाव आ रहें है। इंटरनेट और मोबाइल एसोसिएशन ऑफ इंडिया का अनुमान है कि इसे तेजी से अपनाए जाने के कारण भारत का कृत्रिम बुद्धिमत्ता बाजार 2025 तक 8 बिलियन अमेरिकी डॉलर तक पहुंच जाएगा।[1] भारतीय कानूनी प्रणाली के समक्ष यह एक महत्वपूर्ण चुनौती है कि वह डेटा संरक्षण, निजता और साइबर अपराध के क्षेत्र में एआई द्वारा प्रस्तुत की जा रही चुनौतियों का सामना करने के लिए अपने कानूनों और नीतियों को अनुकूलित करें। यह शोध पत्र इस बात का विस्तृत विश्लेषण प्रस्तुत करता है कि भारत का कानूनी ढांचा कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा से जुड़े मुद्दों पर किस प्रकार प्रतिक्रिया दे रहा है। इसमें हालिया विधायी विकासों– विशेष रूप से ऐतिहासिक डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 का अध्ययन किया गया है, व एआई शासन को लक्षित करने वाली उभरती नीतिगत पहलों का विश्लेषण किया गया है। यह विवेचन गोपनीयता और प्रौद्योगिकी पर माननीय सर्वोच्च न्यायालय के महत्वपूर्ण निर्णयों के संदर्भ में किया गया है, जैसे कि जस्टिस के.एस. पुट्टस्वामी(सेवानिवृत्त) बनाम भारत संघ का वह निर्णय जिसने निजता को एक मौलिक अधिकार के रूप में स्थापित किया, आधार मामला जो बायोमेट्रिक पहचान प्रणालियों से संबंधित था, और ऑनलाइन अभिव्यक्ति की स्वतंत्रता तथा साइबर–निगरानी पर दिए गए अन्य महत्वपूर्ण निर्णय भी शामिल हैं। साहित्य समीक्षा विद्वानों और नीतिगत दृष्टिकोणों को उजागर करती है जो वर्तमान कानूनों में मौजूद कमियों को दर्शाते हैं, जैसे कि एआई–विशिष्ट नियमों और जवाबदेही के तंत्र का अभाव। इस लेख का मुख्य भाग साइबर सुरक्षा के लिए मौजूदा कानूनी ढाँचों (सूचना प्रौद्योगिकी अधिनियम, संबंधित नियम और राष्ट्रीय साइबर सुरक्षा नीतियां) और कृत्रिम बुद्धिमत्ता के नियामक दृष्टिकोण का मूल्यांकन करता है। भारत के दृष्टिकोण को समझने के लिए, यूरोपीय संघ जैसे देशों से तुलनात्मक अंतर्दृष्टि शामिल की गई है, जो एक विशिष्ट कृत्रिम बुद्धिमत्ता अधिनियम और मजबूत डेटा सुरक्षा प्रणाली को आगे बढ़ा रहा है, और संयुक्त राज्य अमेरिका, जिसकी क्षेत्र–विशिष्ट और अपेक्षाकृत कम हस्तक्षेपकारी नियामक शैली है। अंततः, यह शोध पत्र भारत की कानूनी और संस्थागत प्रतिक्रियाओं को सुदृढ़ करने के लिए सुझाव प्रस्तुत करता है। इनमें कृत्रिम बुद्धिमत्ता जवाबदेही के लिए अधिक स्पष्ट दिशानिर्देश लागू करना, साइबर अपराध और डेटा सुरक्षा मानकों को अद्यतन करना, विशेष एजेंसियों के माध्यम से प्रभावी प्रवर्तन सुनिश्चित करना और अंतर्राष्ट्रीय सहयोग को बढ़ावा देना शामिल है। एक सिद्धांत–आधारित कानूनी ढांचे के माध्यम से इन उभरती चुनौतियों का समाधान करके, भारत साइबर सुरक्षा और व्यक्तिगत अधिकारों की सुरक्षा करते हुए तकनीकी नवाचार को प्रोत्साहित कर सकता है।

कीवर्ल्ड– साइबर सुरक्षा, साइबर कानून, कृत्रिम बुद्धिमत्ता, गोपनीयता

[1] भारत में एआई के उपयोग से संबंधित डेटा गोपनीयता संबंधी विचार, https://law.asia/ai-and-data-protection/, प्रकाशित दिनॉक– 2 अप्रैल 2025.

परिचय

आधुनिक डिजिटल युग में, कृत्रिम बुद्धिमत्ता एक उभयभावी शक्ति के रूप में प्रकट हुई है, जहाँ यह एक ओर प्रगति को बढ़ावा दे रही है, वहीं दूसरी ओर साइबर सुरक्षा के जोखिमों को बढ़ा रही है। विश्व के राष्ट्र इस बात पर गहन विचार कर रहे हैं कि किस प्रकार एआई–आधारित तकनीकों को विनियमित किया जाए, जो स्थापित कानूनी व्यवस्थाओं के लिए एक चुनौती प्रस्तुत करती हैं। एक महत्वपूर्ण सूचना प्रौद्योगिकी केंद्र और तीव्र गति से विकसित हो रही डिजिटल अर्थव्यवस्था के रूप में, भारत इस चुनौती का सामना करने में अग्रणी भूमिका निभा रहा है। 900 मिलियन से अधिक इंटरनेट उपयोगकर्ताओं और डिजिटल शासन के लिए महत्वाकांक्षी पहलों के साथ, भारत की एआई और नेटवर्क प्रणालियों पर निर्भरता में तेजी से वृद्धि हो रही है।[2] हालाँकि, इस विकास के साथ साइबर हमलों, डेटा उल्लंघनों और एल्गोरिथम निर्णय लेने से संबंधित बढ़ती चिंताएँ भी जुड़ी हुई हैं, जिनका व्यक्तिगत गोपनीयता और सुरक्षा पर महत्वपूर्ण प्रभाव पड़ता है। परिणामस्वरूप, भारत में नीति निर्माता और कानूनविद इन महत्वपूर्ण सवालों का सामना कर रहे हैं: कानूनी प्रणाली साइबर स्पेस में कृत्रिम बुद्धिमत्ता द्वारा उत्पन्न अभूतपूर्व चुनौतियों का समाधान नवाचार को बाधित किए बिना कैसे करेगी ?, कृत्रिम बुद्धिमत्ता खतरों से नागरिकों की सुरक्षा के लिए किन सुरक्षात्मक उपायों की आवश्यकता है? और हाल के कानून तथा अदालती निर्णय कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के लिए विकसित हो रहे कानूनी ढांचे को किस प्रकार आकार दे रहे हैं?

इन प्रश्नों की महत्ता को भारत के सर्वोच्च न्यायालय द्वारा 2017 में निजता को एक अपरिहार्य अधिकार के रूप में स्वीकार करने से और भी बल मिला, यह एक ऐसा निर्णय है, जिसने सीधे तौर पर डेटा सुरक्षा कानून के निर्माण की दिशा में प्रयासों को प्रेरित किया।[3] इस ऐतिहासिक फैसले के बाद के वर्षों में, भारत ने डिजिटल युग के लिए अपने कानूनी ढांचे को नया रूप देने में उल्लेखनीय प्रगति की है। सबसे महत्वपूर्ण बात यह है कि संसद ने डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 को अधिनियमित किया, जो राष्ट्र का प्रथम व्यापक डेटा सुरक्षा विधान है और जिसका लक्ष्य व्यक्तिगत जानकारी की सुरक्षा करना तथा कृत्रिम बुद्धिमत्ता व्याप्त परिवेश में इसके संसाधन को नियंत्रित करना है।[4] इसके अलावा, सूचना प्रौद्योगिकी अधिनियम, 2000 जैसे दीर्घकालिक साइबर कानूनों में आज के साइबर अपराधों का समाधान करने के लिए परिवर्तन किए गए हैं, और डिजिटल इंडिया अधिनियम जैसे नए नीतिगत विचार इंटरनेट युग के लिए कानूनी व्यवस्था को पूरी तरह से नवीनीकृत और आधुनिक बनाने की प्रक्रिया में हैं।[5] इसी अवधि में, भारत की न्यायपालिका सक्रिय रूप से प्रौद्योगिकी और मौलिक अधिकारों के परस्पर प्रभाव वाले मुद्दों पर विचार करती रही है जिसमें श्रेया सिंघल बनाम भारत संघ मामले में अभिव्यक्ति की ऑनलाइन स्वतंत्रता पर अत्यधिक व्यापक प्रतिबंधों को निरस्त करना शामिल है।[6] अनुराधा भसीन बनाम भारत संघ मामले में इंटरनेट सेवाओं को बंद करने के लिए आनुपातिकता के मानदंडों को स्थापित करने तक[7], अवैध जासूसी सॉफ्टवेयर के उपयोग पर एक विशेषज्ञ समिति गठित करने तक[8]ए ये क्रम एक बदलते हुए कानूनी परिदृश्य को दर्शातें हैं जो तेज गति से हो रहे तकनीकी परिवर्तनों के साथ कदम मिलाकर चलने की कोशिश कर रहें हैं।

निश्चित तौर पर प्रगति हुई है, फिर भी कई महत्वपूर्ण कमियाँ बनी हुई हैं। वर्तमान नियम अक्सर कृत्रिम बुद्धिमत्ता के अनुप्रयोगों के बारे में विशिष्टता की कमी दर्शाते हैं, जिससे जवाबदेही और निगरानी में अंतर उत्पन्न होता हैं। यूरोपीय संघ जैसे न्यायालयों के विपरीत, जिन्होंने एआई प्रणालियों के लिए जोखिम–आधारित नियमों का प्रस्ताव रखा है, भारत अभी भी सामान्य कानूनों और शुरुआती नीतिगत संरचनाओं के एक संयोजन पर निर्भर है। एल्गोरिथम पूर्वाग्रह, स्वचालित निर्णय लेने, एआई प्रसंस्करण में डेटा गोपनीयता और एआई–जनित साइबर हमले जैसी समस्याएं ऐसी चुनौतियाँ प्रस्तुत करती हैं जिनका वर्तमान भारतीय कानूनों में पर्याप्त रूप से समाधान नहीं किया गया है[9]। इससे यह चिंता उत्पन्न होती है कि क्या एआई प्रणालियाँ पर्याप्त पारदर्शिता या जवाबदेही के बिना एक नियामक रुप में कार्य कर सकती है ? साथ ही इससे

---

[2] तनुश्री बसुरॉय , https://www.statista.com/topics/2157/internet-usage-in-india/, प्रकाशित दिनॉक– 18 सितम्बर 2024.

[3]https://navbharattimes.indiatimes.com/india/the-decision-on-the-right-to-privacy-was-to-recognize-the-constitution-as-the-foundation-justice-chandrachud/articleshow/84509254.cms,

[4]https://www.dlapiperdataprotection.com/?c=IN

[5]https://www.mondaq.com/india/it-and-internet/1550060/digital-india-act-looking-through-the-crystal-ball-of-a-new-digital-india, प्रकाशित दिनॉक–26 नवंबर 2024

[6]एआईआर (2015) 5 एससीसी 1.

[7] एआईआर (2020) 3 एससीसी 637.

[8] मनोहर लाल शर्मा बनाम भरत संघ, एआईआर (2023) 11 एससीसी 401.

[9]योशिता सूद,"Addressing Algorithmic Bias in India: Ethical Implications and Pitfalls",प्रकाशित- 30 अक्टूबर 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466681

डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम जैसे कानूनों के माध्यम से प्राप्त डेटा सुरक्षा और गोपनीयता के ढांचे की सत्यनिष्ठा खतरे में पड़ सकती है। कृत्रिम बुद्धिमत्ता का अन्य उभरती हुई तकनीकों (उदाहरण के लिए, एआई–संचालित इंटरनेट ऑफ थिंग्स उपकरण, या ब्लॉकचेन नेटवर्क में एआई अनुप्रयोग) के साथ संयोजन पारंपरिक साइबर घटनाओं और उत्तरदायी कर्ताओं के वर्गीकरण को अस्पष्ट करते हुए कानूनी मुद्दों को और जटिल बनाता है।

यह शोध पत्र ''भारतीय कानूनी प्रणाली में कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा'' का एक व्यापक विश्लेषण प्रस्तुत करने का प्रयास करता है, जिसमें उभरती चुनौतियों और उनसे निपटने के लिए विकसित हो रहे कानूनी ढांचे पर ध्यान केंद्रित किया गया है। इसकी संरचना इस प्रकार है। परिचय में अध्ययन के संदर्भ और महत्व को स्थापित किया गया है, जिसमें तकनीकी नवाचार और कानूनी सुरक्षा उपायों के बीच तनाव को उजागर किया गया है। कृत्रिम बुद्धिमत्ता और साइबर सुरक्षाः अवधारणाएं और उभरते जोखिम पर अध्ययन किया गया है कि एआई प्रौद्योगिकियां साइबर सुरक्षा के साथ कैसे जुड़ती हैं, भारतीय संदर्भ में कृत्रिम बुद्धिमत्ता द्वारा प्रस्तुत खतरों और अवसरों के प्रकारों को दर्शाया गया है। पत्र का मुख्य भाग भारत में कानूनी और नीतिगत ढांचे का विश्लेषण करता है, जिसे उपभागों में विभाजित किया गया हैः डेटा संरक्षण और गोपनीयता कानून (डीपीडीपी अधिनियम, 2023 पर जोर दिया गया है), सूचना प्रौद्योगिकी अधिनियम और साइबर अपराध के प्रावधान, साइबर सुरक्षा नियम और संस्थागत तंत्र, और कृत्रिम बुद्धिमत्ता –विशिष्ट नीतिगत पहल (जैसे एआई पर राष्ट्रीय रणनीति और हालिया सरकारी सलाह)। साथ ही, न्यायिक प्रतिक्रियाओं पर एक समर्पित खंड चर्चा करता है कि भारतीय अदालतों, विशेष रूप से सर्वोच्च न्यायालय ने गोपनीयता, डेटा सुरक्षा और उभरती प्रौद्योगिकियों के मुद्दों को कैसे संबोधित किया है – ऐतिहासिक निर्णयों और निर्देशों के माध्यम से जो कानूनी परिदृश्य को प्रभावित करते हैं।

मौजूदा ढांचे और स्थापित न्यायशास्त्र की पृष्ठभूमि के साथ, यह पत्र फिर उन उभरती चुनौतियों पर गहराई से विचार करता है जो बनी हुई हैं। इसमें एल्गोरिथम पूर्वाग्रह और पक्षपात, एआई के कारण क्षति के लिए दायित्व में स्पष्टता की कमी, सीमा पार डेटा प्रवाह और साइबर संचालन को विनियमित करने की कठिनाई, और साइबर स्पेस में प्रवर्तन मुद्दे जैसी चुनौतियां शामिल हैं। भारत की परिस्थिति के परिप्रेक्ष्य में रखकर कर, अन्य न्यायालयों के दृष्टिकोणों का अध्ययन कर एक तुलनात्मक कानूनी परिप्रेक्ष्य प्रस्तुत किया गया है– विशेष रूप से यूरोपीय संघ की सख्त डेटा संरक्षण व्यवस्था और कृत्रिम बुद्धिमत्ता अधिनियम, संयुक्त राज्य अमेरिका का एआई और साइबर सुरक्षा के प्रति विकसित हो रहे दृष्टिकोण, और अंतर्राष्ट्रीय मंचों से प्रासंगिक उदाहरण प्रस्तुत किये गए है। ये तुलनाएं ऐसे मॉडल और उदाहरण उजागर करती हैं जो भारत के आगे के मार्ग को प्रस्सत कर सकते हैं। अंत में, यह पत्र एआई और साइबर सुरक्षा को नियंत्रित करने वाले भारतीय कानूनी और नियामक ढांचे को मजबूत करने के लिए सुझाव प्रदान करता है। ये सुझाव नीति निर्माताओं और हितधारकों के उद्देश्य से हैं और विधायी सुधारों, संस्थागत क्षमता निर्माण, नैतिक एआई तैनाती के लिए दिशानिर्देशों या मानकों के निर्माण और घरेलू और अंतरराष्ट्रीय स्तर पर बेहतर समन्वय के लिए तंत्र शामिल हैं। और एक सक्रिय और संतुलित कानूनी दृष्टिकोण की आवश्यकता पर विचार करता है जो तकनीकी प्रगति को अनावश्यक रूप से बाधित किए बिना सुरक्षा और गोपनीयता सुनिश्चित करता है।

यह अध्ययन अकादमिक प्रकाशन के लिए उपयुक्त एक औपचारिक, विश्लेषणात्मक स्वर अपनाता है, और यह प्रत्येक बिंदु की पुष्टि करने के लिए कानूनों, सरकारी रिपोर्टों, अदालती निर्णयों और विशेषज्ञ विश्लेषणों सहित विश्वसनीय स्रोतों पर निर्भर करता है। सैद्धांतिक कानूनी विकासों और व्यावहारिक चुनौतियों दोनों की जांच करके, यह पत्र इस समझ में योगदान करने की आकांक्षा रखता है कि भारत एक मजबूत साइबर सुरक्षा और कानूनी ढांचे के साथ कृत्रिम बुद्धिमत्ता युग में कैसे आगे बढ सकता है।

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षाः अवधारणाएँ और नए खतरे

कानूनी ढांचे का विश्लेषण करने से पहले, यह समझना आवश्यक है कि व्यावहारिक स्तर पर कृ त्रिम बुद्धिमत्ता और साइबर सुरक्षा किस प्रकार अंतःक्रिया करते हैं, और डिजिटल दुनिया में कृत्रिम बुद्धिमत्ता किस प्रकार के अनूठे खतरे पैदा कर, साइबर सुरक्षा को प्रभावित कर रही है। सरल शब्दों में कहें तो, कृत्रिम बुद्धिमत्ता तकनीकों का एक संग्रह है जो डेटा, एल्गोरिदम और कंप्यूटिंग शक्ति को एक साथ जोड़ता है। कंप्यूटिंग में प्रगति और डेटा की बढ़ती उपलब्धता कृत्रिम बुद्धिमत्ता के वर्तमान तेजी का प्रमुख कारक हैं।[10] मूल रूप से, कृत्रिम बुद्धिमत्ता उन कंप्यूटर प्रणालियों को इंगित करती है जो ऐसे कार्य करने की क्षमता रखती हैं

[10]European Commission,White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, 19 Feb. 2020, p. 2.

जिनके लिए सामान्यतः मानवीय बुद्धि की आवश्यकता होती है।[11] कृत्रिम बुद्धिमत्ता, साइबर सुरक्षा को बढ़ाने के लिए एक प्रभावशाली साधन है साथ ही साइबर अपराधियों के लिए एक संभावित औजार भी है। साइबर सुरक्षा अमेरिका की साइबर रक्षा एजेंसी के अनुसार, "नेटवर्क, उपकरणों और डेटा को अनधिकृत पहुँच या आपराधिक उपयोग से बचाने की कला है और सूचना की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने का अभ्यास है"।[12] सूचना प्रौद्योगिकी अधिनियम 'साइबर सुरक्षा'' को सूचना, उपकरण, डिवाइस, कंप्यूटर, कंप्यूटर संसाधनों, संचार उपकरणों और उनमें संग्रहीत सूचना को अनधिकृत पहुँच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन या विनाश से बचाने की प्रक्रिया के रूप में परिभाषित करती है।[13] यह परिभाषा अनिवार्य रूप से डिजिटल संपत्तियों और प्रणालियों को साइबर खतरों से बचाने के मूल सिद्धांतों को रेखांकित करती है।

यूरोपीय संघ के कृत्रिम बुद्धिमत्ता अधिनियम के अनुसार, कृत्रिम बुद्धिमत्ता प्रणाली का अर्थ है, एक मशीन–आधारित प्रणाली जिसे स्वायत्तता के विभिन्न स्तरों के साथ संचालित करने के लिए डिजाइन किया गया है और जो तैनाती के बाद अनुकूलता प्रदर्शित कर सकती है, और जो स्पष्ट या अंतर्निहित उद्देश्यों के लिए, प्राप्त इनपुट से यह अनुमान लगाती है कि कैसे पूर्वानुमान, सामग्री, सिफारिशें या निर्णय जैसे आउटपुट उत्पन्न किए जाएं जो भौतिक या आभासी वातावरण को प्रभावित कर सकते हैं।[14] **कृत्रिम बुद्धिमत्ता फ्रेमवर्क कन्वेंशन, 2024** के अनुसार ''कृत्रिम बुद्धिमत्ता प्रणाली'' एक मशीन–आधारित प्रणाली है, जो स्पष्ट या निहित उद्देश्यों के लिए, प्राप्त इनपुट से यह अनुमान लगाती है कि कैसे पूर्वानुमान, सामग्री, सिफारिशें या निर्णय जैसे आउटपुट उत्पन्न किए जाएं जो भौतिक या आभासी वातावरण को प्रभावित कर सकते हैं। विभिन्न कृत्रिम बुद्धिमत्ता प्रणालियाँ तैनाती के बाद अपनी स्वायत्तता और अनुकूलता के स्तर में भिन्न होती हैं।[15] दोनों परिभाषाऐं लगभग एक समान ही हैं। उदाहरण के लिए सीखना, तर्क करना, पैटर्न पहचानना और निर्णय लेना। आधुनिक एआई अक्सर मशीन लर्निंग एल्गोरिदम का उपयोग करता है जो डेटा के संपर्क में आने से बेहतर होते जाते हैं, जिसमें डीप न्यूरल नेटवर्क भी शामिल हैं जो जटिल पैटर्न को पहचान सकते हैं। इन क्षमताओं को विभिन्न साइबर सुरक्षा अनुप्रयोगों में उपयोग किया गया हैः उदाहरण के लिए, एआई–आधारित सिस्टम सिस्टम के व्यवहार में असामान्यताओं को पहचानकर नेटवर्क में घुसपैठ या दुर्भावनापूर्ण सॉफ्टवेयर का पता लगा सकते हैं, और वे किसी भी मानव ऑपरेटर की तुलना में अधिक तेजी से प्रतिक्रियाओं को स्वचालित कर सकते हैं।[16] सरकारें और कंपनियाँ सुरक्षा को मजबूत करने के लिए तेजी से एआई उपकरणों का उपयोग कर रही हैंदृ स्पैम फिल्टर और धोखाधड़ी का पता लगाने वाली प्रणालियों से लेकर परिष्कृत खतरे की खुफिया जानकारी के प्लेटफार्मों तक।

हालांकि, जिन विशेषताओं के कारण कृत्रिम बुद्धिमत्ता सुरक्षा के लिए उपयोगी है, उन्हीं का दुरुपयोग दुर्भावनापूर्ण तरिके से कुछ वर्ग कर सकते हैं। साइबर हमलावर अधिक प्रभावी हमलों के लिए कृत्रिम बुद्धिमत्ता का इस्तेमाल कर रहे हैं, यह एक ऐसी प्रवृत्ति है, जिसे साइबर सुरक्षा विशेषज्ञों ने एक बढ़ती हुई चिंता के रूप में चिन्हित किया है।[17] उदाहरण के लिए, एआई का उपयोग अत्यंत विश्वसनीय फिशिंग ईमेल या आवाज के डीपफेक बनाने के लिए किया जा सकता है ताकि पीड़ितों को धोखा दिया जा सके दृ मूल रूप से बड़े पैमाने पर सामाजिक इंजीनियरिंग हमलों को स्वचालित किया जा सके। ऐसे मामले सामने आए हैं जहाँ मैलवेयर ने सुरक्षा उपायों के जवाब में अपने हस्ताक्षर या व्यवहार को बदलकर पहचान से बचने के लिए प्रारंभिक एआई का उपयोग किया है।[18] भारत 2024 में, जो साइबर हमलों से प्रभावित विश्व के शीर्ष देशों में दूसरे स्थान में है।[19] सुरक्षा एजेंसियों ने दुष्प्रचार फैलाने के लिए डीपफेक वीडियो या महत्वपूर्ण बुनियादी ढांचे पर एल्गोरिथम द्वारा निर्देशित साइबर हमलों जैसे एआई–सक्षम खतरों की चेतावनी दी है। कृत्रिम बुद्धिमत्ता

---

[11]तपेश मेघवाल, "EMERGING CHALLENGES IN REGULATING ARTIFICIAL INTELLIGENCE UNDER CYBER SECURITY LAWS IN INDIA", प्रकाशन दिनांक–17 जनवरी 2024,file:///E:/ARTIFICIAL%20INTELLIGENCE%20UNDER%20CYBER.pdf.

[12]साइबर सुरक्षा क्या है?, प्रकाशन दिनांक–1 फरवरी 2021, https://www.cisa.gov/news-events/news/what-cybersecurity,

[13] धारा 2(1)(nb),सूचना प्रौद्योगिकी अधिनियम,2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–4.

[14]Article 3(1), Regulation (EU) 2024/1689, http://data.europa.eu/eli/reg/2024/1689/oj,

[15]Article 2, Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

[16]रॉबिन सोमर और वर्न पैक्सन, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection", IEEE सुरक्षा और गोपनीयता पर संगोष्ठी, 2010, पृठ सं -305–316.

[17]माइल्स ब्रुंडेज और अन्य,"The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", प्रकाशन– फरवरी 2024,https://www.researchgate.net/publication/323302750_The_Malicious_Use_of_Artificial_Intelligence_Forecasting_Prevention_and_Mitigation

[18]एमडी जोबैर हुसैन फारुक और अन्य, शोध पत्र– "Malware Detection and Prevention using Artificial Intelligence Techniques", प्रकाशन–दिसम्बर 2021,https://www.researchgate.net/publication/357163392_Malware_Detection_and_Prevention_using_Artificial_Intelligence_Techniques

[19]"India second most targeted Nation in term of cyber attacks : cloud SEk", प्रकाशित– 2 जनवरी 2025, https://economictimes.indiatimes.com/tech/technology/india-second-most-targeted-nation-in-terms-of-cyber-attacks-cloudsek/articleshow/116890873.cms?from=mdr

द्वारा प्रदान की गई गति के कारण बड़े पैमाने पर हमलें हो सकते हैं, और लाखों उपकरणों या लोगों को लक्षित कर सकते है, जो पारंपरिक साइबर सुरक्षा बचावों के लिए चुनौती पेश करता है।[20]

चिंता का एक अन्य क्षेत्र स्वयं कृत्रिम बुद्धिमत्ता प्रणालियों की साइबर सुरक्षा जोखिमों के प्रति संवेदनशीलता है। कृत्रिम बुद्धिमत्ता मॉडल, विशेष रूप से मशीन लर्निंग सिस्टम में विशिष्ट कमजोरियाँ होती हैं। कृत्रिम बुद्धिमत्ता को हमलों के ज्ञात तरीकों से धोखा दिया जा सकता है, जहाँ एक हमलावर एआई को भ्रमित करने के लिए इनपुट डेटा में सूक्ष्म बदलाव करता है। उदाहरण के लिए, एक छवि में नगण्य सा परिर्वतन करने से भी एक एआई छवि कि पहचान प्रणाली उसे पूरी तरह से गलत वर्गीकृत कर सकती है। साइबर सुरक्षा के संदर्भ में, एक विरोधी कृत्रिम बुद्धिमत्ता –आधारित घुसपैठ का पता लगाने वाली प्रणाली को विशेष रूप से तैयार किए गए डेटा भेजकर भ्रमित करने का प्रयास कर सकता है, जो एआई की कमजोरियों का फायदा उठाता है। इसके अतिरिक्त, एआई सिस्टम डेटा विषाक्तता ;कंजं च्वपेवदपदहद्ध के शिकार हो सकते हैं– यदि हमलावर एआई मॉडल के प्रशिक्षण डेटा को दूषित करते हैं (मान लीजिए, एक एआई जो नेटवर्क ट्रैफिक से सीखता है), तो वे इसके व्यवहार या सटीकता को प्रभावित कर सकते हैं। उदाहरण के लिए **स्पैम फ़िल्टर**: हमलावर प्रतिकूल डेटा डाल सकते हैं, जिसमे स्पैम फिल्टर गलत तरीके से वैध ईमेल को स्पैम के रूप में चिह्नित्कर सकते है।[21] यह विशेष रूप से चिंताजनक है क्योंकि जैसे–जैसे कृत्रिम बुद्धिमत्ता सिस्टम महत्वपूर्ण प्रक्रियाओं (जैसे बिजली ग्रिड प्रबंधन, यातायात नियंत्रण, या वित्तीय लेनदेन) में एकीकृत होते जाते हैं एआई की अखंडता के सफल समझौते से सार्वजनिक सुरक्षा और व्यवस्था पर व्यापक प्रभाव पड़ सकता है।

कृत्रिम बुद्धिमत्ता द्वारा गोपनीयता पर भी खतरे भी बढ़ जाते हैं। कृत्रिम बुद्धिमत्ता बड़े डेटासेट पर निर्भर करता है, जिसमें व्यक्तिगत डेटा भी शामिल है। उन्नत एआई अनुप्रयोग– सार्वजनिक स्थानों पर सुरक्षा के लिए तैनात चेहरे की पहचान कैमरों से लेकर धोखाधड़ी की रोकथाम के लिए उपयोगकर्ता व्यवहार का विश्लेषण करने वाले एल्गोरिदम में भी अनिवार्य रूप से व्यक्तिगत जानकारी का संग्रह और प्रसंस्करण शामिल है। कुशल डेटा सुरक्षा के बिना, यह गैरकानूनी प्रोफाइलिंग, निगरानी या डेटा उल्लंघनों के जोखिम को बढ़ाता है। उदाहरण के लिए, यदि भारत में कानून प्रवर्तन द्वारा उपयोग किए जाने वाले चेहरे की पहचान करने वाले एआई को हैक कर लिया जाता है या उसका दुरुपयोग किया जाता है, तो यह व्यक्तियों की गतिविधियों और संबंधों के बारे में संवेदनशील जानकारी उजागर कर सकती है, जो सीधे गोपनीयता के मौलिक अधिकार को प्रभावित करती है।[22] इसके अतिरिक्त, कृत्रिम बुद्धिमत्ता मौजूदा जानकारी से नई जानकारी का अनुमान लगा सकती है यह कानूनी परिभाषाओं और सुरक्षा उपायों के लिए एक चुनौती है, जो परंपरागत रूप से डेटा को विशिष्ट श्रेणियों (व्यक्तिगत, संवेदनशील व्यक्तिगत, आदि) में विभाजित करते हैं। डीपीपीडी अधिनियम, 2023 इस परिदृश्य में व्यक्तिगत डेटा को सुरक्षित करने का एक प्रयास है, लेकिन इसकी सफलता इस बात पर निर्भर करेगी कि इसके नियमों के अंतर्गत कृत्रिम बुद्धिमत्ता –आधारित संसाधन की निगरानी और नियंत्रण किस प्रकार किया जाता है।

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के मूल में एक महत्वपूर्ण चुनौती, विशेषता और दायित्व का निर्धारण है। एक विशिष्ट साइबर घटना में, अन्वेषणकर्ता हमले के लिए विशिष्ट व्यक्तियों या समूहों को जिम्मेदार ठहराने का प्रयास करते हैं। कृत्रिम बुद्धिमत्ता इस प्रक्रिया को जटिल बनाती है क्योंकि हमले स्वचालित प्रणालियों द्वारा या मानवीय हमलावरों द्वारा कृत्रिम बुद्धिमत्ता उपकरणों का उपयोग करके किए जा सकते हैं जो उनकी पहचान छिपाते हैं।[23] यदि कोई कृत्रिम बुद्धिमत्ता प्रणाली क्षति का कारण बनती है– उदाहरण के लिए, एक स्वचालित व्यापार एल्गोरिथम जिसे अपहृत कर लिया जाता है और फिर शेयर बाजार को धराशायी कर देता है, या एक स्वायत्त वाहन (कृत्रिम बुद्धिमत्ता द्वारा निर्देशित) जिसे धोखे से दुर्घटना का शिकार बना दिया जाता है दृ तो कानूनी रूप से कौन उत्तरदायी है? क्या यह कृत्रिम बुद्धिमत्ता का मालिक है, सॉफ्टवेयर का विकासकर्ता है, इसमें परिवर्तन करने वाला हमलावर है, या स्वयं कृत्रिम बुद्धिमत्ता प्रणाली ? विश्व भर में कानूनी ढांचे जवाबदेही के इस प्रश्न से जूझ रहे हैं।[24]

---

[20]मार्कस कॉमिटर ,"कृत्रिम बुद्धिमत्ता पर हमलाः एआई की सुरक्षा भेद्यता और नीति निर्माता इसके बारे में क्या कर सकते हैं", प्रकाशित–अगस्त 2019, https://www.belfercenter.org/publication/AttackingAI

[21]Bart Lenaerts-Bergmans,https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/data-poisoning/, प्रकाशित–19 मार्च 2024,

[22]AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data, https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr

[23]European Commission,White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, 19 Feb. 2020, p. 19.

[24]जोआना जे. ब्रायसन और अन्य,"Of, for, and by the people: The legal lacuna of synthetic personhood." Artificial Intelligence and Law, vol. 25, no. 3, 2017, pp. 273-291, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068082

भारत में, वर्तमान कानून के तहत, एक कृत्रिम बुद्धिमत्ता प्रणाली को कानूनी व्यक्तित्व के रूप में मान्यता प्राप्त नहीं है, इसलिए दायित्व मूलतः प्राकृतिक व्यक्तियों पर ही निर्धारित किया जाना चाहिए तथा यह विकसित करने वाली कंपनी (प्रतिनिधिक दायित्व या उत्पाद दायित्व[25] जैसे सिद्धांतों के तहत) या व्यक्तिगत संचालक भी हो सकतें हैं। लेकिन जब निर्णय लेने की प्रक्रिया अस्पष्ट हो तो दोष या लापरवाही साबित करना कठिन होता है। उदाहरण के लिए, यदि एक पूर्वानुमानित पुलिसिंग कृत्रिम बुद्धिमत्ता के परिणामस्वरूप एक साइबर सुरक्षा एजेंसी एक निर्दोष व्यक्ति पर गलत सकारात्मकता परिणाम के कारण साइबर अपराध का झूठा आरोप लगाती है, और उस व्यक्ति के अधिकारों का उल्लंघन होता है, तो कारणता की श्रृंखला में कृत्रिम बुद्धिमत्ता का एल्गोरिथम शामिल होता है, तो यह तय करना कि गलती प्रशिक्षण डेटा, एल्गोरिथम के डिजाइन, या किसी ऑपरेटर द्वारा दुरुपयोग में थी, एक जटिल जाँच हो सकती है एक ऐसी जाँच जिसे संभालने के लिए मौजूदा कानूनी सिद्धांत सीधे तौर पर अपर्याप्त हैं दृ जिसे मौजूदा कानूनी सिद्धांत सीधे तौर पर नियत्रिंत के लिए पर्याप्त रूप से प्रवधानित नहीं हैं। इसके लिए कृत्रिम बुद्धिमत्ता के संदर्भों में दायित्व को स्पष्ट करने वाले अद्यतन कानूनों या दिशानिर्देशों की आवश्यकता है।

कृत्रिम बुद्धिमत्ता के उदय ने साइबर अपराध की नई श्रेणियों या यह कहे कि पुराने अपराधों के नए रूपों को जन्म दिया है। ''साइबर अपराध'' में हैकिंग, वित्तीय धोखाधड़ी, पहचान की चोरी से लेकर साइबर आतंकवाद तक एक विस्तृत श्रृंखला शामिल है। कृत्रिम बुद्धिमत्ता एल्गोरिदम के माध्यम से पहचान की चोरी को स्वचालित कर सकती है जो नकली पहचान उत्पन्न करते हैं या वास्तविक लोगों का अनुकरण करते हैं। भारतीय न्याय संहिता[26] और सूचना प्रौद्योगिकी अधिनियम[27] प्रतिरूपण और धोखाधड़ी को समायोजित करते हैं, उदाहरण के लिए, सूचना प्रौद्योगिकी अधिनियम की धारा 66क कंप्यूटर संसाधनों के माध्यम से ''प्रतिरूपण द्वारा धोखाधड़ी'' को दंडित करता है।[28] हालांकि, ये कानून कृत्रिम बुद्धिमत्ता द्वारा तैयार की गई ऐसी सामग्री से भारतीय अन्वेषण सस्थाओं एवम् विचारण न्यायालयों के सम्मुख स्पष्ट प्रवधान न होने के कारण एक विचारणीय प्रश्न बन सकता है, जिस कारण वास्तविकता से भेद पाना कठिन होगा। यदि चुनाव के दौरान कोई राजनीतिक डीपफेक प्रकट होता है, तो गलत सूचना और मानहानि से संबंधित कानून सक्रिय हो सकते हैं, लेकिन सबसे पहले उस डीपफेक की पहचान करके उसे तुरंत निष्क्रिय करना होगा।[29] सूचना प्रौद्योगिकी अधिनियम के अंतर्गत मध्यवर्ती दिशानिर्देश (2021) सोशल मीडिया मंचों को सूचित किए जाने पर कुछ गैरकानूनी सामग्री को तुरंत हटाने का आदेश देते हैं, लेकिन कृत्रिम बुद्धिमत्ता द्वारा निर्मित भ्रामक सामग्री का समय पर पता लगाना एक तकनीकी समस्या के साथ–साथ एक कानूनी समस्या भी है।[30] 2023 और 2024 में सूचना प्रौद्योगिकी मंत्रालय द्वारा जारी परामर्श विशेष रूप से कृत्रिम बुद्धिमत्ता द्वारा उत्पन्न गलत सूचना और डीपफेक से लड़ने के उद्देश्य से है, जो यह दर्शाता है कि सरकार इसे एक गंभीर साइबर सुरक्षा का विषय मानती है।[31]

संक्षेप में, कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा आपस में घनिष्ठ रूप से जुड़े हुए हैंः जहाँ एक ओर कृत्रिम बुद्धिमत्ता साइबर सुरक्षा तंत्र को सुदृढ़ कर सकता है, वहीं दूसरी ओर यह नए खतरे और कमजोरियाँ भी उत्पन्न कर सकता है। उभरते हुए जोखिमों में शामिल हैंः एआई–जनित साइबर हमले (फिशिंग, मैलवेयर, डीपफेक), एआई प्रणालियों में भेद्यता (प्रतिकूल हमले, डेटा विषाक्तता), गोपनीयता का अतिक्रमण (सामूहिक निगरानी, प्रोफाइलिंग), जिम्मेदारी तय करने में कठिनाई, और कृत्रिम बुद्धिमत्ता कार्यों के लिए कानूनी जवाबदेही में अनिश्चितता। इन जोखिमों की पहचान करना एक ऐसा परिदृश्य प्रस्तुत करता है जिसके आधार पर भारत की कानूनी और नियामक प्रतिक्रियाओं की पर्याप्तता का आकलन किया जा सकता है। यह इस बात पर प्रकाश डालता है कि भारत सहित वैश्विक नियामक क्यों एआई–विशिष्ट उपायों पर विचार कर रहे हैं, उदाहरण के लिए, कुछ एआई अनुप्रयोगों को 'उच्च जोखिम' के रूप में वर्गीकृत करना और उन्हें अधिक कठोर मानकों के अधीन रखना। कृत्रिम बुद्धिमत्ता साइबर परिदृश्य की इस समझ के साथ, अब हम यह विश्लेषण करने के लिए आगे बढ़ते हैं कि भारत का वर्तमान कानूनी और नीतिगत ढांचा इन चुनौतियों का समाधान किस प्रकार करता है।

[25]अध्याय vi, उपभोक्ता संरक्षण अधिनियम, 2019

[26]भारतीय न्याय संहिता, 2023

[27]सूचना प्रौद्योगिकी अधिनियम,2000

[28]पूर्वोक्त 47.

[29]https://timesofindia.indiatimes.com/india/ai-generated-deepfake-videos-voice-cloning-emerge-as-potential-threats-during-election-season/articleshow/108944586.cms, प्रकाशित– 1 अप्रेल 2024,

[30] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ins. by G.S.R. 275(E), dated 6.4.2023.

[31]कृति, MeitY ने गलत सूचना और डीपफेक पर परामर्श जारी कर विशिष्ट मेटाडेटा अनिवार्य किया, https://www.scconline.com/blog/post/2024/03/07/meity-issues-advisory-on-misinformation-and-deepfake-legal-news/, प्रकाशित– 7 मार्च 2024,

भारत में कानूनी और नीतिगत ढांचा

भारत में साइबर सुरक्षा और डिजिटल प्रौद्योगिकी के संबंधित पहलुओं के लिए कानूनी ढांचा पिछले दो दशकों में काफी विकसित हुआ है। हालांकि, हाल तक इसमें कृत्रिम बुद्धिमत्ता को स्पष्ट रूप से शामिल नहीं किया गया था। यह खंड भारत में साइबर सुरक्षा और डेटा संरक्षण को नियंत्रित करने वाले मौजूदा कानूनों, नियमों और नीतियों की रूपरेखा प्रस्तुत करता है, और हाल के उन अद्यतनों की जांच करता है जो कृत्रिम बुद्धिमत्ता के युग में विशेष रूप से प्रासंगिक हैं। इस भाग को निम्नलिखित श्रेणियों में विभाजित किया जा सकता हैः (1) डेटा संरक्षण और गोपनीयता कानून, जो व्यक्तिगत जानकारी को संभालने के लिए नियम निर्धारित करते हैं (2) साइबर अपराध कानून, मुख्य रूप से सूचना प्रौद्योगिकी अधिनियम, जो कुछ ऑनलाइन और कंप्यूटर से संबंधित कार्यों को अपराध बनाता हैय (3) साइबर सुरक्षा विनियम और महत्वपूर्ण सूचना अवसंरचना की सुरक्षा तथा घटनाओं पर प्रतिक्रिया देने के लिए समर्पित संस्थान, और (4) उभरती हुई एआई नीतिगत पहल और मसौदा प्रस्ताव जो भविष्य के विनियमन की दिशा का संकेत देते हैं।

1. डेटा संरक्षण और गोपनीयता कानून (डीपीडीपी अधिनियम, 2023 और संबंधित विकास)

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा चुनौतियों का समाधान करने के लिए एक मजबूत डेटा संरक्षण व्यवस्था एक बुनियादी आवश्यकता है। 2023 से पहले, भारत में एक समर्पित डेटा संरक्षण कानून का अभाव था यह व्यक्तिगत डेटा आंशिक रूप से सूचना प्रौद्योगिकी अधिनियम, 2000 और अधीनस्थ नियमों के माध्यम से संरक्षित था। विशेष रूप से, आईटी अधिनियम की धारा 43। और इसके साथ सूचना प्रौद्योगिकी (उचित सुरक्षा अभ्यास और प्रक्रियाएं और संवेदनशील व्यक्तिगत डेटा या जानकारी) नियम, 2011 ने एक बुनियादी ढांचा प्रदान कियाः उन्होंने संवेदनशील व्यक्तिगत डेटा को संभालने वाली कॉर्पोरेट संस्थाओं को उचित सुरक्षा प्रथाओं को लागू करने की आवश्यकता और डेटा संरक्षण में लापरवाही के लिए मुआवजे की अनुमति दी थी।[32]

हालांकि, इन नियमों का दायरा सीमित था, ये केवल पासवर्ड, वित्तीय जानकारी आदि जैसे कुछ विशिष्ट संवेदनशील डेटा को ही समाहित करते थे, लेकिन सरकारी संस्थाओं पर लागू नहीं होते थे। इसके अतिरिक्त, इनमें प्रभावी कार्यान्वयन तंत्र या उपयोगकर्ता अधिकार भी अनुपस्थित थे। निर्णायक मोड़ तब आया जब 2017 में सर्वोच्च न्यायालय ने पुट्टस्वामी मामले में गोपनीयता को मौलिक अधिकार के रूप में मान्यता दी और स्पष्ट रूप से सरकार से एक मजबूत डेटा सुरक्षा कानून बनाने का आग्रह किया।[33] इसके प्रत्युत्तर में, सरकार ने न्यायमूर्ति बी.एन. श्रीकृष्णा के अधीन एक विशेषज्ञ समिति का गठन किया, जिसने 2018 में व्यक्तिगत डेटा संरक्षण विधेयक का मसौदा तैयार किया।[34] कई पुनरावृत्तियों और सार्वजनिक परामर्शों के बाद, और 2021 में एक पूर्ववर्ती विधेयक की अस्थायी वापसी के बाद भी अंततः संसद ने अगस्त 2023 में डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 पारित किया।

डीपीडीपी अधिनियम, 2023 भारत का प्रथम विस्तृत डेटा संरक्षण विधान है। इसका लक्ष्य डिजिटल व्यक्तिगत डेटा के संसाधन को नियंत्रित करना है, व्यक्तियों के अपने डेटा की सुरक्षा के अधिकार और कानूनी उद्देश्यों के लिए डेटा संसाधित करने की आवश्यकता के मध्य सामंजस्य स्थापित करना है। यह अधिनियम उस व्यक्तिगत डेटा पर लागू होता है जो ऑनलाइन एकत्र किया गया है या ऑफलाइन संग्रह के बाद डिजिटाइज्ड किया गया है। यह कानून व्यक्तिगत डेटा के प्रसंस्करण को सहमति या कुछ वैध उपयोगों पर आधारित होने पर केंद्रित है। इसका उद्देश्य, सीमा, डेटा न्यूनीकरण, सटीकता, भंडारण सीमा, उचित सुरक्षा उपायों और जवाबदेही जैसे सिद्धांतों को स्थापित करता है। उदाहरण के लिए, एक कृत्रिम बुद्धिमत्ता कंपनी को यह सुनिश्चित करना होगा कि वह केवल उस विशिष्ट उद्देश्य के लिए व्यक्तिगत डेटा का उपयोग करे जिसके लिए उपयोगकर्ता ने सहमति दी है, जो बिना नई सहमति के असंबंधित कृत्रिम बुद्धिमत्ता मॉडल प्रशिक्षण के लिए डेटा के पुनः उपयोग को सीमित कर सकता है। यह डेटा प्रिंसिपलों को अधिकार देता हैं, जो व्यक्गित डेटा के दुरुपयोग को राकतें हैं दृ उदाहरण के लिए, यदि कोई कृत्रिम बुद्धिमत्ता –संचालित प्लेटफॉर्म किसी व्यक्ति के बारे में गलत जानकारी रखता है, तो वह व्यक्ति उसे सही करने या मिटाने की मांग कर सकता है। यह व्यक्तिगत डेटा संसाधित करने वाले संगठनों को उल्लंघनों को रोकने के लिए सुरक्षा उपाय लागू करने, डेटा उल्लंघनों की स्थिति में उपयोगकर्ताओं और अधिकारियों को सूचित करने, उद्देश्य के लिए बाद में आवश्यक नहीं होने पर डेटा मिटाने और एक शिकायत निवारण अधिकारी की नियुक्ति सुनिश्चित करें के सबंधं में भी प्रवधानित करता गया हैं। अधिनियम के प्रवधनों के कुछ उल्लंघनों पर भारी वित्तीय दंड जो रू. 250 करोड़ तक अधिकृत हो सकता है, का भी प्रावधान है।[35] इस अधिनियम के तहत अनुपालन की निगरानी और

[32]Data protestion laws in india, https://www.dlapiperdataprotection.com/?t=law&c=IN, प्रकाशित– 6 जनवरी 2025.

[33]पूर्वोक्त,12.

[34]Justice BN Srikrishna Committee, https:/www.drishtiias.com/daily-news-analysis/justice-bn-srikrishna-committee-submits-data-protection-report, प्रकाशित– 18 जुलाई 2018.

[35]THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023).

दंड आरोपित करने के लिए भारतीय डेटा सुरक्षा बोर्ड की स्थापना की गई है। यद्यपि यह एक नियामक प्रणाली सुनिश्चित करता है, लेकिन विधि विद्वनों का मानना है कि इसकी स्वतंत्रता सीमित हो सकती है।[36]

डीपीडीपी अधिनियम सीधे तौर पर कृत्रिम बुद्धिमत्ता पर केंद्रित नहीं है, बल्कि यह एक व्यापक गोपनीयता और सुरक्षा संरचना प्रदान करता है जिसके अंतर्गत भारत में कृत्रिम बुद्धिमत्ता प्रणालियाँ कार्य करेंगी। उदाहरण के लिए, यदि कोई कृत्रिम बुद्धिमत्ता स्वचालित निर्णय लेने के लिए व्यक्तिगत डेटा का उपयोग करती है, तो अधिनियम के पारदर्शिता और उद्देश्य की सीमा के सिद्धांत लागू होंगे। हालाँकि, यह ध्यान रखना महत्वपूर्ण है कि वर्तमान में अधिनियम में स्वचालित निर्णय लेने या प्रोफाइलिंग पर कोई स्पष्ट प्रावधान नहीं हैं। यह भविष्य के नियमों का एक क्षेत्र हो सकता है दृ अधिनियम सरकार को नियम बनाने का अधिकार देता है, और यह अपेक्षित है कि स्वचालित प्रसंस्करण से होने वाले नुकसान का आकलन और उन्हें कम करने संबंधी नियम सामने आ सकते हैं, विशेष रूप से जैसे–जैसे कृत्रिम बुद्धिमत्ता नैतिकता पर वैश्विक चर्चा भारतीय नीति में प्रवेश करती है।[37]

2025 के आरंभ में अधिनियम के अंतर्गत प्रस्तावित नियमों का मसौदा सार्वजनिक राय जानने के लिए प्रस्तुत किया गया था।[38] इस क्रमिक कार्यान्वयन का तात्पर्य है कि वर्तमान में, भारत एक परिवर्तनकारी दौर से गुजर रहा हैः सूचना प्रौद्योगिकी अधिनियम, 2011 के पुराने विधान से नवीन डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम के विधान की ओर अग्रसर है। गोपनीयता कानून में एक अन्य महत्वपूर्ण प्रगति भारत में ''विस्मृति के अधिकार'' को लेकर चल रही चर्चा है। यह अधिकार जिसका मूल अर्थ है, किसी व्यक्ति के निजी डेटा को मिटाना और उसे आगे संसाधित न करना अथवा अप्रासंगिक या हानिकारक निजी सूचना को खोज परिणामों से पृथक करना, अभी तक भारतीय कानून में स्पष्ट रूप से संहिताबद्ध नहीं है। तथापि, न्यायालयों ने कुछ विशिष्ट मामलों में इस पर विचार किया है। वर्तमान में, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम के अस्तित्व में आने के साथ, जो व्यक्तियों को अपने निजी डेटा के उन्मूलन का अनुरोध करने की अनुमति प्रदान करता है, यह विस्मृति के अधिकार का अप्रत्यक्ष रूप से समर्थित है। भविष्य में, इस अधिकार का अन्य अधिकारों, जैसे कि अभिव्यक्ति की स्वतंत्रता और अदालती निर्णयों जैसे सार्वजनिक अभिलेखों के रखरखाव, के साथ किस प्रकार सामंजस्य स्थापित किया जाएगा, यह कानूनी विकास का विषय रहेगा। उच्चतम न्यायालय ने अभी तक विस्मृति के अधिकार पर प्रत्यक्ष निर्णय नहीं दिया है, लेकिन नए कानून के प्रवर्तन और इसके अंतर्गत उत्पन्न होने वाले मामलों के पश्चात, इस क्षेत्र में न्यायिक दृष्टांतों का विकास अपेक्षित है।

डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 भारत के गोपनीयता और डेटा सुरक्षा संबंधी कानूनी संसाधनों को उल्लेखनीय रूप से मजबूत करता है, जो किसी भी कृत्रिम बुद्धिमत्ता विनियमन के लिए एक अनिवार्य आधार प्रदान करता है। डेटा सुरक्षा को अनिवार्य बनाकर और व्यक्तियों को अपने डेटा पर नियंत्रण देकर, यह अप्रत्यक्ष रूप से कृत्रिम बुद्धिमत्ता को इस सीमा तक विनियमित करता है कि अब कृत्रिम बुद्धिमत्ता प्रणालियों को इन आवश्यकताओं का पालन करने के लिए अभिकल्पित किया जाना चाहिए, उदाहरण के लिए, उपयोगकर्ता के अनुरोध पर डेटा हटाने की क्षमता, प्रसंस्करण के लिए वैध आधार सुनिश्चित करना। हालाँकि, निजी डेटा सुरक्षा से परे, कृत्रिम बुद्धिमत्ता कानून के अन्य क्षेत्रों, विशेष रूप से साइबर अपराध और साइबर सुरक्षा को भी प्रभावित करती है, जिसका विवेचन हम आगे करेंगे।

2. साइबर अपराध और कृत्रिम बुद्धिमत्ता के सन्दर्भ में सूचना प्रौद्योगिकी अधिनियम में उपबंध

सूचना प्रौद्योगिकी अधिनियम, 2000 दो दशकों से अधिक समय से भारत में डिजिटल अपराधों, इलेक्ट्रॉनिक अभिलेखों और साइबर कानून के संबंधित पहलुओं को शासित करने वाला प्रमुख विधान रहा है। 20 वी शताब्दी के प्रारंभ में मुख्य रूप से इलेक्ट्रॉनिक वाणिज्य को वैधानिक मान्यता प्रदान करने और कंप्यूटर संबंधी अपराधों को दंडित करने के उद्देश्य से अधिनियमित किया गया, जिसको (विशेष रूप से 2008 में) संशोधित किया गया।[39] ताकि साइबर अपराधों और नियामक शक्तियों की एक विस्तृत श्रृंखला को समाहित किया जा सके। यद्यपि अधिनियम में स्पष्ट रूप से ''कृत्रिम बुद्धिमत्ता'' का उल्लेख नहीं है, लेकिन इसके प्रावधान वह आधारशिला निर्मित कर सकते हैं जिसके द्वारा कृत्रिम बुद्धिमत्ता से संबंधित अनेक साइबर मुद्दों के कानूनी समाधान किया जा सके।

साइबर सुरक्षा और संभावित रूप से कृत्रिम बुद्धिमत्ता के लिए आईटी अधिनियम के मुख्य उपबंध :

[36]अभिषेक कुमार और अन्य, India's New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023, https://bpasjournals.com/library-science/index.php/journal/article/view/2513/1640, प्रकाशित– जुलाई–दिसंबर 2024,पृष्ठ.11776–11782

[37]पूर्वोक्त,1.

[38]इलेक्ट्रॉनिक्स और आईटी मंत्रालय,https://www.pib.gov.in/PressReleasePage.aspx?PRID=2090048, प्रकाशित–3 जनवरी 2025.

[39]THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008 BE 2008. No. 10 OF 2009

- **अनाधिकृत अभिगम और हैकिंगः** सूचना प्रौद्योगिकी अधिनियम की धारा 43 और धारा 66 कंप्यूटर प्रणालियों और डेटा की चोरी तक अनधिकृत पहुँच से संबंधित हैं। धारा 43 किसी भी ऐसे व्यक्ति पर दायित्व आरोपित करती है जो बिना अनुमति के कंप्यूटर संसाधन तक पहुँचता है और यह निर्धारित करती है कि वह प्रभावित व्यक्ति को नुकसान भरने के लिए उत्तरदायी है।[40] इसके अनुरूप, धारा 66 ऐसे अनधिकृत अभिगम को 3 वर्ष तक के कारावास के साथ एक आपराधिक अपराध बनाती है।[41] यदि किसी हैकर द्वारा कंप्यूटरों को स्कैन करने और उनमें घुसपैठ करने के लिए एक कृत्रिम बुद्धिमत्ता प्रणाली का उपयोग किया जाता है, तो अपराधी के पकड़े जाने पर ये उपबंध लागू होंगे (तथ्य यह है कि उन्होंने कृत्रिम बुद्धिमत्ता का उपयोग किया वह गौण है ये कानून अनधिकृत अभिगम के कार्य पर केंद्रित है)। इसके विपरीत, यदि कोई कृत्रिम बुद्धिमत्ता स्वयं स्वायत्त रूप से प्रणालियों में प्रवेश करना ''सीख'' जाती है, तो वर्तमान कानून के तहत उस कृत्रिम बुद्धिमत्ता का स्वामी या नियंत्रक इन आरोपों का सामना कर सकता है।
- **डेटा और सिस्टम क्षतिः** धारा 43 में कंप्यूटर या उसके डेटा को क्षति पहुँचाना भी शामिल है। उदाहरण के लिए, मैलवेयर (वायरस, वर्म्स, ट्रोजन) डालना स्पष्ट रूप से क्षति या व्यवधान उत्पन्न करने के रूप में शामिल है। धारा 66थ (साइबर आतंकवाद) में राष्ट्रीय सुरक्षा को खतरे में डालने के इरादे से सेवा से इनकार करने या सिस्टम को दूषित करने के कार्य शामिल हैं।[42] कृत्रिम बुद्धिमत्ता ऐसे हमलों को बढ़ा सकती है। उदाहरण के लिए, एक कृत्रिम बुद्धिमत्ता, समन्वित वितरित सेवा अस्वीकार हमला ;क्क्वे जजंबा) जो एक ऐसा साइबर हमला है जो किसी लक्ष्य, जैसे कि किसी वेबसाइट या नेटवर्क, को कई स्रोतों से दुर्भावनार्पूवक ट्रैफिक को बाधित करने का प्रयास करता है।[43] कानून मूलतः उपकरण की परवाह किए बिना परिणाम (क्षति, व्यवधान) को अपराध घोषित करता है, इसलिए कृत्रिम बुद्धिमत्ता–आधारित हमले इसके दायरे में आते हैं।
- **पहचान की चोरी और प्रतिरूपण द्वारा धोखाधड़ीः** धारा 66ब पहचान की चोरी (किसी अन्य के डिजिटल हस्ताक्षर, पासवर्ड आदि का उपयोग करना) को दंडित करती है[44] और धारा 66क कंप्यूटर संसाधनों के माध्यम से प्रतिरूपण द्वारा धोखाधड़ी को दंडित करती है। ये डीपफेक और कृत्रिम बुद्धिमत्ता–जनित प्रतिरूपण के कृ त्रिम बुद्धिमत्ता संदर्भ में अत्यधिक प्रासंगिक हैं। उदाहरण के लिए, यदि कोई व्यक्ति बैंक अधिकारी का प्रतिरूपण करने और एक उपभोक्ता को धोखा देने के लिए एक कृत्रिम बुद्धिमत्ता आवाज जनरेटर का उपयोग करता है, तो धारा 66क लागू होगी।[45] भारतीय न्याय संहिता, प्रतिरूपण द्वारा धोखाधड़ी को धारा 319 को अपराध को बनाती है।[46] यह ऑफलाइन और ऑनलाइन धोखाधड़ी कानूनों को समेकित करने के प्रयास को दर्शाता है। अश्लीलता, उत्पीड़न और अन्य अपराधः आईटी अधिनियम की धारा 67, 67।, 67ठ ऑनलाइन अश्लील सामग्री, यौन रूप से स्पष्ट सामग्री और बाल यौन शोषण सामग्री के प्रकाशन या प्रसारण को अपराध घोषित करती है।[47] यदि कोई व्यक्ति कृत्रिम बुद्धिमत्ता का उपयोग करके अश्लील डीपफेक बनाता और प्रसारित करता है, तो ये प्रावधान लागू होंगे। उदाहरण के लिए, किसी व्यक्ति का गैर–सहमति वाला स्पष्ट डीपफेक बनाना धारा 67ए67। के तहत दडंनीय है। कानून प्रवर्तन के लिए कृत्रिम बुद्धिमत्ता डीपफेक के निर्माता की पहचान करना चुनौती एक है। ये कृत्रिम बुद्धिमत्ता इमेजरी का पता लगाने के लिए उपकरण विकसित किए जा रहे हैं, लेकिन कानूनी रूप से अपराधियों के ज्ञात होने पर उन पर आरोपित करने के प्रावधान मौजूद हैं।
- **आतंकवाद एवं उग्रवादः** साइबर आतंकवाद, साइबर माध्यमों का उपयोग करके किए गए उन कृत्यों को संबोधित करती है जो भारत की एकता, सुरक्षा या संप्रभुता को संकट में डालते हैं – जैसे महत्वपूर्ण प्रणालियों में अंतर्भेद या उन्हें बाधित करने का प्रयास करना, या राज्य को क्षति पहुँचाने या आतंक उत्पन्न करने के आशय से गोपनीय डेटा तक अभिगम प्राप्त करना। यदि कृत्रिम बुद्धिमत्ता का उपयोग, स्वचालित रूप से दुष्प्रचार उत्पन्न करने और प्रसारित करने या महत्वपूर्ण अवसंरचना पर आक्रमण करने के लिए किए गए आईओटी उपकरणों के समूह को नियंत्रित करने के लिए किया जाता है, तो ऐसे कृत्य साइबर आतंकवाद के अंतर्गत आ सकते हैं। दोषसिद्धि पर आजीवन कारावास तक की सजा का प्रावधान है।[48] इसी प्रकार, घृणा का सप्रवर्तन भारतीय न्याय संहिता, 2023 की धाराओं के अंतर्गत आ सकता है।[49], परन्तु यदि यह ऑनलाइन किया जाता है, तो सूचना प्रौद्योगिकी अधिनियम हस्तक्षेप कर सकता है।

---

[40]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–22.

[41]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–32.

[42]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–34.

[43]DDoS हमला क्या है ?, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[44]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–33.

[45]पूर्वोक्त,52.

[46]भारतीय न्याय संहिता, 2023,सं.45 ऑफ 2023, प्रकाशक–कमल पब्लिशर्स (लॉमेनस), द्विभाषी संस्करण, पृष्ठ सं–98.

[47]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–35.

[48]धारा 66F, प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–34.

[49]धारा 196A, भारतीय न्याय संहिता, 2023,सं.45 ऑफ 2023, प्रकाशक–कमल पब्लिशर्स (लॉमेनस), द्विभाषी संस्करण, पृष्ठ सं–64

- **मध्यवर्ती दायित्व एवं विषयवस्तु निगरानीः** सूचना प्रौद्योगिकी अधिनियम की धारा 79 मध्यस्थों (जैसे इंटरनेट सेवा प्रदाता, सोशल मीडिया प्लेटफॉर्म) को तृतीय–पक्ष की विषयवस्तु के लिए ''सुरक्षित आश्रय'' संरक्षण प्रदान करती है, जब तक कि वे सम्यक तत्परता बरतते हैं और कुछ विषयवस्तु को हटाने के लिए सरकार या न्यायालय के आदेशों का अनुपालन करते हैं।[50] सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 इस धारा के तहत बनाए गए थे, जिसमें मध्यस्थों को अवैधता की वास्तविक जानकारी होने पर (शिकायतों या अदालतध्सरकारी आदेशों के माध्यम से) सामग्री को हटाने और उपयोगकर्ता समझौतों जैसे उचित परिश्रम करने की आवश्यकता थी जो कुछ सामग्री पर प्रतिबंध लगाते हैं।[51] 'एआई के संदर्भ में, ये नियम सीधे तौर पर तब प्रासंगिक हो गए जब इलेक्टॉनिक्स और सूचना प्रसारण मंत्रालय ने 2023–24 में एआई–जनित सामग्री और डीपफेक से संबंधित सलाह जारी की।[52] सलाह में मध्यस्थों को 2021 के नियमों के नियम 3(1)(इ) के तहत उनके कर्तव्य की याद दिलाई गई कि वे ऐसी सामग्री को होस्ट न करें जो झूठी या भ्रामक हो और उस तर्क को एआई–जनित गलत सूचना तक विस्तारित किया।[53] इस प्रकार, यद्यपि अधिनियम में कृत्रिम बुद्धिमत्ता–विशिष्ट दायित्व संहिताबद्ध नहीं हैं, लेकिन सरकार व्याख्या और अनुपूरक दिशानिर्देशों द्वारा कृत्रिम बुद्धिमत्ता विषयवस्तु के मुद्दों को संबोधित करने के लिए विद्यमान प्रावधानों का उपयोग कर रही है।
- **एन्क्रिप्शन एवं डिक्रिप्शन आदेशः** सूचना प्रौद्योगिकी अधिनियम की धारा 69 सरकार की एजेंसियों को राष्ट्रीय सुरक्षा, रक्षा, सार्वजनिक व्यवस्था आदि के हित में किसी भी कंप्यूटर संसाधन के माध्यम से जानकारी को अवरोधित, मॉनिटर या विगूढ़न करने का अधिकार देती है।[54] जो प्रक्रियात्मक सुरक्षा उपायों के अधीन है। कृत्रिम बुद्धिमत्ता के साथ, एन्क्रिप्शन और भी व्यापक हो जाता है। मजबूत एन्क्रिप्शन बनाम विधि सम्मत अभिगम पर एक सतत वैश्विक नीतिगत बहस जारी है ये भारत का कानून सरकार को एन्क्रिप्टेड डेटा तक अभिगम की माँग करने का अधिकार देता है। इसके अतिरिक्त, धारा 69। किसी भी ऑनलाइन जानकारी तक सार्वजनिक अभिगम को अवरुद्ध करने की अनुमति देती है, जिसके द्वारा वेबसाइटोंए यूआरएल को ब्लॉक किया जाता है, उदाहरण के लिए, फिशिंग साइटों या चरमपंथी विषयवस्तु को हटाने के लिए। व धारा 69ठ साइबर सुरक्षा के लिए नेटवर्क ट्रैफिक की निगरानी की अनुमति देती है।[55] कृत्रिम बुद्धिमत्ता संदर्भ में, यदि कोई एआई–संचालित बॉटनेट किसी हमले को अंजाम दे रहा है, तो धारा 69। का उपयोग नियंत्रण सर्वर या दुर्भावनापूर्ण एआई सेवाओं को ब्लॉक करने के लिए किया जा सकता है, और धारा 69ठ का उपयोग ट्रैफिक पैटर्न की निगरानी के लिए किया जा सकता है।

सूचना प्रौद्योगिकी अधिनियम में हाल ही में जन विश्वास (उपबंधों का संशोधन) अधिनियम, 2023 के माध्यम से संशोधन किए गए हैं। इस अधिनियम ने अनुपालन भार को कम करने और मामूली अपराधों को गैर–अपराधीकरण करने के लिए विभिन्न कानूनों में संशोधन किया। सूचना प्रौद्योगिकी अधिनियम में, कई धाराओं में संशोधन किया गयाः उदाहरण के लिए, कुछ उल्लंघनों के लिए कारावास की शर्तों को कम या समाप्त कर दिया गया और जुर्माना बढ़ा दिया गया।[56] विशेष रूप से, आवश्यकता होने पर सरकारी एजेंसियों को जानकारी प्रदान करने में विफल रहने (धारा 69ठ का गैर–अनुपालन) के लिए, सजा को अधिकतम एक वर्ष (तीन से कम) और रू 1 करोड़ तक का निर्धारित जुर्माना कर दिया गया। इसी प्रकार, धारा 70ठ (जो ब्म्त्ज–प्द की आवश्यकताओं के अनुपालन से संबंधित है) के जुर्माने को 100 गुना (रू 1 लाख से रू 1 करोड़) बढ़ा दिया गया और कुछ विफलताओं के लिए एक वर्ष तक का कारावास कर दिया गया।[57] ये संशोधन अपेक्षाकृत नवीन हैं, और उनका प्रभाव तभी देखा जाएगा जब इस प्रकार के मामले सामने आयेंगे।[58] उदाहरण के लिए, यदि कोई मध्यस्थ कृत्रिम बुद्धिमत्ता–आधारित नकली खाता नेटवर्क के बारे में आवश्यक जानकारी प्रस्तुत करने में विफल रहता है, तो अब कारावास के बजाय जुर्माना प्राथमिक परिणाम हो सकता है– अति–अपराधीकरण के बिना अनुपालन सुनिश्चित करना।

यद्यपि सूचना प्रौद्योगिकी अधिनियम कृत्रिम बुद्धिमत्ता को ध्यान में रखकर नहीं बनाया गया था, परन्तु इसके प्रावधान व्यापक रूप से कई ऐसे कृत्यों को समाहित करते हैं जो कृत्रिम बुद्धिमत्ता का

[50]प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–42.

[51]Vide G.S.R. 139(E), dated 25.2.2021, published in the Gazette of India, Extra., Pt. II, Sec. 3(i), dated 25.2.2021.

[52]अर्जुन एड्रियन डिसूजा, https://iapp.org/news/a/indias-foray-into-regulating-ai, प्रकाशित–24 अप्रैल 2024.

[53]सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021,सी.जी.डी.एल.अ.–25022021–225464, दिनॉक–25 फरवरी 2021

[54]धारा 69, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–37.

[55]धारा 69B, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–37.

[56]THE JAN VISHWAS (AMENDMENT OF PROVISIONS) ACT, 2023 NO. 18 OF 2023.

[57]पूर्वोक्त,65.

[58]सौरव सिंह, जन विश्वास अधिनियम, 2023 और आईपी कानूनः दंड से अनुपात की ओर बदलाव, https://www.livelaw.in/articles/jan-vishwas-act-2023-ip-law-a-shift-from-punishment-to-proportion-293447,प्रकाशित–26 मई 2025.

उपयोग करके किए जा सकते हैं। इसमें कृत्रिम बुद्धिमत्ता की विशिष्ट चुनौतियाँ शामिल नहीं हैं, जैसे स्वायत्त निर्णय लेने से होने वाली हानियाँ, जो पारंपरिक ''अपराध'' नहीं हैं, परन्तु क्षति या भेदभाव का कारण बन सकती हैं। उनके लिए, किसी को अन्य विधियों का सहारा लेना पड़ सकता है। उदाहरण के लिए, यदि कोई कृत्रिम बुद्धिमत्ता उत्पाद दोषपूर्ण है तो उपभोक्ता संरक्षण, या लापरवाही के लिए अपकृत्य विधि। सूचना प्रौद्योगिकी अधिनियम की सीमाओं को स्वीकार करते हुए, सरकार ने इसे एक नए कानून – डिजिटल इंडिया अधिनियम से प्रतिस्थापित करने के आशय की घोषणा की है। आधिकारिक खाकों के अनुसार, प्रस्तावित डिजिटल इंडिया अधिनियम न केवल सूचना प्रौद्योगिकी अधिनियम द्वारा समाहित विषयों से निपटेगा, बल्कि ''कृत्रिम बुद्धिमत्ता और ब्लॉकचेन जैसी नवीन प्रौद्योगिकियों के विनियमन'' से भी निपटेगा।[59] डिजिटल इंडिया अधिनियम के लिए परामर्श 2023 में प्रारंभ हुआ, और इसमें ऑनलाइन सुरक्षा, उभरती प्रौद्योगिकियों की जवाबदेही और संभवतः निरीक्षण के लिए कृत्रिम बुद्धिमत्ता प्रणालियों का वर्गीकरण पर प्रावधान शामिल होने की संभावना है।[60] जब तक वह नया कानून अधिनियमित नहीं हो जाता, तब तक सूचना प्रौद्योगिकी अधिनियम भारत में साइबर विधिक मुद्दों के लिए प्रभावी विधान बना रहेगा।

संक्षेप में, भारत के साइबर अपराध कानून कंप्यूटरों और नेटवर्क से जुड़ी दुर्भावनापूर्ण गतिविधियों, जिनमें कृत्रिम बुद्धिमत्ता द्वारा सक्रिय गतिविधियाँ भी शामिल हैं, के लिए एक आवश्यक निवारक और प्रतिक्रिया तंत्र प्रदान करते हैं। वे अपराधियों को जवाबदेह ठहराने और अधिकारियों को साइबर खतरों के विरुद्ध कार्यवाही करने का अधिकार देने के लिए आधार निर्मित करते हैं। तथापि, ये कानून प्रतिक्रियात्मक रूप से कार्य करते हैं। और सक्रिय रूप से यह विनियमित नहीं करते हैं कि कृत्रिम बुद्धिमत्ता को कैसे विकसित या उपयोग किया जाना चाहिए।

3. साइबर सुरक्षा विनियम एवं संस्थागत ढाँचा

भारत ने साइबर सुरक्षा पर केंद्रित विनियमों और संस्थानों का एक तत्रं विकसित किया है, जो साइबर सुरक्षा पर कृत्रिम बुद्धिमत्ता के प्रभाव पर विचार करते समय अत्यंत प्रासंगिक है। साइबर सुरक्षा सुनिश्चित करने में संगठनों के लिए प्रणालियों और डेटा की सुरक्षा के लिए कानूनी आदेश और साइबर घटनाओं को रोकने, निगरानी करने और प्रतिक्रिया देने के लिए एजेंसियों की उपस्थिति, दोनों शामिल हैं।

भारत के साइबर सुरक्षा तंत्र में एक महत्वपूर्ण भूमिका भारतीय कंप्यूटर आपातकालीन मोचन दल ;ब्म्ज्.प्दद्ध निभाता है। सूचना प्रौद्योगिकी अधिनियम की धारा 70ठ के तहत सरकार द्वारा स्थापित, ब्म्ज्.प्द घटना प्रतिक्रिया के लिए राष्ट्रीय एजेंसी है। वर्षों से, कंप्यूटर आपात मोचन दल ने भारत में साइबर सुरक्षा की स्थिति को बेहतर बनाने के लिए विभिन्न दिशानिर्देश और निर्देश जारी किए हैं।[61] विशेष रूप से धारा 70ठ (6)[62] का प्रयोग करते होए, अप्रैल 2022 में, कंप्यूटर आपात मोचन दल ने ''सुरक्षित और विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा प्रथाओं, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग पर निर्देश'' का एक समुच्चय जारी किया।[63]

सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों और संगठनों पर निर्देश[64]

- सभी साइबर घटनाओं (नेटवर्क की लक्षित स्कैनिंगध्जॉच, आईटी प्रणालियों तक अनधिकृत पहुंच, दुर्भावनापूर्ण कोड हमले से लेकर डेटा उल्लंघनों और आनुप्रयोग काल तक) को बहुत कम समय सीमा के भीतर ब्म्ज्.प्द को रिपोर्ट करने का आदेश दिया।(शुरुआत में घटना की सूचना मिलने के 6 घंटे के भीतर)। यह विश्व स्तर पर सबसे सख्त रिपोर्टिंग आवश्यकताओं में से एक है, जिसका उद्देश्य यह सुनिश्चित करना है कि सरकार को प्रतिक्रियाओं का समन्वय करने के लिए समय पर जानकारी मिले।

कृत्रिम बुद्धिमत्ता के लिए, इसका मतलब है कि यदि कोई कृत्रिम बुद्धिमत्ता–संचालित प्रणाली भंग हो जाती है या

यदि किसी कंपनी पर हमले में कृत्रिम बुद्धिमत्ता का उपयोग किया जाता है, तो उस कंपनी को तुरंत इसकी रिपोर्ट करनी होगी।

---

[59]आहिल शेख, पारदर्शिता डिजिटल इंडिया अधिनियम का आधार होना चाहिए, https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/, प्रकाशित– 23 अप्रैल 2024.

[60]भारत का डिजिटल भविष्यः डिजिटल इंडिया अधिनियम 2023, https://www.drishtiias.com/daily-updates/daily-news-editorials/india-s-digital-future-the-digital-india-act-2023, प्रकाशित– 9 अक्टूबर 2023.

[61]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण, पृष्ठ सं–39.

[62]पूर्वोक्त,70.

[63]Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In), No. 20(3)/2022-CERT-In, प्रकाशित– 28 अप्रैल 2022.

[64]पूर्वोक्त 72.

- सेवा प्रदाताओं (वीपीएन[65] प्रदाताओं, क्रिप्टोक्यूरेंसी आदान–प्रदान, क्लाउड सेवाओं सहित) को उपयोगकर्ता गतिविधियों और कुछ डेटा (जैसे ग्राहक नाम, आईपी पते) के विस्तृत लॉग को एक निश्चित अवधि के लिए बनाए रखने की आवश्यक बताया। गोपनीयता के दृष्टिकोण से यह विवादास्पद था और वैश्विक वीपीएन प्रदाताओं के लिए अनुपालन संबंधी मुद्दे उठाए, सरकार ने इसे साइबर अपराधों का पता लगाने के लिए आवश्यक बताया। यह आवश्यकता कृत्रिम बुद्धिमत्ता के साथ इस मायने में प्रतिच्छेद करती है कि कई कृत्रिम बुद्धिमत्ता प्रणालियाँ क्लाउड इंफ्रास्ट्रक्चर पर चलती हैं – क्लाउड प्रदाताओं को ऐसी जानकारी लॉग करनी चाहिए जो कृत्रिम बुद्धिमत्ता–संबंधित घटनाओं की जांच के लिए महत्वपूर्ण हो सकती है।
- निर्देशों में यह अनिवार्य किया गया है कि सभी सेवा प्रदाता, मध्यस्थ, डेटा केंद्र, निकाय कॉर्पोरेट और सरकारी संगठन अनिवार्य रूप से अपने सभी आईसीटी सिस्टम के लॉग को सक्षम करेंगे और उन्हें भारतीय अधिकार क्षेत्र में 180 दिनों की अवधि के लिए सुरक्षित रूप से बनाए रखेंगे। ऐसे लॉग को किसी भी घटना की रिपोर्टिंग के साथ या ब्म्त्ज्.प्द द्वारा आदेशधनिर्देश दिए जाने पर ब्म्त्ज्.प्द को प्रदान करना होगा।
- संस्थाओं को लॉग में स्थिरता के लिए सिस्टम घड़ियों को भारतीय मानक समय के अनुसार करने को कहा गया।
- किसी भी घटना के मामले में, संदर्भित संस्थाओं को ब्म्त्ज्.प्द द्वारा मांगे गए विवरण प्रस्तुत करने होंगे। सूचना प्रस्तुत करने में विफलता या पूर्वोक्त निर्देशों का पालन न करने पर, आईटी अधिनियम, 2000 की धारा 70ठ की उपधारा (7) और अन्य लागू कानूनों के तहत दंडात्मक कार्यवाही हो सकती है।

ये ब्म्त्ज्.प्द निर्देश साइबर सुरक्षा अनुपालन पर भारत के दृढ़ रुख को प्रदर्शित करते हैं। जबकि वे कृत्रिम बुद्धिमत्ता–विशिष्ट नहीं हैं, पर वे एक सुरक्षा–उन्मुख वातावरण बनाते हैं, जिसमें कृत्रिम बुद्धिमत्ता डेवलपर्स और उपयोगकर्ता काम करते हैं। उदाहरण के लिए, कृत्रिम बुद्धिमत्ता–आधारित सेवाओं को तैनात करने वाली कंपनी को न केवल अपनी प्रणाली की सुरक्षा करनी होगी, बल्कि कुछ गलत होने पर कठोर रिपोर्टिंग के लिए तैयार रहना चाहिए।[66]

एक अन्य क्षेत्र **नाजुक सूचना अवसंरचना** (बतपजपबंस पदवितउंजपवद पदतिंजतनबजनतम) संरक्षण है। सूचना प्रौद्योगिकी अधिनियम की धारा 70 के तहत, सरकार किसी भी कंप्यूटर संसाधन को ''संरक्षित'' घोषित कर सकती है।[67] यदि वह राष्ट्रीय अवसंरचना (बिजली ग्रिड, दूरसंचार, वित्त आदि) के लिए महत्वपूर्ण है। राष्ट्रीय तकनीकी अनुसंधान संगठन के तहत **राष्ट्रीय नाजुक सूचना अवसंरचना संरक्षण केंद्र** (छब्प्च्ब्) को नाजुक सूचना अवसंरचना (ब्प्) की सुरक्षा का कार्य सौंपा गया है।[68]

बिजली, बैंकिंग, दूरसंचार आदि जैसे क्षेत्रों को महत्वपूर्ण के रूप में पहचाना गया है। इन क्षेत्रों की संस्थाओं में आमतौर पर अतिरिक्त साइबर सुरक्षा आवश्यकताएं होती हैं। जैसे–जैसे ये क्षेत्र कृत्रिम बुद्धिमत्ता को शामिल करते हैं (उदाहरण के लिए, ऊर्जा में स्मार्ट ग्रिड, एल्गोरिथम ट्रेडिंग या बैंकिंग में ऋण निर्णयों में कृत्रिम बुद्धिमत्ता), कृत्रिम बुद्धिमत्ता प्रणालियों की लचीलापन और सुरक्षा ब्प् संरक्षण का हिस्सा बन जाती है। यदि, मान लीजिए, बिजली ग्रिड के एक हिस्से को नियंत्रित करने वाली कृत्रिम बुद्धिमत्ता पर हमला किया जाता है, तो यह केवल एक कंपनी का मुद्दा नहीं बल्कि राष्ट्रीय सुरक्षा का मुद्दा है, और छब्प्च्ब् या ब्म्त्ज्–प्द रक्षा और प्रतिक्रिया का समन्वय करेंगे।[69] कंपनी (प्रबंधन और प्रशासन) नियम, 2014 भी इलेक्ट्रॉनिक रिकॉर्ड को अनधिकृत पहुंच से सुरक्षित रखना एक कॉर्पोरेट जिम्मेदारी बनाते हैं, जो अप्रत्यक्ष रूप से कंपनियों को साइबर सुरक्षा उपायों में निवेश करने के लिए प्रेरित करता है।[70]

क्षेत्रीय दिशानिर्देश भी हैं, उदाहरण के लिए, भारतीय रिजर्व बैंक (त्ठप्) के पास बैंकों और वित्तीय संस्थानों के लिए विस्तृत सूचना प्रौद्योगिक ढॉचा है, जिसमें साइबर सुरक्षा नियंत्रण और आवधिक ऑडिट शामिल हैं।[71] आरबीआई ने 2023 में बैंकोंध्एनबीएफसी के लिए आईटी सेवाओं की आउटसोर्सिंग पर मास्टर निर्देश भी जारी किए, जिसमें आउटसोर्स किए गए तकनीक (जिसमें आउटसोर्स किए गए कृत्रिम बुद्धिमत्ता सेवाएं शामिल हो सकती हैं) के जोखिमों को संबोधित किया गया।[72]

---

[66]CERT-IN इंडिया की 6 घंटे की समयसीमा का अनुपालन कैसे करें ?, https://www.ardentprivacy.ai/blog/how-to-comply-with-the-cert-in-6-hours-timeline/

[67]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–38.

[68]धारा 70A, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–38.

[69]डॉ. पवन दुग्गल,साइबर लॉ, प्रकाशक–यूनिर्वसल लेक्सी नेक्सी, तृतीय संस्करण 2003, ISBN:978-81-962410-7-0,पृष्ठ सं–336.

[70]नियम 28, कंपनी(प्रबंधन एवं प्रशासन)नियम,2014, https://ca2013.com/rule-28-companies-management-administration-rules2014/

[71]https://www.rbi.org.in/Commonman/English/scripts/Notification.aspx?Id=1721

[72]भारती रिर्जव बैंक, RBI/2023-24/102DoS.CO.CSITEG/SEC.1/31.O1.O15/2023-24, https://fidcindia.org.in/wp-content/uploads/2023/04/RBI-OUTSOURCING-OF-IT-SERVICES-10-04-23.pdf,प्रकाशित–10 अप्रैल 2023.

2018 में भारतीय दूरसंचार नियामक प्राधिकरण (ज्त्।ै) ने दूरसंचार डेटा की गोपनीयता और सुरक्षा पर सिफारिशें दि थी। यह एक मजबूत डेटा सुरक्षा व्यवस्था की प्रत्याशा करता है।[73] उदाहरण के लिए, ग्राहक डेटा का विश्लेषण करने के लिए कृत्रिम बुद्धिमत्ता का उपयोग करने वाले बैंक को न केवल डीपीपीडी अधिनियम का पालन करना होगा बल्कि आरबीआई के साइबर सुरक्षा मानदंडों का भी पालन करना होगा और यह सुनिश्चित करना होगा कि कोई भी कृत्रिम बुद्धिमत्ता विक्रेता उन मानकों को पूरा करता है।

संस्थागत ढांचे के संदर्भ में: ब्त्ज्.प्द और छब्प्च्ब् के अलावा, हमारे पास राज्य पुलिस में साइबर अपराध सेल और एक केंद्रीय साइबर अपराध रिपोर्टिंग पोर्टल है।[74] कानून प्रवर्तन, कृत्रिम बुद्धिमत्ता–सहायता प्राप्त धोखाधड़ी जैसे अपराधों से निपटने की क्षमता बढ़ा रहा है। केंद्रीय जांच ब्यूरो (ब्ठै) के पास एक साइबर अपराध इकाई है ये राज्य पुलिस, साइबर पुलिस स्टेशन बना रही है।[75] नयी क्षमतो का निर्माण जारी है क्योंकि कृत्रिम बुद्धिमत्ता से संबंधित अपराधों की जांच के लिए नए कौशल की आवश्यकता होती है।

अंतर्राष्ट्रीय सहयोग को महत्वपूर्ण माना जाता है। साइबर और कृत्रिम बुद्धिमत्ता खतरे सीमाहीन हैं। ब्त्ज्.प्द भारत के बाहर उत्पन्न होने वाली घटनाओं के लिए दुनिया भर के समकक्षों के साथ समन्वय करता है।[76] भारत, साइबर अपराध पर बुडापेस्ट कन्वेंशन[77] का हस्ताक्षरकर्ता नहीं होने के बावजूद, साइबर सुरक्षा पर द्विपक्षीय और बहुपक्षीय प्रयासों में संलग्न है। जैसे–जैसे कृत्रिम बुद्धिमत्ता खतरे बढ़ते हैं, यह सहयोग गहरा होने की संभावना है।

भारतीय मानक ब्यूरो (ठपै) की एक दिलचस्प नीति कृत्रिम बुद्धिमत्ता के लिए मानकों का विकास है। ठपै के पास कृत्रिम बुद्धिमत्ता पर एक समिति है जिसने मसौदा मानक प्रस्तावित किए हैं।[78] जबकि मानक स्वैच्छिक हैं, वे विनियमन को सूचित कर सकते हैं। उदाहरण के लिए, भारतीय मानक ब्यूरो कृत्रिम बुद्धिमत्ता प्रणाली की मजबूती या विश्वसनीयता पर मानक निर्धारित कर सकता है ये नियामक बाद में उन्हें सर्वोत्तम प्रथाओं के रूप में संदर्भित कर सकते हैं। ठपै ने 2020 में डेटा गोपनीयता आश्वासन ;ै **17428द्ध** पर एक मानक भी जारी किया। जिसे संगठन गोपनीयता सिद्धांतों के अनुपालन को प्रदर्शित करने के लिए अपना सकते हैं।[79] ये मानकीकरण प्रयास सुरक्षित कृत्रिम बुद्धिमत्ता के लिए तकनीकी बेंचमार्क को परिभाषित करने के लिए एक सक्रिय दृष्टिकोण का संकेत देते हैं।

इस प्रकार, राष्ट्रीय साइबर सुरक्षा नीति (छैब्ब्) 2013 और प्रतीक्षित राष्ट्रीय साइबर सुरक्षा रणनीति जैसी नीतियों को सरकारी प्रणालियों और महत्वपूर्ण सेवाओं में कृत्रिम बुद्धिमत्ता को ध्यान में रखना होगा। राष्ट्रीय साइबर सुरक्षा नीति 2013 के उद्देश्य – एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाना, कानूनों को मजबूत करना और कार्यबल बनाना – प्रासंगिक बने हुए हैं, लेकिन नई रणनीति दस्तावेजों ने कथित तौर पर 2020 के आसपास तैयार किए गए नए रणनीति दस्तावेज एआई और आईओटी जैसी उभरती हुई तकनीक को सुरक्षित करने के लिए आगे बढ़ते हैं।

4. कृत्रिम बुद्धिमत्ता नीतिगत पहल और मसौदा प्रस्ताव

कृत्रिम बुद्धिमत्ता की अंतर्निहित क्षमता और जोखिमों दोनों को स्वीकार करते हुए, भारत सरकार और संबद्ध संस्थानों ने कृत्रिम बुद्धिमत्ता से संबंधित कई प्रयास प्रारंभ की हैं और भविष्य की विनियामक योजनाओं का संकेत दिया है। यह उल्लेखित है कि , भारत में अभी तक कोई समर्पित ''कृत्रिम बुद्धिमत्ता कानून'' अस्तित्व में नहीं है, ये पहलें एक संभावित कानूनी ढांचे की आधारशिला रखती हैं।

इस दिशा में नीति आयोग की पहल '**कृत्रिम बुद्धिमत्ता के लिए राष्ट्रीय रणनीति**', 2018, जिसका उपशीर्षक **''सभी के लिए कृत्रिम बुद्धिमत्ता''** था, के साथ प्रारंभ हुई। यह एक महत्वपूर्ण दस्तावेज था जिसने कृत्रिम बुद्धिमत्ता के कार्यान्वयन के लिए प्राथमिकता वाले क्षेत्रों (स्वास्थ्य, कृषि, शिक्षा, स्मार्ट शहर, स्मार्ट गतिशीलता) की पहचान की और उपयुक्त नीतियों और विनियमों की आवश्यकता को भी स्वीकार किया। इसने सिफारिश की, कि भारत, डेटा सुरक्षा कानूनों तथा **क्षेत्रीय विनियामक ढाँचों** की स्थापना करे, और कृत्रिम बुद्धिमत्ता के

[73]अरुण प्रभु ,दूरसंचार क्षेत्र में गोपनीयता, सुरक्षा और डेटा के स्वामित्व पर ट्राई की सिफारिशें, 2018, https://corporate.cyrilamarchandblogs.com/2018/07/trai-recommendations-privacy-security-ownership-data-telecom-sector-2018, प्रकाशित– 30 जुलाई 2018.

[74]https://services.india.gov.in/service/detail/national-cyber-crime-reporting-portal

[75]CID Crime Branch Odisha Police , Cyber Crime Police Station through a notification (No. 22730/CP dated 09.06. 2004).

[76]राहुल सुन्दरम् ,https://www.indialaw.in/blog/civil/cert-in-india-cybersecurity-framework/, प्रकाशित– 25 नवम्बर 2024.

[77]Convention on Cybercrime Budapest,European Treaty Series - No. 185, https://rm.coe.int/1680081561

[78]एआई विनियमनः सरकार अनुप्रयोगों के लिए मानकों का व्यापक सेट तैयार कर रही है, https://www.policycircle.org/policy/ai-regulation-in-india-bis-standard/, प्रकाशित– 29 अगस्त 2024.

[79]अकशय नेंर, IS17428 -A New Privacy Assurance Standard in India, https://www.foxmandal.in/is-17428-a-new-privacy-assurance-standard-in-india/, प्रकाशित– 2 जनवरी 2022.

लिए अंतर्राष्ट्रीय मानकों को अपनाने को बढ़ावा दें।[80] इसने कृत्रिम बुद्धिमत्ता अनुसंधान और कौशल विकास के लिए बुनियादी ढांचे के निर्माण का भी सुझाव दिया। महत्वपूर्ण रूप से, कृत्रिम बुद्धिमत्ता के लिए राष्ट्रीय रणनीति ने उच्च स्तर पर नैतिक विचारों (पूर्वाग्रह, पारदर्शिता, जवाबदेही) पर चर्चा की और सुझाव दिया कि किसी भी कृत्रिम बुद्धिमत्ता विनियमन को प्रारंभिक रूप से नवाचार को बाधित न करने के लिए सहज होना चाहिए।

इसी आधार पर, 2021 में नीति आयोग ने **''जिम्मेदार कृत्रिम बुद्धिमत्ता''** पर दो–भाग दृष्टिकोण जारी किया। भाग 1 फरवरी 2021, ने सिद्धांत निर्धारित किए दृ जैसे सुरक्षा और विश्वसनीयता, समानता (पूर्वाग्रह से बचाव), समावेशिता और गैर–भेदभाव, गोपनीयता और सुरक्षा, और जवाबदेही।[81] भाग 2 अगस्त 2021, ने इन सिद्धांतों को क्रियान्वित करने के लिए एक दृष्टिकोण प्रदान किया। इसने सरकार और निजी क्षेत्र दोनों से भागीदारी का आह्वान किया ताकि यह सुनिश्चित किया जा सके कि कृत्रिम बुद्धिमत्ता प्रणालियाँ सर्वोत्तम प्रथाओं जैसे पूर्वाग्रह परीक्षण, एल्गोरिथम प्रभाव आकलन आदि के माध्यम से नैतिक मानदंडों का पालन करें।[82] यद्यपि ये दस्तावेज स्वयं कानून नहीं हैं, फिर भी वे किसी भी भविष्य के बाध्यकारी दिशानिर्देशों के लिए संदर्भ के रूप में कार्य करते हैं। उदाहरण के लिए, यदि भविष्य में सरकार सूचना प्रौद्योगिकी अधिनियम या कृत्रिम बुद्धिमत्ता निरीक्षण के लिए एक नए कानून के तहत नियम जारी करती है, तो यह अपेक्षित है कि ये नीति आयोग के सिद्धांत उन नियमों को प्रभावित करेंगे। जैसे–महत्वपूर्ण डोमेन में कृत्रिम बुद्धिमत्ता प्रणालियों के लिए जोखिम मूल्यांकन या मानव निरीक्षण की आवश्यकता।

समांतर रूप से, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (डमपजल) ने विशिष्ट कृत्रिम बुद्धिमत्ता विषयों पर समितियाँ गठित कीं। उदाहरण के लिए, कृत्रिम बुद्धिमत्ता शासन पर एक समिति एक रिपोर्ट तैयार कर सकती है। ऐसी रिपोर्टें और सिफारिशें अक्सर कानून निर्माण से पूर्व की स्थिति को दर्शाती हैं। इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय ने कृत्रिम बुद्धिमत्ता को विनियमित करने के बारे में अवधारणा नोट भी प्रसारित किए हैं। 2023 में, डमपजल ने संसद में सार्वजनिक रूप से कहा कि वह तत्काल **'कृत्रिम बुद्धिमत्ता को विनियमित करने के लिए"** कोई कानून लाने पर विचार नहीं कर रही है।[83] वह एक नवाचार–समर्थक दृष्टिकोण को प्राथमिकता दे रहा है। यह बिंजळच्ज जैसी जेनेरेटिव कृत्रिम बुद्धिमत्ता के वैश्विक पटल में आने का समय था, जिसने कई देशों को विनियामक कदम उठाने पर विचार करने के लिए प्रेरित किया। हालाँकि, डमपजल का रुख सूक्ष्म था, भले ही उसने कहा कि कोई तत्काल कृत्रिम बुद्धिमत्ता–विशिष्ट कानून नहीं है, फिर भी वह साथ ही साथ डिजिटल इंडिया एक्ट के खाके पर काम कर रहा था जिसमें ''उच्च–जोखिम वाली कृत्रिम बुद्धिमत्ता प्रणालियों का विनियमन'' एक घटक के रूप में शामिल था।[84] इससे पता चलता है कि यूरोपीय संघ के दृ ष्टिकोण की तरह एक पृथक अधिनियम के बजाय, भारत एक व्यापक डिजिटल कानून के भीतर कृत्रिम बुद्धिमत्ता को शामिल कर सकता है।

2024 के शुरुआती दिनों में कृत्रिम बुद्धिमत्ता विनियमन पर सरकार की सोच और विभिन्न सरकारी एजेंसियों के बीच चल रही चर्चा को सार्वजनिक किया गया। मार्च 2024 में, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (डमपजल) ने एक गैर–बाध्यकारी सलाह जारी की, जिसने प्रभावी रूप से कृत्रिम बुद्धिमत्ता मॉडलों पर तत्काल प्रभाव से कुछ नियंत्रण लगा दिए। कृत्रिम बुद्धिमत्ता आउटपुट को स्पष्ट रूप से कृत्रिम बुद्धिमत्ता–जनित के रूप में लेबल किया जाए। चुनाव संबंधी गलत सूचना या मौजूदा सूचना प्रौद्योगिकी अधिनियम नियमों के तहत किसी भी गैरकानूनी सामग्री के निर्माण के लिए कृत्रिम बुद्धिमत्ता के उपयोग पर प्रतिबंधित किया गया।[85] मूल रूप से, प्लेटफार्मों से यह सुनिश्चित करने के लिए कहा गया कि उनके द्वारा प्रदान किए गए कृत्रिम बुद्धिमत्ता उपकरण गैरकानूनी सामग्री (जैसे घृणास्पद भाषण, नकली समाचार, आदि, जो प्रतिबंधित हैं) को बढ़ावा न दें। इसमें यह चेतावनी भी जोड़ी गई कि इन अपेक्षाओं का अनुपालन न करने पर अधिनियम और आईपीसी (बीएनएस) के तहत कानूनी कार्यवाही की जा सकती है।[86] हालाँकि एक सलाह

---

[80]National Strategy for Artificial Intelligence, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

[81] Part 1– Principles for Responsible AI, https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf, प्रकाशित–फरवरी 2021.

[82] Part 2 - Operationalizing Principles for Responsible AI, https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf, प्रकाशित– अगस्त 2021.

[83]आईटी मंत्रालय ने संसद को बताया, एआई को विनियमित करने की कोई योजना नहीं, https://www.thehindu.com/news/national/no-plan-to-regulate-ai-it-ministry-tells-parliament/article66702044.ece, प्रकाशित–5 अप्रैल 2023.

[84]अम्लान मोहंती एवं शतक्रतु शाहु,India's Advance on AI Regulation, https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en, प्रकाशित–21 नवम्बर 2024.

[85]अर्जुन एड्रियन डिसूजा, एआई को विनियमित करने में भारत का कदम, https://iapp.org/news/a/indias-foray-into-regulating-ai, प्रकाशित–24 अप्रैल 2024.

[86]Meity's guidance on AI: Aynalyzing March Advisory and Legal Perspectives, https://kaizenlaw.in/2024/04/03/meitys-guidance-on-ai-analyzing-march-15th-advisory-and-legal-perspectives/, प्रकाशित–3 अप्रैल 2024.

होने के नाते इसकी भाषा बाध्यकारी नियम की नहीं थी, लेकिन इसने एक चेतावनी अवश्य दी। इस सलाह का त्वरित संशोधन इस आंतरिक अहसास को दर्शाता है कि एक संतुलन बनाना आवश्यक है, कृत्रिम बुद्धिमत्ता में उपयोगकर्ता सुरक्षा और विश्वास सुनिश्चित करना, लेकिन नवाचार को बाधित न करना या ऐसी बोझिल अनुमतियाँ बनाना जो वैध कृत्रिम बुद्धिमत्ता उपयोग को भी बाधित कर सकती हैं।[87] रिपोर्टों से पता चलता है कि इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (डमपजल) आम तौर पर कृत्रिम बुद्धिमत्ता के लिए एक **''सामान्य नियामक दृष्टिकोण''** का समर्थन करता है, जो नवाचार पर ध्यान केंद्रित करता है, जबकि कुछ अन्य एजेंसियों ने कृत्रिम बुद्धिमत्ता के जोखिमों के कारण अधिक सख्त विनियमन का आह्वान किया।[88] भारत सरकार के प्रधान वैज्ञानिक सलाहकार कार्यालय ने तो कृत्रिम बुद्धिमत्ता के सक्रिय विनियमन का आग्रह करते हुए एक रिपोर्ट भी प्रकाशित की थी, जिसमें इसे निगरानी की आवश्यकता वाली **''जटिल अनुकूली प्रणाली''** बताया गया था।

भारत कृत्रिम बुद्धिमत्ता नैतिकता और शासन पर अंतरराष्ट्रीय स्तर पर सक्रिय है। दिसंबर 2023 में, भारत ने नई दिल्ली मेंकृत्रिम बुद्धिमत्ता पर वैश्विक भागीदारी (ळच।ए) शिखर सम्मेलन की मेजबानी की, जहाँ इसने आथिक सहयोग और विकास संगठन ;व्ब्व्द्ध कृत्रिम बुद्धिमत्ता सिद्धांतों के प्रति अपनी प्रतिबद्धता दोहराई दृ जो भरोसेमंद कृत्रिम बुद्धिमत्ता, मानवाधिकारों, निष्पक्षता और पारदर्शिता पर जोर देते हैं। मंत्रिस्तरीय घोषणा ने जिम्मेदार कृत्रिम बुद्धिमत्ता के लिए नियमों और मानकों के विकास का समर्थन किया।[89] ळच।ए में और ळ20 में (अपनी 2023 की अध्यक्षता के दौरान, भारत ने कृत्रिम बुद्धिमत्ता सहित डिजिटल मुद्दों को एजेंडा में रखा) भारत की सक्रिय भूमिका अपनी घरेलू दृष्टिकोण को परिष्कृत करते हुए भी वैश्विक कृत्रिम बुद्धिमत्ता शासन मानदंडों को आकार देने के इरादे को दर्शाती है।

यह नीतिगत संदर्भ इस बात को प्रभावित करेगा कि कानूनी ढांचा किस प्रकार विकसित होगा। फिलहाल, भारत में हितधारक सामान्य कानूनों और सामान्य दिशानिर्देशों के तहत काम कर रहे हैं। वे अधिक ठोस नियमों की उम्मीद करते हैं लेकिन अंतरिम में स्व–विनियमन के लिए वैश्विक ढाँचों से भी अनुकरण लेते हैं। इस पत्र का अगला भाग विश्लेषण करेगा कि प्रमुख वादों में इन्हें कैसे लागू या व्याख्यायित किया गया है, और फिर शेष अनसुलझी चुनौतियों पर चर्चा करेगा।

न्यायिक प्रतिक्रियाएँः सर्वोच्च न्यायालय का गोपनीयता और प्रौद्योगिकी पर दृष्टिकोण

भारत के सर्वोच्च न्यायालय ने गोपनीयता, डेटा संरक्षण और साइबर कानून दृ उन क्षेत्रों को जो कृ त्रिम बुद्धिमत्ता और साइबर सुरक्षा के विनियमन को सीधे प्रभावित करते हैं दृ की कानूनी रूपरेखा को आकार देने में महत्वपूर्ण भूमिका निभाई है। हाल के वर्षों में कई ऐतिहासिक निर्णयों के माध्यम से, न्यायालय ने आधारभूत सिद्धांतों को स्थापित किया, और कई बार अपने निर्णयों द्वारा कानूनी आवशकताओं को पूरा किया है। यह खंड गोपनीयता, साइबर सुरक्षा और उभरती प्रौद्योगिकियों से संबंधित महत्वपूर्ण सर्वोच्च न्यायालय के फैसलों का अध्ययन करता है, और भारतीय कानूनी प्रणाली में कृत्रिम बुद्धिमत्ता शासन के लिए उनके निहितार्थों का विश्लेषण करता है।

निजता के मौलिक अधिकार के रूप में स्थापना दृ के.एस. पुट्टस्वामी बनाम भारत संघ[90] (2017)

भारत में गोपनीयता और प्रौद्योगिकी से संबंधित किसी भी चर्चा का आरंभ बिंदु सर्वोच्च न्यायालय का न्यायमूर्ति के.एस. पुट्टस्वामी (सेवानिवृत्त) एवं अन्य बनाम भारत संघ एवं अन्य, का निर्णय होना अपरिहार्य है। सर्वोच्च न्यायालय की नौ न्यायाधीशों की संविधान पीठ ने सर्वसम्मति से यह अभिनिर्धारित किया कि निजता का अधिकार भारतीय संविधान द्वारा प्रदत्त एक मौलिक अधिकार है। इस ऐतिहासिक निर्णय ने पूर्ववर्ती न्यायिक दृ ष्टांतों को निरस्त करते हुए यह स्थापित किया कि निजता भारतीय संविधान के अनुच्छेद 21 के अंतर्गत जीवन और स्वतंत्रता के अधिकार का और संविधान के भाग प्प् में निहित स्वतंत्रताओं का एक अंतर्निहित पहलू है। न्यायालय के निजता के व्यापक दृष्टिकोण में व्यक्तिगत डेटा पर स्वायत्तता, निजी संचार की अभेद्यता और निगरानी से मुक्ति शामिल थी दृ साथ ही यह भी स्वीकार किया गया कि यद्यपि उचित प्रतिबंध लगाए जा सकते हैं, निजता का अधिकार निरपेक्ष नहीं है।

पुट्टस्वामी का निर्णय ऐसे समय में आया जब डिजिटल प्रौद्योगिकियों के प्रसार ने व्यक्तिगत डेटा के संग्रह में अभूतपूर्व वृद्धि की थी। यद्यपि यह मामला स्वयं आधार बायोमेट्रिक पहचान योजना को चुनौती देने के कारण उत्पन्न हुआ था, संविधान पीठ ने एक व्यापक संवैधानिक प्रश्न तैयार किया। इस निर्णय ने इस

[87]No.eNo.2(4)/2023-CyberLaws–3,Government of India Ministry of Electronics and Information Technology Cyber Law and Data Governance Group, प्रकाशित–15 मार्च 2024.

[88]पूर्वोक्त,91.

[89]https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1986475, प्रकाशित–14 दिसंबर 2023.

[90]पूर्वोक्त,12. एआईआर 2017 एससीसी 416.

तथ्य को रेखांकित किया कि **बिग डेटा** और **सूचना की सर्वव्यापकता** के वर्तमान युग में, व्यक्तियों के पास गोपनीयता का एक निश्चित दायरा अवश्य होना चाहिए। न्यायालय ने यह भी स्पष्ट रूप से कहा कि राज्य पर एक प्रभावी डेटा संरक्षण व्यवस्था स्थापित करने की जिम्मेदारी है। न्यायालय ने यह अभिमत व्यक्त किया कि निजता के खतरे न केवल राज्य से बल्कि गैर–राज्य अभिकर्ताओं (जैसे निगमों) से भी उत्पन्न होते हैं, और इसलिए एक सुदृढ़ डेटा संरक्षण कानून की आवश्यकता पर बल दियां।[91] यह आह्वान अंततः डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 के अधिनियमन का कारण बना है।

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के संदर्भ में, पुट्टस्वामी का निर्णय अत्यधिक महत्व रखता है। प्रथम, निजता को एक संवैधानिक अधिकार के रूप में स्थापित करके, यह एक ऐसा मानक निर्धारित करता है जिसका सरकार द्वारा किसी भी कृत्रिम बुद्धिमत्ता के कार्यान्वयन या साइबर सुरक्षा उपाय को पालन करना आवश्यक है।[92] उदाहरण के लिए, यदि विधि प्रवर्तन एजेंसियां बड़े पैमाने पर निगरानी के लिए कृत्रिम बुद्धिमत्ता का उपयोग करती हैं (जैसे सार्वजनिक स्थानों पर चेहरे की पहचान या कृत्रिम बुद्धिमत्ता–आधारित सोशल मीडिया निगरानी), तो ऐसी कार्रवाइयाँ पुट्टस्वामी में निर्धारित सिद्धांतों के अधीन होंगीः वैधता आवश्यकता और आनुपातिकता (उपाय को एक वैध उद्देश्य की पूर्ति करनी चाहिए और इसे प्राप्त करने का सबसे कम प्रतिबंधात्मक तरीका होना चाहिए), और दुरुपयोग के विरुद्ध सुरक्षा उपाय। इसका प्रभाव पहले से ही बाद के न्यायिक निर्णयों में देखा जा सकता हैः उदाहरण के लिए, 2018 में, जब आधार कार्यक्रम को निजता के आधार पर चुनौती दी गई थी, तो पुट्टस्वामी के सिद्धांतों ने न्यायिक विश्लेषण का मार्गदर्शन किया था।

द्वितीय, पुट्टस्वामी के निर्णय ने विधायी और कार्यकारी कार्रवाई को प्रेरित किया। डेटा गोपनीयता विनियमन की कमी को स्वीकार करते हुए, सरकार ने प्रत्यक्ष परिणाम के रूप में डेटा संरक्षण पर श्रीकृष्णा समिति का गठन किया।[93] डिजिटल अधिकारों से संबंधित किसी भी बहस में इस निर्णय का बार–बार उल्लेख किया जाता है। यदि भविष्य में कोई कृत्रिम बुद्धिमत्ता के किसी पहलू को चुनौती देता है – उदाहरण के लिए, यदि कोई याचिका यह तर्क देती है कि किसी सरकारी एजेंसी द्वारा उपयोग किया जाने वाला एल्गोरिथम अपारदर्शी है और निजता या उचित प्रक्रिया का उल्लंघन करता है, तो पुट्टस्वामी उस तर्क का आधारशिला होगा, जो निजता को एक मौलिक अधिकार के रूप में स्थापित करेगा जिसका एल्गोरिथम का उपयोग यदि ठीक से विनियमित या न्यायसंगत नहीं ठहराया जाता है तो उल्लंघन कर सकता है। पुट्टस्वामी में सर्वोच्च न्यायालय ने अन्य पहलुओं पर भी विचार व्यक्त किए, जैसे निजी कंपनियों के विरुद्ध निजता की रक्षा करने की आवश्यकता (कुछ मामलों में अधिकारों के क्षैतिज अनुप्रयोग की अवधारणा को स्वीकार करते हुए)।[94] इसका अर्थ है, सैद्धांतिक रूप से, यदि कोई कृत्रिम बुद्धिमत्ता कंपनी व्यक्तिगत निजता का गंभीर उल्लंघन करती है, तो निजता के संवैधानिक मूल्य कानूनों की व्याख्या को प्रभावित कर सकते हैं या मामलों में निजी अभिकर्ताओं को सीधे मौलिक मानकों के लिए उत्तरदायी ठहराने वाली नई न्यायिक व्याख्याओं को भी जन्म दे सकते हैं।[95]

बायोमेट्रिक पहचान और डेटा का उपयोग दृ के. एस. पुट्टस्वामी बनाम भारत संघ (आधार निर्णय, 2018)[96]

2018 में एक और मामला, जिसका शीर्षक भी के.एस. पुट्टस्वामी बनाम भारत संघ था, पाँच न्यायाधीशों की पीठ के समक्ष आया, जो विशिष्ट रूप से आधार बायोमेट्रिक पहचान परियोजना से संबंधित था। इसे प्रायः आधार निर्णय कहा जाता है। इस मामले में, सर्वोच्च न्यायालय ने 4–1 के बहुमत से आधार (वित्तीय और अन्य सब्सिडी का लक्षित वितरण) अधिनियम, 2016 की संवैधानिकता को बनाए रखा, जबकि कुछ प्रावधानों को निरस्त या सीमित कर दिया। आधार योजना से जुड़े मुद्दे साइबर सुरक्षा और डेटा संरक्षण के लिए प्रत्यक्ष रूप से महत्वपूर्ण थे। इस परियोजना में एक अरब से अधिक व्यक्तियों के उंगलियों के निशान का स्कैन संग्रह और उस पहचान को विभिन्न सेवाओं से जोड़ना शामिल था। याचिकाकर्ताओं ने निगरानी, डेटा उल्लंघनों और नागरिकों के व्यक्तिगत सूचना पर नियंत्रण खोने की आशंकाएं व्यक्त कीं दृ अनिवार्य रूप से यह पूर्वानुमान लगाया कि यदि इस केंद्रीकृत डेटाबेस का दुरुपयोग या हैकिंग होती है तो क्या संभावित हानियाँ हो सकती हैं।

[91]वृंदा भंडारी और रेणुका साने, "PROTECTING CITIZENS FROM THE STATE POST PUTTASWAMY: ANALYSING THE PRIVACY IMPLICATIONS OF THE JUSTICE SRIKRISHNA COMMITTEE REPORT AND THE DATA PROTECTION BILL, 2018", https://docs.manupatra.in/newsline/articles/Upload/7B08CF55-E27D-4A44-A292-3882F08E9053.pdf.

[92]अधिवक्ता अपूर्वा ठाकुर और अधिवक्ता मनीष कुमार, "Right to Privacy vis-à-vis Artificial Intelligence: Indian Scenario",International Journal of Law Management and Humanities, Volume 7,issue 2,page 3370-3384.

[93]पूवोक्त,102.

[94]पूवोक्त,12

[95]पूवोक्त,103.

[96]एआईआर 2018 एससीसी 1841 .

न्यायमूर्ति ए.के. सीकरी के नेतृत्व वाली बहुमत पीठ ने यह निष्कर्ष निकाला कि आधार अधिनियम में संवैधानिक मानदंडों को पूरा करने के लिए पर्याप्त सुरक्षा और गोपनीयता उपाय विद्यमान थे, विशेष रूप से उन प्रावधानों को निरस्त करने के पश्चात जो अनियंत्रित साझाकरण की अनुमति देते थे। महत्वपूर्ण रूप से, न्यायालय ने आधार अधिनियम की धारा 57 को निरस्त कर दिया, जिसने निजी कंपनियों को पहचान स्थापित करने के लिए आधार प्रमाणीकरण का उपयोग करने की अनुमति दी थी। न्यायालय ने यह अभिमत व्यक्त किया कि निजी संस्थाओं को आधार की मांग करने की अनुमति देना (जैसे मोबाइल कनेक्शन या बैंकिंग सेवाओं के लिए) असंवैधानिक था, क्योंकि यह एक वैध राज्य हित के उद्देश्य से बनाए गए कानून द्वारा समर्थित नहीं था और यह असंगत था। इसने सभी क्षेत्रों में एक एकल पहचान के उपयोग के प्रसार को रोका, जिसे न्यायालय ने महसूस किया कि गोपनीयता अधिकारों के विपरीत वाणिज्यिक शोषण और प्रोफाइलिंग को बढ़ावा दे सकता है।[97]

न्यायालय ने धारा 33(2) को भी न्यायिक निरीक्षण की आवश्यकता लागू करके सीमित कर दिया, जिससे सुरक्षा की एक अतिरिक्त परत जुड़ गई। एक अन्य परिणाम न्यायालय द्वारा उस विनियमन का अमान्यकरण था जिसने बैंक खातों और सिम कार्ड के साथ आधार को अनिवार्य रूप से जोड़ने का आदेश दिया थाए जो अधिनियम में स्वयं निहित नहीं थे, और न्यायालय ने उन्हें अनावश्यक और असंगत पाया।[98] हालाँकि, न्यायालय ने सरकारी कल्याणकारी योजनाओं (अधिनियम की धारा 7) के लिए आधार के अनिवार्य उपयोग को बरकरार रखा, यह तर्क देते हुए कि सब्सिडी के लक्षित वितरण का उद्देश्य वैध था और धोखाधड़ी को रोकने के लिए आधार एक उचित साधन था।

कृत्रिम बुद्धिमत्ता के संदर्भ में, आधार निर्णय व्यक्तिगत डेटा का प्रबंधन करने वाले बड़े पैमाने के तकनीकी बुनियादी ढांचे के प्रति सर्वोच्च न्यायालय के दृष्टिकोण को दर्शाता है। पीठ आंशिक रूप से इस तथ्य से संतुष्ट थी कि आधार प्राधिकरण (न्प्ब्।ै) ने एन्क्रिप्शन का उपयोग किया था, एक संक्षिप्त अवधि से परे लेनदेन के मेटा–डेटा को संग्रहीत नहीं किया था, और एक निरीक्षण तंत्र मौजूद था। न्यायमूर्ति डी.वाई. चंद्रचूड़ के अकेले असहमतिपूर्ण मत ने अधिक संशयवादी दृष्टिकोण व्यक्त किया, यह तर्क देते हुए कि सुरक्षा उपायों के साथ भी व्यापक डेटा संग्रह की अनुमति देना गोपनीयता के लिए गंभीर जोखिम उत्पन्न करता है और डेटा के अभिसरण (जब विभिन्न स्रोतों से डेटा संयुक्त होता है, जिसे कृत्रिम बुद्धिमत्ता बड़े पैमाने पर कर सकती है) की संभावना को देखते हुए ''निगरानी राज्य'' की ओर ले जा सकता है। यद्यपि बहुमत पीठ ने उस खतरे को पूरी तरह से साझा नहीं किया, फिर भी इसने आधार के दायरे को सीमित करके गोपनीयता संबंधी चिंताओं को स्वीकार किया।

यदि सरकार बड़े पैमाने पर कृत्रिम बुद्धिमत्ता की प्रणालियों को नियुक्त करती है तो, आधार मामला इंगित करता है कि न्यायालय गोपनीयता के अतिक्रमण के विरुद्ध ऐसी प्रणाली की आवश्यकता का मूल्यांकन करेगा। यदि यह कल्याणकारी योजनाओं सामाजिक हित के लिए है और कानूनी सुरक्षा उपायों के साथ है, तो न्यायालय इसे बरकरार रख सकता है। इस निर्णय ने डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम के प्रावधानों में योगदान दिया और यह उल्लेखित किया, कि कृत्रिम बुद्धिमत्ता में बायोमेट्रिक या अन्य संवेदनशील डेटा को कैसे संभाला जाए।

ऑनलाइन अभिव्यक्ति की स्वतंत्रता – श्रेया सिंघल बनाम भारत संघ (2015)[99]

यह निर्णय कृत्रिम बुद्धिमत्ता के प्रसार से पहले सुनाया गया था, श्रेया सिंघल वाद साइबर स्पेस में सर्वोच्च न्यायालय का ऑनलाइन सामग्री को विनियमित करने के सबंधं में एक महत्वपूर्ण का वाद है। उपरोक्त में सर्वोच्च न्यायालय ने सूचना प्रौद्योगिकी अधिनियम के कई प्रावधानों की संवैधानिकता की जांच की। इस वाद ने अधिनियम की धारा 66। को निरस्त कर दिया, जिसने कंप्यूटर के माध्यम से ऐसी कोई भी जानकारी भेजना अपराध बना दिया था जो ''घोर आपत्तिजनक'' या धमकी देने वाली प्रकृति की थी, या अन्य अस्पष्ट शब्दों की हो। न्यायालय ने माना कि धारा 66। ए भारतीय संविधान के अनुच्छेद 19(1)(।) (भाषण की स्वतंत्रता) का उल्लंघन करती है, और अनुच्छेद 19(2) में उचित प्रतिबंधों द्वारा इसे संरक्षणित नही किया गया है।[100] क्योंकि इसके शब्द अपरिभाषित, अत्यधिक व्यापक थे, और ऑनलाइन मुक्त अभिव्यक्ति पर इसका भयावह प्रभाव पड़ा। न्यायालय ने अपने विश्लेषण में इस बात पर प्रकाश डाला कि धारा 66। का दुरुपयोग राजनीतिक आलोचना

[97]Constitutionality of Aadhaar Act: Judgment Summary, https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/

[98]पूवोक्त,108.

[99]एआईआर (2015) 5 एससीसी 1

[100] अनुच्छेद 19(1)(A), भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण,पृष्ठ सं–23.

या कलात्मक अभिव्यक्ति को दबाने के लिए कैसे किया जा सकता है, क्योंकि ''आपत्तिजनक'' क्या है, यह व्यक्तिपरक है।[101]

इसके अतिरिक्त, श्रेया सिंघल वाद ने धारा 69।[102] और 2009 के अवरुद्ध नियमों को बरकरार रखा, यह देखते हुए कि उनमें पर्याप्त प्रक्रियात्मक सुरक्षा उपाय थे (अनुरोधों को एक समिति से गुजरना पड़ता था और कारण बताने पड़ते थे, आदि)। इसने धारा 79[103] मध्यवर्ती दायित्व को भी सीमित कर दिया दृ इसने तत्कालीन मौजूदा मध्यवर्ती दिशानिर्देशों (2009)[104] को उस हद तक निरस्त कर दिया जहाँ उन्हें अदालत या सरकार के आदेश के बिना सामग्री की सक्रिय निगरानी या हटाने की आवश्यकता थी। न्यायालय ने स्पष्ट किया कि मध्यस्थों को केवल कानूनी आदेश प्राप्त होने पर ही सामग्री हटानी चाहिए, न कि केवल किसी निजी शिकायत पर, सेंसरशिप के लिए एक उच्च सीमा को बहाल रखा।

श्रेया सिंघल का फैसला कई तरह से कृत्रिम बुद्धिमत्ता के लिए अत्यधिक प्रासंगिक है। जैसे–जैसे कृत्रिम बुद्धिमत्ता प्रणालियाँ सामग्री उत्पन्न करती हैं, गैरकानूनी या हानिकारक सामग्री के प्रश्न उठते हैं। उदाहरण के लिए, यदि एक जेनेरेटिव कृत्रिम बुद्धिमत्ता घृणास्पद भाषण या मानहानिकारक सामग्री उत्पन्न करती है, तो क्या इसे होस्ट करने वाले प्लेटफॉर्म को उत्तरदायी ठहराया जा सकता है ?। श्रेया सिंघल वाद के सिद्धांत बताते हैं कि जब तक प्लेटफॉर्म विशिष्ट अवैध सामग्री को हटाने के लिए अदालतध्सरकार का आदेश मिलने पर प्रतिक्रिया करता है, तब तक वे सुरक्षित हैं।[105] बाद में आए मध्यवर्ती नियम 2021, सावधानीपूर्वक इससे संरेखित किए गए थे दृ वे निगरानी का आदेश नहीं देते हैं, लेकिन शिकायतों के माध्यम से वास्तविक ज्ञान होने पर त्वरित हटाने की आवश्यकता होती है।[106]

यह निर्णय तकनीक में अस्पष्ट कानूनों की समस्या का समाधान करता है। यह कृत्रिम बुद्धिमत्ता विनियमन के लिए शिक्षाप्रद है दृ कृत्रिम बुद्धिमत्ता से संबंधित कृत्यों को अपराधीकरण या प्रतिबंधित करने का प्रयास उचित होना चाहिए। लेकिन निरस्त किए जाने के बाद भी, धारा 66। को कुछ कानून प्रवर्तन एजेंसियों द्वारा लागू किया जाता रहा, जिससे सर्वोच्च न्यायालय को पीपुल्स यूनियन फॉर सिविल लिबर्टी बनाम भारत संघ[107], 2022 में सभी अधिकारियों को धारा 66। के तहत अपराध के कथित उल्लंघन के लिए मुकदमा न दर्ज करने के निर्देश जारी करने पड़े। इस प्रकरण ने तकनीक–कानून इंटरफेस में न्यायालय के फैसलों के बारे में जागरूकता और अनुपालन की आवश्यकता को रेखांकित किया।[108]

इंटरनेट अभिगम और निलंबन दृ अनुराधा भसीन बनाम भारत संघ[109] (2020)

वर्ष 2020 में, सर्वोच्च न्यायालय ने अनुराधा भसीन बनाम भारत संघ के मामले में एक महत्वपूर्ण निर्णय दिया, जो अगस्त 2019 में अनुच्छेद 370[110] के निरस्तीकरण के पश्चात जम्मू और कश्मीर में लंबे समय तक इंटरनेट सेवाओं के निलंबन से संबंधित था। याचिकाकर्ताओं ने तर्क प्रस्तुत किया कि इंटरनेट संचार का अनिश्चितकालीन स्थगन भाषण की स्वतंत्रता, अनुच्छेद 19(1)(।)[111] और व्यवसाय या वृत्ति करने की स्वतंत्रता, अनुच्छेद 19(1)(ह)[112] के मौलिक अधिकारों का उल्लंघन करता है, साथ ही प्रेस की स्वतंत्रता और सूचना तक पहुँच को भी बाधित करता है।

सर्वोच्च न्यायालय ने इस मामले में सीधे तौर पर इंटरनेट सेवाओं की बहाली का आदेश नहीं दिया, क्योंकि निर्णय के समय तक कुछ सेवाएं धीरे–धीरे बहाल की जा रही थीं, परन्तु इसने इंटरनेट निलंबन को नियंत्रित करने वाले महत्वपूर्ण सिद्धांतों को प्रतिपादित किया।[113] न्यायालय ने यह अभिमत व्यक्त किया कि **''इंटरनेट के माध्यम से'' भाषण और अभिव्यक्ति की स्वतंत्रता संवैधानिक रूप से संरक्षित है**। जिसने प्रभावी रूप से यह स्वीकार किया कि इंटरनेट तक पहुँच मौलिक अधिकारों को साकार करने का एक साधन है। न्यायालय

---

[101] अभिनव के शुक्ला,"Shreya Singhal v. Union of India: A Critical Analysis", https://www.tscld.com/shreya-singhal-v-union-of-india-a-critical-analysis, प्रकाशित–10 अप्रैल 2024.

[102]धारा 69A, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–37.

[103]धारा 79A, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–42.

[104]भारत का राजपत्र,जी.एस.आर. 781(ई), दिनॉक–27–10–2009.

[105]Devadasan Vasudev, "Conceptualising India's Safe Harbour in the Era of Platform Governance", Indian Journal of Law and Technology: Vol. 19: Iss. 1, Article 1. DOI: 10.55496/NBQQ3956, https://repository.nls.ac.in/ijlt/vol19/iss1/1

[106]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 20211 ,updated - 6.4.2023.

[107]पीपुल्स यूनियन फॉर सिविल लिबर्टी बनाम भारत संघ, रिट याचिका सं. 199/2013

[108]कृष्णेश बापट, सुप्रीम कोर्ट का निर्देशः असंवैधानिक एस.66ए के तहत लोगों पर मुकदमा चलाना बंद करें, https://internetfreedom.in/sc-direction-stop-prosecuting-people-under-the-unconstitutional-s-66a, प्रकाशित–12 अक्टूबर 2022.

[109]एआईआर (2020) 3 एससीसी 637.

[110] अनुच्छेद 370(निरसित), भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण,पृष्ठ सं–199.

[111]अनुच्छेद 19(1)(A), भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण,पृष्ठ सं–23.

[112]अनुच्छेद 19(1)(g), भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण,पृष्ठ सं–24.

[113]Kriti Bhatnagar, Internet access and COVID-19: A constitutional argument to right to internet access in India,(2022),International Journal of Health Sciences, 6(S8), 1833– 1865. https://doi.org/10.53730/ijhs.v6nS8.11588

ने आगे यह भी निर्धारित किया कि इंटरनेट का अनिश्चितकालीन निलंबन अस्वीकार्य है, और इंटरनेट अभिगम पर किसी भी प्रतिबंध को आनुपातिकता की आवश्यकता का अनुपालन करना चाहिए और समय–समय पर उसकी समीक्षा की जानी चाहिए। सरकार को इंटरनेट निलंबन के सभी आदेश प्रकाशित करने का निर्देश दिया गया, जिससे व्यथित पक्ष उन्हें न्यायालय में चुनौती दे सकें। न्यायालय ने इस बात पर भी जोर दिया कि एक उपाय के रूप में इंटरनेट का पूर्ण व्यापक अवरोध अंतिम विकल्प होना चाहिए, जिसका तात्पर्य है कि कम दखल देने वाले उपायों (जैसे कुछ सेवाओं या वेबसाइटों को अवरुध) करना, या प्रतिबंध लगाने पर पहले विचार किया जाना चाहिए।

साइबर सुरक्षा और कृत्रिम बुद्धिमत्ता के संदर्भ में, अनुराधा भसीन मामले के कुछ निहितार्थ हैं। प्रथम, यह इस विचार को सुदृढ़ करता है कि **डिजिटल कनेक्टिविटी अत्यंत महत्वपूर्ण है और इसका व्यवधान संकीर्ण रूप से परिभाषित होना चाहिए,** जो साइबर आपात स्थितियों जैसे परिदृश्यों में लागू हो सकता है। उदाहरण के लिए, यदि सरकार को एक गंभीर साइबर हमले का सामना करना पड़ता है, तो क्या वह इसे सीमित करने के लिए क्षेत्रों में इंटरनेट सेवाओं को बंद कर सकती है? संभवतः हाँ, परन्तु अनुराधा भसीन मामले के अनुसार, ऐसा निलंबन समयबद्ध, आवश्यक और समीक्षित होना चाहिए। यह सुनिश्चित करता है कि साइबर खतरों (यहां तक कि कृत्रिम बुद्धिमत्ता द्वारा प्रचारित, जैसे वायरस का प्रसार) की प्रतिक्रियाएँ आवश्यकता से अधिक समय तक अनावश्यक रूप से अधिकारों का अतिक्रमण न करें।

द्वितीय, यह मामला पारदर्शिता और जवाबदेही पर प्रकाश डालता है दृ सभी आदेश प्रकाशित किए जाने चाहिए। कृत्रिम बुद्धिमत्ता के संदर्भ में, यदि सरकार गुप्त आदेश जारी करती है, उदाहरण के लिए, किसी कृ त्रिम बुद्धिमत्ता प्लेटफॉर्म को अवरुद्ध करने या कृत्रिम बुद्धिमत्ता आउटपुट को सेंसर करने के लिए (राष्ट्रीय सुरक्षा का हवाला देते हुए), तो अनुराधा भसीन मामला इंगित करता है कि उन्हें भी सार्वजनिक जांच के लिए प्रकाशित किया जाना चाहिए, जब तक कि कोई संकीर्ण रूप से परिभाषित अपवाद न हो।

तृतीय, यह मामला अप्रत्यक्ष रूप से सूचना तक पहुँच से संबध रखता है। आधुनिक समय में, यह कृत्रिम बुद्धिमत्ता उपकरणों और ज्ञान तक पहुँच तक विस्तारित हो सकता है। उदाहरण के लिए, यदि कोई राज्य सुरक्षा चिंताओं का हवाला देते हुए एक कृत्रिम बुद्धिमत्ता शैक्षिक ऐप पर प्रतिबंध लगाता है, तो उपयोगकर्ता ज्ञान तक पहुँच के अपने अधिकार का आह्वान कर सकते हैं।

अनुराधा भसीन के फैसले के बाद 2020 में एक और फैसला आया दृ फाउंडेशन **फॉर मीडिया प्रोफेशनल्स बनाम जम्मू और कश्मीर केंद्र शासित प्रदेश,**[114] जहाँ सर्वोच्च न्यायालय ने कश्मीर में 4जी इंटरनेट को बहाल करने का सीधे तौर पर आदेश देने से इनकार कर दिया, लेकिन एक समीक्षा समिति का गठन किया। अंततः, लगभग 18 महीनों के बाद 2021 के शुरुआती दिनों में 4जी बहाल कर दिया गया। ये मामले न्यायालय के दूरस्थ दृष्टिकोण को दर्शाते हैं, भले ही तत्काल राहत नहीं दे पाते, लेकिन ऐसे सिद्धांतों की स्थापना करते है, जो कार्यकारी अतिरेक पर अंकुश लगाते हैं।

निगरानी और साइबर खतरे दृ पेगासस प्रकरण (2021)[115]

वर्ष 2021 में, यह आरोप लगाया गया कि इजरायली कंपनी एनएसओ समूह द्वारा विकसित एक परिष्कृत जासूसी सॉफ्टवेयर, पेगासस का उपयोग विपक्षी राजनेताओं, कार्यकर्ताओं और पत्रकारों सहित विभिन्न भारतीय नागरिकों के फोन को लक्षित करने के लिए किया गया था। इस खुलासे ने गैरकानूनी निगरानी के मुद्दे पर राष्ट्रीय स्तर पर आक्रोश उत्पन्न किया। कई याचिकाकर्ताओं ने सर्वोच्च न्यायालय का रुख किया, जिसके परिणामस्वरूप यह मामला पेगासस प्रकरण के नाम से जाना गया।[116] अक्टूबर 2021 में, सर्वोच्च न्यायालय ने आरोपों की गंभीरता और गोपनीयता तथा अभिव्यक्ति की स्वतंत्रता पर संभावित नकारात्मक प्रभाव को स्वीकार करते हुए, इस मामले की जांच के लिए एक स्वतंत्र विशेषज्ञ तकनीकी समिति का गठन किया।[117]

न्यायालय ने कुछ महत्वपूर्ण टिप्पणियाँ कीः न्यायालय ने कहा कि सरकार द्वारा मात्र ''राष्ट्रीय सुरक्षा'' का हवाला देने से न्यायपालिका मूक दर्शक नहीं बन सकती है, विशेष रूप से जब नागरिक मौलिक अधिकारों के उल्लंघन का आरोप लगाते हैं, न्यायालय ने इस बात पर जोर दिया कि संचार और डेटा की गोपनीयता को प्रभावित करने वाली निगरानी साक्ष्य–आधारित और कानूनी सीमाओं के भीतर होनी चाहिए। महत्वपूर्ण रूप से, सर्वोच्च न्यायालय ने समिति को न केवल पेगासस के उपयोग पर तथ्यों के अन्वेषण का

[114](2020) 5 एस सी सी 746

[115]मनोहर लाल शर्मा एवं अन्य बनाम भारत संघ, रिट याचिका (सीआरएल) सं 314/2021.,ए आई आर 2021 एसी 5396.

[116]अरून दिप, एप्पल अलर्ट के बाद भारतीय पत्रकारों के फोन में पेगासस संक्रमण पाया गयाः एमनेस्टी इंटरनेशनल, https://www.thehindu.com/news/national/pegasus-infection-found-on-indian-journalists-phones-after-apple-alert-amnesty-international/article67682427.ece, प्रकाशित दिनॉक–28 दिसम्बर 2023.

[117]एवीएस नम्बूदिरी, ऐतिहासिक पेगासस फैसलाः नागरिकों के अधिकारों को मान्यता देना, निगरानी को लेकर राज्य को चेतावनी देना, https://www.deccanherald.com/opinion/landmark-pegasus-verdict-acknowledging-citizens-rights-warning-state-over-surveillance-1045180.html, प्रकाशित दिनॉक–28 अक्टूबर 2021.

कार्य सौंपा, बल्कि निगरानी पर मौजूदा कानूनी प्रावधानों की समीक्षा करने और आधुनिक प्रौद्योगिकी के आलोक में गोपनीयता की सुरक्षा के लिए उनमें सुधार के तरीकों पर सुझाव देने का भी कार्य सौंपा। इस जनादेश में ''गोपनीयता का बेहतर अधिकार'' और ''बेहतर साइबर सुरक्षा और खतरों आकलन कर उपायों'' को सुनिश्चित करने के लिए कानूनों के अधिनियमन या संशोधन पर सिफारिशें करना शामिल था।[118]

पेगासस प्रकरण डिजिटल युग में निगरानी को संवैधानिक नियंत्रण में रखने में सर्वोच्च न्यायालय की सक्रिय रुचि को दर्शाता है। यद्यपि तकनीकी समिति की अंतिम रिपोर्ट (2022 में प्रस्तुत) पूरी तरह से सार्वजनिक नहीं की गई। इस मामले ने एक मिसाल कायम की कि सर्वोच्च न्यायालय साइबर निगरानी के लिए कार्यकारी जवाबदेही सुनिश्चित करने के लिए हस्तक्षेप कर सकता है। यह पहली बार है जब न्यायालय ने बेहतर साइबर सुरक्षा की आवश्यकता को गोपनीयता अधिकारों की सुरक्षा के साथ स्पष्ट रूप से जोड़ा, अनिवार्य रूप से यह स्वीकार करते हुए कि सरकारी हैकिंग न केवल गोपनीयता का उल्लंघन करती है बल्कि, कमजोरियों का फायदा उठाकर साइबर सुरक्षा को भी कमजोर करती है।

कृत्रिम बुद्धिमत्ता के संदर्भ में, पेगासस प्रकरण प्रासंगिक है क्योंकि सरकारें निगरानी के लिए कृत्रिम बुद्धिमत्ता–संचालित उपकरणों का उपयोग कर सकती हैं। सर्वोच्च न्यायालय यह संकेत दिए कि ऐसे उपयोगों को अधिकारों के साथ संतुलित किया जाना चाहिए। यदि कोई ऐसा मामला उठता है जहाँ एक कृत्रिम बुद्धिमत्ता प्रणाली पर्याप्त कानूनी आधार के बिना निजी संचार या सोशल मीडिया को स्कैन कर रही है, तो पेगासस और पुट्टस्वामी के सिद्धांत इसे चुनौती देने के लिए लागू होंगे। इसके अलावा, सरकार अब समिति की संभावित सिफारिशों के अधार पर जो भी कानून बनाती है, उसे स्वतंत्र निरीक्षण, आवश्यकता और आनुपातिकता जैसे नियंत्रण सुनिश्चित करने होंगे।

अन्य विशिष्ट मामले और विकास

कुछ अन्य न्यायिक और अर्ध–न्यायिक घटनाक्रम–:

•विस्मृति का अधिकार : कुछ उच्च न्यायालयों के निर्णयों में विस्मृति के अधिकार पर विचार किया गया है। यद्यपि ये सर्वोच्च न्यायालय के अंतिम निर्णय नहीं हैं, फिर भी वे इस दिशा में संभावित कानूनी रुझान को दर्शाते हैं। यदि कोई ऐसा मामला सर्वोच्च न्यायालय में प्रस्तुत होता है जिसमें विस्मृति के अधिकार की मांग की जाती है। उदाहरण के लिए, यदि कोई व्यक्ति यह अनुरोध करता है कि पुराने आपराधिक मुकदमे, जिनमें उसे निर्दोष घोषित किया गया था, उन्हें खोज इंजनों की सूची से हटा दिया जाए, तो न्यायालय को सूचना की स्वतंत्रता के साथ व्यक्तिगत गोपनीयता के अधिकार को संतुलित करना होगा।[119] वर्तमान में डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम के अस्तित्व को देखते हुए, न्यायालय डेटा संरक्षण बोर्ड या सरकार को इस विषय को उस कानूनी ढांचे के अंतर्गत संबोधित करने के लिए निर्देशित कर सकता है। कर्नाटक, गुजरात और ओडिशा के उच्च न्यायालयों ने कुछ परिस्थितियों में एक उभरते हुए विस्मृति के अधिकार को मान्यता दी है।[120] उदाहरण के लिए, **सुभ्रांशु राउत बनाम ओडिशा राज्य** मामले में ओडिशा उच्च न्यायालय ने एक महिला के लिए विस्मृति के अधिकार के महत्व को स्वीकार किया, अदालत के फैसले ने डिजिटल युग में ''भूल जाने के अधिकार'' के महत्व को उजागर किया, खासकर उन मामलों में जिनमें निजी और संवेदनशील जानकारी को अनधिकृत रूप से साझा किया जाता है। यह मामला व्यक्तियों को उनकी ऑनलाइन उपस्थिति के परिणामों से बचाने के लिए तंत्र की आवश्यकता को रेखांकित करता है, खासकर जब उनकी स्पष्ट छवियों को उनकी सहमति के बिना साझा किया जाता है।[121] वर्ष 2021 में, मद्रास उच्च न्यायालय ने, तथापि, एक दोषमुक्त व्यक्ति के नाम को निर्णय से हटाने की याचिका अस्वीकार कर दी। न्यायालय ने विधिक संरचना के अभाव का उल्लेख करते हुए यह राय व्यक्त की कि डेटा संरक्षण कानून की प्रतीक्षा करना अधिक समीचीन होगा।[122]

•मध्यवर्ती का दायित्व दृ मानहानिः सर्वोच्च न्यायालय उन मुकदमों की सुनवाई कर रहा है जिनमें यह प्रश्न अंतर्निहित है कि क्या भारतीय अदालतों द्वारा सामग्री हटाने का आदेश जारी किए जाने के पश्चात वैश्विक स्तर पर उस सामग्री को हटाने की आवश्यकता है। एक वाद में न्यायालय ने गूगल की दलील को खारिज करते हुए यह निर्णीत किया की, गूगल यह प्रदर्शित करने में विफल रहा कि उसने अधिसूचित होने के बावजूद अपमाजनक सामग्री को हटाने के लिए उचित सावधानी बरती थी, अतः वह धारा 79 में मध्यस्थ को मिलने वाले का दायी नहीं है।[123] **एएनआई मीडिया बनाम विकिमीडिया फाउंडेशन** के मामले में न्यायालय ने निर्धारित किया कि, विकिपीडिया को एएनआई के बारे में आपत्तिजनक और मानहानिकारक सामग्री को तुरंत हटाना होगा,

[118]पूर्वोक्त 127.

[119]श्री वसुनाथन बनाम रजिस्ट्रार जनरल कर्नाटक उच्च न्यायालय, 2017 एस सी सी आनलाईन कर्नाटक 420

[120]श्री वसुनाथन बनाम रजिस्ट्रार जनरल कर्नाटक उच्च न्यायालय, याचिका सं 62038,2016

[121]सुभ्रांशु राउत बनाम ओडिशा राज्य ,बीएलएपीएल 4592 ऑफ 2020.

[122]कार्तिक थियोड्रे बनाम रजिस्ट्रार जनरल मद्रास उच्च न्यायालय, याचिका सं. 12015 वर्ष 2021.

[123]गूगल इंडिया प्राइवेट लिमिटेड बनाम मेसर्स विशाखा इंडस्ट्रीज(2020) 4 एस सी सी 162.

विकिमीडिया धारा 79 के तहत पूरी तरह से ''सुरक्षित बंदरगाह'' का दावा नहीं कर सकता, क्योंकि किसी ऑनलाइन प्लेटफॉर्म को यदि मानहानिकारक सामग्री की जानकारी है और उसके पास उसे हटाने के साधन हैं, तो उसे हटाना होगा, अन्यथा उसकी जवाबदेही बढ़ेगी।[124] इस संबंध में अभी तक सर्वोच्च न्यायालय का कोई निश्चित न्यायिक निर्णय नहीं आया है, परन्तु कृत्रिम बुद्धिमत्ता के संदर्भ में समान प्रश्न यह है कि यदि कोई कृ त्रिम बुद्धिमत्ता चौटबॉट मानहानिकारक पाठ उत्पन्न करता है, तो क्या भारतीय अदालतें वैश्विक स्तर पर उस कृत्रिम बुद्धिमत्ता सेवा को भविष्य में ऐसी सामग्री उत्पन्न न करने का आदेश दे सकती हैं? ये तकनीकी व्यवहार्यता और न्यायिक क्षेत्राधिकार से जुड़े जटिल मुद्दे हैं।

•क्रिप्टोकरेंसी प्रतिबंध मामला (2020): इंटरनेट एंड मोबाइल एसोसिएशन ऑफ इंडिया बनाम भारतीय रिजर्व बैंक[125] के मामले में, सर्वोच्च न्यायालय ने भारतीय रिजर्व बैंक द्वारा जारी किए गए एक परिपत्र को निरस्त कर दिया था, जिसने प्रभावी रूप से बैंकों को क्रिप्टोकरेंसी एक्सचेंजों के साथ लेन–देन करने से प्रतिबंधित कर दिया था। न्यायालय ने आनुपातिकता के सिद्धांत को लागू किया (चूंकि भारतीय रिजर्व बैंक ने यह कदम मनी लॉन्ड्रिंग और उपभोक्ता हितों की हानि को रोकने के लिए उठाया था, परन्तु कम प्रतिबंधात्मक उपाय भी संभव थे)। यद्यपि यह मामला क्रिप्टोकरेंसी से संबंधित था, यह वित्त के क्षेत्र में उभरती हुई प्रौद्योगिकी के प्रति न्यायालय के दृष्टिकोण को दर्शाता है दृ स्पष्ट हानि के अभाव में पूर्ण प्रतिबंध न लगाना, और नवाचार का सम्मान करना। यह दृष्टिकोण अनुरूप रूप से कृत्रिम बुद्धिमत्ता पर भी लागू हो सकता है – न्यायालय कृत्रिम बुद्धिमत्ता प्रौद्योगिकी पर व्यापक प्रतिबंध को संशय की दृष्टि से देख सकता है (उदाहरण के लिए, यदि कोई व्यक्ति डीपफेक तकनीक पर एक काल्पनिक प्रतिबंध को चुनौती देता है, तो न्यायालय बारीकियों की मांग कर सकता हैः यदि वैकल्पिक उपाय मौजूद हैं तो तकनीक पर नहीं, बल्कि उसके दुरुपयोग पर प्रतिबंध लगाया जाए)।

•प्रतिस्पर्धा और डेटाः भारतीय प्रतिस्पर्धा आयोग ने भी डेटा और एल्गोरिथम आधारित मिलीभगत के मुद्दों पर ध्यान दिया है। वर्ष 2022 में, सीसीआई ने व्हाट्सएप की गोपनीयता नीति में किए गए परिवर्तनों की जांच का आदेश दिया, जिसमें प्रभुत्व के दुरुपयोग पर विचार किया गया। और उनकी 2021 की गोपनीयता नीति के लिए 213 करोड़ का जुर्माना लगाया।[126] यद्यपि यह प्रत्यक्ष रूप से कृत्रिम बुद्धिमत्ता का मामला नहीं है, फिर भी यह प्रासंगिक है क्योंकि प्रमुख कृत्रिम बुद्धिमत्ता प्लेटफॉर्म (जैसे क्लाउड कृत्रिम बुद्धिमत्ता प्रदाता) यदि वे डेटा से संबंधित उपभोक्ताओं के प्रति प्रतिस्पर्धा–विरोधी प्रथाओं या अनुचित शर्तों में संलग्न होते हैं तो जांच के दायरे में आ सकते हैं।

न्यायपालिका का दृष्टिकोण स्पष्ट है, वे डिजिटल परिदृश्य के अनुरूप संवैधानिक सिद्धांतों को अपनाने के लिए तत्पर हैं, व्यक्तिगत अधिकारों का समर्थन करते हैं और राज्य को अपने अतिक्रमणों को कठोरता से न्यायसंगत ठहराने की आवश्यकता पर बल देते हैं। हालाँकि, सर्वोच्च न्यायालय कुछ विशिष्ट उपायों की आवश्यकता को भी उचित महत्व देता है।

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के क्षेत्र में हितधारकों के लिए, इन न्यायिक निर्णयों का अर्थ है कि किसी भी कार्यवाही या नीति का मौलिक अधिकारों के आलोक में परीक्षण किया जाना चाहिए। गोपनीयता, अभिव्यक्ति की स्वतंत्रता और उचित प्रक्रिया जैसे विषय सदैव सामने आते हैं। साथ ही, ये मामले अक्सर साइबर खतरों और प्रौद्योगिकी के दुरुपयोग से निपटने की वैधता को भी स्वीकार करते हैं – वे **''कोई विनियमन नहीं''** का समर्थन नहीं करते हैं, बल्कि **''सावधानीपूर्वक और जवाबदेही के साथ विनियमन''** की वकालत करते हैं। यह न्यायिक दृष्टांत एक ऐसा ढाँचा प्रदान करता है जिसका पालन उभरते हुए कृत्रिम बुद्धिमत्ता नियमों द्वारा किए जाए, तथा संवैधानिक अधिकारों का सम्मान करते हुए प्रौद्योगिकी के लाभकारी उपयोगों को सक्षम बनाना है।

कानूनी ढांचे और न्यायिक परिदृश्य की जांच करने के पश्चात, अब हम उन विद्यमान और उभरती हुई चुनौतियों की पहचान कर सकते हैं जिनका सामना भारत को कृत्रिम बुद्धिमत्ता को प्रभावी ढंग से विनियमित करने और साइबर सुरक्षा सुनिश्चित करने में करना पड़ता है –

- **कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा शासन में उभरती चुनौतियाँ**

कानूनी ढाँचों और न्यायिक मार्गदर्शन में हुई प्रगति के बावजूद, कृत्रिम बुद्धिमत्ता, साइबर सुरक्षा और विधि के अंतर्संबंध पर महत्वपूर्ण चुनौतियाँ विद्यमान हैं। ये चुनौतियाँ मुख्य रूप से प्रौद्योगिकी के तीव्र विकास की गति से उत्पन्न होती हैं, जो विधायी प्रयासों से कहीं अधिक तेज है, साथ ही कृत्रिम बुद्धिमत्ता

[124] एएनआई मीडिया बनाम विकिमीडिया फाउंडेशन और अन्य,. दिल्ली उच्च न्यायालय, याचिका सं. 524,2024.

[125](2020) 10 एस सी सी 274.

[126]COMPETITION COMMISSION OF INDIA, Suo Motu Case No. 01 of 2021, Against: WhatsApp LLC , Meta Platforms, Inc. https://www.cci.gov.in/images/antitrustorder/en/order1732001619.pdf

प्रणालियों की अंतर्निहित जटिलता और अपारदर्शिता, तथा साइबर खतरों की वैश्विक प्रकृति भी इसमें योगदान करती है। यह खंड कई प्रमुख नवोदित चुनौतियों पर विचार करता है जिनका सामना भारत कृत्रिम बुद्धिमत्ता को शासित करने और साइबर सुरक्षा बनाए रखने के प्रयास में कर रहे हैं, विशेष रूप से कानूनी परिप्रेक्ष्य में।

एल्गोरिथम पूर्वाग्रह और उत्तरदायित्व

वैश्विक स्तर पर सर्वाधिक चर्चित विषयों में से एक यह है कि कृत्रिम बुद्धिमत्ता प्रणालियाँ अनजाने में प्रशिक्षण डेटा में मौजूद पूर्वाग्रहों को बनाए रख सकती है या उन्हें और भी प्रबल कर सकती है। कृत्रिम बुद्धिमत्ता में पूर्वाग्रह का मतलब है, नस्ल, लिंग या अन्य संरक्षित विशेषताओं के आधार पर कुछ समहों के साथ अनुचित या अन्यायपूर्ण व्यवहार करना, यह पूर्वाग्रह खुद को कई तरीकों से प्रकट कार सकता है, जैसे भेदभवपूर्ण भर्ती प्रथाएँ, पक्षपातपूर्ण ऋण स्वीकृति या स्वायत्त वाहनों द्वारा लिए गए घातक निर्णय। [127]

भारत के बहुलवादी समाज में, यह एक गंभीर चिंता का विषय है। उदाहरण के लिए, यदि किसी बैंक द्वारा ऋण पात्रता निर्धारण के लिए उपयोग की जाने वाली कृत्रिम बुद्धिमत्ता को मुख्य रूप से कुछ विशिष्ट शहरों के पुरुष आवेदकों के डेटा पर प्रशिक्षित किया जाता है, तो यह एक ऐसा मॉडल विकसित कर सकती है जो अनजाने में महिलाओं या ग्रामीण क्षेत्रों के व्यक्तियों को हानि पहुँचा सकता है। इसी प्रकार, चेहरे की पहचान करने वाली कृत्रिम बुद्धिमत्ता विश्व स्तर पर गहरे रंग की त्वचा वाले व्यक्तियों या महिलाओं के लिए उच्च त्रुटि दर वाली पाई गई है, क्योंकि प्रशिक्षण डेटासेट असंतुलित थे।[128] पुलिसिंग या निगरानी के संदर्भ में, ऐसी अशुद्धियाँ विशिष्ट समुदायों को अनुचित रूप से लक्षित या गलत पहचान का कारण बन सकती हैं। कानूनी दृष्टिकोण से, यह भेदभाव–विरोधी कानूनों और संवैधानिक समानता[129] तथा समान संरक्षण के सिद्धांतों के तहत प्रश्न उत्पन्न करता है। हालाँकि, वर्तमान में भारतीय कानून में एल्गोरिथम पूर्वाग्रह को संबोधित करने वाले विशिष्ट प्रावधानों का अभाव है। लेकिन सूचना प्रौद्योगिकी अधिनियम, 2000 और सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया अचार सहिंत)नियम, 2021 के दृष्टिगत प्रौद्योगिकी मत्रांलय भारत सरकार द्वारा परार्मश के मध्यम से सभी मध्यस्थों को आवश्यक सुक्षावों का अनुपालन किये जाने हेतु जारी कि गई है जिसमें सभी मध्यस्थों या मंच को यह सुनिश्चित करना चाहिए कि उनके कम्प्यूटर संसाधन किसी भी पूर्वाग्रह या भेदभाव की अनुमति नहीं देते है, जिसमें कृत्रिम बुद्धिमत्ता माडल,एल एल एम, जनरेटिव ए आई, सॉफ्टवेयर या एल्गारिदम का उपयोग शामिल है।[130] उदाहरण के लिए, कोई व्यक्ति कृत्रिम बुद्धिमत्ता से प्रभावित निर्णय को मनमाना या भेदभावपूर्ण कहकर चुनौती दे सकता है यदि वे यह प्रदर्शित कर सकें कि एल्गोरिथम पक्षपाती था।

कृत्रिम बुद्धिमत्ता निर्णयों के लिए उत्तरदायित्व एक महत्वपूर्ण पहलू है। जब कोई मानव अधिकारी निर्णय लेता है, तो उस व्यक्ति को उस निर्णय को उचित ठहराने के लिए कहा जा सकता है और यदि वह निर्णय गलत साबित होता है तो उसे जवाबदेह ठहराया जा सकता है। कृत्रिम बुद्धिमत्ता के मामले में, अक्सर न तो अंतिम उपयोगकर्ता और न ही निर्माता किसी विशिष्ट निर्णय के आधार को पूरी तरह से समझ पाते हैं। वर्तमान में, संवेदनशील अनुप्रयोगों में, ''मानव–इन–द–लूप'' दृष्टिकोण बनाए रखना उचित होगा , उदाहरण के लिए, एक कृत्रिम बुद्धिमत्ता नौकरी के लिए उम्मीदवारों को सूचीबद्ध करती है, लेकिन अंतिम निर्णय एक मानव द्वारा लिया जाता है। हालाँकि, जैसे–जैसे प्रणालियाँ अधिक स्वायत्तता की ओर बढ़ती हैं, हम उत्तरदायित्व कैसे सुनिश्चित करते हैं? एक उल्लेखनीय केस 2018 में उबर द्वारा विकसित एक सेल्फ–ड्राइविंग कार से जुड़ी घातक दुर्घटना है। कार ने स्वायत्त मोड में संचालन करते समय एक पैदल यात्री को टक्कर मार दी और उसकी मौत हो गई। जांच से पता चला कि प्रौद्योगिकी के डिजाइन में खामियां थीं और सुरक्षा उपाय अपर्याप्त थे। यह दुखद घटना कंपनियों को यह सुनिश्चित करने के लिए जवाबदेह ठहराने के महत्व को रेखांकित करती है।[131]

भारत में एक चुनौती यह है कि विभिन्न क्षेत्रों ने अभी तक एल्गोरिथम पारदर्शिता को अनिवार्य नहीं किया है। डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम व्यक्तियों को सुधार या मिटाने का अधिकार प्रदान

---

[127] Crawford K., Calo R., Barocas S., Beasley B., Friedler S., Kroll J. (2019). AI Now Report 2018. Retrieved from https://ainowinstitute.org/AI_Now_2018_Report.pdf

[128]George Benneh Mensah, "Artificial Intelligence and Ethics: A Comprehensive Reviews of Bias Mitigation, Transparency, and Accountability in AI Systems",https://www.researchgate.net/profile/George-Benneh-Mensah/publication/375744287_Artificial_Intelligence_and_Ethics_A_Comprehensive_Review_of_Bias_Mitigation_Transparency_and_Accountability_in_AI_Systems/links/656c8e46b86a1d521b2e2a16/Artificial-Intelligence-and-Ethics-A-Comprehensive-Review-of-Bias-Mitigation-Transparency-and-Accountability-in-AI-Systems.pdf

[129]अनुच्छेद 14, भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण,पृष्ठ सं–5.

[130]No.eNo.2(4)/2023-CyberLaws–3,Government of India Ministry of Electronics and Information Technology Cyber Law and Data Governance Group, प्रकाशित–15 मार्च 2024.

[131]रेबेका रीस और जो सोटाइल , "उबर सेल्फ–ड्राइविंग कार के परीक्षण चालक ने पैदल यात्री की मौत के मामले में खतरे में डालने का दोष स्वीकार किया", https://edition.cnn.com/2023/07/29/business/uber-self-driving-car-death-guilty,प्रकाशित–29 जुलाई 2023.

करता है,[132] लेकिन स्वचालित निर्णय की व्याख्या का अधिकार नहीं देता है। इसके अतिरिक्त, यदि कोई कृत्रिम बुद्धिमत्ता से क्षति पहुँचाती है– उदाहरण के लिए, यदि चिकित्सा निदान में उपयोग की जाने वाली कृत्रिम बुद्धिमत्ता त्रुटि करती है जिसके परिणामस्वरूप गलत उपचार होता है,तो रोगी उत्तरदायित्व की तलाश करेगा। क्या वे अस्पताल, डॉक्टर या कृत्रिम बुद्धिमत्ता सॉफ्टवेयर कंपनी पर मुकदमा करेंगे? पारंपरिक अपकृत्य कानून संभवतः अस्पतालएडॉक्टर पर दायित्व डालेगें क्योंकि उन्होंने उस उपकरण का उपयोग किया था और बदले में उनका विक्रेता के खिलाफ अनुबंध का दावा हो सकता है। लेकिन लापरवाही साबित करने के लिए यह दिखाना पड़ सकता है कि कृत्रिम बुद्धिमत्ता त्रुटिपूर्ण थी। कृत्रिम बुद्धिमत्ता की जटिलता को देखते हुए, यह वादियों के लिए एक कठिन कार्य हो सकता है। भारतीय उत्पाद दायित्व न्यायशास्त्र को डिजिटल उत्पादों तक विस्तारित करने में एक चुनौती है। उपभोक्ता संरक्षण अधिनियम 2019 और उत्पाद दायित्व पर इसके नियम संभावित रूप से एक कृत्रिम बुद्धिमत्ता प्रणाली को ''उत्पाद'' के रूप में मान सकते हैं और उपभोक्ताओं को नुकसान पहुँचाने वाले दोषों के लिए निर्माता को उत्तरदायी ठहरा सकते हैं।[133] लेकिन यह अभी भी अपरीक्षित है।

कानूनी ढांचे में नवीनीकरण की आवश्यकता है, जैसेः उच्च–जोखिम वाली कृत्रिम बुद्धिमत्ता प्रणालियों के लिए एल्गोरिथम प्रभाव आकलन की आवश्यकता है, तैनाती से पहले पूर्वाग्रह की जाँच, कृत्रिम बुद्धिमत्ता निर्णय कैसे लिए जाते हैं, इसका रिकॉर्ड रखने का आदेश (कृत्रिम बुद्धिमत्ता मॉडल ऑडिटिंग या दस्तावेजीकरण जैसी तकनीकों के माध्यम से), और देयता नियमों को स्पष्ट करना ,संभवतः कुछ कृत्रिम बुद्धिमत्ता उपयोगों के लिए सख्त देयता का एक रूप पेश करना दृ जैसे अपकृत्य कानून में अति–खतरनाक गतिविधियों के लिए सख्त देयता है। ये ऐसे क्षेत्र हैं जिन पर भारतीय नियामक विचार–विमर्श कर रहे हैं। उदाहरण के लिए, नीति आयोग ने जिम्मेदार कृत्रिम बुद्धिमत्ता दस्तावेजों में स्वैच्छिक पूर्वाग्रह ऑडिट का सुझाव दिया गया है ।[134]

डेटा गोपनीयता और कृत्रिम बुद्धिमत्ताः सहमति, पूर्ण गोपनीयता और डीपफेक

यद्यपि डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम[135] ने सहमति–आधारित डेटा व्यवस्था स्थापित की है, कृत्रिम बुद्धिमत्ता पारंपरिक नोटिस–और–सहमति मॉडल के लिए चुनौतियाँ प्रस्तुत करती है। कृत्रिम बुद्धिमत्ता प्रणालियाँ अक्सर विशाल डेटासेट से अंतदृष्टि प्राप्त करती हैं, और कभी–कभी ये सीधे व्यक्तियों से एकत्र नहीं किए जाते हैं, बल्कि कई स्रोतों से एकत्रित किए जाते हैं। मशीन लर्निंग जैसी तकनीकों के साथ, एक कृत्रिम बुद्धिमत्ता व्यक्तिगत डेटा का अनुमान लगा सकती है जो उपयोगकर्ता ने कभी स्पष्ट रूप से प्रदान नहीं किया था। उदाहरण के लिए, किसी व्यक्ति के सोशल मीडिया लाइक्स के पैटर्न का विश्लेषण करने से एक कृत्रिम बुद्धिमत्ता उनकी यौन अभिविन्यास या राजनीतिक विचारों की भविष्यवाणी कर सकती है दृ ऐसी जानकारी जो सीधे नहीं दी गई व इसलिए संग्रह के लिए भी सहमति नहीं दी गई।[136] यह घटना सहमति ढांचे पर दबाव डालती हैः व्यक्ति केवल अपसंस्कृत डेटा संग्रह (ू) के लिए सहमति दे सकते हैं, अनुमानों के लिए नहीं। डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम[137], सामान्य तौर पर ''व्यक्तिगत डेटा के प्रसंस्करण'' पर ध्यान केंद्रित करके, इन अनुमानों को भी व्यक्तिगत डेटा के रूप में शामिल करता है। लेकिन व्यावहारिक रूप से, कंपनियाँ व्युत्पन्न डेटा या गुमनाम डेटा (जिससे ये अनुमान आते हैं) को व्यक्तिगत डेटा नहीं मान सकती हैं। अधिनियम के गुमनाम डेटा के लिए सुरक्षा उपाय न्यूनतम हैं। इसलिए एक चुनौती यह सुनिश्चित करना है कि भारतीय उपयोगकर्ता डेटा पर प्रशिक्षित कृत्रिम बुद्धिमत्ता मॉडल अप्रत्यक्ष रूप से दी गई सहमति से परे गोपनीयता को कम न करें। कृत्रिम बुद्धिमत्ता के लिए डेटा गुमनामीकरण और साझाकरण को नियंत्रित करने के लिए मानकों या नियमों की आवश्यकता होगी, ताकि यह सुनिश्चित किया जा सके कि जिसे ''गुमनाम'' लेबल किया गया है, उसे वास्तव में कृत्रिम बुद्धिमत्ता का उपयोग करके फिर से पहचाना नहीं जा सकता है।[138]

एक अन्य गोपनीयता चुनौती बड़े पैमाने पर निगरानी बनाम लक्षित निगरानी है। कृत्रिम बुद्धिमत्ता बड़े पैमाने पर डेटा (जैसे सभी शहर के कैमरों से वास्तविक समय में सीसीटीवी फुटेज चेहरों के लिए) का विश्लेषण करने में सक्षम बनाती है। यह निगरानी की स्वीकार्य सीमा को आगे बढ़ाती है। वर्तमान कानून व

[132]धारा 12, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[133]धारा 82–87, उपभोक्ता संरक्षण अधिनियम, 2019.

[134]नीति आयोग रिर्पोट 2021, file:///E:/MietY%20Advisory/NITI%20Report%202021%20Responsible-AI-.pdf

[135]डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[136]राहुल कपूर एवं थेरेसा टी. कलाथिल , भारत में एआई विनियमनः वर्तमान स्थिति और भविष्य के परिप्रेक्ष्य, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/01/ai-regulation-in-india-current-state-and-future-perspectives, प्रकाशित–26 जनवरी 2024.

[137]पूवोक्त 142.

[138]अक्षय सुरेश व दृश्य कामथ,"आर्टिफिशियल इंटेलिजेंस में गोपनीयता और डेटा सुरक्षा",https://www.mondaq.com/india/data-protection/1556598/privacy-and-data-protection-in-artificial-intelligenceizdkf"kr,26 दिसम्बर 2024.

पुट्टस्वामी वाद[139] सिद्धांतों के तहत, निगरानी लक्षित और संदेह पर आधारित होनी चाहिए। यदि पुलिस हर समय हर किसी पर नजर रखने के लिए कृत्रिम बुद्धिमत्ता का उपयोग करना शुरू कर देती है, तो क्या यह अप्रत्यक्ष रूप से गोपनीयता का उल्लंघन है? अदालतों ने अभी तक ऐसे परिदृश्य पर फैसला नहीं सुनाया है। एक विशिष्ट कानून के अभाव में, पुलिस ऐसा प्रयोग कर सकती है। सीमाएं निर्धारित करना संभवतः न्यायपालिका या भविष्य के गोपनीयता न्यायशास्त्र पर निर्भर करेगा। कुछ क्षेत्राधिकार (जैसे यूरोपीय संघ का मसौदा कृत्रिम बुद्धिमत्ता अधिनियम) न्यायिक प्राधिकरण के साथ गंभीर खतरों को छोड़कर कानून प्रवर्तन के लिए सार्वजनिक स्थानों पर वास्तविक समय में दूरस्थ बायोमेट्रिक पहचान पर प्रतिबंध लगाने का प्रस्ताव करते है।[140] भारत में अभी तक ऐसा कोई नियम नहीं है, इसलिए यह एक खुली चुनौती है।

डीपफेक और गलत सूचनाः डीपफेक से तात्पर्य एक ऐसी तकनीक से है, जो कृत्रिम बुद्धिमत्ता का उपयोग करके वीडियो, ऑडियो या चित्रों को इस प्रकार से परिर्वत्ति कर देती है की वे वास्तविक लगते हैं।[141] कृत्रिम बुद्धिमत्ता की अति–यथार्थवादी नकली चित्र, वीडियो और ऑडियो उत्पन्न करने की क्षमता गोपनीयता, प्रतिष्ठा और सार्वजनिक व्यवस्था के लिए गंभीर परिणाम हो सकते है। डीपफेक पोर्नोग्राफी, गोपनीयता और विशेष रूप से गरिमा का घोर उल्लंघन है अक्सर महिलाओं को बिना सहमति के स्पष्ट सामग्री पर चेहरे प्रत्यारोपण करके लक्षित किया जाता है। वर्तमान कानूनी उपायों में सूचना प्रौद्योगिकी अधिनियम की धारा 67ए67।[142] और भारतीय न्याय संहिता के प्रावधान जैसे महिला की शालीनता का अपमान करना शामिल हैं।[143] हालाँकि, कानून में स्पष्ट रूप से डीपफेक का उल्लेख नहीं है, लेकिन अनुच्छेद 21[144], डीपफेक का अनधिकृत निर्माण गोपनीय के अधिकार का उल्लंघन है। डीपफेक के निर्माण को विशेष रूप से अपराधीकरण करने के लिए कानूनों को अद्यतन करने की आवश्यकता है। भारत ने मध्यवर्ती दायित्व (पहचान होने पर डीपफेक को तुरंत हटाने के लिए प्लेटफार्मों को जिम्मेदार बनाना) और कुछ उपयोगों को अपराधीकरण करने के संयोजन पर ध्यान केंद्रित किया है।[145] हमने 2024, के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के परामर्श देखे, वे कृत्रिम बुद्धिमत्ता–जनित सामग्री की अनिवार्य लेबलिंग के लिए पहला प्रयास थे।[146] ये अनिवार्य रूप से एक नियम को इंगित करते हैं कि डीपफेक को वॉटरमार्क या लेबल किया जाना चाहिए। यह भविष्य में डिजिटल इंडिया एक्ट या सूचना प्रौद्योगिकी अधिनियम के नियमों के तहत एक नियम बनाया जा सकता है।

कृत्रिम बुद्धिमत्ता के माध्यम से गलत सूचनादृ कृत्रिम बुद्धिमत्ता बड़े पैमाने पर नकली समाचार उत्पन्न कर सकती है, संभावित रूप से पूरी नकली पहचान या वेबसाइटें भी स्वतः उत्पन्न कर सकती है। साइबर सुरक्षा के लिए चुनौती यह है कि इसे सूचना युद्ध में या हिंसा भड़काने के लिए हथियार बनाया जा सकता है उदाहरण के लिए, एक सार्वजनिक व्यक्ति का भड़काऊ भाषण देते हुए डीपफेक वीडियो अशांति पैदा कर सकता है। कानूनी रूप से, भारत में उकसाने और झूठी अफवाहों के खिलाफ कानून हैं।[147] लेकिन प्रवर्तन तब मुश्किल हो जाता है, जब मूल निर्माता प्रौद्योगिकी के पीछे छिप जाते हैं। सरकार का दृष्टिकोण मूल प्रवर्तक का पता लगाने की क्षमता को मजबूत करना रहा है। मध्यवर्ती नियम, 2021 के अनुसार **महत्वपूर्ण संदेश प्लेटफार्मों** को आदेश दिए जाने पर संदेशों के मूल प्रवर्तकों का पता लगाने में सक्षम होना आवश्यक है। गोपनीयता (एन्क्रिप्शन) और नकली समाचारों को खोज करने के बीच तनाव अनसुलझा है। कृत्रिम बुद्धिमत्ता नकली सामग्री को अधिक तेजी से फैलने वाला बनाकर स्थिति को और खराब कर सकता है। इसलिए कानूनी प्रणाली को नई तकनीकों या संभवतः ऐसे कानून के साथ अनुकूलित करना होगा जो जानबूझकर बड़े पैमाने पर धोखे के लिए कुछ कृत्रिम बुद्धिमत्ता को तैनात करने के लिए दंडित करें है।

साइबर सुरक्षा खतरे और कानूनी तत्परता

कृत्रिम बुद्धिमत्ता, खतरे के परिदृश्य को बदल रही है, लेकिन क्या कानूनी प्रणाली इसके लिए तैयार है ? **स्वायत्त साइबर हथियारों** पर विचार करें – मैलवेयर[148] जो कृत्रिम बुद्धिमत्ता का उपयोग करके फैल सकता है और अनुकूलित हो सकता है। यदि कोई राज्य या गैर–राज्य ऐसा हथियार जारी करता है, तो क्या हमारे पास प्रतिक्रिया देने के लिए पर्याप्त कानूनी उपकरण हैं? घरेलू स्तर पर, हाँ, ऐसा कृत्य (नुकसान पहुँचाना, आदि)

---

[139]पूवोक्त,12. एआईआर 2017 एससीसी 416.

[140]EU AI Act, Article 5: Prohibited AI Practices , https://artificialintelligenceact.eu/article/5/.

[141]जे सॉटेल रिक्सन, डीपफेक क्या है ?, https:?//builtin.com/machine-learning/deepfake.

[142]सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–37.

[143]धारा 79, भारतीय न्याय संहिता, 2023, प्रकाशक–कमल पब्लिशर्स, द्विभाषी संस्करणए पृष्ठ सं–31, ISBN NO.978-93-92295-27-0.

[144]अनुच्छेद 21, भारत का संविधान, आलिया लॉ एजेंसी, द्विभाषी संस्करण, पृष्ठ सं–26.

[145]सूचना प्रौद्योगिकी(मध्यावर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता)नियम,2021

[146]https://regmedia.co.uk/2024/03/04/meity_ai_advisory_1_march.pdf.

[147]धारा 192, 353, भारतीय न्याय संहिता, 2023

[148] मैलवेयर–दुर्भावनापूर्ण सॉफ्टवेयर का संक्षिप्त रूप है, जो जानबूझकर कंप्यूटर सिस्टम, नेटवर्क या उपकरणों को नुकसान पहुंचाने, बाधित करने या अनधिकृत पहुंच प्राप्त करने के लिए डिजाइन किया गया कोई भी सॉफ्टवेयर है , https://www.mcafee.com/en-in/antivirus/malware.html

आपराधिक है[149], लेकिन आरोपण असंभव हो सकता है या भारतीय क्षेत्राधिकार से परे विदेशी संस्थाओं से सम्बधित हो सकता है। यह अंतर्राष्ट्रीय कानून और सहयोग की ओर झुकता है। भारत को साइबर युद्ध और कृत्रिम बुद्धिमत्ता पर अंतर्राष्ट्रीय नियम–निर्माण में शामिल होने की आवश्यकता हो सकती है (भारत आईसीटी सुरक्षा पर संयुक्त राष्ट्र के ओपन–एंडेड वर्किंग ग्रुप का हिस्सा है, जो साइबरस्पेस में राज्य के व्यवहार के मानदंडों पर चर्चा कर रहा है)।[150] घरेलू स्तर पर, हमारे कानून व्यक्तियों को दंडित करते हैं, लेकिन क्या होगा यदि एक कृत्रिम बुद्धिमत्ता बॉटनेट बिना किसी स्पष्ट मानव अपराधी के नुकसान पहुँचाता हैदृ क्या हम उसे एक दुर्घटना मानगें ? विश्व स्तर पर एक उभरता हुआ विचार है कि कुछ कृत्रिम बुद्धिमत्ता विफलताओं को उसी तरह माना जाए जैसे हम औद्योगिक दुर्घटनाओं को मानते हैंदृ आपराधिक दोषारोपण के बजाय बीमा और मुआवजा योजनाओं के माध्यम से, खासकर जब कोई इरादा शामिल न हो।

कृत्रिम बुद्धिमत्ता के साथ एक चुनौती **महत्वपूर्ण बुनियादे ढॉचे का संरक्षण** भी है। जैसे–जैसे हमारी बिजली, परिवहन और वित्तीय प्रणालियाँ दक्षता के लिए अधिक कृत्रिम बुद्धिमत्ता का उपयोग करती हैं जैसे–स्मार्ट ग्रिड, स्वायत्त ट्रेन नियंत्रण, एल्गोरिथम ट्रेडिंग, एक साइबर हमला या खराबी विनाशकारी हो सकती है। आईटी अधिनियम की धारा 70[151] जैसे कानून महत्वपूर्ण प्रणालियों को नामित करते हैं और उनसे छेड़छाड़ करने पर सजा का प्रवधान करता हैं, लेकिन यह सुनिश्चित करना कि क्रिटिकल इन्फॉर्मेशन इन्फ्रास्ट्रक्चर (सीआईआई) चलाने वाली कंपनियाँएसरकार सर्वोत्तम साइबर सुरक्षा प्रथाओं का पालन करें, एक चुनौती है। मौजूदा राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (छब्प्च्ब्) और भारतीय कंप्यूटर आपात मोचन दल (ब्म्त्ज्.प्द) के निर्देश काफी हद तक नीति–स्तर के हैं। हमें महत्वपूर्ण अवसंरचना में कृत्रिम बुद्धिमत्ता सुरक्षा मानकों को अनिवार्य करने वाले अधिक क्षेत्र–विशिष्ट नियमों की आवश्यकता हो सकती है, जैसे कृत्रिम बुद्धिमत्ता–नियंत्रित प्रणालियों के लिए मजबूत फेल–सेफ की आवश्यकता, अतिरेक की आवश्यकता (यदि कृत्रिम बुद्धिमत्ताविफल हो जाती है, तो मैनुअल ओवरराइड मौजूद हो), आदि। ये कानूनी मानकों की तुलना में अधिक इंजीनियरिंग मानक हैं, लेकिन कानून द्वारा अनिवार्य किए जा सकते हैं।

सीमा पार डेटा प्रवाह और क्षेत्राधिकारः कृत्रिम बुद्धिमत्ता सेवाएं अक्सर क्लाउड–आधारित होती हैं, जिसका अर्थ है कि डेटा सीमाओं के पार प्रवाहित होता है। डीपीपीडी अधिनियम वर्तमान में डिफॉल्ट रूप से सभी देशों को सीमा पार डेटा हस्तांतरण की अनुमति देता है, सिवाय संभावित प्रतिबंधित के।[152] यदि भारत बाद में संवेदनशील व्यक्तिगत डेटा को अपनी सीमाओं से बाहर जाने से प्रतिबंधित करने का निर्णय लेता है, तो यह वैश्विक कृत्रिम बुद्धिमत्ता कंपनियों के संचालन को प्रभावित कर सकता। क्षेत्राधिकार के लिहाज से, यदि भारत में कोई भौतिक उपस्थिति न होने वाली कृत्रिम बुद्धिमत्ता कंपनी भारतीयों को नुकसान पहुँचाती है, तो उन्हें जवाबदेह ठहराने की हमारी कानूनी क्षमता सीमित है। हमारे पास साइबर अपराध के लिए एमएलएटी (पारस्परिक कानूनी सहायता संधियाँ) हैं।[153] लेकिन सभी देश साइबर मुद्दों पर समान रूप से सहयोग नहीं करते हैं, खासकर राज्य अभिकर्ताओं या ग्रे जोन से जुड़े मामलों में।[154] यह विदेशी नीति साइबर कूटनीति के लिए एक चुनौती है, लेकिन यह कानूनी परिणामों को प्रभावित करती है।

प्रवर्तन और क्षमता अवरोध

सबसे अच्छे कानूनों का भी प्रभावी प्रवर्तन के बिना कोई मतलब नहीं है। भारत को कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा जैसे अत्यधिक तकनीकी क्षेत्रों में क्षमता की कमी का सामना करना पड़ता है। पुलिस और नियामक एजेंसियों को कृत्रिम बुद्धिमत्ता से संबंधित घटनाओं की जांच करने के लिए तकनीकी विशेषज्ञता की आवश्यकता होती है, चाहे वह डीपफेक अपराध हो या जटिल डेटा उल्लंघन। साइबर घटनाओं की संख्या बहुत अधिक है भारतीय कंप्यूटर आपात मोचन दल ने कुछ वर्षों में दस लाख से अधिक घटनाओं की सूचना दी।[155] कृत्रिम बुद्धिमत्ता के साथ, घटना की मात्रा और बढ़ सकती है स्वचालित हमले एक बड़े हमले के बजाय हजारों छोटी घटनाओं का कारण बन सकते हैं। जांच और न्यायिक क्षमता को बढ़ाना चूनौतीपूर्ण है। विशेष साइबर

[149]धारा 43(C), धारा 66, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–24,32.

[150]https://ccgnludelhi.wordpress.com/2021/12/28/cyber-security-at-the-un-where-does-india-stand-part-1/.

[151]धारा 70, सूचना प्रौद्योगिकी अधिनियम, 2000, प्रकाशक–युनिवर्सल लॉ पब्लिशर्स,द्विभाषी संस्करण,प्रतिस्थापित–27-10-2009, पृष्ठ सं–38.

[152]अध्याय 4, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[153]GUIDELINES ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS, Ministryofhomeaffairs,https://www.mha.gov.in/sites/default/files/ISII_ComprehensiveGuidelines_17122019.pdf

[154]यशस्वी कुमार और लक्ष्य सुखीजा, पारस्परिक कानूनी सहायता संधि और भारतः एक व्यापक विश्लेषण, Indian Journal of Law and Legal Research,https://www.ijllr.com/post/mutual-legal-assistance-treaty-and-india-a-comprehensive-analysis

[155]तनुश्री बसुरॉय, Breakdown of security incidents handled by CERT-In India 2022, https://www.statista.com/statistics/1428463/india-security-incidents-handled-by-cert-in/, प्रकाशित–16 सितम्बर 2024.

फोरेंसिक प्रयोगशालाओं और कानून प्रवर्तन के लिए प्रशिक्षण को बढ़ाया जा रहा है, लेकिन तकनीकी प्रगति की गति का अर्थ है कि निरंतर परिशोधन।

न्यायपालिका को भी तकनीकी साक्ष्यों को समझने में चुनौतियों का सामना करना पड़ेगा। साइबर मामलों में, अदालतें विशेषज्ञों की गवाही और डिजिटल साक्ष्यों पर निर्भर करती हैं। भारतीय साक्ष्य अधिनियम[156] में सन् 2000 में डिजिटल साक्ष्यों की अनुमति देने के लिए संशोधन किया गया था, और सर्वोच्च न्यायालय ने **अर्जुन पंडित राव कोतकर बनाम कैलाश गोरंट्याल (2020)**[157] में उन आवश्यकताओं को परिष्कृत किया। लेकिन कृत्रिम बुद्धिमत्ता के साथ, साक्ष्यों में एल्गोरिथम आउटपुट शामिल हो सकते हैंदृ ऐसी चीजें जो अदालत में आसानी से व्याख्या योग्य नहीं हैं। भविष्य में ऐसी वादों की कल्पना की जा सकती है जहाँ एक पक्ष पूर्वाग्रह या त्रुटि साबित करने के लिए कृत्रिम बुद्धिमत्ता के स्रोत कोड या मॉडल के निरीक्षण करने की मांग करता है। अदालतों को यह तय करना होगा कि ऐसे अनुरोधों को कैसे संभाला जाए। हमें एल्गोरिथम के लिए खोज नियमों के समान नए प्रावधानों की आवश्यकता हो सकती है।

इसके अतिरिक्त, डीपीपीडी अधिनियम[158] के तहत स्थापित होने वाले डेटा संरक्षण बोर्ड[159] को संभावित रूप से हजारों शिकायतों का सामना करना पड़ेगा। यदि उनमें से कई में डेटा के कृत्रिम बुद्धिमत्ता उपयोग शामिल हैं, तो बोर्ड के कर्मचारियों को मामलों में न्याय करने के लिए कृत्रिम बुद्धिमत्ता प्रक्रियाओं को समझने की आवश्यकता होगी। जैसे यदि कोई शिकायतकर्ता कहता है कि, एक कृत्रिम बुद्धिमत्ता ने मेरी सहमति से बिना मेरे डेटा का उपयोग किया, तो क्या यह सच था या नहीं?। इस प्रकार संस्थागत क्षमता निर्माण एक महत्वपूर्ण चुनौती है।

नवाचार और विनियमन में सन्तुलन

इन सभी चुनौतियों के पीछे नीतिगत दुविधा यह है कि लाभकारी कृत्रिम बुद्धिमत्ता नवाचार को कैसे प्रोत्साहित किया जाए, जो जोखिमों को कम कर अधिकारों की रक्षा करते हुए आर्थिक विकास और सामाजिक भलाई को बढ़ावा दे सकतें हैं। अत्यधिक विनियमन स्टार्टअप को रोक सकता है और निवेश को दूर भगा सकता है, जबकि कम विनियमन नुकसान और सार्वजनिक प्रतिक्रिया का कारण बन सकता है जो अंततः नवाचार को भी नुकसान पहुंचाता है। भारत का दृष्टिकोण अब तक नवीन कृत्रिम बुद्धिमत्ता उद्योग के बारे में सतर्क रहा है। भारत के पास अपने सूचना प्रौद्योगिकी प्रतिभा के साथ तुलनात्मक लाभ है, जैसा कि कुछ लोगों ने कहा है कि यह दुनिया के लिए ''कृत्रिम बुद्धिमत्ता गैराज'' बन सकता है।[160]

इस प्रकार, विधि निर्माताओं के लिए एक चुनौती यह है कि वे ऐसे नियम बनाएं जो यथासंभव निर्देशात्मक होने के बजाय लचीले और सिद्धांत–आधारित हों। उदाहरण के लिए, विशेष कृत्रिम बुद्धिमत्ता उप–प्रौद्योगिकियों पर प्रतिबंध लगाने के बजाय, परिणामों पर ध्यान केंद्रित करें, जैसे कि ऐसे उपयोगों पर प्रतिबंध लगाना जो कुछ नुकसान पहुंचाते हैं। 2024 में सूचना प्रौद्योगिकी मंत्रालय सलाह (संशोधित) ने ऐसा ही दृष्टिकोण अपनायाः इसने एल्गोरिदम को स्वयं नियंत्रित करने पर जोर नहीं दिया, बल्कि गैरकानूनी सामग्री को रोकने और गलत आउटपुट को लेबल करने पर जोर दिया।[161] सैंडबॉक्सिंग और परीक्षण विनियामक[162] व्यवस्थाएं रणनीति हो सकती हैं, उसी तरह जैसे भारत में फिनटेक सैंडबॉक्स या ड्रोन नीति ने शुरू में काम किया था।

संक्षेप में, भारत में कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा प्रशासन के लिए उभरती चुनौतियाँ हैं। कृत्रिम बुद्धिमत्ता प्रणालियों में निष्पक्षता, जवाबदेही और पारदर्शिता सुनिश्चित करना, गोपनीयता की रक्षा करना और डीपफेक जैसे दुर्भावनापूर्ण उपयोगों को रोकना, कृत्रिम बुद्धिमत्ता सम्बन्धित खतरों के खिलाफ साइबर सुरक्षा को मजबूत करना और नवाचार को बाधित किए बिना कानूनों को लागू एक कठिन कार्य है। इन चुनौतियों के लिए गतिशील और सूक्ष्म समाधानों की आवश्यकता है। इनमें से कई मुद्दे भारत के लिए अद्वितीय नहीं हैं, वे प्रकृति में वैश्विक हैं। इसलिए यह जांचना शिक्षाप्रद है कि, अन्य क्षेत्राधिकार एआई और साइबर सुरक्षा के लिए कैसे दृष्टिकोण अपना रहे हैं, ताकि अंतर्दृष्टि और तुलनात्मक दृष्टिकोण प्राप्त हो सकें जो भारत के आगे के मार्ग को सूचित कर सकें।

---

[156]धारा 63(65B), भारतीय साक्ष्य अधिनियम, 2023,(प्रतिस्थापित–01–07–2024)

[157]ए आई आर 2020 एस सी 4908.

[158]डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[159]धारा 18, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[160]ए. शाजी जॉर्ज, India's Ascent as the Global Epicenter of Artificial Intelligence, Partners Universal Innovative Research Publication (PUIRP), Volume: 02 Issue: 01, January-February 2024, www.puirp.com

[161]अक्षय सुरेश और नीरजा शंकर, एआई मॉडलों की तैनाती पर संशोधित MeitY सलाह,प्रकाशित–25 अप्रैल 2024 https://www.lexology.com/library/detail.aspx?g=adbe9168-1b7a-4cc0-aa72-090e7dde14f3

[162]सैंडबॉक्सिंग और परीक्षण विनियामक– विनियामक सैंडबॉक्स एक ऐसा उपकरण है जो इस बारे में साक्ष्य विकसित करता है कि कोई नया उत्पाद, तकनीक या व्यवसाय मॉडल (नवाचार) कैसे काम करता है और इसके क्या परिणाम निकलते हैं। सेना लेजगिओग्लू ओजर, एआई में विनियामक सैंडबॉक्स नवाचार और सुरक्षा के बीच कार्य करते हैं, https://digi-con.org/regulatory-

तुलनात्मक वैश्विक कानूनी परिदृष्य

भारत समय के साथ कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के प्रति अपने दृष्टिकोण को परिष्कृत कर रहा है, एसे में अन्य न्यायक्षेत्रों पर विचार करना मूल्यवान संदर्भ प्रदान करता है। विभिन्न देशों और क्षेत्रों ने कई तरह की रणनीतियाँ अपनाई हैं– व्यापक कानून से लेकर उद्योग स्व–नियमन तक – जो उनकी कानूनी प्रणालियों और नीति प्राथमिकताओं को दर्शाती हैं। यह खंड यूरोपीय संघ, संयुक्त राज्य अमेरिका और अन्य उल्लेखनीय अधिकार क्षेत्रों (जैसे चीन और अंतर्राष्ट्रीय ढांचे) पर ध्यान केंद्रित करते हुए एक संक्षिप्त तुलनात्मक अवलोकन प्रस्तुत करता है, ताकि यह समझा जा सके कि वे कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा की चुनौतियों से कैसे निपट रहे हैं। ये तुलनाएँ सर्वोत्तम प्रथाओं और संभावित खर्तरों को समझने में मदद करेंगी जो भारत की नीति और नियामक विकल्पों का मार्गदर्शन कर सकती हैं।

यूरोपीय संघः व्यापक विनियमन (जीडीपीआर और प्रस्तावित कृत्रिम बुद्धिमत्ता अधिनियम)

तकनीकी नियमों के निर्माण में यूरोपीय संघ प्रायः अग्रणी रहा है, जहाँ मौलिक अधिकारों और उपभोक्ता संरक्षण को प्राथमिकता दी जाती है। वर्ष 2018 में लागू हुआ यूरोपीय संघ का **सामान्य डेटा संरक्षण विनियमन (जीडीपीआर)**[163] डेटा सुरक्षा के लिए एक वैश्विक मानक के रूप में उभरा है। भारत के डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (डीपीपीडी अधिनियम) के कई प्रावधान जीडीपीआर के सिद्धांतों को प्रतिबिंबित करते हैं – उदाहरण के लिए, प्रसंस्करण के लिए वैध आधार, डेटा विषय के अधिकार (अभिगम, सुधार, मिटाना), और डेटा नियंत्रक की जवाबदेही।[164] जीडीपीआर स्वचालित निर्णय लेने के मुद्दे को भी स्पष्ट रूप से संबोधित करता हैः **अनुच्छेद 22** व्यक्तियों को ऐसे निर्णयों के अधीन न होने का अधिकार प्रदान करता है जो पूर्णतः स्वचालित प्रसंस्करण पर आधारित होते हैं और जिनका कानूनी या समान रूप से महत्वपूर्ण प्रभाव होता है, कुछ विशिष्ट अपवादों के साथ (जैसे, स्पष्ट सहमति या अनुबंध के लिए आवश्यक होना, जिसमें मानव समीक्षा जैसे सुरक्षा उपाय शामिल हों)।[165] भारत के डीपीपीडी अधिनियम में अभी तक कोई समतुल्य प्रावधान मौजूद नहीं है, जिसका अर्थ है कि यूरोपीय संघ के नागरिकों के पास विशुद्ध रूप से स्वचालित निर्णयों को चुनौती देने के लिए एक अधिक स्पष्ट मार्ग उपलब्ध है। यह एक ऐसा पहलू हो सकता है जिस पर भारत भविष्य के संशोधनों या नियमों में विचार कर सकता है, विशेष रूप से जब स्वचालित प्रोफाइलिंग एक सामान्य प्रक्रिया बनती जा रही है।

यूरोपीय संघ एक समर्पित कृत्रिम बुद्धिमत्ता विनियमन की दिशा में अग्रसर है। यूरोपीय संघ का कृ त्रिम बुद्धिमत्ता अधिनियमदृ जून 2024 में, यूरोपीय संघ ने कृत्रिम बुद्धिमत्त पर दुनिया के पहले नियमों को अपनाया। कृत्रिम बुद्धिमत्ता अधिनियम लागू होने के 24 महीने बाद 2 अगस्त 2026 से पूरी तरह से लागू हो जाएगा, लेकिन कुछ हिस्से पहले भी लागू होंगे।[166] कृत्रिम बुद्धिमत्ता प्रणालियों को अस्वीकार्य जोखिम पैदा करने वाली कृत्रिम बुद्धिमत्ता प्रणालियों पर प्रतिबंध 2 फरवरी 2025 से लागू होना शुरू हो गए है, **उच्च–जोखिम** की अनुमति कठोर शर्तों के अधीन दि गई है, **सीमित जोखिम** को पारदर्शिता संबंधी दायित्वों के साथ दिया गया है, उदाहरण के लिए, बॉट्स[167] को अपनी पहचान बतानी होगी। उच्च–जोखिम वाली कृत्रिम बुद्धिमत्ता प्रणालियों, जैसे महत्वपूर्ण अवसंरचना, रोजगार संबंधी निर्णय, क्रेडिट स्कोरिंग, कानूनी प्रणालियाँ आदि में उपयोग की जाने वाली को अनुरूपता आकलन, लॉगिंग, उपयोगकर्ताओं के लिए पारदर्शिता, मानवीय देखरेख, और मजबूत सटीकता एवं साइबर सुरक्षा मानकों जैसी आवश्यकताओं का पालन करना होगा।[168] ऐसी कृत्रिम बुद्धिमत्ता के निर्माताओं या प्रदाताओं को उन्हें यूरोपीय संघ के एक डेटाबेस में पंजीकृत करना होगा। यूरोपीय संघ का कृत्रिम बुद्धिमत्ता अधिनियम **सामान्य प्रयोजन कृत्रिम बुद्धिमत्ता** (जीपीएआई), जैसे बड़े भाषा मॉडल (चौटजीपीटी), के लिए भी दायित्वों पर विचार करता है।[169]

भारत के लिए, यूरोपीय संघ का मॉडल एक संभावित व्यापक मार्ग प्रदर्शित करता है। यदि भारत यूरोपीय संघ का अनुसरण करता है, तो वह भविष्य में अनुकूलित नियमों के साथ कृत्रिम बुद्धिमत्ता का वर्गीकरण लागू कर सकता है। हालाँकि, यूरोपीय संघ का कठोर दृष्टिकोण उसकी मूल्य प्रणाली और आर्थिक संदर्भ से उत्पन्न हुआ है। भारत, एक प्रगतिशील आईटी उद्योग और कई छोटे कृत्रिम बुद्धिमत्ता स्टार्टअप के

[163]REGULATION (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[164]https://www.taxmann.com/post/blog/dpdp-act-vs-eu-gdpr-compliance#7, अंतिम अपडेट –4 मई 2025.

[165]Article 22, General Data Protection Regulation (GDPR), REGULATION (EU) 2016/679 , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[166]Article 113, Artificial Intelligence(AI Act), Regulation (EU) 2024/1689 , http://data.europa.eu/eli/reg/2024/1689/oj

[167]बॉट्स ऐसे सॉफ्टवेयर अनुप्रयोग हैं जिन्हें स्वचालित कार्य करने के लिए डिजाइन किया गया है, जो अक्सर ऑनलाइन मानवीय गतिविधियों की नकल करते हैं, https://entro.security/glossary/bot-identity/

[168]Article 6, Regulation (EU) 2024/1689, http://data.europa.eu/eli/reg/2024/1689/oj

[169]Article 53, Regulation (EU) 2024/1689, http://data.europa.eu/eli/reg/2024/1689/oj

साथ, यूरोपीय संघ–शैली की व्यवस्था के अनुपालन बोझ को भारी महसूस कर सकता है।[170] फिर भी, कुछ अवधारणाओं को भावना में अपनाया जा सकता हैः उदाहरण के लिए, महत्वपूर्ण कृत्रिम बुद्धिमत्ता उपयोग–मामलों की पहचान करना जिन्हें निरीक्षण की आवश्यकता है, जैसे–डेटा के लिए डीपीपीडी अधिनियम के तहत ''महत्वपूर्ण डेटा न्यासी''[171] की अवधारणा भविष्य के नियमों में ''महत्वपूर्ण कृत्रिम बुद्धिमत्ता प्रणाली'' के रूप में एक समानांतर अवधारणा हो सकती है। इसके अतिरिक्त, अधिकारों का उल्लंघन करने वाली कृत्रिम बुद्धिमत्ता –जैसे व्यवहार के आधार पर नागरिकों को श्रेणीबद्ध करने वाली सामाजिक स्कोरिंग प्रणाली, पर प्रतिबंध लगाने का यूरोपीय संघ का दृष्टिकोण शिक्षाप्रद है[172]– भारत भी ऐसे अत्यधिक उपयोगों को सक्रिय रूप से प्रतिबंधित कर सकता है जो संवैधानिक मूल्यों के साथ असंगत हैं।

एक अन्य प्रासंगिक यूरोपीय संघ एजेंसी, **यूरोपीय नेटवर्क और सूचना सुरक्षा एजेंसी** ;म्छै।द्ध के **नेटवर्क और सूचना सुरक्षा निर्देश** (छै2) 2022 है, जो विभिन्न क्षेत्रों में आवश्यक और महत्वपूर्ण संस्थाओं के लिए साइबर सुरक्षा दायित्वों को अद्यतन करता है। यह जोखिम प्रबंधन उपायों और घटना रिपोर्टिंग को अनिवार्य करता है।[173] जबकि भारत के **कंप्यूटर आपात मोचन दल** (ब्म्ज्.प्द) निर्देश एक समान कार्य करते हैं, नेटवर्क और सूचना सुरक्षा निर्देश की क्षेत्रीय व्यापकता और दंड भविष्य के भारतीय क्षेत्र–विशिष्ट नियमों के लिए एक खाका प्रस्तुत कर सकते हैं।

अंत में, यूरोप की परिषद ने कृत्रिम बुद्धिमत्ता, मानवाधिकार और लोकतंत्र और कानून के शासन पर , एक कन्वेंशन को अतिंम रूप दे दिया है। जिसे 17 मई, 2024 को अपनाया गया था और 5 सितंबर, 2024 से हस्ताक्षर के लिए सभी देशों के लिए खुला गया है। यह मुख्य रूप से कृत्रिम बुद्धिमत्ता प्रणालियों से प्रभावित व्यक्तियों के मानवाधिकारों के संरक्षण पर जोर देता है और यूरोपय संघ के कृत्रिम बुद्धिमत्ता अधिनियम से स्वतंत्र रूप से संचालित होता है।[174] यह कृत्रिम बुद्धिमत्ता नैतिकता पर पहली बाध्यकारी अंतर्राष्ट्रीय संधि है। भारत भले ही वर्तमान इसका सदस्य नहीं है, परन्तु ऐसे प्रयासों से उत्पन्न वैश्विक मानदंड राष्ट्रीय नीतियों को अप्रत्यक्ष रूप से प्रभावित करते हैं।

संयुक्त राज्य अमेरिकाः क्षेत्र–विशिष्ट और सतर्कतापूर्ण दृष्टिकोण के साथ नवीनत्म पहलें

संयुक्त राज्य अमेरिका, जहाँ कई प्रमुख तकनीकी और कृत्रिम बुद्धिमत्ता कंपनियाँ स्थित हैं, ने पारंपरिक रूप से एक कम बाध्यकारी और नवाचार–प्रेरित नीति का समर्थन किया है। यूरोपीय संघ के **सामान्य डेटा संरक्षण विनियमन(जीडीपीआर)**[175] या भारत के **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (डीपीपीडी)**[176] के समान कोई एकल संघीय डेटा संरक्षण कानून यहाँ मौजूद नहीं है। इसके विपरीत, अमेरिका में क्षेत्र–विशेष गोपनीयता कानून लागू हैं–जैसे स्वास्थ्य डेटा के लिए **हेल्थ इंश्योरेंस पोर्टेबिलिटी एंड एकाउंटेबिलिटी जवाबदेही एक्ट(भ्च्।।)**[177], छात्र डेटा के लिए **फैमिली एजुकेशनल राइट्स एंड प्राइवेसी एक्ट;थ्त्च्।द्ध**[178], वित्तीय डेटा के लिए **ग्रैम–लीच–ब्लिले एक्ट**[179] और राज्य–स्तरीय कानून–जैसे **कैलिफोर्निया कंज्यूमर प्राइवेसी एक्ट** (ब्ब्च्।)[180], जो कैलिफोर्निया के निवासियों को कुछ जीडीपीआर जैसे अधिकार प्रदान करता है। साइबर सुरक्षा के क्षेत्र में, अमेरिका महत्वपूर्ण क्षेत्रों के लिए नियमों और बाजार–आधारित मानकों के मिश्रण का उपयोग करता है, **राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान** (छैप्ज्), साइबर सुरक्षा ढाँचा व्यापक रूप से सर्वोत्तम अभ्यास के रूप में अपनाया गया है[181], हालाँकि राष्ट्रपति बिडेन की 2023 की राष्ट्रीय साइबर सुरक्षा रणनीति महत्वपूर्ण बुनियादी ढांचे पर अधिक अनिवार्य आवश्यकताओं को बढ़ावा दे रही है[182]।

कृत्रिम बुद्धिमत्ता के संबंध में, अमेरिका ने हाल के समय तक संघीय स्तर पर अधिकतर अहस्तक्षेप की नीति अपनाई थी, और कृत्रिम बुद्धिमत्ता के प्रभावों को नियंत्रित करने के लिए मौजूदा कानूनों (भेदभाव–विरोधी,

---

[170]निधि सिंह, Navigating AI Regulation% A Comparative Analysis of EU and Indian Perspectives, https://digi-con.org/navigating-ai-regulation-a-comparative-analysis-of-eu-and-indian-perspectives/

[171]धारा 2(z), डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[172]Article 5(1)c, Regulation (EU) 2024/1689, http://data.europa.eu/eli/reg/2024/1689/oj

[173](NIS 2 Directive),DIRECTIVE (EU) 2022/2555, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[174]Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law ,Council of Europe Treaty Series - No. 225, https://rm.coe.int/1680afae3c

[175]REGULATION (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[176]डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[177]Health Insurance Portability and Accountability Act of 1996.Public law 104-191,110 stat.1936.

[178]Family Educational Rights and Privacy Act of 1974,20 U.S.C § 1232g.Congress.

[179]Gramm-Leach-bliley Act of 1999.Pulic law 106-102,113 stat.1338.

[180]California Consumer Privacy Act of 2018,Cal.Civ.Code § 1798.100-1798.199.

[181]टेरी ओलेस, एनआईएसटी साइबर सुरक्षा (सीएसएफ) 2.0 फ्रेमवर्क क्या है?,https://www.balbix.com/insights/nist-cybersecurity-framework/,अंतिम अद्यतन–17 जनवरी 2025.

[182]डेविड ई. सेंगर, ''नई बिडेन साइबर सुरक्षा रणनीति तकनीकी फर्मों को जिम्मेदारी सौंपती है'', https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html, प्रकाशित–2 मार्च 2023.

उत्पाद देयता, आदि) पर भरोसा किया था। हालाँकि, पिछले एक या दो वर्षों में महत्वपूर्ण बदलाव देखे गए हैं। अक्टूबर 2022 में, व्हाइट हाउस ऑफिस ऑफ साइंस एंड टेक्नोलॉजी पॉलिसी ने एक गैर–बाध्यकारी ''एआई बिल ऑफ राइट्स के लिए ब्लूप्रिंट'' जारी किया। यह पाँच सिद्धांतों की रूपरेखा प्रस्तुत करता है: सुरक्षित और प्रभावी प्रणालियाँ, एल्गोरिथम भेदभाव से सुरक्षा, डेटा गोपनीयता (जिसमें डिजाइन द्वारा गोपनीयता निर्मित करने और उपयोगकर्ताओं को नियंत्रण प्रदान करने जैसी सिफारिशें शामिल हैं), सूचना और स्पष्टीकरण (पारदर्शिता), और मानवीय विकल्पध्फॉलबैक (कई मामलों में स्वचालित प्रणालियों से बाहर निकलने की क्षमता)।[183] यद्यपि यह ब्लूप्रिंट कानून नहीं है, यह संघीय प्राथमिकताओं का संकेत देता है और भविष्य के नियमों या खरीद मानकों को प्रभावित कर सकता है।

अक्टूबर 2023 में, बिडेन प्रशासन ने व्यापक रूप से एक अधिक ठोस कदम उठाया, श्सुरक्षित, संरक्षित और भरोसेमंद एआई पर कार्यकारी आदेशश।[184] इस कार्यकारी आदेश के तहत, अन्य बातों के साथ–साथ, आधारभूत मॉडल के विकासकर्ताओं को, जो राष्ट्रीय सुरक्षा, अर्थव्यवस्था या स्वास्थ्य के लिए गंभीर जोखिम उत्पन्न करते हैं, सरकार को सूचित करने और कुछ सुरक्षा परीक्षण परिणाम साझा करने की आवश्यकता है।[185] यह राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान (छैप्ज्) को एआई सुरक्षा के लिए मानक निर्धारित करने का निर्देश देता है[186], सामग्री वॉटरमार्किंग (कृत्रिम बुद्धिमत्ता –जनित सामग्री की पहचान करने के लिए) पर दिशानिर्देशों का आह्वान करता है[187], और कृत्रिम बुद्धिमत्ता –सक्षम धोखाधड़ी और भेदभाव से सुरक्षा पर जोर देता है।[188] यह रक्षा उत्पादन अधिनियम जैसे कानूनों के तहत विद्यमान प्राधिकार का लाभ उठाते हुए उन्नत कृत्रिम बुद्धिमत्ता पर काम करने वाली कम्पनियों को सुरक्षा उपायों को प्राथमिकता देने के लिए बाध्य करता है।[189]

इस प्रकार अमेरिका का दृष्टिकोण नवाचार को बाधित न करने के लिए विनियमन में सावधानी बरतने का सुझाव देता है, इसके बजाय उद्योग का मार्गदर्शन करने के लिए ढाँचों और प्रोत्साहनों का उपयोग करता है। इसका नकारात्मक पहलू संभावित नियामक कमियाँ और कंपनी के स्व–शासन पर निर्भरता है। उदाहरण के लिए, बड़ी तकनीकी कंपनियों ने नैतिक दिशानिर्देशों पर स्वेच्छा से सहमत होने के लिए भागीदारी बनाई है, और जुलाई 2023 में कई प्रमुख एआई फर्मों ने व्हाइट हाउस से सुरक्षा परीक्षण और एआई सामग्री की वॉटरमार्किंग जैसे उपायों को लागू करने का वादा किया।[190] भारत, जो इसी तरह अपने तकनीकी उद्योग के विकास को महत्व देता है, अमेरिका के इस क्रमिक दृष्टिकोण से आकर्षित हो सकता है – दिशा निर्देशों पर ध्यान केंद्रित करना, स्व–नियमन के लिए उद्योग के साथ सहयोग करना, मुख्य रूप से उच्च–जोखिम परिदृश्यों में या नुकसान के प्रमाण के बाद कानून के साथ हस्तक्षेप करना। हालाँकि, अमेरिका के पास मजबूत उपभोक्ता संरक्षण एजेंसियाँ और एक मुकदमेबाजी का माहौल भी है जो कुछ हद तक कॉर्पोरेट कदाचार को रोक सकता है लेकिन भारत की प्रवर्तन संस्कृति भिन्न है। इस प्रकार, समानांतर प्रवर्तन क्षमताओं के बिना अमेरिकी शैली की पूर्ण प्रतिलिपि प्रभावी नहीं हो सकती है।

विशेष रूप से, अमेरिका के राज्य तेजी से आगे बढ़ रहे हैं: उदाहरण के लिए, 2008 में इलिनोइस राज्य ने बायोमेट्रिक सूचना गोपनीयता अधिनियम (ठप्ज्।) लागू किया , जिसके कारण बड़े मुकदमे हुए हैं (जैसे चेहरे की पहचान सुविधाओं के लिए फेसबुक के खिलाफ)।[191] यदि कृत्रिम बुद्धिमत्ता सिस्टम बायोमेट्रिक्स संसाधित करते हैं, तो बीआईपीए जैसे नियम शिक्षाप्रद हो सकते हैं। भारत में, हमारा आधार अधिनियम[192] और बायोमेट्रिक्स पर डिजिटल व्यक्तिगत डेटा अधिनियम[193] नियम उस भूमिका को निभा सकते हैं।

अंतर्राष्ट्रीय प्रयास

[183]Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

[184]"Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order 14110,88 Fed. Reg. 75191 (October 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[185]पूर्वोक्त 196, Section 4.1.

[186]पूर्वोक्त 196, Section 4.2.

[187]पूर्वोक्त 196, Section 4.5.

[188]पूर्वोक्त 196, Section 7,8.

[189]पूर्वोक्त 198.

[190]FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

[191]Illinois Biometric Information Privacy Act (740 ILCS 14/),https://law.justia.com/codes/illinois/chapter-740/act-740-ilcs-14/.

[192]आधार (वित्तीय और अन्य सब्सिडी, लाभ और सेवाओं का लक्षित वितरण) अधिनियम, 2016,

[193]डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

राष्ट्रीय कानूनों के अतिरिक्त, कुछ महत्वपूर्ण अंतर्राष्ट्रीय प्रयास भी उल्लेखनीय हैं। आर्थिक सहयोग और विकास संगठन ;व्म्ब्द्ध के कृत्रिम बुद्धिमत्ता पर सिद्धांत , जो 2019 में अपनाए गए और 2024 में अद्यतन किए गए, जिसे दर्जनों देशों (संयुक्त राज्य अमेरिका और यूरोपीय संघ के कई राष्ट्रों सहित – और जी20 के संदर्भ में, भारत ने भी इन सामान्य सिद्धांतों के प्रति समर्थन व्यक्त किया है) द्वारा समर्थन प्राप्त है, कुछ आधारभूत मूल्यों को स्थापित करते हैं। इनके अनुसार, कृत्रिम बुद्धिमत्ता को मानव कल्याण के लिए लाभकारी होना चाहिए, साथ ही निष्पक्ष, पारदर्शी, सुदृढ़ और जवाबदेह भी होना चाहिए।[194] यद्यपि ये सिद्धांत गैर–बाध्यकारी हैं, फिर भी वे एक आम सहमति वाला खाका तैयार करते हैं। वैश्विक भागीदारी कृत्रिम बुद्धिमत्ता पहल (जीपीएआई) में भारत की सक्रिय भागीदारी[195] और जी20 में इसके वक्तव्य इन सिद्धांतों के साथ सामंजस्य दर्शाते हैं।[196]

संयुक्त राष्ट्र एक अन्तराष्ट्रीय मंच है, 24 दिसंबर 2024 को, संयुक्त राष्ट्र महासभा ने साइबर अपराध को रोकने और उससे निपटने के लिए एक ऐतिहासिक कन्वेंशन अपनाया।[197] पाँच साल की कड़ी बातचीत के बाद, यह संयुक्त राष्ट्र **साइबर अपराध विरोध कन्वेंशन** अंतरराष्ट्रीय सहयोग को बढ़ावा देने और विशेष रूप से विकासशील देशों के लिए डिजिटल खतरों से लड़ने में आवश्यक तकनीकी सहायता और क्षमता–निर्माण प्रदान करने के लिए बनाया गया है। यह कन्वेंशन, दो दशकों में पहली अंतरराष्ट्रीय अपराध–रोधी संधि होने के कारण, एक महत्वपूर्ण मील का पत्थर है। इसका उद्देश्य साइबर अपराधों द्वारा उत्पन्न बढ़ती चुनौतियों का समाधान करना है, जो तेजी से फैल रहे हैं और विनाशकारी हो गए हैं, कमजोरियों का फायदा उठा रहे हैं और वैश्विक अर्थव्यवस्थाओं से सालाना खरबों डॉलर निकाल रहे हैं।[198]

कन्वेंशन के प्रमुख पहलुओं में शामिल हैं: अंतरराष्ट्रीय सहयोग को मजबूत करना, साइबर अपराधों को परिभाषित करना और उन्हें अपराधीकरण करना, कमजोर आबादी की रक्षा करना, और निवारक उपायों पर जोर देना।[199] यह मानता है कि प्रौद्योगिकी जहाँ समाज के विकास के लिए अपार क्षमता प्रदान करती है, वहीं यह साइबर अपराध के खतरे को भी बढ़ाती है।[200] इसका उद्देश्य सदस्य राष्ट्रों को लोगों और उनके अधिकारों को ऑनलाइन सुरक्षित रखने के लिए आवश्यक उपकरण और साधन प्रदान करना है। यह कन्वेंशन जुलाई 2025 में वियतनाम के हनोई में एक औपचारिक समारोह में हस्ताक्षर के लिए खोला जाऐगा और 40वें हस्ताक्षरकर्ता द्वारा इसकी पुष्टि के 90 दिनों के बाद लागू होगा।[201] यह विश्व स्तर पर एक सुरक्षित और अधिक सुरक्षित डिजिटल वातावरण बनाने की दिशा में एक महत्वपूर्ण कदम को दर्शाता है।

इसके अतिरिक्त, साइबर युद्ध के परिप्रेक्ष्य में, संयुक्त राष्ट्र ने **मुक्त–अंत कार्य समूह ;व्म्ळद्ध**[202] और पूर्ववर्ती में संयुक्त राष्ट्र **सरकारी विशेषज्ञों का समूह(ळळम्)**[203] ने यह स्पष्ट किया है कि अंतर्राष्ट्रीय कानून, विशेष रूप से संयुक्त राष्ट्र चार्टर, साइबर स्पेस पर लागू होता है – जिसका अर्थ है कि एक विनाशकारी राज्य–समर्थित साइबर हमला बल के प्रयोग के रूप में देखा जा सकता है। यह स्थिति तब महत्वपूर्ण हो जाती है जब संघर्ष में राज्य अभिकर्ताओं द्वारा कृत्रिम बुद्धिमत्ता का उपयोग किया जाता है ये मानदंडों पर स्पष्टता बढ़ने से तनाव को कम करने में सहायता मिल सकती है।[204] भारत सामान्यतः साइबर स्पेस में अंतर्राष्ट्रीय कानून की प्रयोज्यता का समर्थन करता है, परन्तु राज्य की संप्रभुता और अहस्तक्षेप के सिद्धांत पर जोर देता है।

तुलनात्मक सर्वेक्षण एक व्यापक परिदृश्य प्रस्तुत करता है, यूरोपीय संघ की विस्तृत नियम पुस्तिकाओं से जो प्रत्येक चरण पर अधिकारों को सुनिश्चित करती हैं, संयुक्त राज्य अमेरिका की लचीली और नवाचार–केंद्रित पद्धतियों तक जो लक्षित हस्तक्षेपों और कॉर्पोरेट जिम्मेदारी द्वारा समर्थित हैं। भारत के लिए

---

[194]Organisation for Economic Co-operation and Development (OECD). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, 22 May 2019. OECD.org, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[195]India joins Global Partnership on Artificial Intelligence (GPAI) as a founding member to support the responsible and human-centric development and use of AI, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1631676

[196]https://community.nasscom.in/communities/ai/india-sets-global-narrative-responsible-ai-digital-public-infra-g20

[197]United Nations Convention against Cybercrime,Resolution 79/243 adopted by the General Assembly on 24 December 2024, https://docs.un.org/en/A/RES/79/243

[198]"Statement by Executive Director of the United Nations Office on Drugs and Crime (UNODC) Ghada Waly on the Adoption of UN Convention against Cybercrime," UNIS Vienna, 24 दिसंबर 2024, https://unis.unvienna.org/unis/pressrels/2024/uniscp1183.html.

[199]Article 1, Res/79/243, https://docs.un.org/en/A/RES/79/243.

[200]Preamble, Res/79/243, https://docs.un.org/en/A/RES/79/243.

[201]https://unodaweb-meetings.unoda.org/public/2025-02/Concept%20note%20The%20Road%20to%20HN%20-%20OEWG.pdf.

[202]UN A/Res/73/27,https://disarmament.unoda.org/open-ended-working-group/

[203]UN A/Res/73/266, https://disarmament.unoda.org/group-of-governmental-experts/#:~:text=In%20GA%20resolution%2073/266,Brazil%20to%20Chair%20the%20Group.&text=The%20members%20of%20the%20GGE,Uruguay

[204]जेम्स एंड्रयू लुईस, वैश्विक साइबर मानदंडों के लिए जवाबदेही बनाना, https://www.csis.org/analysis/creating-accountability-global-cyber-norms, प्रकाशित –23 फरवरी 2022.

एक ऐसा मॉडल विकसित करना चुनौतिपूर्ण है, जो अपने संवैधानिक मूल्यों, विकास की आवश्यकताओं और संस्थागत क्षमता के अनुरूप हो। संभावित परिणाम एक मिश्रित दृष्टिकोण हो सकते हैं। दूसरों से सीखते हुए, भारत कई पहलुओं में नए सिरे से आविष्कार करने से बच सकता है – उदाहरण के लिए, राष्ट्रीय तकनीकी मानकों के बजाय अंतर्राष्ट्रीय तकनीकी मानकों को अपनाना, सिवाय उन मामलों के जहाँ राष्ट्रीय संदर्भ एक अलग दृष्टिकोण की मांग करता है जैसे यह सुनिश्चित करना कि कृत्रिम बुद्धिमत्ता इंटरफेस भारतीय भाषाओं को शामिल करें, जिसे पश्चिमी ढाँचे उपेक्षित कर सकते हैं। ये तुलनात्मक अंतर्दृष्टि, भारत की वर्तमान स्थिति और चुनौतियों के विश्लेषण के साथ मिलकर, भारत के लिए आगे की राह पर ठोस सिफारिशें प्रस्तावित करने के लिए आधार तैयार करती हैं।

सुझावः भविष्य के लिए मार्ग प्रशस्त करना

उपर्युक्त विश्लेषण के आधार पर, कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा की बढ़ती चुनौतियों से प्रभावी ढंग से निपटने के लिए भारत के कानूनी और संस्थागत ढांचे को मजबूत करने के उद्देश्य से कुछ सुझाव प्रस्तुत है। इन सुझाव का मुख्य लक्ष्य यह सुनिश्चित करना है कि भारत कृत्रिम बुद्धिमत्ता और डिजिटल नवाचार की अपार संभावनाओं का लाभ उठा सके, साथ ही व्यक्तिगत अधिकारों, राष्ट्रीय सुरक्षा और व्यापक जनहित की सुरक्षा भी सुनिश्चित कर सके। इन सुझावों में विनियमन और नवाचार के बीच संतुलन स्थापित करने का प्रयास किया गया है, वैश्विक स्तर पर अपनाई गई सर्वोत्तम प्रथाओं से प्रेरणा लेते हुए और उन्हें भारतीय परिस्थितियों के अनुरूप बनाया गया है।

1. एक व्यापक और अनुकूलनीय कृत्रिम बुद्धिमत्ता शासन प्रणाली का निर्माण

भारत को कृत्रिम बुद्धिमत्ता के विकास और उपयोग के लिए एक सुसंगत राष्ट्रीय कृत्रिम बुद्धिमत्ता कानून या नीतिगत ढांचा तैयार करने पर विचार करना चाहिए। तत्काल कठोर कानूनी प्रावधानों को लागू करने के बजाय, इसकी शुरुआत एक विस्तृत नीति या एक व्यापक कानून के रूप में की जा सकती है जो विभिन्न क्षेत्रों के नियामकों को कृत्रिम बुद्धिमत्ता से संबंधित दिशानिर्देश जारी करने का अधिकार प्रदान करे। इस ढांचे को जोखिम–आधारित दृष्टिकोण अपनाना चाहिए – उच्च–जोखिम वाले कृत्रिम बुद्धिमत्ता अनुप्रयोगों –जैसे स्वास्थ्य सेवा निदान, स्वायत्त वाहन, कानून प्रवर्तन, या कोई भी प्रणाली जो मौलिक अधिकारों या सुरक्षा को महत्वपूर्ण रूप से प्रभावित कर सकती है, की पहचान करना और उनके लिए पारदर्शिता और जवाबदेही के उच्च मानकों को अनिवार्य बनाना। ऐसे उच्च–प्रभाव वाले प्रणालियों के लिए, नियामक तैनाती से पहले पूर्वाग्रह, निष्पक्षता और संभावित नुकसान के आकलन के लिए अनिवार्य ऑडिट की आवश्यकता कर सकते हैं। कम जोखिम वाले कृ त्रिम बुद्धिमत्ता उपयोगों को व्यापक सिद्धांतों द्वारा निर्देशित उद्योग के स्व–नियमन पर छोड़ा जा सकता है। महत्वपूर्ण रूप से, इस ढांचे को अनुकूलनशील होना चाहिए – संभवतः एक समीक्षा तंत्र स्थापित करना, ताकि कानून तकनीकी परिवर्तनों के साथ तालमेल बनाए रख सके। इस ढांचे में नैतिक सिद्धांतों (जैसे नीति आयोग के जिम्मेदार कृत्रिम बुद्धिमत्ता[205] या आर्थिक सहयोग और विकास संगठन ;व्ब्ब्द्ध[206] कृत्रिम बुद्धिमत्ता सिद्धांतों से) को शामिल करने से यह सुनिश्चित होगा कि कृत्रिम बुद्धिमत्ता प्रणालियाँ डिजाइन से लेकर उपयोग तक संवैधानिक मूल्यों और मानवाधिकारों के अनुरूप ऐसा ढांचा, चाहे एक समर्पित कृत्रिम बुद्धिमत्ता अधिनियम हो या डिजिटल इंडिया अधिनियम में एकीकृत हो, उद्योग और नागरिकों दोनों को संचालन के नियमों के बारे में विश्वास दिलाएगा।

2. कृत्रिम बुद्धिमत्ता के संदर्भ में डेटा संरक्षण प्रवर्तन और गोपनीयता सुरक्षा को सुदृढ़ करना

डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम[207] के लागू होने के साथ, तत्काल सिफारिश इसके प्रभावी कार्यान्वयन को सुनिश्चित करना है। सरकार को भारतीय डेटा संरक्षण बोर्ड[208] की स्थापना में तेजी लानी चाहिए और इसे कृत्रिम बुद्धिमत्ता और बड़े डेटा को समझने वाले प्रौद्योगिकीविदों सहित पर्याप्त विशेषज्ञता से सुसज्जित करना चाहिए, ताकि यह कृत्रिम बुद्धिमत्ता एल्गोरिथम जैसे जटिल प्रसंस्करण से संबंधित शिकायतों को कुशलतापूर्वक संभाल सके। बोर्ड को स्पष्ट दिशानिर्देश जारी करने चाहिए कि डीपीपीडी अधिनियम के सिद्धांत कृत्रिम बुद्धिमत्ता पर कैसे लागू होते हैं।

विशेष रूप से कृत्रिम बुद्धिमत्ता के लिए, सरकार कृत्रिम बुद्धिमत्ता प्रणालियों में गोपनीयता को डिजाइन द्वारा प्रोत्साहित या अनिवार्य कर सकती है – यह गोपनीयता–अनुकूल कृत्रिम बुद्धिमत्ता प्रथाओं को प्रमाणित या मान्यता देकर प्राप्त किया जा सकता है। उदाहरण के लिए, गुमनामीकरण और संघीय

[205]Responsible AI, https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf

[206]What are the OECD Principles on AI?, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/what-are-the-oecd-principles-on-ai_f5a9a903/6ff2a1c4-en.pdf.

[207]डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

[208]धारा 18, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023.

शिक्षण ;मिकमतंजमक समंतदपदहद्ध[209] (जहां सभी व्यक्तिगत डेटा को केंद्रीकृत किए बिना कृत्रिम बुद्धिमत्ता मॉडल प्रशिक्षित किए जाते हैं) के उपयोग को बढ़ावा देने से गोपनीयता जोखिमों को कम करने में मदद मिल सकती है। डीपीपीडी ढांचे के तहत गुमनामीकरण और सिंथेटिक डेटा[210] के लिए मानक या सर्वोत्तम अभ्यास दस्तावेज जारी करने से संगठनों को व्यक्तिगत गोपनीयता से समझौता किए बिना कृत्रिम बुद्धिमत्ता विकास के लिए डेटा का सुरक्षित रूप से उपयोग करने में सहायता मिलेगी। इसके अलावा, भारत को मौजूदा अधिकारों के माध्यम से अप्रत्यक्ष रूप से ''एल्गोरिथम निष्पक्षता के अधिकार'' की अवधारणा को शामिल करना चाहिए – उदाहरण के लिए, समानता के संवैधानिक अधिकार और डीपीपीडी अधिनियम के प्रावधानों की व्याख्या करनी चाहिए ताकि यह निहित हो सके कि कृत्रिम बुद्धिमत्ता के माध्यम से व्यक्तिगत डेटा का प्रसंस्करण अनुचित भेदभाव का कारण नहीं बनना चाहिए। अदालतों और नियामकों को प्रशिक्षण के माध्यम से उन उदाहरणों को पहचानने और उन पर कार्यवाही करने के लिए प्रोत्साहित किया जा सकता है जहां कृत्रिम बुद्धिमत्ता निर्णय व्यवस्थित रूप से संरक्षित समूहों को नुकसान पहुंचाते हैं, इसे गोपनीयता और समानता दोनों अधिकारों का उल्लंघन मानते हुए।

3. साइबर सुरक्षा कानूनों और नीतियों का आधुनिकीकरण और डिजिटल इंडिया अधिनियम

दो दशक पुराने सूचना प्रोद्योगिकी अधिनियम को प्रस्तावित डिजिटल इंडिया अधिनियम से पुर्नस्थापित कर साइबर कानून को आधुनिक बनाने का एक सुनहरा अवसर है। यह अनुशंसा की जाती है कि डिजिटल इंडिया अधिनियम स्पष्ट रूप से कृत्रिम बुद्धिमत्ता, इंटरनेट ऑफ थिंग्स (आईओटी)[211], और क्वांटम क्रिप्टोग्राफी[212] जैसी भविष्य की तकनीकी प्रणालियों को शामिल करे। अधिनियम में ऐसे प्रावधान हो जोः (1) जुड़े उपकरणों और सॉफ्टवेयर के लिए सुरक्षित डिजाइन आवश्यकताओं को लागू करें (2) साइबर सुरक्षा में कृत्रिम बुद्धिमत्ता को संबोधित करें– संभवतः महत्वपूर्ण कृत्रिम बुद्धिमत्ता प्रणालियों को तैनात करने वाली कंपनियों को साइबर सुरक्षा सर्वोत्तम प्रथाओं का पालन करने और कृत्रिम बुद्धिमत्ता में कमजोरियों की रिपोर्ट करने की आवश्यकता है, और (3) सरकार को साइबर संकट के दौरान आपातकालीन निर्देश जारी करने के लिए एक कानूनी आधार प्रदान करें तथा उचित प्रक्रिया और ऐसे निर्देशों की कार्योत्तर समीक्षा भी सुनिश्चित करें।

डिजिटल इंडिया अधिनियम को मध्यस्थों के लिए सुरक्षित आश्रय के सिद्धांत को बनाए रखना चाहिए, लेकिन परिभाषाओं को अद्यतन करना चाहिए। यह ''महत्वपूर्ण एल्गोरिथम सिस्टम'' की एक नई श्रेणी पेश कर सकता है, जो वर्तमान नियमों में महत्वपूर्ण सोशल मीडिया मध्यस्थों के समान जिम्मेदारियां वहन करते हैं।

इसके अतिरिक्त, भारत को एक नई राष्ट्रीय साइबर सुरक्षा रणनीति की आवश्यकता है। लंबित रणनीति को अंतिम रूप दिया जाना चाहिए और एक समन्वित दृष्टिकोण प्रदान करने के लिए सार्वजनिक किया जाना चाहिए। इस रणनीति में ये सिफारिशों शामिल हैंः कृत्रिम बुद्धिमत्ता–संचालित हमलों का मुकाबला करने के लिए कृत्रिम बुद्धिमत्ता क्षमताओं के साथ विशेष साइबर इकाइयाँ बनाना, खतरों पर सार्वजनिक–निजी सूचना साझाकरण को बढ़ाना और राष्ट्रीय कंप्यूटर आपात मोचन दल और क्षेत्रीय कंप्यूटर आपात मोचन दल में साइबर सुरक्षा रक्षा के लिए कृत्रिम बुद्धिमत्ता उपकरणों में निवेश करना। रणनीति उन्नत साइबर सुरक्षा उपायों को लागू करने वाली कंपनियों के लिए प्रोत्साहन का भी प्रस्ताव कर सकती है, जिससे साइबर सुरक्षा की संस्कृति को बढ़ावा मिलेगा।[213]

कृत्रिम बुद्धिमत्ता–सक्षम साइबर अपराध में वृद्धि को देखते हुए, कानून प्रवर्तन प्रशिक्षण महत्वपूर्ण है, सरकार को राष्ट्रीय स्तर पर एक समर्पित ''साइबर और कृत्रिम बुद्धिमत्ता अपराध प्रकोष्ठ'' स्थापित करना चाहिए, जो तकनीकी विशेषज्ञों और पुलिस को एक साथ लाऐ, ताकि कृत्रिम बुद्धिमत्ता से जुड़े जटिल जांचों में सहायता मिल सके। यह इकाई अंतरराष्ट्रीय स्तर पर भी संपर्क कर सकती है, क्योंकि कई कृत्रिम बुद्धिमत्ता अपराध अंतर्राष्ट्रीय होंगे।

4. कृत्रिम बुद्धिमत्ता के नैतिक उपयोग को सरकार और सार्वजनिक क्षेत्र में सुनिश्चित करना

---

[209]फेडरेटेड लर्निंग, डेटा को किसी के देखे या छुए बिना एआई मॉडलों को प्रशिक्षित करने का एक तरीका है, जो नए एआई अनुप्रयोगों को फीड करने के लिए जानकारी को अनलॉक करने का एक तरीका प्रदान करता है. https://research.ibm.com/blog/what-is-federated-learning

[210]सिंथेटिक डेटा गैर–मानव निर्मित डेटा होता है जो वास्तविक दुनिया के डेटा की नकल करता है। इसे जनरेटिव कृत्रिम बुद्धिमत्ता तकनीकों पर आधारित कंप्यूटिंग एल्गोरिदम द्वारा बनाया जाता है। एक सिंथेटिक डेटा सेट में वही गणितीय गुण होते हैं जो उस वास्तविक डेटा पर आधारित होते हैं., https://mostly.ai/what-is-synthetic-data

[211]इंटरनेट ऑफ थिंग्स भौतिक उपकरणों का एक नेटवर्क है। ये उपकरण बिना किसी मानवीय हस्तक्षेप के एक–दूसरे को डेटा स्थानांतरित कर सकते हैं। ये उपकरण केवल कंप्यूटर या मशीनरी तक सीमित नहीं हैं। इसमें कोई भी ऐसी चीज शामिल हो सकती है जिसके सेंसर को एक विशिष्ट पहचानकर्ता दिया गया हो, https://www.coursera.org/in/articles/internet-of-things.

[212]क्वांटम क्रिप्टोग्राफी नियमों का एक समूह है जो सूचना को सुरक्षित रूप से एन्क्रिप्ट, संचारित और डिकोड करने के लिए क्वांटम यांत्रिकी के विचित्र लेकिन सुविचारित नियमों का उपयोग करती है। क्वांटम क्रिप्टोग्राफी, डेटा को प्रतिकूल हमले से बचाने के लिए, प्रकाश के अलग–अलग कणों (फोटॉन) को रिकॉर्ड करने में सक्षम सेंसर जैसे क्वांटम उपकरणों का उपयोग करती है,https://www.nist.gov/cybersecurity/what-quantum-cryptography

[213]https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks

सरकार स्वयं कृत्रिम बुद्धिमत्ता की एक प्रमुख उपयोगकर्ता है, इसलिए यह अनिवार्य है कि राज्य कृत्रिम बुद्धिमत्ता के नैतिक और नियमानुसार उपयोग में एक आदर्श उदाहरण प्रस्तुत करें व एक ''सरकारी कृत्रिम बुद्धिमत्ता उपयोग प्रोटोकॉल'' विकसित करे, जो दिशा निर्देशों का एक समूह होगा जिसको अनिर्वाय रूप से सभी सार्वजनिक अधिकारियों को कृत्रिम बुद्धिमत्ता के तैनात करते समय पालन करना चाहिए। इस प्रोटोकॉल में निम्नलिखित आवश्यकताएं होनी चाहिएः कृत्रिम बुद्धिमत्ता परियोजनाओं के लिए मानवाधिकार प्रभाव आकलन करना, पूर्ण पैमाने पर तैनाती से पहले स्वतंत्र विशेषज्ञों द्वारा ऑडिट किए गए परिणामों के साथ परीक्षण चरण और आमजन के लिए पारदर्शिता कि कौन सी कृत्रिम बुद्धिमत्ता प्रणालियाँ उपयोग में हैं। पेगासस मामले[214] में सर्वोच्च न्यायालय की चिंताओं से पता चलता है कि निगरानी तकनीक के उपयोग को सावधानीपूर्वक नियंत्रित किया जाना चाहिए, इसलिए सरकार को निगरानी कानूनों में सुधार के लिए जोर देना चाहिए, किसी भी कृत्रिम बुद्धिमत्ता–आधारित जन निगरानी के उपयोग के लिए न्यायिक या संसदीय निरीक्षण शुरू करना चाहिए, और यह सुनिश्चित करना चाहिए कि ऐसा उपयोग संकीर्ण रूप से तैयार और समयबद्ध हो। इसे कानून में घुसपैठ करने वाले साइबर संचालन के लिए वारंट या उचित प्राधिकरण प्राप्त करने की आवश्यकता को भी शामिल करना चाहिए, जो पुट्टस्वामी निर्णय[215] आवश्यकताओं के अनुरूप हो।

इसके अलावा, सार्वजनिक क्षेत्र के कृत्रिम बुद्धिमत्ता समाधानों को जहां तक संभव हो ओपन–सोर्स या ऑडिट योग्य एल्गोरिदम का वरीयता दि जानी चाहिए, ताकि विश्वास बढ़ाया जा सके और पूर्वाग्रह या त्रुटियों के लिए जांच की अनुमति दी जा सके। कृत्रिम बुद्धिमत्ता प्रणालियों के लिए निविदाओं में गोपनीयता और एल्गोरिथम निष्पक्षता के अनुपालन के बारे में मानदंड शामिल किये जा सकते हैं। सरकार सार्वजनिक सेवाओं में कृत्रिम बुद्धिमत्ता के लिए एक ''नियामक सैंडबॉक्स'' भी बना सकती है, जहॉ नए कृत्रिम बुद्धिमत्ता समाधानों को प्रौद्योगिकीविदों और नैतिकतावादियों दोनों की देखरेख में एक पायलट प्रयोग किया जा सकता है और प्रयोग से प्राप्त सबक का उपयोग सिस्टम को बेहतर बनाने के लिए किया जाता है।

5. सार्वजनिक जागरूकता, शिक्षा और बहु–हितधारक जुड़ाव को बढ़ावा देना

केवल कानून और नियम वांछित परिणाम प्राप्त नहीं कर सकते हैं जब तक कि उपयोगकर्ता और व्यवसाय अपने अधिकारों और जिम्मेदारियों के बारे में जागरूक न हों। कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा के बारे में हितधारकों को शिक्षित करने के लिए एक ठोस प्रयास की आवश्यकता है। इसमें स्कूल और कॉलेज के पाठ्यक्रम में कृत्रिम बुद्धिमत्ता, नैतिकता और साइबर सुरक्षा की बुनियादी बातों को एकीकृत करना और वित्तीय साक्षरता या डिजिटल भुगतान जागरूकता अभियानों के जागरूकता अभियान चलाना शामिल है। उपयोगकर्ताओं को यह जानना चाहिए कि जानकारी को कैसे सत्यापित किया जाए, अपने डेटा की सुरक्षा कैसे करें, और यदि उन्हें लगता है कि एक कृत्रिम बुद्धिमत्ता प्रणाली ने उनके डेटा का दुरुपयोग किया है या नुकसान पहुंचाया है तो कानूनों के तहत निवारण कैसे प्राप्त करें।

उद्योग और शिक्षा जगत की महत्वपूर्ण भूमिकाएँ हैं। सरकार के अधिकारियों, कृत्रिम बुद्धिमत्ता उद्योग के नेताओं, साइबर कानून विशेषज्ञों, नागरिक समाज, और संभवतः प्रधान वैज्ञानिक सलाहकार या सूचना प्रोद्योगिकी मंत्रालय की अध्यक्षता में एक बहु–हितधारक कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा परिषद की स्थापना की जाए। यह परिषद उभरते मुद्दों पर चर्चा करने और सहयोगात्मक तरीके से नीतिगत अद्यतन पर सरकार को सलाह देने के लिए एक सतत मंच के रूप में कार्य कर सकती है, जैसे कि इंटरनेट शासन में बहु–हितधारक प्रक्रियाएँ शामिल हैं। यह सुनिश्चित करेगा कि तेजी से आगे बढ़ रहे उद्योग के दष्टिकोण और नागरिक स्वतंत्रता संबंधी चिंताओं को नीति कार्यान्वयन में लगातार शामिल किया जाए, जिससे नियम अधिक प्रभावशाली और स्वीकार्य होंगे।

6. अंतर्राष्ट्रीय सहयोग को बढ़ावा और वैश्विक मानकों के साथ सांमजस्य

साइबर खतरे और कृत्रिम बुद्धिमत्ता विकास, सीमाओं से परे हैं, इसलिए भारत को सक्रिय रूप से अंतर्राष्ट्रीय मानदंडों में भाग लेना चाहिए और उन्हें आकार देना चाहिए। यह सुझाव है कि भारत कृत्रिम बुद्धिमत्ता नैतिकता और शासन पर वैश्विक पहलुओं में शामिल हो या सहयोग करे – उदाहरण के लिए, कृत्रिम बुद्धिमत्ता पर वैश्विक भागीदारी (जीपीएआई) और आर्थिक सहयोग और विकास संगठन (ओईसीडी) के साथ अपना जुड़ाव जारी रखे, और कृत्रिम बुद्धिमत्ता पर संभावित यूरोपीय परिषद कन्वेंशन पर हस्ताक्षर करने पर विचार करे या कम से कम घरेलू मानकों को ऐसे अंतर्राष्ट्रीय सर्वोत्तम प्रथाओं के साथ संरेखित करे। साइबर सुरक्षा पर, भारत को साइबर और कृत्रिम बुद्धिमत्ता से संबंधित अपराधों के लिए विशिष्ट पारस्परिक कानूनी सहायता व्यवस्थाओं को दृढ़ता से आगे बढ़ाना चाहिए, ताकि सीमा पार अन्वेषण निमानुसार सरल हो सकें।

[214]मनोहर लाल शर्मा बनाम भरत संघ, एआईआर (2023) 11 एससीसी 401.

[215]एआईआर 2017 एससीसी 416.

इसके अतिरिक्त, भारत विकासशील देशों में कृत्रिम बुद्धिमत्ता के लिए एक गठबंधन या मंच बनाकर वैश्विक दक्षिण में नेतृत्व कर सकता है, जो सामाजिक भलाई के लिए कृत्रिम बुद्धिमत्ता और विकासशील संदर्भों में कृत्रिम बुद्धिमत्ता शासन के लिए क्षमता निर्माण जैसे मुद्दों पर ध्यान केंद्रित करता है। यह भारत की आवाज को बढ़ाया सकता है और यह भी सुनिश्चित कर सकता है कि वैश्विक मानक केवल यूरोपीय संघ–अमेरिका द्वारा निर्धारित न हों, बल्कि विकासशील दुनिया में अरबों लोगों के लिए प्रासंगिक दृष्टिकोण भी शामिल हों। मानकों के साथ तालमेल बिठाने का अर्थ है भारतीय विनियमन में कृत्रिम बुद्धिमत्ता सुरक्षा के लिए तकनीकी मानकों, साथ ही साइबर सुरक्षा मानकों (आईएसओ 27001)[216] को अपनाना, जिनका कई कंपनियाँ पहले से ही पालन करती हैं। इससे वैश्विक कंपनियों के लिए अनुपालन आसान हो जाता है और यह सुनिश्चित होता है कि गैर–अनुपालन के कारण भारतीय कंपनियाँ वैश्विक मूल्य श्रृंखलाओं से बाहर न रह जाएँ। उदाहरण के लिए, यदि आईएसओ कृत्रिम बुद्धिमत्ता जोखिम प्रबंधन के लिए एक मानक विकसित करता है, तो भारत का बीआईएस इसे एक भारतीय मानक के रूप में अपना सकता है ताकि यहाँ की कंपनियाँ अंतरराष्ट्रीय स्तर पर मान्यता प्राप्त अभ्यास का पालन करें।

भारत को साइबर अपराध पर बुडापेस्ट कन्वेंशन[217] पर हस्ताक्षर करने पर विचार करना चाहिए या कम से कम एक भविष्य के संयुक्त राष्ट्र साइबर अपराध कन्वेंशन[218] को ऐसे प्रावधानों के साथ संरेखित करना चाहिए जो सीमाओं के पार इलेक्ट्रॉनिक साक्ष्य के समय पर साझाकरण को सुगम बनाते हैं। चूंकि कृत्रिम बुद्धिमत्ता अपराधों में अक्सर विदेशी क्षेत्राधिकारों में स्थित सर्वर और लॉग शामिल होंगे, इसलिए संधियों के माध्यम से उस साक्ष्य तक सुव्यवस्थित पहुंच प्रवर्तन को काफी सीमा तक बढ़ा सकती है।

निष्कर्षः डिजिटल भविष्य की नींव

कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा 21वीं सदी की डिजिटल क्रांति के दो अपरिहार्य स्तंभ हैं, जो भारत की कानूनी प्रणाली के समक्ष अद्वितीय अवसर और जटिल चुनौतियां प्रस्तुत करते हैं। इस शोध में, हमने यह विश्लेषण किया है कि कैसे भारत डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 जैसे नवीन कानूनों और सर्वोच्च न्यायालय के विकसित हो रहे न्यायिक सिद्धांतों के माध्यम से इन महत्वपूर्ण मुद्दों को संबोधित करने की प्रारंभिक प्रक्रिया में है। साथ ही, हमने उन अंतरालों और क्षेत्रों को भी रेखांकित किया है जिन पर विशेष ध्यान देने की आवश्यकता है। यह विश्लेषण इस बात पर जोर देता है कि भारत एक निर्णायक मोड़ पर खड़ा है। वर्तमान में कानून और नीति के क्षेत्र में लिए गए निर्णय यह निर्धारित करेंगे कि क्या कृत्रिम बुद्धिमत्ता प्रौद्योगिकियों का उपयोग भारत के संवैधानिक मूल्यों और सुरक्षा आवश्यकताओं के अनुरूप किया जा रहा है, या क्या वे अनपेक्षित नकारात्मक परिणामों के साथ अनियंत्रित हो जाती हैं। इस शोध से कई प्रमुख निष्कर्ष सामने आते हैं।

प्रथम, पुट्टस्वामी मामले में निजता को एक मौलिक अधिकार के रूप में मान्यता और डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 का अधिनियमन कृत्रिम बुद्धिमत्ता के युग में व्यक्तिगत डेटा की सुरक्षा के लिए एक आधारभूत कानूनी संरचना प्रदान करता है। यह व्यक्तियों को अपनी सूचना पर अधिकार प्रदान करने और डेटा को नियंत्रित करने वालों पर जिम्मेदारी डालने की दिशा में एक महत्वपूर्ण कदम है। किसी भी सार्थक कृत्रिम बुद्धिमत्ता विनियमन के लिए यह एक आवश्यक पूर्व शर्त है, क्योंकि डेटा ही कृत्रिम बुद्धिमत्ता का जीवन निर्वाह है। हालांकि, जैसा कि हमने देखा, केवल गोपनीयता कानून पर्याप्त नहीं है, इसका प्रभावी कार्यान्वयन और एल्गोरिथम पारदर्शिता तक विस्तार यह तय करेगा कि यह कृत्रिम बुद्धिमत्ता से जुड़ी विशिष्ट बारीकियों को कितनी कुशलता से संबोधित करता है।

द्वितीय, मौजूदा साइबर कानून कई साइबर अपराधों और मुद्दों को कवर करते हैं, लेकिन उनकी कल्पना कृत्रिम बुद्धिमत्ता को ध्यान में रखकर नहीं की गई थी। श्रेया सिंघल या अनुराधा भसीन जैसे मामलों में सर्वोच्च न्यायालय के हस्तक्षेप ने साइबर कानून प्रवर्तन में संवैधानिक सुरक्षा उपायों को स्थापित किया है, ऑनलाइन अभिव्यक्ति की स्वतंत्रता की रक्षा करना और इंटरनेट प्रतिबंधों में आनुपातिकता पर जोर देना आदि। ये न्यायिक सिद्धांत कृत्रिम बुद्धिमत्ता शासन के लिए एक दिशा प्रदान करते हैं, कृत्रिम बुद्धिमत्ता कि भी विनियमन को अभिव्यक्ति की स्वतंत्रता, समानता और उचित प्रक्रिया का सम्मान करना चाहिए, और अदालतें इन मानदंडों के आधार पर राज्य की कृत्रिम बुद्धिमत्ता से संबंधित कार्यवाहियों की संभावित रूप से गहन जांच करेंगी।

तृतीय, एल्गोरिथम पूर्वाग्रह से लेकर डीपफेक और कृत्रिम बुद्धिमत्ता–संचालित साइबर हमलों तक उभरती चुनौतियाँ एक गतिशील खतरे के परिदृश्य को दर्शाती हैं जो पारंपरिक नियामक दृष्टिकोणों पर दबाव डालता

[216]https://www.iso.org/standard/27001

[217]Convention on Cybercrime Budapest,European Treaty Series - No. 185, https://rm.coe.int/1680081561

[218]पूर्वोक्त 210.

है। कृत्रिम बुद्धिमत्ता जवाबदेही को अस्पष्ट कर सकती है, और साइबर खतरों को तीव्र कर सकती है, जिसके लिए नवीन नियामक सोच, बेहतर तकनीकी क्षमता और संभवतः नए कानूनी सिद्धांतों की आवश्यकता है। तुलनात्मक अध्ययन से पता चला कि भारत इन मुद्दों का सामना करने में अकेला नहीं है। कई देश समाधानों के साथ प्रयोग कर रहे हैं, चाहे वह यूरोपीय संघ के व्यापक लेकिन जटिल नियम हों या कार्यकारी मार्गदर्शन द्वारा समर्थित अमेरिका का अधिक लचीला दृष्टिकोण। भारत एक मध्य मार्ग अपनाता हुआ प्रतीत होता है, और इस पत्र में दी गई सुझाव उस मार्ग को बुद्धिमानी से तैयार करने के तरीके रेखाकिंत हैं।

अंततः, हम कह सकते हैं कि एक सर्वव्यापी दक्षता और बहु–विषयक सहयोग की आवश्यकता है। प्रौद्योगिकी के क्षेत्र में कानून, दूरदर्शिता या तकनीकी जानकारी के बिना तैयार किए जाने पर अप्रचलित या अतिव्यापी हो सकते हैं। कृत्रिम बुद्धिमत्ता की तीव्र प्रगति का अर्थ है कि नियामकों को सूविज्ञ और अनुकूलनशील रहना चाहिए। यही कारण है कि चल सतत संवाद के लिए मंच स्थापित करना और कानूनों की आवधिक समीक्षा के लिए प्रतिबद्ध होना इतना महत्वपूर्ण है। डिजिटल इंडिया अधिनियम की विकास प्रक्रिया, जिसमें हितधारकों के परामर्श शामिल हैं, एक सकारात्मक संकेत है इससे समावेशी दृष्टिकोण को जारी रखने में यह सुनिश्चित करने में मदद मिलेगी कि परिणामी कानून मजबूत और अनुकूलनीय हो।

निष्कर्ष रूप में, यह स्पष्ट है कि भारत की कानूनी प्रणाली ने कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा की दिशा में अपनी यात्रा शुरू कर दी है, लेकिन अभी भी बहुत काम करना बाकी है। डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम का पारित होने और संबंधित मामलों में सर्वोच्च न्यायालय का सक्रिय रुख इसे गति प्रदान करता है। आगे बढ़ते हुए, विभिन्न सुझावों को लागू करना जैसे एक समर्पित कृत्रिम बुद्धिमत्ता शासन ढांचे का निर्माण करना, डिजिटल इंडिया अधिनियम के माध्यम से साइबर कानूनों को अद्यतन करना, प्रवर्तन एजेंसियों को मजबूत करना और वैश्विक सर्वोत्तम प्रथाओं के साथ तालमेल बिठाना महत्वपूर्ण होगें। ये उपाय गोपनीयता उल्लंघनों, भेदभाव और साइबर हमलों जैसे जोखिमों को कम करने में मदद करेंगे, जिससे कृत्रिम बुद्धिमत्ता प्रणालियों में सार्वजनिक विश्वास का निर्माण होगा। कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा का सफल शासन अंततः भारत को आर्थिक विकास और सामाजिक कल्याण के लिए कृत्रिम बुद्धिमत्ता की परिवर्तनकारी क्षमता को साकार करने में सक्षम करेगा, साथ ही अपने नागरिकों के अधिकारों और सुरक्षा की रक्षा करेगा। यह एक नाजुक संतुलन है, लेकिन साक्ष्य द्वारा सूचित और संवैधानिक सिद्धांतों द्वारा निर्देशित विवेकपूर्ण विनियमन के साथ, भारत यह सुनिश्चित कर सकता है कि कृत्रिम बुद्धिमत्ता उत्पीड़न या अराजकता का नहीं, बल्कि सशक्तिकरण और सुरक्षा का एक उपकरण बने। भारतीय कानूनी प्रणाली, अपने मजबूत संवैधानिक ढांचे और विकसित हो रहे विधायी उपकरणों से सुसज्जित होकर, इन चुनौतीयों का सामना करे। भारत वैश्विक अनुभवों से सीखते हुए यह प्रदर्शित सकता है कि लोकतंत्र कृत्रिम बुद्धिमत्ता की, प्रकृति को कैसे संभालता है।