Shikshan Sanshodhan : Journal of Arts, Humanities and Social Sciences ISSN(o): 2581-6241
Monthly, Peer-Reviewed, Refereed, Indexed Journal Impact Factor: 7.384
Volume - 8, Issue - 4, April - 2025

DOIs:10.2018/SS/202504006 --:-- Research Paper / Article / Review

आधार (यूआईडीएआई) आधारित अपराधों की रोकथाम: प्रौद्योगिकी और कानून का समन्वयन

डॉ.चंद्रमौली पाण्डेय
प्रवक्ता राजनीति शास्त्र, (राजकीय इण्टर कॉलेज)
Email - chandramoulipandey65@gmail.com

शोध सार :- भारतीय विशिष्ट पहचान प्राधिकरण (UIDAI) द्वारा स्थापित आधार प्रणाली, भारतीय निवासियों के लिए एक विशिष्ट पहचानकर्ता के रूप में कार्य करती है, जिसका उद्देश्य सरकारी सेवाओं और सामाजिक लाभों तक पहुँच में सुधार करना है। हालाँकि, सामाजिक और आर्थिक विकास में इसकी महत्वपूर्ण भूमिका के बावजूद, आधार का दुरुपयोग होने की संभावना बढ़ गई है, जिसके कारण पहचान की चोरी, वित्तीय धोखाधड़ी और साइबर अपराध जैसे आधार-आधारित अपराधों के विभिन्न रूप सामने आए हैं। यह शोधपत्र आधार से जुड़े जोखिमों की पड़ताल करता है एवं इसके दुरुपयोग से उत्पन्न होने वाले अपराधों के प्रकारों का विश्लेषण करता है, जिसमें सरकारी योजनाओं में धोखाधड़ी, अनधिकृत वित्तीय गतिविधियाँ और डेटा उल्लंघन शामिल हैं। यह इन अपराधों को कम करने में प्रौद्योगिकी की भूमिका की जाँच करता है, धोखाधड़ी गतिविधियों का पता लगाने के लिए बायोमेट्रिक सुरक्षा, एन्क्रिप्शन और AI-संचालित निगरानी के महत्व पर जोर देता है। इसके अतिरिक्त शोध आधार अधिनियम 2016, संवैधानिक गोपनीयता चिंताओं और प्रासंगिक साइबर अपराध कानूनों सहित आधार के आसपास के कानूनी ढांचे की पड़ताल करता है। हालांकि तकनीकी प्रगति ने सुरक्षा को मजबूत किया है फिर भी बायोमेट्रिक धोखाधड़ी, कानूनी अपर्याप्तता और सामाजिक विश्वास के मुद्दे जैसी चुनौतियाँ बनी हुई हैं। इस शोधपत्र का उद्देश्य आधार आधारित अपराधों को रोकने के लिए प्रौद्योगिकी और कानूनी सुधारों को मिलाकर एक सामंजस्यपूर्ण दृष्टिकोण प्रदान करना है, जिसमें उन्नत एन्क्रिप्शन, मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) और डिजिटल सुरक्षा पर सार्वजनिक शिक्षा है। आधार प्रणाली अपनी सार्थकता सिद्ध करते हुए नागरिकों को संभावित दुरुपयोग से बचाने के लिए मजबूत सुरक्षा उपायों, कानूनी सुधारों और व्यापक जागरूकता की आवश्यकता पर प्रकाश डालते हैं।

बीज शब्द : आधार प्रणाली, यूआईडीएआई, आधार-आधारित अपराध, पहचान की चोरी, वित्तीय धोखाधड़ी, बायोमेट्रिक सुरक्षा, डेटा एन्क्रिप्शन, कानूनी ढांचा, साइबर अपराध कानून, मल्टी-फैक्टर प्रमाणीकरण ।

1. प्रस्तावना :

भारत में 2009 में शुरू की गई आधार प्रणाली दुनिया की सबसे बड़ी बायोमेट्रिक पहचान प्रणालियों में से एक है, जो प्रत्येक निवासी को उनके बायोमेट्रिक और जनसांख्यिकीय डेटा के आधार पर एक अद्वितीय 12-अंकीय पहचान संख्या प्रदान करती है। भारतीय विशिष्ट पहचान प्राधिकरण (UIDAI) द्वारा जारी आधार कई सरकारी सेवाओं और कल्याण कार्यक्रमों के लिए आधार के रूप में कार्य करता है, पहुँच को सुव्यवस्थित करता है और रिसाव को कम करता है। UIDAI के उद्देश्यों में प्रत्येक निवासी के लिए एक सार्वभौमिक, आसानी से सुलभ पहचान प्रदान करना, कुशल सेवा वितरण सुनिश्चित करना और वित्तीय समावेशन को बढ़ावा देना शामिल है। आधार भारत में महत्वपूर्ण सामाजिक और आर्थिक महत्व रखता है। यह सब्सिडी, पेंशन और स्वास्थ्य सेवा जैसे

सरकारी लाभों तक पहुँच को सुगम बनाता है, यह सुनिश्चित करता है कि सेवाएँ इच्छित लाभार्थियों तक पहुँचें। इसके अतिरिक्त, यह वित्तीय क्षेत्र में एक महत्वपूर्ण भूमिका निभाता है, जिसमें आधार-आधारित भुगतान और बैंक खाते ग्रामीण और शहरी भारत में वित्तीय समावेशन का विस्तार करते हैं। हालाँकि, आधार की सर्वव्यापकता ने गोपनीयता और दुरुपयोग की संभावना के बारे में चिंताएँ पैदा की हैं। आधार-आधारित अपराध, जिनमें धोखाधड़ी, पहचान की चोरी और संवेदनशील डेटा तक अनधिकृत पहुँच शामिल हैं, महत्वपूर्ण मुद्दे बन गए हैं। धोखाधड़ी के मामले बढ़ रहे हैं, जहाँ अपराधी अवैध उद्देश्यों के लिए चोरी या जाली आधार जानकारी का उपयोग करते हैं। इसी तरह, पहचान की चोरी में आधार विवरण का उपयोग करके व्यक्तियों का प्रतिरूपण शामिल है, जिससे व्यक्तिगत और वित्तीय नुकसान होता है। आधार का समर्थन करने वाला प्रौद्योगिकी बुनियादी ढांचा, जबकि मजबूत है, शोषण की भी पर्याप्त संभावना है, जो प्रभावी निवारक उपायों की आवश्यकता को उजागर करता है। इस शोध का उद्देश्य आधार-आधारित अपराधों को रोकने में तकनीकी प्रगति और कानूनी ढाँचों के सामंजस्य का पता लगाना है। इसमें आधार के व्यापक उपयोग से उत्पन्न जोखिमों को समझना, मौजूदा सुरक्षा उपायों का विश्लेषण करना और एकीकृत समाधानों का प्रस्तुत करना शामिल है। अध्ययन यह सुनिश्चित करने का प्रयास करता है कि आधार नवाचार और समावेशन को आगे बढ़ाता रहे, लेकिन यह व्यक्तियों की सुरक्षा और गोपनीयता से समझौता किए बिना लक्ष्य की ओर अग्रसर हो।

2. आधार आधारित अपराधों के प्रकार और उनका प्रभाव

पहचान की चोरी

पहचान की चोरी आधार के दुरुपयोग से जुड़े सबसे महत्वपूर्ण अपराधों में से एक है। यह तब होता है जब किसी व्यक्ति के आधार डेटा को चुराया जाता है या उसका दुरुपयोग करके उसका प्रतिरूपण किया जाता है। इससे व्यक्तिगत जानकारी तक अनधिकृत पहुँच, धोखाधड़ी की गतिविधियाँ या वित्तीय नुकसान हो सकता है। उदाहरण के लिए, 2018 में, आधार डेटाबेस में बड़े पैमाने पर डेटा की चोरी ने व्यक्तिगत जानकारी की सुरक्षा को लेकर चिंताएँ पैदा कर दीं। कथित तौर पर यह डाटा लीक नकली दस्तावेज़ बेचने वाली वेबसाइटों पर आधार विवरण की उपलब्धता के कारण हुआ था। आधार डेटा की चोरी और दुरुपयोग से गंभीर परिणाम हो सकते हैं जैसे पीड़ित के नाम पर नकली खाते खोले जा सकते हैं और कुछ मामलों में धोखाधड़ी से ऋण या क्रेडिट सुविधाएँ प्राप्त की जा सकती हैं। इसके प्रभावस्वरुप पहचान की चोरी से दीर्घकालिक वित्तीय नुकसान, व्यक्तिगत छवि की हानि और कानूनी जटिलताएँ हो सकती हैं। पीड़ितों को अक्सर अपनी छवि सुधारने और अपनी साख बहाल करने में बड़ी चुनौतियों का सामना करना पड़ता है।

धोखाधड़ी और वित्तीय अपराध

वर्तमान में आधार वित्तीय लेन-देन करने के लिए एक ज़रूरी साधन बन गया है, जिसमें बैंक खाते खोलना, टैक्स भरना और ऋण लेना शामिल है। हालाँकि, इस व्यापक उपयोग ने इसे धोखेबाज़ों के लिए एक आकर्षक अवसर प्रदान कर दिया है। वित्तीय धोखाधड़ी के एक सामान्य प्रकार में चोरी या नकली आधार विवरण का उपयोग करके अनधिकृत रूप से बैंक खाते खोलना शामिल है। कुछ मामलों में, अपराधियों ने लोक कल्याण निधि तक पहुँचने या सरकारी योजनाओं और सब्सिडी का लाभ उठाने के लिए नकली पहचान बनाने के लिए आधार संख्या का उपयोग किया है।

हाल ही की घटनाओं और रिपोर्टों से संकेत मिलता है कि धोखेबाज़ों ने बैंक खातों तक पहुँचने और विभिन्न सरकारी योजनाओं के तहत पैसे निकालने के लिए चोरी किए गए आधार नंबरों का उपयोग किया। एक अन्य प्रमुख चिंता प्रत्यक्ष लाभ हस्तांतरण (DBT) प्रणाली का दुरुपयोग है, जहाँ वैध लाभार्थियों के लिए निर्धारित सब्सिडी को हड़पने के लिए नकली पहचान बनाई जाती है।[i] आधार का उपयोग करके वित्तीय धोखाधड़ी का व्यक्तियों और संस्थानों दोनों पर गहरा प्रभाव पड़ता है। इससे वित्तीय नुकसान होता है, कल्याण लाभों के वितरण में बाधा आती है और आधार-आधारित वित्तीय प्रणालियों में विश्वास कम होता है।

अधिकृत सेवाओं का दुरुपयोग

आधार प्रणाली विभिन्न सरकारी कल्याणकारी योजनाओं, जैसे कि पीडीएस (सार्वजनिक वितरण प्रणाली), मनरेगा (महात्मा गांधी राष्ट्रीय ग्रामीण रोजगार गारंटी अधिनियम), आदि का अभिन्न अंग है। दुर्भाग्य से, अपराधियों ने चोरी किए गए आधार विवरणों का उपयोग करके अवैध रूप से सब्सिडी, राशन या अन्य लाभों तक पहुँच प्राप्त करके इन सेवाओं का दुरुपयोग किया है। ये धोखाधड़ी वाले दावे वास्तविक लाभार्थियों के लिए निर्धारित संसाधनों को हटा देते हैं, जिससे गरीबी और सामाजिक असमानता बढ़ जाती है।

2024 में, एक रिपोर्ट ने कई राज्यों में अवैध रूप से सब्सिडी का दावा करने के लिए आधार विवरणों के दुरुपयोग पर प्रकाश डाला, जिसमें अपराधी लाभ का दावा करने के लिए झूठी पहचान का उपयोग करते हैं। इस तरह का दुरुपयोग वास्तविक लाभार्थियों को सेवाएँ देने में बाधाएँ भी पैदा करता है। इसका प्रभाव दोहरा है: एक तरफ, यह वैध लाभार्थियों को उनके उचित अधिकारों से वंचित करता है, और दूसरी तरफ, यह सरकारी योजनाओं की प्रभावशीलता को बाधित करता है, जिससे ऐसे कार्यक्रमों में जनविश्वास में कमी आती है।

साइबर अपराध

आधार से जुड़ी सेवाओं के बढ़ते डिजिटलीकरण के साथ, आधार से जुड़े ऑनलाइन अपराध बढ़ गए हैं। हैकर्स और साइबर अपराधी आधार डेटा चुराने के लिए कमज़ोर सिस्टम को निशाना बनाते हैं, जिसका इस्तेमाल फिर कई तरह की धोखाधड़ी वाली गतिविधियों के लिए किया जा सकता है। इसमें फ़िशिंग जैसे हमले शामिल हैं, जहाँ लोगों को फ़र्जी वेबसाइट या ईमेल के ज़रिए अपने आधार विवरण देने के लिए प्रेरित किया जाता है, और ओटीपी मिलते ही साइबर अपराधी आधार डेटा वाले सर्वर को हैक कर लेते हैं।

सेंटर फ़ॉर इंटरनेट एंड सोसाइटी (CIS) द्वारा 2023 में किए गए एक अध्ययन में फ़िशिंग के कई मामले सामने आए, जहाँ UIDAI के पोर्टल की नकल करने वाली फ़र्जी वेबसाइट का इस्तेमाल आधार के डेटा को चुराने के लिए किया गया। आधार जनित साइबर अपराध एक बढ़ती हुई चिंता है, क्योंकि इसमें अक्सर बड़े पैमाने पर डेटा चोरी शामिल होते हैं जो लाखों व्यक्तियों को प्रभावित कर सकते हैं।[ii] आधार-आधारित ऑनलाइन अपराधों का प्रभाव बहुत बड़ा है, क्योंकि वे व्यक्तिगत डेटा की हानि, वित्तीय चोरी और यहाँ तक कि बड़ी आपराधिक गतिविधियों को अंजाम देने का कारण बन सकते हैं। रोकथाम के लिए कड़े साइबर सुरक्षा उपायों, जागरूकता और कानूनी ढाँचों की आवश्यकता होती है।

3. आधार आधारित अपराधों की रोकथाम में प्रौद्योगिकी का एकीकरण सुरक्षा

आधार आधारित अपराधों की रोकथाम में प्रौद्योगिकी का एकीकरण सुरक्षा बढ़ाने और व्यक्तिगत डेटा की सुरक्षा में महत्वपूर्ण भूमिका निभाता है। आधार प्रणाली, जो अंगूठे के निशान और आईरिस स्कैन जैसे बायोमेट्रिक डेटा पर निर्भर करती है, पारंपरिक तरीकों की तुलना में प्रमाणीकरण की एक अतिरिक्त लेयर सुनिश्चित करती है। बायोमेट्रिक डेटा प्रत्येक व्यक्ति के लिए अद्वितीय होता है, जिससे पहचान की चोरी जैसी धोखाधड़ी गतिविधियों का होना बेहद मुश्किल हो जाता है। बायोमेट्रिक सुरक्षा प्रणाली उपयोगकर्ता की पहचान की विश्वसनीयता को बढ़ाती है, अनधिकृत पहुँच या दुरुपयोग के खिलाफ़ एक महत्वपूर्ण सुरक्षा कवच प्रदान करती है।[iii]

आधार डेटा की सुरक्षा को और मज़बूत करने के लिए एन्क्रिप्शन तकनीक का उपयोग किया जाता है, जो संवेदनशील व्यक्तिगत जानकारी के भंडारण और प्रसारण को सुरक्षित करता है। आधार डेटा को एन्क्रिप्ट करके, इसे अनधिकृत पक्षों के लिए अपठनीय बना दिया जाता है, इस प्रकार डेटा उल्लंघनों और साइबर हमलों से सुरक्षा मिलती है। इसके अतिरिक्त, डिजिटल हस्ताक्षरों का उपयोग यह सुनिश्चित करता है कि डेटा प्रामाणिक बना रहे और प्रसारण के दौरान उसके साथ छेड़छाड़ न की गई हो। सख्त सुरक्षा

प्रोटोकॉल के साथ संयुक्त ये एन्क्रिप्शन विधियाँ व्यक्तिगत जानकारी के लिए एक मज़बूत सुरक्षा प्रदान करती हैं। इसके अलावा, आर्टिफिशियल इंटेलिजेंस (AI) और मशीन लर्निंग के आगमन ने आधार प्रणाली में नई क्षमताएँ ला दी हैं। AI बड़ी मात्रा में डेटा का विश्लेषण कर सकता है और वास्तविक समय में विसंगतियों का पता लगा सकता है, जैसे कि आधार नंबर के उपयोग में अनियमितताएँ या धोखाधड़ी वाले लेन-देन के प्रयास। मशीन लर्निंग एल्गोरिदम लगातार अपने पता लगाने के तरीकों को अनुकूलित और परिष्कृत कर सकते हैं, समय के साथ सुधार कर सकते हैं और संदिग्ध गतिविधियों की अधिक प्रभावी ढंग से पहचान कर सकते हैं। AI और स्मार्ट तकनीकों का तालमेल संभावित खतरों का जल्द पता लगाना, जोखिमों को कम करना और आधार के दुरुपयोग से संबंधित अपराधों को रोकना सुनिश्चित करता है। कानूनी ढाँचों के साथ तकनीक का सामंजस्य यह सुनिश्चित करने के लिए आवश्यक है कि ये तकनीकी प्रगति प्रभावी ढंग से और गोपनीयता कानूनों के अनुपालन में लागू की जाए, जिससे व्यक्तिगत डेटा की सुरक्षा के लिए एक संतुलित दृष्टिकोण प्रदान किया जा सके।

आधार अधिनियम 2016 आधार प्रणाली की स्थापना और संचालन के लिए एक कानूनी ढांचा प्रदान करता है, जिसका उद्देश्य भारत के निवासियों को एक विशिष्ट पहचान संख्या प्रदान करना है। अधिनियम आधार संख्या के जारी करने, सत्यापन और प्रमाणीकरण के साथ-साथ व्यक्तिगत डेटा की गोपनीयता और सुरक्षा की रक्षा के लिए सुरक्षा उपायों के प्रावधान निर्धारित करता है। हालाँकि, आधार के कार्यान्वयन ने सुरक्षा, गोपनीयता और दुरुपयोग की संभावना के बारे में चिंताएँ पैदा की हैं।

4. आधार विनियमन हेतु कानूनी ढांचा

आधार अधिनियम के साथ आधार डेटा की सुरक्षा के लिए बनाए गए कानूनी नियम भी हैं। इसमें धारा 29 जैसे प्रावधान शामिल हैं, जो प्रमाणीकरण या अदालत के आदेश (आधार अधिनियम, 2016) जैसे निर्दिष्ट उपयोगों को छोड़कर, व्यक्ति की सहमति के बिना बायोमेट्रिक या जनसांख्यिकीय डेटा को साझा करने पर रोक लगाता है। इसके अतिरिक्त, यह अधिनियम आधार प्रणाली के संचालन की देखरेख करने और सुरक्षा प्रोटोकॉल के अनुपालन को सुनिश्चित करने के लिए UIDAI (भारतीय विशिष्ट पहचान प्राधिकरण) की स्थापना को अनिवार्य बनाता है। इन सुरक्षा उपायों को धारा 33 द्वारा पूरक बनाया गया है, जो अनधिकृत डेटा उपयोग के मामलों में दंड की अनुमति देता है, लेकिन दुरुपयोग को रोकने में इन उपायों की पर्याप्तता पर चिंता बनी हुई है।

आधार और गोपनीयता के इर्द-गिर्द संवैधानिक बहस के.एस. पुट्टस्वामी बनाम भारत संघ (2017) में सुप्रीम कोर्ट के ऐतिहासिक फैसले के साथ सामने आई, जिसने भारतीय संविधान के अनुच्छेद 21 के तहत निजता के अधिकार को मौलिक अधिकार के रूप में मान्यता दी। न्यायालय के फैसले ने आधार के उपयोग पर बैंकिंग और मोबाइल कनेक्शन जैसी सेवाओं के साथ गैर-स्वैच्छिक लिंकिंग के संबंध में प्रतिबंध लगा दिए। इस निर्णय ने आधार की तकनीकी दक्षता के लाभों को व्यक्तिगत गोपनीयता अधिकारों की सुरक्षा के साथ संतुलित करने की आवश्यकता को रेखांकित किया। इसने गोपनीयता सुरक्षा के साथ आधार के उपयोग को सुसंगत बनाने के लिए एक महत्वपूर्ण कानूनी मिसाल कायम की, जिसके परिणामस्वरूप आधार अधिनियम के प्रावधानों की एक संकीर्ण व्याख्या हुई।

साइबर अपराधों के मुद्दे पर, भारत के कानूनी ढांचे में सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 शामिल है, जो डेटा सुरक्षा और साइबर अपराधों को संबोधित करता है। आईटी अधिनियम के तहत धारा 66सी (पहचान की चोरी के लिए दंड) जैसे विशिष्ट प्रावधान सीधे आधार से संबंधित धोखाधड़ी से संबंधित हैं। हालांकि, साइबर अपराध के विकसित होते तरीकों के साथ तालमेल बनाए रखने के लिए इन कानूनी साधनों को और मजबूत करने की आवश्यकता है। आधार से संबंधित धोखाधड़ी के लिए पर्याप्त दंड और सजा के प्रावधान, जैसे कि आधार अधिनियम की धारा 37 में उल्लिखित हैं, दुरुपयोग को रोकने के लिए अधिक सख्ती से लागू किए जाने चाहिए। मौजूदा प्रावधानों के बावजूद, आधार-आधारित अपराधों के बढ़ते जोखिम व्यापक कानूनी सुधारों की आवश्यकता को उजागर करते हैं। इन सुधारों को डेटा सुरक्षा उपायों को बढ़ाने, आधार के दुरुपयोग के लिए दंड के दायरे का विस्तार करने और यह सुनिश्चित करने पर ध्यान केंद्रित करना चाहिए कि सार्वजनिक जन कल्याण के लिए आधार की उपयोगिता को

बनाए रखते हुए गोपनीयता अधिकारों का सम्मान किया जाए।[iv] कानूनी सुरक्षा उपायों के साथ प्रौद्योगिकी के उपयोग को सुसंगत बनाने के लिए स्पष्ट दिशानिर्देशों की भी आवश्यकता है, यह सुनिश्चित करते हुए कि डिजिटल डोमेन में प्रगति के शर्त पर व्यक्तिगत अधिकारों से समझौता न हो।

5. आधार जनित अपराध और चुनौतियां

भारत की विशिष्ट पहचान प्रणाली 'आधार' ने सेवाओं और कल्याणकारी योजनाओं तक आम आदमी के पहुंच के संदर्भ में क्रांति ला दी है। हालाँकि, इसके व्यापक उपयोग ने आधार-आधारित अपराधों को रोकने में कई चुनौतियों को सामने लाया है, जो तकनीकी और सामाजिक दोनों बाधाओं से उपजी हैं। एक महत्वपूर्ण मुद्दा प्रौद्योगिकी की सीमाएँ और डेटा सुरक्षा प्रणालियों में निहित कमज़ोरियाँ हैं। उन्नत एन्क्रिप्शन और सुरक्षा प्रोटोकॉल के बावजूद, हैकर्स लगातार डेटाबेस में सेंध लगाने, सिस्टम की खामियों का फायदा उठाने और बायोमेट्रिक डेटा में हेरफेर करने के लिए नए तरीके विकसित कर रहे हैं। संग्रहीत व्यक्तिगत डेटा की बड़ी मात्रा भी साइबर अपराधियों के लिए एक लक्ष्य बनाती है, जिससे डेटा का उल्लंघन और दुरुपयोग एक बढ़ती चिंता बन जाती है।[v] बायोमेट्रिक सिस्टम, पहचान सत्यापन का एक सुरक्षित तरीका प्रदान करने के उद्देश्य से है, लेकिन धोखाधड़ी के लिए यह अतिसंवेदनशील है। फ़िंगरप्रिंट और आईरिस स्कैन की नकल की जा सकती है, और कुछ मामलों में, लोगों ने सुरक्षा उपायों को दरकिनार करने के लिए बायोमेट्रिक विवरण बनाने के तरीके भी खोज लिए हैं। आधार प्रमाणीकरण प्रणाली में सुरक्षा संबंधी खामियों की पहचान की गई है, जहाँ तकनीक हमेशा बायोमेट्रिक जानकारी को रिकॉर्ड से सटीक रूप से मेल नहीं खाती है, जिससे गलत पहचान होती है और संभावित रूप से पहचान की चोरी को बढ़ावा मिलता है। कानूनी दृष्टिकोण से, कानून और तकनीक के बीच सामंजस्य स्थापित करने में एक महत्वपूर्ण चुनौती है। जबकि आधार के पीछे की तकनीक उन्नत है, इसे नियंत्रित करने वाला कानूनी ढांचा अक्सर तकनीकी प्रगति से पीछे रह जाता है। डेटा गोपनीयता और सुरक्षा के बारे में स्पष्ट और व्यापक कानूनों की कमी का मतलब है कि कानूनी प्रणाली आधार-आधारित अपराधों को प्रभावी ढंग से संबोधित करने के लिए संघर्ष करती है।[vi] एक मजबूत ढांचे की अनुपस्थिति अक्सर दुरुपयोग के लिए जगह छोड़ती है, जैसे कि व्यक्तिगत जानकारी तक अनधिकृत पहुँच, धोखाधड़ी और भेदभाव। इसके अतिरिक्त, भारत के डेटा गोपनीयता कानून, हालांकि विकसित हो रहे हैं, फिर भी अन्य देशों की तरह व्यापक नहीं हैं, जिससे आधार डेटा को लीक होने से बचाना सुनिश्चित करना कठिन हो जाता है। आधार की सफलता में सामाजिक और मानसिक बाधाएं भी अहम भूमिका निभाती हैं। आधार के दुरुपयोग के संभावित जोखिमों और अपनी जानकारी को कैसे सुरक्षित रखा जाए, इस बारे में आम जनता में भी जागरूकता की कमी है। कई नागरिक अपने आधार डेटा तक अनधिकृत पहुँच के असली निहितार्थों से अनजान रहते हैं, जिससे गलतफहमियाँ पैदा होती हैं और सतर्कता की कमी होती है। इसके अलावा, व्यक्तिगत जानकारी की सुरक्षा करने की प्रणाली की क्षमता के प्रति समाज में गहरा अविश्वास मौजूद है, जो इस प्रणाली को अपनाने में अनिच्छा को और बढ़ाता है। आधार-आधारित अपराधों को कम करने के लिए जन जागरूकता को मजबूत करना और प्रणाली में विश्वास पैदा करना महत्वपूर्ण होगा।

6. आधार जनित अपराधों से बचाव

आधार-आधारित अपराधों को रोकने के लिए उन्नत तकनीक, कानूनी सुधार और जन जागरूकता को मिलाकर बहुआयामी दृष्टिकोण की आवश्यकता है। सुरक्षा बढ़ाने का एक महत्वपूर्ण पहलू बेहतर एन्क्रिप्शन और बायोमेट्रिक तकनीकों के कार्यान्वयन के माध्यम से है। आधार डेटा अत्यधिक संवेदनशील होने के कारण, अनधिकृत पहुँच से बचने के लिए एन्क्रिप्ट किया जाना चाहिए। अत्याधुनिक एन्क्रिप्शन एल्गोरिदम का उपयोग यह सुनिश्चित करेगा कि डेटा भंडारण और संचरण दोनों के दौरान सुरक्षित रहे। इसके अतिरिक्त, फिंगरप्रिंट और आईरिस स्कैन जैसी बायोमेट्रिक तकनीकों को अधिक उन्नत तकनीकों के साथ बढ़ाने की आवश्यकता है, ताकि अधिक सटीकता सुनिश्चित हो और प्रतिरूपण के जोखिम को कम किया जा सके।[vii]

आधार सुरक्षा के इर्द-गिर्द ढांचे को मजबूत करने के लिए कानूनी सुधार आवश्यक हैं। आधार अधिनियम में संशोधन, यह सुनिश्चित करते हुए कि यह डेटा प्रोसेसिंग के लिए सुरक्षा प्रावधानों को सख्ती से अनिवार्य करता है, को प्राथमिकता दी जानी चाहिए। कानून में लापरवाही के लिए दंड भी शामिल होना चाहिए।[viii] इसके अलावा, आधार के दुरुपयोग से जुड़े साइबर अपराधों के खिलाफ और अधिक कड़े कानूनी प्रावधान होने चाहिए, जिसमें अपराधियों पर मुकदमा चलाने के लिए स्पष्ट दिशा-निर्देश हों।

इस प्रक्रिया में जन जागरूकता और शिक्षा भी उतनी ही महत्वपूर्ण है। नागरिकों को आधार सुरक्षा के महत्व और उनकी व्यक्तिगत जानकारी की सुरक्षा के बारे में जागरूक किया जाना चाहिए। एक राष्ट्रीय जागरूकता अभियान आधार विवरण की सुरक्षा के बारे में विस्तृत दिशा-निर्देश प्रदान कर सकता है। इसके अतिरिक्त, डिजिटल सुरक्षा और गोपनीयता अधिकारों के बारे में जनता को शिक्षित करने से उन्हें डिजिटल दुनिया में आम नुकसानों से बचने के लिए सशक्त बनाया जा सकता है, जिससे यह सुनिश्चित हो सके कि व्यक्ति धोखेबाजों के लिए आसान लक्ष्य न बन सके।[ix]

7. निष्कर्ष

UIDAI द्वारा संचालित आधार प्रणाली भारत के सामाजिक और आर्थिक परिदृश्य में एक महत्वपूर्ण भूमिका निभाती है, जो लाखों नागरिकों को एक विशिष्ट पहचान प्रदान करती है। हालाँकि, इसके व्यापक उपयोग ने पहचान व डेटा की चोरी, धोखाधड़ी और अधिकृत सेवाओं के दुरुपयोग सहित विभिन्न आधार-आधारित अपराधों को भी जन्म दिया है। इन चुनौतियों ने एक एकीकृत दृष्टिकोण की तत्काल आवश्यकता को उजागर किया है जो आधार की सुरक्षा और अखंडता सुनिश्चित करने के लिए कानूनी ढाँचों के साथ तकनीकी प्रगति का सामंजस्य स्थापित करता है। जबकि आधार की सुरक्षा में सुधार करने में महत्वपूर्ण प्रगति हुई है - जैसे कि बायोमेट्रिक सिस्टम, डेटा एन्क्रिप्शन और AI-संचालित निगरानी को अपनाना - फिर भी ऐसी कमज़ोरियाँ हैं जिन्हें संबोधित करने की आवश्यकता है। बायोमेट्रिक धोखाधड़ी, डेटा लीक और साइबर अपराधों से जुड़े जोखिम उपयोगकर्ताओं की गोपनीयता और सुरक्षा के लिए लगातार खतरा पैदा करते हैं। आधार अधिनियम और विभिन्न साइबर सुरक्षा कानूनों के तहत कानूनी प्रावधान एक मजबूत आधार प्रदान करते हैं, लेकिन उन्हें साइबर खतरों की बढ़ती संभावनाओं और दुरुपयोग के लिए सख्त दंड सुनिश्चित करने के लिए विकसित होना चाहिए।

एक मजबूत और दूरदर्शी समाधान के साथ ही बेहतर सुरक्षा उपायों को अपनाने की आवश्यकता है, जिसमें बहु-कारक प्रमाणीकरण और उन्नत एन्क्रिप्शन तकनीक शामिल हैं। कानूनी सुधार, खास तौर पर निजता सुरक्षा को मजबूत करने वाले और संवैधानिक अधिकारों के साथ संरेखित करने वाले सुधार भी महत्वपूर्ण हैं। इसके अलावा, जागरूकता अभियानों और डिजिटल साक्षरता के माध्यम से नागरिकों को सशक्त बनाना आधार-आधारित अपराधों को रोकने में महत्वपूर्ण भूमिका निभाएगा। तकनीकी सुरक्षा और कानूनी सुरक्षा उपायों को मजबूत करके, हम यह सुनिश्चित कर सकते हैं कि आधार शोषण के बजाय सशक्तिकरण का साधन बना रहे, जिससे सभी के लिए इसके लाभों की सुरक्षा हो जिससे आधार के लिए एक सुरक्षित भविष्य सुनिश्चित हो सके।

संदर्भ-सूची :-

[i] कुमार ए,(2022). प्रिवेंशन ऑफ आधार बेस्ड क्राइमस: हार्मोनाइजेशन ऑफ टेक्नोलॉजी एंड लॉ, जर्नल ऑफ साइबर सिक्योरिटी ऐंड लॉ. 10(3), 101-110.

[ii] सेंटर फॉर इंटरनेट एंड सोसाइटी. (2017). आधार एंड साइबर सिक्योरिटी: एन एनालिसिस ऑफ सिक्योरिटी ब्रेनचेज.

[iii] स्मिथ, 2020, पृष्ठ 124

[iv] एस. कुमार, 2020, जर्नल ऑफ साइबर लॉ, पृष्ठ 125

[v] चंद्रन.आर. (2018). सिक्योरिटी मेजर इन आधार टेक्नोलॉजी,जर्नल ऑफ़ डिजिटल सिक्योरिटी,45(2), 250-260.

[vi]मेहता , आर.(2020). लीगल फ्रेमवर्क फॉर डाटा सिक्योरिटी ऐंड प्राइवेसी. जर्नल ऑफ इन्फोर्मेशन लॉ,34(1), 40-50.

[vii] वर्मा और सिंह, 2020, जर्नल ऑफ़ साइबरसिक्यूरिटी, पृष्ठ 112

[viii]घोष, 2019, द लीगल आस्पेक्ट ऑफ आधार: चैलेंजेस ऐंड ऑपर्च्युनिटीज पृष्ठ .28

[ix] चंद्रन, 2020, जर्नल ऑफ़ डिजिटल सिक्योरिटी, पृष्ठ 88