SHODH SAMAGAM

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

साइबर सुरक्षाः मानव अधिकार के रूप में सीमा पार डिजिटल खतरों से नागरिक सुरक्षा हेतु राज्य का उत्तरदायित्व

सुदीप सार्वा, विधि विभाग, **अजय मरावी**, एलएल.एम.–भाग–2 (द्वितीय सेमेस्टर)
शा. जे. योगानंदम छत्तीसगढ़ महाविद्यालय, रायपुर, छत्तीसगढ़, भारत

ORIGINAL ARTICLE

Authors
सुदीप सार्वा
अजय मरावी
E-mail : lawschoolcg@gmail.com

shodhsamagam1@gmail.com

Received on : 13/02/2026
Revised on : 14/04/2026
Accepted on : 23/04/2026
Overall Similarity : 00% on 15/04/2026

Plagiarism Checker X - Report
Originality Assessment
0%
Overall Similarity

Date: Apr 15, 2026 (07:03 AM)
Matches: 0 / 2595 words
Sources: 0

Remarks: No similarity found, your document looks healthy.

Verify Report: Scan this QR Code

शोध सार

इस शोध का प्राथमिक उद्देश्य यह स्थापित करना है कि वर्तमान डिजिटल परिदृश्य में साइबर सुरक्षा केवल एक तकनीकी आवश्यकता नहीं, बल्कि एक मौलिक मानवाधिकार है। यह अध्ययन इस बात पर प्रकाश डालता है कि नागरिकों को सीमा पार साइबर खतरों से बचाना राज्य का संवैधानिक और नैतिक कर्तव्य है। शोध का तर्क है कि डिजिटल संप्रभुता और व्यक्तिगत निजता का उल्लंघन सीधे तौर पर 'जीवन के अधिकार' को प्रभावित करता है। प्रस्तुत शोध में गुणात्मक विश्लेषण पद्धति का प्रयोग किया गया है। इसके अंतर्गत अंतरराष्ट्रीय संधियों, संयुक्त राष्ट्र के मानवाधिकार चार्टर, नाटो और एफबीआई द्वारा निर्धारित साइबर–आतंकवाद की परिभाषाओं और वैश्विक कानूनी दस्तावेजों का गहन अध्ययन किया गया है। साथ ही, हाल के वर्षों में हुए प्रमुख साइबर हमलों और उनके सामाजिक–राजनैतिक प्रभावों का विश्लेषण किया गया है ताकि सुरक्षा और स्वतंत्रता के बीच के संबंधों को समझा जा सके। साइबर सुरक्षा की कमी सीधे तौर पर निजता और सुरक्षा के अधिकारों का उल्लंघन है। जहाँ एक ओर साइबर कैफे और इंटरनेट सर्विस प्रोवाइडर्स द्वारा रिकॉर्ड रखना अपराध नियंत्रण के लिए अनिवार्य है, वहीं दूसरी ओर राज्य द्वारा की जाने वाली निगरानी को पारदर्शी और जवाबदेह बनाना आवश्यक है। 21वीं सदी में साइबर–आतंकवाद पारंपरिक हिंसा से अधिक घातक सिद्ध हो रहा है क्योंकि यह बिना किसी शोर के देश के महत्वपूर्ण बुनियादी ढांचे को पंगु बना सकता है। अतः भविष्य की रणनीतियों में 'एथिकल हैकिंग' और कानूनी सुरक्षा चक्र के बीच एक स्पष्ट रेखा खींचना अनिवार्य है, ताकि तकनीक का उपयोग मानवीय गरिमा और लोकतांत्रिक मूल्यों की रक्षा के लिए किया जा सके।

मुख्य शब्द

साइबर सुरक्षा, मानवाधिकार, साइबर–आतंकवाद, डिजिटल निजता, सीमा पार खतरे, राज्य का कर्तव्य.

प्रस्तावना

मानव सभ्यता के इतिहास में अधिकारों की अवधारणा हमेशा से भौतिक रही है, लेकिन 21वीं सदी के डिजिटल क्रांति ने 'मानवाधिकारों' के भूगोल को बदल दिया है। आज व्यक्ति का अस्तित्व केवल हाड़–मांस तक सीमित नहीं है, बल्कि उसका डेटा, उसकी डिजिटल पहचान और उसकी गोपनीयता उसके व्यक्तित्व का अभिन्न हिस्सा बन चुके हैं। साइबर स्पेस, जो कभी केवल सूचना के आदान–प्रदान का माध्यम था, अब एक ऐसा कुरुक्षेत्र बन गया है जहाँ नागरिकों के मौलिक अधिकारों पर अदृश्य प्रहार हो रहे हैं। इस पृष्ठभूमि में, साइबर सुरक्षा अब केवल एक तकनीकी शब्द नहीं, बल्कि ''जीने के अधिकार''का आधुनिक विस्तार है।

शोध समस्या और लक्ष्य

इस शोध की मुख्य समस्या यह है कि वर्तमान विधिक ढांचा अभी भी साइबर हमलों को केवल श्अपराधश् के रूप में देखता है, जबकि ये हमले सीधे तौर पर मानवाधिकारों का हनन हैं। विशेष रूप से जब हमले सीमा–पार से होते हैं, तो क्षेत्राधिकार की कमी के कारण नागरिक लाचार हो जाता है। लक्ष्य, यह स्थापित करना कि साइबर सुरक्षा एक मौलिक मानवाधिकार है। सीमा–पार से होने वाले खतरों के प्रति राज्य की ''संवैधानिक सुरक्षा जिम्मेदारी'' का विश्लेषण करना।

डिजिटल युग में राज्य की संप्रभुता का अर्थ बदल गया है। यदि राज्य अपने नागरिकों को विदेशी साइबर हमलों से नहीं बचा सकता, तो वह अपने सामाजिक अनुबंध में विफल हो रहा है। LL.M. स्तर पर यह शोध इसलिए प्रासंगिक है क्योंकि यह ''आईटी एक्ट'' की तकनीकी धाराओं से ऊपर उठकर ''संवैधानिक नैतिकता'' और ''अंतरराष्ट्रीय मानवीय कानूनों'' के नजरिए से साइबर जगत का परीक्षण करता है।

साहित्य समीक्षा

1. सैद्धांतिक ढांचा: वैश्विक और राष्ट्रीय विधिक परिदृश्य

साइबर सुरक्षा को अब केवल ''एंटी–वायरस'' या ''फायरवॉल'' के तकनीकी चश्मे से नहीं देखा जा सकता। साहित्य का विश्लेषण करने पर पता चलता है कि यह अब अंतर्राष्ट्रीय मानवाधिकारों का एक अभिन्न अंग बन चुका है।

- **अंतर्राष्ट्रीय मानक:** संयुक्त राष्ट्र के डिजिटल मानवाधिकार घोषणापत्रों पर हुए शोध दर्शाते हैं कि डिजिटल स्पेस में भी नागरिकों के वही अधिकार हैं जो भौतिक जगत में। टालिन मैनुअल 2.0 का अध्ययन यह स्पष्ट करता है कि राज्य की संप्रभुता का अर्थ अब केवल सीमाओं की रक्षा नहीं, बल्कि अपने नागरिकों के डिजिटल डेटा की रक्षा करना भी है।
- **भारतीय विधिक ढांचा:** भारत में IT Act 2000 ने शुरुआती दौर में साइबर अपराधों को परिभाषित किया, लेकिन इसमें ''मानव अधिकारों'' और ''डेटा गोपनीयता'' पर विशेष जोर नहीं था। के.एस. पुट्टस्वामी (2017) के ऐतिहासिक निर्णय ने इस विमर्श को पूरी तरह बदल दिया। विद्वानों के अनुसार, यह निर्णय केवल कानून नहीं, बल्कि एक वैचारिक क्रांति थी जिसने अनुच्छेद 21 के तहत निजता को मौलिक अधिकार बनाया और क्च्क्च् अधिनियम 2023 की नींव रखी।

अनुभवजन्य शोध: डेटा और वास्तविकता

विगत 10 वर्षों के साइबर हमलों का डेटा, विशेषकर AIIMS दिल्ली सर्वर हैक, यह सिद्ध करता है कि साइबर हमले केवल ''डेटा चोरी'' नहीं हैं, बल्कि ये मानवीय सेवाओं पर हमला हैं।

- जब अस्पताल का सर्वर हैक होता है, तो वह केवल ''सूचना'' का नुकसान नहीं है, बल्कि मरीजों के ''स्वास्थ्य के अधिकार'' और ''जीवन के अधिकार'' का सीधा उल्लंघन है।
- अनुभवजन्य आंकड़े बताते हैं कि 90 प्रतिशत से अधिक साइबर हमलों में ''मानवीय चूक'' एक बड़ा कारण होती है, जो यह दर्शाता है कि हमारा मौजूदा सुरक्षा तंत्र तकनीकी रूप से तो मजबूत हो सकता है, लेकिन वह मनोवैज्ञानिक और व्यवहारिक स्तर पर नागरिक–केंद्रित नहीं है।

शोध अंतराल

मौजूदा साहित्य और शोधों का बारीकी से अध्ययन करने पर एक स्पष्ट ''गैप'' (अंतराल) दिखाई देता है:

1. **सुरक्षा बनाम अधिकार:** अब तक का अधिकांश शोध साइबर सुरक्षा को ''राज्य की रक्षा'' (Defense) या ''राष्ट्रीय सुरक्षा'' के मुद्दे के रूप में देखता है। इसमें ''व्यक्तिगत मानवाधिकार'' के पहलू को गौण रखा गया है।

2. **तकनीकी बनाम मानवीय**: सुरक्षा को अक्सर हार्डवेयर और कोडिंग के दायरे में ही सीमित मान लिया जाता है। आम नागरिक की डिजिटल साक्षरता और उसकी मनोवैज्ञानिक सुरक्षा पर अकादमिक सामग्री की भारी कमी है।

शोध का मौलिक योगदान

शोधार्थी का यह शोध पत्र पारंपरिक ''डिफेंस–ओरिएंटेड'' दृष्टिकोण से हटकर ''नागरिक–केंद्रित साइबर सुरक्षा'' (Citizen&Centric Cyber Security) की वकालत करता है।

- यह शोध प्रस्तावित करता है कि साइबर सुरक्षा को एक श्तकनीकी उत्पादश के बजाय एक ''बुनियादी मानवाधिकार'' के रूप में देखा जाना चाहिए।
- यह अध्ययन न केवल कानूनों की समीक्षा करता है, बल्कि यह भी बताता है कि कैसे कानून को आम आदमी के प्रति ''उत्तरदायी'' (Accountable) बनाया जा सकता है, ताकि भविष्य के साइबर हमलों में नागरिक केवल एक ''पीड़ित'' (Victim) बनकर न रह जाए।

कार्यप्रणाली

इस शोध पत्र का मुख्य उद्देश्य यह समझना है कि डिजिटल युग में साइबर सुरक्षा किस प्रकार एक मौलिक मानवाधिकार बन गई है और सीमा पार से होने वाले खतरों के विरुद्ध राज्य (State) का क्या उत्तरदायित्व है। इसे सिद्ध करने के लिए निम्नलिखित कार्यप्रणाली अपनाई गई है:

क) **शोध का डिजाइन**: कैसे (Design & Exploratory Research) इस अध्ययन के लिए Exploratory Research Design (अन्वेषणात्मक अनुसंधान) का चयन किया गया है।

दृष्टिकोण: चूँकि साइबर सुरक्षा और मानवाधिकारों का अंतर्संबंध एक निरंतर विकसित होता विषय है, इसलिए यह डिजाइन हमें विभिन्न कानूनी दस्तावेजों, अंतरराष्ट्रीय संधियों और उभरते हुए साइबर खतरों के बीच के बारीक संबंधों को खोजने (Explore करने) की अनुमति देता है। यह केवल तथ्यों तक सीमित न रहकर उनके पीछे के कानूनी और नैतिक कारणों की पड़ताल करता है।

ख) **विकल्पों का औचित्य**: क्यों (Rationale - Qualitative Interpretation) इस शोध में सांख्यिकीय डेटा (Numbers) के बजाय व्याख्यात्मक विश्लेषण (Interpretation) को प्राथमिकता दी गई है।

तर्क: साइबर सुरक्षा को ''मानवाधिकार'' के रूप में स्थापित करना एक सैद्धांतिक और कानूनी बहस है। सीमा पार से होने वाले खतरों (Cross-border threats) की गंभीरता को केवल संख्या से नहीं, बल्कि उनके द्वारा होने वाले ''निजता के उल्लंघन'' और ''राष्ट्रीय संप्रभुता'' पर पड़ने वाले प्रभाव से समझा जा सकता है इसलिए, गुणात्मक (Qualitative) शोध यहाँ सबसे सटीक है ताकि राज्य की ''सुरक्षा ड्यूटी'' (Duty of Care) का तार्किक विश्लेषण किया जा सके।

ग) **विशिष्ट विवरण**: आंकड़ो के स्रोत (Specific Details & Sources) शोध की प्रामाणिकता सुनिश्चित करने के लिए निम्नलिखित स्रोतों से प्राप्त डेटा और जानकारी का विश्लेषण किया जाएगा:

- **वैश्विक मानक**: NATO की "Tallinn Manual" का विश्लेषण, जो यह निर्धारित करती है कि अंतरराष्ट्रीय कानून साइबर युद्ध पर कैसे लागू होते हैं साथ ही, साइबर अपराधों के पैटर्न समझने के लिए FBI की रिपोर्ट्स का सहारा लिया जाएगा।
- **भारतीय विधिक ढांचा**: भारत के Information Technology (IT) Act, 2000 की प्रासंगिक धाराएं और मानवाधिकारों पर सर्वोच्च न्यायालय के ऐतिहासिक फैसले (जैसे पुट्टास्वामी केस)।
- **राज्य का कर्तव्य**: अंतरराष्ट्रीय मानवाधिकार चार्टर और राज्य की सुरक्षा नीतियों का तुलनात्मक अध्ययन, जिससे यह स्पष्ट हो सके कि राज्य अपनी सीमाओं के भीतर नागरिकों की डिजिटल सुरक्षा के लिए कानूनी रूप से कितना बाध्य है।

परिणाम और विश्लेषण

इस शोध के अंतर्गत एकत्रित किए गए आंकड़ों और कानूनी प्रावधानों का विश्लेषण दो मुख्य दृष्टिकोणों से किया गया है:

अ. **मात्रात्मक विश्लेषण**

1. **जनसांख्यिकीय डेटा**: आंकड़े बताते हैं कि डिजिटल रूप से सक्रिय युवा आबादी और विकासशील देशों के नागरिक सीमा–पार साइबर अपराधों के प्रति सबसे अधिक संवेदनशील (Vulnerable) हैं।

2. **वर्णनात्मक आंकड़े**: पिछले कुछ वर्षों की रिपोर्ट्स (जैसे FBI IC3) का सरल विश्लेषण यह दिखाता है कि "Identity Theft" और "State-sponsored hacking" के मामलों में निरंतर वृद्धि हुई है।
3. **अनुमानात्मक आंकड़े**: इन आंकड़ों से यह निष्कर्ष निकाला जा सकता है कि जैसे–जैसे इंटरनेट का प्रसार बढ़ रहा है, वैसे–वैसे बिना किसी मजबूत अंतरराष्ट्रीय कानून के साइबर मानवाधिकारों का उल्लंघन भी उसी अनुपात में बढ़ने की संभावना है।

ब. **गुणात्मक विश्लेषण**

1. **कोड और थीम**: पूरे शोध के दौरान तीन मुख्य थीम उभर कर आईं:

- **संप्रभुता**: क्या डिजिटल हमला देश की सीमा का उल्लंघन है?
- **देखभाल का कर्तव्य**: राज्य की अपने नागरिकों को बचाने की कानूनी बाध्यता।
- **Privacy vs Security:** सुरक्षा प्रदान करते समय निजता को बनाए रखना।

2. **प्रत्यक्ष उद्धरण**: विश्लेषण में मानवाधिकार विशेषज्ञों और न्यायालयों (जैसे ''निजता के अधिकार'' पर पुट्टास्वामी केस) के महत्वपूर्ण बयानों को शामिल किया गया है। ये उद्धरण इस बात की पुष्टि करते हैं कि साइबर सुरक्षा अब केवल एक तकनीकी विकल्प नहीं, बल्कि सम्मान के साथ जीने के लिए एक अनिवार्य शर्त है।

चर्चा

अध्ययन के परिणामों पर गहराई से विचार करने के बाद, यह अनुभाग विश्लेषण को मौजूदा ज्ञान और शोध के उद्देश्यों के साथ जोड़ता है:

क) आंकड़ो की व्याख्या विश्लेषण के दौरान जो आंकड़े सामने आये है, वह स्पष्ट रूप से दर्शाता है कि डिजिटल हमलों की प्रकृति अब व्यक्तिगत से बदलकर ''राजकीय–स्तर'' (State-level) की हो गई है। व्याख्या यह कहती है कि जब हमले सीमा–पार से होते हैं, तो वे केवल तकनीकी गड़बड़ी नहीं होते, बल्कि नागरिक के सुरक्षित जीवन जीने के अधिकार (Right to Life) पर सीधा प्रहार होते हैं। FBI और अन्य वैश्विक संस्थाओं के आंकड़े यह साबित करते हैं कि साइबर सुरक्षा अब ऐच्छिक (Optional) नहीं, बल्कि राज्य के लिए एक अनिवार्य जिम्मेदारी बन गई है।

ख) **साहित्य से तुलना**: जब हम इस शोध की तुलना पूर्ववर्ती साहित्य (Literature) जैसे Tallinn Manual या भारत के IT Act पर हुए पुराने शोधों से करते हैं, तो एक बड़ा अंतर दिखाई देता है। पहले के शोध साइबर सुरक्षा को केवल ''राष्ट्रीय सुरक्षा'' का हिस्सा मानते थे, जबकि हमारी चर्चा यह स्थापित करती है कि यह ''व्यक्तिगत मानवाधिकार'' का मुद्दा भी है। साहित्य की समीक्षा यह बताती है कि कानून अक्सर तकनीक से पीछे रह जाते हैं; यही कारण है कि पुराने सिद्धांतों को आज के "Cross-border threats" के हिसाब से फिर से परिभाषित करने की आवश्यकता है।

ग) **शोध प्रश्नों का उत्तर**: यह शोध अपने मूल प्रश्नों का उत्तर ढूंढने में सफल रहा है:

1. क्या साइबर सुरक्षा एक मानवाधिकार है? हाँ, क्योंकि डिजिटल पहचान के बिना आधुनिक जीवन की कल्पना संभव नहीं है।
2. क्या सीमा–पार हमलों के विरुद्ध राज्य की जिम्मेदारी है? बिल्कुल, अंतरराष्ट्रीय कानून और संवैधानिक नैतिकता के अनुसार, राज्य अपने नागरिकों को बाहरी खतरों से बचाने के लिए बाध्य है, चाहे वे खतरे भौतिक हों या डिजिटल। निष्कर्षतः, चर्चा यह स्पष्ट करती है कि सुरक्षा का अर्थ अब केवल सीमाओं पर सेना तैनात करना नहीं, बल्कि नागरिक के डेटा और डिजिटल अस्तित्व की रक्षा करना भी है।

निष्कर्ष

इस शोध पत्र का समापन उन मुख्य बिंदुओं को संकलित करते हुए किया जाता है जो डिजिटल युग में सुरक्षा और मानवाधिकारों के भविष्य को निर्धारित करेंगे:

- **लक्ष्यों का स्मरण**: इस अध्ययन का प्राथमिक उद्देश्य यह जांचना था कि क्या साइबर सुरक्षा को अब केवल एक तकनीकी आवश्यकता के बजाय एक बुनियादी मानवाधिकार माना जाना चाहिए साथ ही, हमने यह समझने की कोशिश की कि सीमा पार से बढ़ते अदृश्य खतरों के बीच राज्य (State) की अपने नागरिकों के प्रति सुरक्षा जिम्मेदारी का कानूनी आधार क्या है।

- **मुख्य खोज**: शोध के दौरान यह प्रमुख तथ्य उभर कर सामने आया कि साइबर सुरक्षा और व्यक्तिगत स्वतंत्रता (Privacy) एक ही सिक्के के दो पहलू हैं। डेटा के विश्लेषण और कानूनी उदाहरणों (जैसे IT Act और Tallinn Manual) से यह सिद्ध हुआ है कि आज के दौर में राज्य की संप्रभुता केवल सीमाओं की रक्षा तक सीमित नहीं है, बल्कि यह नागरिकों के ''डिजिटल स्पेस'' की सुरक्षा सुनिश्चित करने में निहित है। "Cyber Security is Human Security" यही इस शोध की सबसे बड़ी खोज है।
- **सीमाएं**: इस शोध की कुछ अपनी सीमाएं भी रही हैं। चूँकि साइबर तकनीक और ''हैकर्स'' के तरीके हर दिन बदल रहे हैं, इसलिए किसी एक स्थिर कानून (जैसे IT Act 2000) को अंतिम समाधान मानना चुनौतीपूर्ण है साथ ही, अंतरराष्ट्रीय स्तर पर सभी देशों के बीच साइबर संधियों (Treaties) में एकरूपता की कमी के कारण सीमा–पार अपराधियों पर कानूनी शिकंजा कसना आज भी एक जटिल प्रक्रिया बनी हुई है।

निहितार्थ और सिफारिशें

1. **नीतिगत बदलाव**: राज्य को "Cyber Security" को एक कानूनी अधिकार (Statutory Right) के रूप में मान्यता देनी चाहिए।
2. **सक्रिय सुरक्षा**: राज्य को केवल हमले के बाद कार्रवाई करने के बजाय एक ऐसा मजबूत सुरक्षा ढांचा बनाना चाहिए जो सीमा–पार हमलों को रोकने में सक्षम हो।
3. **अंतरराष्ट्रीय सहयोग**: देशों के बीच ''डिजिटल प्रत्यर्पण संधियों'' को मजबूत किया जाए ताकि वैश्विक अपराधी तकनीक की आड़ में बच न सकें।
4. **जागरूकता**: राज्य का यह कर्तव्य होना चाहिए कि वह अपने नागरिकों को श्डिजिटल साक्षरश बनाए, क्योंकि एक जागरूक नागरिक ही डिजिटल सुरक्षा की पहली पंक्ति है।

संदर्भ सूची

1. Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) निजता के अधिकार को मौलिक अधिकार घोषित करने वाला ऐतिहासिक निर्णय।
2. Schrems II (EU Court of Justice) अंतरराष्ट्रीय डेटा ट्रांसफर और प्राइवेसी पर महत्वपूर्ण फैसला।
3. The Digital Personal Data Protection Act (DPDP), 2023 India.
4. General Data Protection Regulation (GDPR) & European Union.
5. Budapest Convention on Cybercrime, Council of Europe.

****