डिजिटल शासन और साइबर अपराधो पर सार्वजनिक, संवैधानिक जवाबदेहीः—नागरिको की सुरक्षा के परिपेक्ष्य में

विवेचना पाण्डेय,
असिस्टेंट प्रोफेसर—आर.के.डी.एफ. युनिवर्सिटी भोपाल (म0प्र0)

सारां"ाः— डिजिटल युग में सूचना और तकनीक का विस्तार अभूतपूर्व स्तर पर हुआ हैं। इंटरनेट भोसल मीडिया और डिजिटल प्लेटफार्म ने संचार व्यापार, f" ाक्षा और भाासन की नई दि" ा तय की हैं परंतु इस तकनीकी क्रांति के साथ साईबर अपराधो की चुनौतिया भी सामने आई हैं। जैसे हकिंग साइबर ठगी डेटा चोरी, आनलाईन उत्पीड़न और फेक न्यूज और निजी गोपनियता का हनन। भारतीय संविधान और विविध ढाचां इन अपराधो से नागरिको की रक्षा के लिये निरंतर विकसित हो रहा हैं। सूचना प्रौद्योगिकी अधिनियम, 2000 दंड संहिता की विभिन्न धाराएँ और न्यायालयो के निर्णय डिजिटल सुरक्षा के संरक्षण में महत्वपूर्ण निभाते हैं। डिजिटल शासन (Digital Governance) के बढ़ते विस्तार ने प्रशासनिक पारदर्शिता, सेवा वितरण की दक्षता तथा नागरिकों की भागीदारी को सशक्त किया है। ई—गवर्नेंस, डिजिटल इंडिया, ऑनलाइन सार्वजनिक सेवाएँ और डेटा—आधारित निर्णय प्रणाली ने शासन को अधिक सुलभ और उत्तरदायी बनाने का प्रयास किया है। किंतु इसी के साथ साइबर अपराधोंकृजैसे डेटा चोरी, साइबर धोखाधड़ी, पहचान की चोरी, ऑनलाइन उत्पीड़न और सरकारी डिजिटल प्रणालियों पर हमलो में तीव्र वृद्धि हुई है, जिससे सार्वजनिक संवैधानिक जवाबदेही (Public Constitutional Accountability) की अवधारणा नई चुनौतियों के समक्ष खड़ी हो गई है।यह शोध पत्र डिजिटल शासन के संदर्भ में साइबर अपराधों से उत्पन्न संवैधानिक, विधिक एवं प्रशासनिक प्रश्नों का विश्लेषण करता है। भारतीय संविधान द्वारा प्रदत्त मौलिक अधिकारोंकृविशेषकर अनुच्छेद 14 (समानता का अधिकार), अनुच्छेद 19 (अभिव्यक्ति की स्वतंत्रता) और अनुच्छेद 21 (जीवन एवं व्यक्तिगत स्वतंत्रता का अधिकार)कृपर साइबर अपराधों के प्रभाव का विवेचन किया गया है। डिजिटल प्लेटफार्मों पर नागरिकों के व्यक्तिगत डेटा की सुरक्षा, गोपनीयता के अधिकार तथा राज्य की जवाबदेही को इस शोध पत्र का केंद्रीय विषय बनाया गया है। शोध पत्र में यह तर्क प्रस्तुत किया गया है कि डिजिटल शासन केवल तकनीकी नवाचार का विषय नहीं है, बल्कि यह संवैधानिक मूल्योंकृन्याय, स्वतत्रता, समानता और गरिमाकृमें गहराई से जुड़ा हुआ है। जब राज्य डिजिटल माध्यमों के माध्यम से सेवाएँ प्रदान करता है, तब उस पर यह संवैधानिक दायित्व भी बढ़ जाता है कि वह साइबर अपराधों से नागरिकों की रक्षा करे और प्रभावी शिकायत निवारण तंत्र उपलब्ध कराए। सूचना प्राद्योगिकी अधिनियम, 2000, प्रस्तावित डिजिटल व्यक्तिगत डेटा संरक्षण कानून तथा न्यायिक निर्णयों के माध्यम से राज्य की जवाबदेही के ढांचे का विश्लेषण करता है।कि साइबर अपराधों की रोकथाम हेतु केवल दंडात्मक कानून पर्याप्त नहीं हैं, बल्कि पारदर्शी डिजिटल नीतियाँ, स्वतंत्र निगरानी तंत्र, न्यायिक सक्रियता तथा नागरिक जागरूकता भी आवश्यक है। डिजिटल शासन में सार्वजनिक संवैधानिक जवाबदेही को सुदृढ़ करने के लिए तकनीक, कानून और संवैधानिक नैतिकता के समन्वय की आवश्यकता है। यह शोध पत्र नीति निर्माताओं, विधि विशेषज्ञों के लिए डिजिटल युग में शासन और अधिकारों के संतुलन को समझने का एक महत्वपूर्ण आधार प्रदान करता है।

[Pandey, V. **डिजिटल भाासन और साइबर अपराधो पर सार्वजनिक, संवैधानिक जवाबदेहीः—नागरिको की सुरक्षा के परिपेक्ष्य में**. *The International Journal of Interpretation, Observation and Analysis*, 2026; Volume 1, Issue 2 (January-March): Page Number: 79-85. **ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 6.489. (INTERNATIONAL CONFERENCE ON EDUCATIONAL RESEARCH & INNOVATION, Organised by Mudo Tamo Memorial College, Ziro (Arunachal Pradesh)** Collaboration with COSMOSSKY HORIZON (OPC) PRIVATE LIMITED, Date: 8th February, 2026, Mode: Online/Offline (Hybrid).

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

प्रस्तवानाः— 21वीं सदी का भारत सूचना और प्रद्योगिकी के क्षेत्र में तीव्र गति से प्रगति कर रहा हैं। इंटरनेट का प्रसार न केवल ज्ञान और जानकारी का स्त्रोत बना हैं, बल्कि यह सामाजिक राजनीतिक और आर्थिक क्रियाकलापो का केन्द्र भी बन गया हैं। सो" ाल मीडिया ने अभिव्यक्ति की स्वतंत्रता का नए आयाम दिये हैं— जहाँ पर हर नागरिक अपनी बात वि" व पटल पर रख सकता हैं। लेकिन इस प्रगति का दूसरा पहलू हैं। साइबर अपराध और सो" ाल मीडिया का दुरूपयोग। आज हैकिंग, आनॅलाइन,धोखा धड़ी, डेटा चोरी अ" लील सामग्री का प्रसार, अफवाह फैलाना, ट्रोलिंग और साइबर बुलिंग जैसी घटनाएँ आम हो गई हैं। इनसे न केवल व्यक्ति निजता प्रभावित होती हैं। बल्कि समाज और राश्ट्र की सुरक्षा पर भी असर पड़ता हैं। इस प्रकार से भारतीय संविधान एवं विधियो की भूमिका अत्यन्त महत्वपूर्ण हो जाती हैं। क्योकि ये नागरिको के मौलिक अधिकारो की रक्षा करते हुए डिजिटल स्पेस में जवाब देही और नियंत्रण सुनि" चत करते हैं।

इक्कीसवीं सदी को डिजिटल युग कहा जाता है। सूचना एवं संचार प्रौद्योगिकी (प्ब्ज्) के तीव्र विकास ने शासन व्यवस्था की प्रकृति को मौलिक रूप से परिवर्तित कर दिया है। परंपरागत प्रशासनिक ढाँचे अब डिजिटल माध्यमों में परिवर्तित हो रहे हैं, जिसे सामान्यतः डिजिटल शासन (क्पहपजंस ळवअमतदंदबम) या ई—गवर्नेंस कहा जाता है। भारत जैसे विकासशील लोकतांत्रिक देश में डिजिटल शासन को पारदर्शिता, दक्षता, समावेशन और जवाबदेही का माध्यम माना गया है।

हालाँकि, डिजिटल शासन के विस्तार के साथ—साथ साइबर अपराधों में भी अभूतपूर्व वृद्धि हुई है। डेटा चोरी, साइबर धोखाधड़ी, फिशिंग, रैनसमवेयर, पहचान की चोरी, साइबर आतंकवाद और ऑनलाइन उत्पीड़न जैसी समस्याएँ न केवल व्यक्तिगत स्तर पर नागरिकों को प्रभावित कर रही हैं, बल्कि राज्य की डिजिटल प्रणालियों और लोकतांत्रिक संस्थाओं के लिए भी गंभीर चुनौती बन चुकी हैं। इस संदर्भ में यह प्रश्न अत्यंत महत्वपूर्ण हो जाता है कि डिजिटल शासन के युग में सार्वजनिक संवैधानिक जवाबदेही को कैसे सुनिश्चित किया जाए। यह लेख डिजिटल शासन, साइबर अपराधों और संवैधानिक जवाबदेही के बीच संबंधों का विश्लेषण करता है तथा यह स्पष्ट करने का प्रयास करता है कि राज्य पर नागरिकों के मौलिक अधिकारों की रक्षा हेतु कौन—कौन से संवैधानिक दायित्व आरोपित होते हैं।

डिजिटल शासन की अवधारणा एवं स्वरूपः— डिजिटल शासन का आशय केवल सरकारी कार्यों के कंप्यूटरीकरण तक सीमित नहीं है, बल्कि यह एक ऐसी शासन प्रणाली है जिसमें डिजिटल तकनीक के माध्यम से नीति निर्माण, प्रशासन, सेवा वितरण और नागरिक सहभागिता को सुदृढ़ किया जाता है। भारत में डिजिटल शासन की अवधारणा को "डिजिटल इंडिया" पहल के माध्यम से संस्थागत रूप प्रदान किया गया है। डिजिटल शासन के प्रमुख घटक निम्नलिखित हैंकृ ई—गवर्नेंस सेवाएँ (ऑनलाइन प्रमाणपत्र, कर भुगतान, पेंशन, सब्सिडी),डिजिटल पहचान प्रणाली (आधार),डिजिटल भुगतान प्रणाली,सरकारी डेटा का डिजिटलीकरण नागरिक—सरकार संवाद हेतु डिजिटल मंच इन उपायों का उद्देश्य शासन को उत्तरदायी, पारदर्शी और नागरिक—केंद्रित बनाना है। किंतु जब शासन डिजिटल होता है, तब नागरिकों का विशाल व्यक्तिगत और संवेदनशील डेटा भी राज्य के पास एकत्र होता है, जिससे डेटा सुरक्षा और गोपनीयता के प्रश्न अत्यंत महत्वपूर्ण हो जाते हैं। साइबर अपराध रू अर्थ, प्रकृति और बढ़ता प्रभाव की बात करें तो साइबर अपराध वे अपराध होते हैं, जो कंप्यूटर, इंटरनेट या डिजिटल नेटवर्क के माध्यम से किए जाते हैं। इन अपराधों की विशेषता यह है कि वे सीमाओं से परे होते हैं, पहचान करना कठिन होता है और इनका प्रभाव व्यापक होता है।

साइबर अपराधों के प्रमुख रूप हैंकृ
साइबर धोखाधड़ी और ऑनलाइन ठगी
डेटा चोरी और हैकिंग,पहचान की चोरी,
साइबर स्टॉकिंग,और ऑनलाइन उत्पीड़न
सरकारी वेबसाइटों पर साइबर हमला,
डिजिटल वित्तीय अपराध,डिजिटल शासन के युग में साइबर अपराध केवल व्यक्तिगत क्षति तक सीमित नहीं रहते, बल्कि वे राज्य की विश्वसनीयता, नागरिकों के अधिकारों और लोकतांत्रिक प्रक्रियाओं को भी प्रभावित करते हैं।

https://ijioa.com/ cosmospub2023@gmail.com

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

जब सरकारी पोर्टल हैक होते हैं या नागरिकों का डेटा लीक होता है, तब यह राज्य की प्रशासनिक विफलता का संकेत देता है।

सार्वजनिक संवैधानिक जवाबदेही की अवधारणाः—

सार्वजनिक संवैधानिक जवाबदेही का अर्थ है— राज्य और उसके अंगों का संविधान के प्रति उत्तरदायी होना। लोकतांत्रिक शासन में राज्य की शक्ति निरंकुश नहीं होती, बल्कि वह संविधान द्वारा सीमित और निदशित होती है।

भारतीय संविधान के अंतर्गतकृराज्य नागरिकों के मौलिक अधिकारों की रक्षा के लिए बाध्य है,शासन में पारदर्शिता और न्याय सुनिश्चित करना राज्य का कर्तव्य है

प्रशासनिक कार्यों के लिए न्यायिक समीक्षा का प्रावधान बताता है,

डिजिटल शासन के संदर्भ में यह जवाबदेही और अधिक महत्वपूर्ण हो जाती है, क्योंकि राज्य अब तकनीकी माध्यमों से सीधे नागरिकों के जीवन को प्रभावित करता है।

साइबर अपराध और मौलिक अधिकारों पर प्रभावों की बात करें तो साइबर अपराध सीधे–सीधे भारतीय संविधान द्वारा प्रदत्त मौलिक अधिकारों को प्रभावित करते हैं।अनुच्छेद 21 दृ जीवन और व्यक्तिगत स्वतंत्रता का अधिकार,

डिजिटल युग में "जीवन" का अर्थ केवल भौतिक अस्तित्व नहीं, बल्कि डिजिटल गरिमा, डेटा सुरक्षा और गोपनीयता भी है। साइबर अपराधों के कारण जब नागरिकों का डेटा लीक होता है या उनकी डिजिटल पहचान का दुरुपयोग होता है, तब यह अनुच्छेद 21 का उल्लंघन है।अनुच्छेद 14 दृ समानता का अधिकार,डिजिटल शासन में यदि साइबर सुरक्षा उपाय सभी नागरिकों के लिए समान रूप से प्रभावी नहीं हैं, तो यह असमानता को जन्म देता है। डिजिटल विभाजन (क्पहपजंस क्पअपकम) भी समानता के अधिकार को प्रभावित करता है।अनुच्छेद 19 दृ अभिव्यक्ति की स्वतंत्रता को बताता है,ऑनलाइन प्लेटफार्मों पर साइबर उत्पीड़न, ट्रोलिंग और निगरानी से नागरिकों की अभिव्यक्ति की स्वतंत्रता बाधित होती है। राज्य का दायित्व है कि वह डिजिटल माध्यमों पर सुरक्षित वातावरण प्रदान करे। राज्य की संवैधानिक जिम्मेदारी और विधिक ढाँचा की बात करें तो

डिजिटल शासन में राज्य की संवैधानिक जिम्मेदारी केवल सेवा प्रदान करने तक सीमित नहीं है, बल्कि साइबर सुरक्षा और डेटा संरक्षण भी उसका कर्तव्य है।

भारत में साइबर अपराधों से निपटने हेतु कई अधिनियम बनाए गए हैं —

सूचना प्रौद्योगिकी अधिनियम, 2000,आईटी नियम, 2021,प्रस्तावित डिजिटल व्यक्तिगत डेटा संरक्षण कानून,

न्यायपालिका के निर्णय (जैसे गोपनीयता को मौलिक अधिकार घोषित करना) इन विधिक प्रावधानों के माध्यम से राज्य पर यह दायित्व डाला गया है कि वह नागरिको के डिजिटल अधिकारों की रक्षा करे। यदि राज्य इस दायित्व में विफल रहता है, तो यह संवैधानिक जवाबदेही का उल्लंघन माना जाएगा।

डिजिटल शासन में जवाबदेही की चुनौतियाँ – डिजिटल शासन में सार्वजनिक संवैधानिक जवाबदेही के समक्ष कई चुनौतियाँ हैं— तकनीकी जटिलता के कारण पारदर्शिता का अभाव,साइबर अपराधों की अंतरराष्ट्रीय प्रकृति,कानूनों का अपर्याप्त या धीमा क्रियान्वयन,नागरिकों में डिजिटल जागरूकता की कमी, प्रशासनिक लापरवाही और जवाबदेही तंत्र की कमजोरी इन चुनौतियों के कारण नागरिकों का राज्य पर विश्वास कमजोर हो सकता है, जो लोकतंत्र के लिए घातक है।

भारतीय संवधिान की भूमिका साइबर अपराधो एवं सो"ाल मीडिया नियंत्रण मेंः—

भारतीय संवधिान दे"ा का सवोर्च्य विधिक दस्तावेज हैं जो नागरिको के मौलिक अधिकारों की सुरक्षा करता हैं और भाासन के लिए मार्गद"ार्न प्रदान करता हैं। साइबर अपराधो और सो"ाल मीडिया के सन्दर्भ ये संविधान की निम्नलिखित धाराएँ अत्यंत प्रसांगिक हैं–

1. अनुच्छेद 19 (1) (ए):– अभिव्यक्ति की स्वतंत्रता का अधिकार हमें बताता हैं कि सो"ाल मीडिया के युग में यह अधिकार हमें नागरिको को अपने विचार स्वतंत्र रूप से व्यक्त करने की छूट देता हैं।

https://ijioa.com/ cosmospub2023@gmail.com

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

किन्तु अनुच्छेद 19 (2) अंतर्गत इस स्वतंत्रता पर य" ोचित प्रतिबंध लगाए गए है– जैसे राश्ट्र की सुरक्षा सार्वजनिक व्यवस्था भाालीनता और नैतिकता के आधार पर। अतः यदि कोई व्यक्ति सो" ाल मीडिया का उपयोग अफवाह फैलाने घृणा भाशण या हिंसा भड़काने के लिए करता है, तो वह संविधान के अनुच्छेद 19 (2) के दायरे में दंडनीय हो सकता हैं।

2. अनुच्छेद 21– जीवन और व्यक्तिगत स्वतंत्रता का अधिकार हमें बताता हैं कि डिजिटल युग में ''जीवन का अधिकार'' केवल भाारीरिक नहीं बल्कि डिजिटल प्राइवेसी का भी अधिकार होता हैं। सुप्रीम कोर्ट ने ''के.एस. पुटुस्वामी बनाम भारत संघ (2017)'' में निजता के अधिकार को अनुच्छेद 21 के तहत मौलिक अधिकार घोशित किया। इस निर्णय ने आनलाइन डेटा सुरक्षा और सो" ाल मीडिया प्लेटफॉर्म्स की जवाबदेही के लिए संवैधानिक आधार तैयार किया।
3. अनुच्छेद 32 और 226 हमें न्यायिक संरक्षण का अधिकार प्रदान करते हुए ये अधिकार प्रदान कराता हैं कि साइबर अपराधा या निजता के उल्लंघन की स्थिति में नागरिक सीधे उच्च न्यायालय या सर्वोच्य न्यायालय में संवैधानिक उपचार प्राप्त कर सकते हैं।

विधिक ढांचाः साइबर अपराधो से सुरक्षा हेतु कानून

1. सूचना प्रौद्योगिकी अधिनियम 2000ः– यह भारत का प्रमुख साइबर कानून हैं, जो इलेक्ट्रानिक लेनदेन, डिजिटल हस्ताक्षर और साइबर अपराधो से संबंधित प्रावधानों को नियंत्रित करता हैं। इस अधिनियम की कुछ प्रमुख धाराएँ इस प्रकार हैं– धारा 43ः– कम्प्यूटर सिस्टम में अनाधिकृत प्रवे" ा या डेटा चोरी। धारा–66 कम्प्यूटर हैकिंग या साइबर ठगी के अपराध। धारा 66सी और 66डी पहचान की चोरी और आनलाइन धोखाधड़ी। धारा 67– अ" लील सामग्री का आनलाइन प्रसार। धारा 69–राश्ट्रीय सुरक्षा के हित में इंटरनेट गतिविधियों की निगरानी का अधिकार।
2. भारतीय न्याय संहिता 2023 (BNS) के प्रावधानों में सूचना प्रौद्योगिकी अधिनियम के साथ–साथ BNS की विभिन्न धाराएँ भी लागू होती हैं– धारा 318 और 319– धोखाधड़ी और छल को बताती हैं। धारा 78–महिलाओ के आनलाइन उत्पीडन स्टॉकिंग, या माफिंग के मामले को बताती हैं। धारा–356 हमें मानहानि से संबंधित अपराधो से सुरक्षा प्रदान करती हैं।
3. डिजिटल डेटा संरक्षण अधिनियम 2023 (Digital Personal Data Protection Act 2023) यह नवीनतम कानून हैं जो नागरिको के डिजिटल डेटा की गोपनीयता सुनि" चत करता हैं इसमे कम्पनियो और भोसल मीडिया प्लेटफार्म को उपयोगकर्ताओं के डेटा की सुरक्षा के लिए सख्त दायित्व दिए गए हैं।

सोसल मीडिया के प्रभाव–

1. सकारात्मक प्रभावो की बात करे तो यह लोकतंत्र में अभिव्यक्ति और सहभागिता का विस्तार कराता हैं ि" ाक्षा, जागरूकता और सूचना को तीव्र रूप से प्रसार करने में सहायक हैं जन आंदोलनो और सामाजिक सुधारों को बल मिलता हैं एवं व्यवसाय और रोजगार के नए अवसर प्रदान करने में सहायता प्रदान करवाता हैं।
2. नकारात्मक प्रभावों की बात करें तो फेक न्यूज और अफवाहों का प्रसार अत्यधिक मात्राम में होता हैं, मानसिक तनाव अवसाद और सामाजिक अलगाव को बढ़ावा देता हैं, ट्रालिंग साइबर बुलिंग और महिलाओ के प्रति डिजिटलहिंसा को बढ़ाता हैं और इन सब के साथ–साथ व्यक्ति के निजी डेटा की चोरी और निजता का हनन के लिए भी मुख्य रूप से जिम्मेदार होता हैं।

साइबर अपराधो की प्रमुख श्रेणियाँः–

https://ijioa.com/ cosmospub2023@gmail.com

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

- आनलाइन बैंकिंग फ्राड, यु.पी.आई. ठगी क्रेडिट कार्ड स्कैम आदि अपराध का हम वित्तीय अपराधो की श्रेणी में मानते हैं।
- किसी व्यक्ति की व्यक्तिगत पहिचान की चोरी या उसके नाम या पहिचान का दुरूपयोग करना भी साइबर अपराध की श्रेणी में आता हैं।
- साइबर बुलिंग और आनॅलाइन उत्पीडन भी वि" ोशकर महिलाओं और बच्चों के प्रति सबसे ज्यादा होता हैं।
- डेटा हैकिंग और रैनसमवेयर अटैक भी साइबर अपराध की श्रेणी में आता हैं।
- फेक न्यूज और राजनीतिक दुश्प्रचार के कारण भी व्यकि साइबर के अपराधो से पीड़ित हैं।
- इंटरनेट पर संवेदन" ील सामग्री का अवैध प्रसार भी बाल अ" लीलता को बढ़ावा दे रहा हैं। और साइबर ठगो की अपराधिक श्रेणियों को बढ़ावा मिल रहा हैं।

न्यायालयीन दृश्टिकोणः– भारतीय न्यायपालिका ने साहबर अपराधों से निपटने के लिए कई प्रकार के महत्वपूर्ण निर्णय दिए हैं:–

1. श्रेया सिंघल बनाम भारत संघ (2015)– इस केस के निर्णय में सुप्रीम कोर्ट ने IT Act की धारा 66 A को असंवैधानिक घोशित किया क्योंकि यह अभिव्यक्ति की स्वतंत्रता का उल्लंघन करती थी। यह फसला डिजिटल फ्रीडम और संविधान के बीच संतुलन का प्रतीत हें।
2. पुटुस्वामी बनाम भारत संघ (2017) के केस में निजता को मौलिक अधिकार घोशित किया गया, जिससे सो" ाल मीडिया प्लेटफार्क्स के डेटा उपयोग पर संवैधानिक निगरानी स्थापित हुई।
3. फेसबुक बनाम दिल्ली विधानसभा (2021) के मामले में अदालत ने माना कि सो" ाल मीडिया प्लेटफार्क्स को जवाबदेही से मुक्त नहीं किया जा सकता हैं क्योंकि उनके माध्यम से समाज में गलत सूचना फैल सकती हैं।

साइबर अपराध को कम करने के लिए आने वाली वर्तमान चुनौतियाँः–

- ग्रामीण और पिछड़े क्षेत्रो के लोगो में ऑनलाइन ठगी के प्रति डिजिटल साक्षरता की कमी के कारण जागरूकता नही हैं।
- अधिकतर व्यक्ति प्रौद्योगिकी का दुरूपयोग कर रहे हैं।
- साइबर अपराधो की जाच में समय और संसाधनो की कमी होने के कारण कानूनी प्रक्रिया में अनेक प्रकार की कठिनाइयो का सामना करना पड़ता हैं।
- अंतराश्ट्रीय अपराध बढ़ने से अपराधी अक्सर विदे" ाी सबट या VPN का उपयोग करते हैं।
- सो" ाल मीडिया पर नियंत्रण का अभाव होने के कारण कंपनियों की पारद" िता और जवाब देही सीमित हो गई हैं।

साइबर एवं उपायः– डिजिटल शासन में साइबर अपराधों से निपटने और संवैधानिक जवाबदेही सुनिश्चित करने हेतु निम्नलिखित उपाय आवश्यक हैं कृ सशक्त डेटा संरक्षण कानून,स्वतंत्र साइबर निगरानी और ऑडिट तंत्र ,प्रशासनिक अधिकारियों की जवाबदेही तय करना न्यायपालिका की सक्रिय भूमिका नागरिकों के लिए प्रभावी शिकायत निवारण तंत्र,डिजिटल साक्षरता और जागरूकता का प्रसार,इन उपायों के माध्यम से डिजिटल शासन को संवैधानिक मूल्यों के अनुरूप बनाया जा सकता है।

1. साइबर कानूनों का सुद्वढ़ीकरण से तात्पर्य सूचना प्रौद्योगिकी अधिनियम 2000 को नवीन तकनीकी चुनौतिया जैसे आर्टिफि" ायल डंटेलिजेंस (AI) डीपफेक डेटा लीक साइबर टेररिज्म के अनुरूप संसोधित किया जाए। एवं भारतोय न्याय संहिता (2023) में साइबर अपराधों के लिए वि" ोश प्रावधान जोड़े ताकि अपराधों की परिभाशा स्पश्ट और प्रभावी हो,
2. सो" ाल मीडिया प्लेटफार्म्स की जवाबदेही बढ़ाना चाहिए से ताम्पर्य है कि सो" ाल मीडिया कंपनियों को यह सुनि" चत

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

करना चाहिए कि उनके प्लेटफार्म पर फेंक न्यूज हेट स्पीच या अ” लील सामग्री का प्रसार न हो सके और सरका को इन प्लेटफार्म से डेटा पारदर्” िता रिपोर्ट नियमित रूप से प्राप्त करनी चाहिए एवं IT Rules 2021 के तहत ''ग्रेविएस ऑफिसट'' की व्यवस्था को सख्ती से लागू किया जाए ताकि नागरिको की ि” ाकायतो का त्वरित समाधान हो सके।

3. साइबर सुरक्षा जागरूकता अभियान चलाकर विद्यालयो कालेजों और वि” वविद्यालयों में ''साइबर सुरक्षा एवं डिजिटल नैतिकता'' विशय को अनिवार्य किया जाए। आम नागरिको को जागरूक करने के लिए राश्ट्रीय स्तर पर अभियान चलाए जाऍ–जैसे Cyber Suraksha Abhiyan या Digital Hygiene Drive एवं वि” ोशकर महिलाओ और कि” ाोरी का आनलाइन सुरक्षा गोपनीयता और रिपोर्टिंग तंत्र की जानकारी दी जाए।
4. निजटा एवं डेटा संरक्षण को प्रोत्साहन देना चाहिए जिससे डिजिटल पर्सनल डेटा प्रोटेक” ान एक्ट 2023 को प्रभावी ढंग से लागू किया जाए। एवं नागरिको को यह अधिकार दिया जाए कि वे अपने डेटा के उपयोग संग्रहण और हटाने के संबंध में स्पश्ट अनुमति दे। और सो” ाल मीडिया कंपनियो को ''डेटा मिनिमइजे” ान नीति'' अपनानी चाहिए–यानी केवल उतना आकड़े संग्रहित करे जितना आव” यक हो।
5. साइबर अपराध जॉच पणाली को स” ाक्त बनाना चाहिए और प्रत्येक जिले में साहबर पुलिस स्टे” ान और डिजिटल फारेसिक प्रयोग” ााला की स्थापना की जानी चाहिए। एवं पुलिस अधिकारियों को साइबर फारेसिक डिजिटल साक्ष्य संगृहण और आनलाइन ट्रैकिंग का वि” ोश प्र” ाक्षण दिया जाना चाहिए एवं ि” ाकायत दर्ज करने की प्रक्रिया को सरल औन आनलाइन बनाया जाए– जैसे '' Cyber Crime gov.in पोर्टल का विस्तार ज्यादा से ज्यादा करना चाहिए।
6. अंतरराश्ट्रीय सहयोग के लिए भारत को अन्य दे” ाो के साथ साइबर अपराध रोकथाम संधियाँ करनी चाहिए ताकि अपराधियों को ट्रैक करना आसान हो सके। और Interpol और UN Cyber Crime Cell जैसे संगठनो के साथ मिलकर सूचना साझा की जानी चाहिए।
7. सो” ाल मीडिया पर नैतिक उपयोग को प्रोत्साहित करने के लिए नागरिको में डिजिटल नागरिकता की भावना विकसित की जानी चाहिए। एवं ''थिंक बिफोट यू पोस्ट'' (पोस्ट करने से पहले सोचे) जैसे अभियानों को प्रोत्साहित करने के महत्वपूर्ण प्रोग्राम चलाए जाने चाहिए तथा धार्मिक राजनीतिक या व्यक्गित आधार पर नफरत फैलाने वाले खातों पर त्वरित कार्यवाही की जानी चाहिए।
8. वि” ोश न्यायालयो की स्थापना कर के त्वरित न्याय की व्यवस्था करनी चाहिए तथा आनलाइन ट्रायल और डिजिटल सबूतो के उपयोग को वैध और व्यवस्थित बनाया जाना चाहिए।
9. महिलाओ और बच्चों की आनलाइन सुरक्षा के लिए महिला एवं बाल विकास मंत्रालय द्वारा Cyber Helpline 1930 और National cyber safety Portal को और अधिक प्रभाव” ाालो बनाने के प्रयास करने चाहिए एवं सो” ाल मीडिया पर अ” लील या मार्फ्ड तस्वीरे अपलोड करने वाले अपराधियों के खिलाफ कठोर दण्ड के प्रावधान बनाने चाहिए एवं स्कूल स्तर पर बच्चों को सुरक्षित इंटरनेट उपयोग के बारे में ि” ाक्षित करने का प्रयास करना चाहिए।
10. संवैधानिक मूल्यों का अनुपालन करते हुए अभिव्यक्ति की स्वतंत्रता (अनुच्छेद 19 (1) (a)) और सार्वजनिक व्यवस्था (अनुच्छेद 19 (2)) के बीच संतुलन बनाए रखा जाना चाहिए। तथा न्यायपालिका को यह

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026

सुनिर्” चत करना चाहिए कि कानून का उपयोग न तो अभिव्यक्ति की स्वतंत्रता को दबाने के लिए हो न ही दुरूपयोग के लिए खुली छूट प्रदान करें।

निश्कर्शः— डिजिटल युग में संविधान और कानून की भूमिका केवल सुरक्षा तक सीमित नही हैं। बल्कि यह नागरिकों के अधिकारों और स्वतंत्रता के संतुलन का भी प्र” न हैं। साइबर अपराधों की रोकथाम के लिए तकनीकी उपायो के साथ–साथ संविधानिक मूल्यो समानता, स्वतंत्रता, गरिमा और न्याय का पालन आव” यक हैं। भारतीय विधिक व्यवस्था लगातार विकसित हो रही हैं। नई नीतियाँ, डैट सुरक्षा कानून और न्यायिक व्यवख्याएँ इस दि” ाा में मील का पत्थर साबित हो रही हैं। साइबर अपराध और सो” ाल मीडिया का दरूपयोग आधुनिक भारत की सबसे बड़ी डिजिटल चुनौतियों में से एक हैं। इससे निपटने के लिए केवल कानून पर्याप्त नही हैं। इसके साथ नागरिकों की जागरूकता सामाजिक जिम्मेदारी और तकनीकी सहयोग भी अत्यन्त आव” यक हैं। भारतीय संवधिान का लक्ष्य ''न्याय स्वतंत्रता समानता और बंधुत्व'' डिजिटल युग में भी लागू हो–यही सच्चा सामाधान हैं। परंतु अंतिम सफलता तभी संभव हैं जब नागरिक सरकार और तकनीकी संस्थान तीनो मिलकर डिजिटल नैतिकता औव संवैधानिक जिम्मेदारी का पालन करें। डिजिटल शासन आधुनिक प्रशासन की अनिवार्यता बन चुका है, कितु इसके साथ साइबर अपराधों की चुनौती भी उतनी ही गंभीर है। इस संदर्भ में सार्वजनिक संवैधानिक जवाबदेही केवल एक सैद्धांतिक अवधारणा नहीं है ,बल्कि लोकतांत्रिक शासन की आधारशिला है।राज्य का दायित्व है कि वह डिजिटल तकनीक का उपयोग नागरिकों के अधिकारों के संरक्षण और सशक्तिकरण के लिए करे, न कि उनके उल्लंघन के लिए। साइबर अपराधों से प्रभावी ढंग से निपटने के लिए कानून, तकनीक और संवैधानिक नैतिकता के समन्वय की आवश्यकता है।अंततः, डिजिटल शासन तभी सफल और लोकतांत्रिक माना जाएगा, जब वह संवैधानिक जवाबदेही, नागरिक अधिकारों और साइबर सुरक्षा के बीच संतुलन स्थापित करने में सक्षम होगा।

संदर्भ सूचीः—

- डॉ. देवेन्द्र पाल सिंह यादव — सूचना प्रौद्योगिकी अधिनियम 2000
- बी.एस. खेत्रपाल, पूजा खेत्रपाल — सूचना प्रौद्योगिकी अधिनियम 2000
- डॉ. वी.आर. अम्बेडकर — भारत का संविधान
- डॉ. बसन्ती लाल बाबेल — भारत का संविधान
- Indian Kanoon.org & Shreya Singhal V/S union of India (2015) AIR 2015 Sc 834
- Indian Kannon.org & K.S. Puttaswamy V/s union of India (2017) AIR 2017 Sc 4161
- Dr. M.K. Bhandari & Digital Personal data Protection Act 2023,
- गृह मंत्रालय भारत सरकार — साइबर अपराध प्रकोश्ठ की रिपोर्ट (2023)
- विभिन्न सामाचार स्त्रोत एवं न्यायिक निर्णय संगृह
- इन्टरनेट संचार माध्यम
- स्वयं के विचार

Paper received: 02.02.2026 Reviewed: 03.02.2026 Accepted: 07.02.2026 Published: 08.02.2026