ऑनलाइन दुर्व्यवहार से निपटना

प्रिलिम्स के लिये:

साइबर उत्पीड़न, भारतीय न्याय संहिता (BNS), 2023, सूचना प्रौद्योगिकी (IT) अधिनियम, 2000, उच्च न्यायालय, सर्वोच्च न्यायालय, डिजिटल व्यक्तिगत डेटा संरक्षण (DPDP) अधिनियम, 2023, डीपफेक, डिजिटल साक्षरता कार्यक्रम।

मेन्स के लिये:

ऑनलाइन दुर्व्यवहार तथा उसके स्वरूप, भारत में ऑनलाइन दुर्व्यवहार से निपटने के लिये चुनौतियाँ और उपचारात्मक कदम।

स्रोत: द हिंदू

चर्चा में क्यों?

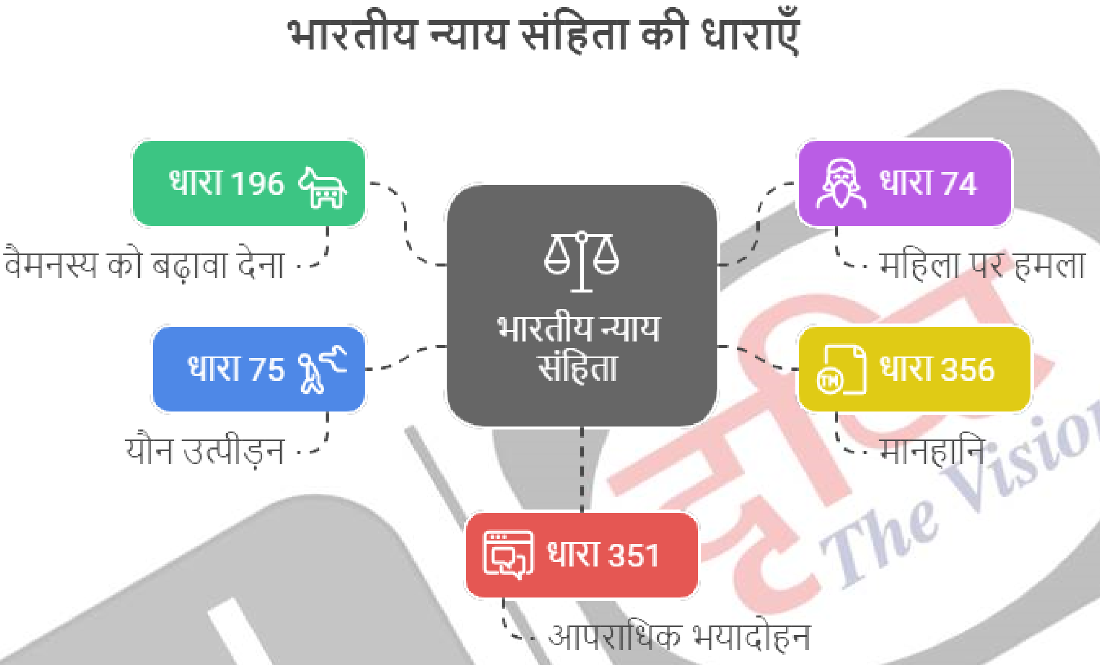
पहलगाम आतंकी हमले के बाद एक पीड़ित की **शांति अपील के कारण उसे नृशंसतापूर्वक ट्रोल किया गया।** इसी तरह भारत के विदेश सचिव को भारत-पाकिस्तान युद्ध विराम की घोषणा के बाद अपमानजनक टिप्पणियों का सामना करना पड़ा।

- इसने भारत में साइबर उत्पीड़न के बढ़ते संकट एवं कमज़ोर विनियमन पर प्रकाश डाला तथा कानूनी सुधार,**प्लेटफॉर्म जवाबदेही और पीड़ितों की सुरक्षा की आवश्यकता पर बल दिया।**

ऑनलाइन दुर्व्यवहार क्या है?

- **परिचय: ऑनलाइन दुर्व्यवहार (साइबर दुर्व्यवहार, डिजिटल दुर्व्यवहार या इंटरनेट उत्पीड़न)** से तात्पर्य डिजिटल प्लेटफॉर्म के माध्यम से होने वाले किसी भी प्रकार के **हानिकारक, धमकी भरे या अपमानजनक व्यवहार से है।**
  - यह किसी **व्यक्ति, समूह या पूरे समुदाय** पर लक्षित हो सकता है और मौखिक हमलों तथा उत्पीड़न से लेकर निजी जानकारी या छवियों के गैर-सहमति वाले साझाकरण तक कई रूप ले सकता है।
- **प्रकार:**
  - **साइबरबुलिंग:** यह डिजिटल प्लेटफॉर्म का उपयोग करके किसी को बार-बार **परेशान करना, धमकी देना या अपमानित करना है,** जिससे उसे **भावनात्मक क्षति** पहुँचती है।
  - **साइबरस्टॉकिंग:** यह **लगातार अवांछित ऑनलाइन निगरानी** और उत्पीड़न है, जो बार-बार **संदेश भेजने, गतिविधि पर नज़र रखने** या स्पाइवेयर और फर्जी खातों का उपयोग करने से भय उत्पन्न करता है।
  - **ट्रोलिंग:** ट्रोलिंग में लोगों को परेशान करने या बातचीत को बाधित करने के लिये जानबूझकर ऑनलाइन **आपत्तिजनक या उत्तेजक संदेश पोस्ट करना शामिल है।**
  - **डॉक्सिंग:** डॉक्सिंग, **"डॉक्सिंग डॉक्स" (दस्तावेज़) का संक्षिप्त रूप है,** जो पते या फोन नंबर जैसी **निजी जानकारी को अनधिकृत** रूप से ऑनलाइन साझा करना है, जिसका उपयोग अक्सर पीड़ितों को परेशान करने या धमकाने के लिये किया जाता है।
  - **रिवेंज पोर्न:** इसमें **बिना सहमति के अंतरंग चित्रों को साझा करना या साझा करने की धमकी देना,** गोपनीयता का उल्लंघन करना और प्रायः ब्लैकमेल या अपमान के लिये उपयोग किया जाता है।
  - **कैटफिशिंग:** इसमें दूसरों को धोखा देने के लिये **नकली ऑनलाइन पहचान** बनाना शामिल है, जिसका उद्देश्य प्रायः **भावनात्मक, वित्तीय या दुर्भावनापूर्ण** होता है।
- **भारत में साइबरबुलिंग की स्थिति:** भारत में साइबरबुलिंग की दर विश्व स्तर पर सबसे अधिक है, जहाँ 85% से अधिक बच्चों ने इसकी रिपोर्ट की है।
  - लगभग **46% ने अपरिचितों को परेशान करने** की बात कही (विश्व स्तर पर यह आँकड़ा 17% है) तथा **48% ने किसी ऐसे व्यक्ति को परेशान किया जिसे वे जानते थे** (विश्व स्तर पर यह आँकड़ा 21% है)।
  - इनमें सबसे प्रमुख रूप से **झूठी अफवाहें फैलाना (39%), चैट/ग्रुप से बहिष्कृत करना (35%) और अपशब्द कहना (34%) शामिल हैं।**
- **ऑनलाइन दुर्व्यवहार से निपटने के लिये कानूनी प्रावधान:**

- भारतीय न्याय संहिता (BNS), 2023:
- सूचना प्रौद्योगिकी (IT) अधिनियम, 2000:
    - धारा 66C: पहचान की चोरी
    - धारा 66D: प्रतिरूपण धोखाधड़ी
    - धारा 67: इलेक्ट्रॉनिक रूप से अश्लील सामग्री प्रकाशित या प्रसारित करना।
- **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (DPDP), 2023:** DPDP उत्पीड़न को बढ़ावा देने वाले डेटा उल्लंघनों को रोकने में विफल रहने पर दंड का प्रावधान करता है।
- **सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 :** सोशल मीडिया प्लेटफॉर्म को **बलात्कार, मौत की धमकी, यौन रूप से स्पष्ट सामग्री और राज्य के सद्भाव या अंतरराष्ट्रीय संबंधों को खतरा पहुँचाने वाली सामग्री** जैसे अपराधों की जाँच के लिये सामग्री के पहले स्रोत का खुलासा करना होगा।



- **न्यायिक रुख:**
    - ***[illegible], 2024*** **:** दिल्ली **उच्च न्यायालय ने** एक महिला के वैयक्तिक **विवरण को प्रकट करने वाले ट्वीट को हटाने** का आदेश दिया, विशिष्ट कानूनी स्थिति के अभाव के बावजूद **डॉक्सिंग के गंभीर गोपनीयता और सुरक्षा जोखिमों को मान्यता दी।**
    - ***[illegible], 2015*** **:** सर्वोच्च न्यायालय **ने IT अधिनियम की धारा 66 A को असंवैधानिक करार देते हुए रद्द कर दिया,** जो **"आपत्तिजनक" ऑनलाइन भाषण को अपराधी बनाती थी** - अभिव्यक्ति की स्वतंत्रता की रक्षा करते हुए इस बात पर ज़ोर दिया कि **उचित प्रतिबंधों को** संकीर्ण रूप से परिभाषित किया जाना चाहिये।
    - ***[illegible], 2017*** **:** सर्वोच्च न्यायालय ने निजता **को एक मौलिक अधिकार (अनुच्छेद 21) घोषित किया, जिसने व्यक्तिगत डेटा की सुरक्षा** और **अनधिकृत ऑनलाइन प्रकटीकरण या डॉक्सिंग को रोकने** की नींव रखी।

भारत में ऑनलाइन दुर्व्यवहार से निपटने में क्या चुनौतियाँ हैं?

- **संबद्ध कानूनों का अभाव**: भारत में वर्तमान में **ऐसे विशिष्ट कानून का अभाव है** जो **ऑनलाइन हेट स्पीच और ट्रोलिंग को** व्यापक रूप से संबोधित करता हो।
    - मौजूदा कानून ऑनलाइन दुर्व्यवहार को कवर नहीं करते हैं, जब तक कि यह **अश्लील, धमकी भरा या धोखाधड़ी वाला न हो।**
    - पीछा करने से संबंधित कानून **लिंग-विशिष्ट हैं (महिलाओं को लक्षित करने वाले पुरुषों तक सीमित)** और व्यक्तिगत उद्देश्य को लक्षित करते हैं तथा **सामूहिक ऑनलाइन उत्पीड़न को नज़रअंदाज करते हैं।**
- **सामग्री मॉडरेशन चुनौतियाँ:** सोशल मीडिया कंपनियाँ **अमेरिका** और **यूरोपीय संघ** की तुलना में **भारत में हेट स्पीच से** निपटने के लिये **सामग्री की जाँच** एवं **सक्रिय कदम कम उठा रही हैं।**
    - **टेलीग्राम** जैसे प्लेटफॉर्म को **आपराधिक गतिविधि की अनुमति देने** के लिये कानूनी कार्रवाई का सामना करना पड़ रहा है, जबकि **लाभ उद्देश्यों ने** संयम को कमज़ोर कर दिया है, जिससे **हेट स्पीच को फैलने का मौका मिल गया है।**

- **"सार्वजनिक रूप से उपलब्ध डेटा" पर अस्पष्टता**: डिजिटल व्यक्तिगत डेटा संरक्षण (DPDP) **अधिनियम, 2023 "सार्वजनिक रूप से उपलब्ध"** व्यक्तिगत डेटा को छूट देता है लेकिन **इसमें स्पष्ट परिभाषा का अभाव है,** जिससे अस्पष्टता उत्पन्न होती है।
    - यह अंतर **डॉक्सिंग जैसे साइबर अपराधों को सक्षम कर सकता है,** क्योंकि विभिन्न प्लेटफार्मों से **खंडित डेटा को उत्पीड़न या धमकी के लिये आसानी से जोड़ा जा सकता है।**
- **प्रवर्तन अंतराल**: **भारत** में **IT नियमों** का **कार्यान्वयन कमज़ोर है,** जिसके परिणामस्वरूप **डिजिटल सुरक्षा** और **जवाबदेही मानकों का प्रवर्तन कमज़ोर है।**
    - पीड़ितों, विशेषकर **लैंगिक दुर्व्यवहार के पीड़ितों** को अविश्वास का सामना करना पड़ता है तथा **उन्हें ही दोषी ठहराया जाता है,** जिससे कानूनी सहायता लेने में बाधा उत्पन्न होती है।

भारत में ऑनलाइन दुर्व्यवहार से निपटने के लिये क्या उपचारात्मक कदम हो सकते हैं?

- **कानूनी और नीतिगत सुधार:** डॉक्सिंग, डीपफेक **दुर्व्यवहार और समन्वित ट्रोलिंग को** स्पष्ट रूप से परिभाषित करने एवं अपराधीकरण करने के लिये एक समर्पित **साइबर उत्पीड़न कानून बनाया जाना चाहिये।**
    - स्पष्टता के लिये तथा दुरुपयोग को रोकने के लिये **अश्लील, धमकी भरे और हेट स्पीच को** स्पष्ट रूप से परिभाषित करने के लिये **IT अधिनियम** और **BNS** में संशोधन करना।
- **प्रवर्तन को मज़बूत करना: साइबर अपराध से प्रभावी ढंग से निपटने के लिये विशेष साइबर सेल स्थापित करना** और **IP ट्रैकिंग तथा अनाम खातों की पहचान जैसे क्षेत्रों में पुलिस को प्रशिक्षित करना** आवश्यक है।
    - इसका एक प्रमुख उदाहरण **केरल का साइबरडोम** है, जो **साइबर अपराध का पता लगाने, डिजिटल फोरेंसिक और AI-आधारित निगरानी को** आगे बढ़ाने के लिये **पुलिस, नैतिक हैकर्स, शिक्षाविदों एवं तकनीकी फर्मों को एक साथ लाता है।**
    - **ऑनलाइन दुर्व्यवहार की** रिपोर्ट करने वाले पीड़ितों को प्रतिशोध और **प्रति-उत्पीड़न से बचाने के लिये** मज़बूत **व्हिसिलब्लोअर सुरक्षा** लागू करना।
- **तकनीक और प्लेटफॉर्म-स्तरीय समाधान: हेट स्पीच, डीपफेक और अपमानजनक प्रवृत्तियों को चिह्नित करने के लिये AI-संचालित पहचान** और मशीन लर्निंग का लाभ उठाना, जिससे हिंसक और यौन सामग्री का वास्तविक समय में नियंत्रण संभव हो सके।
    - **फर्जी प्रोफाइल** और **बॉट-चालित उत्पीड़न को** दंडित करने के लिये **उपयोगकर्त्ता सत्यापन प्रणाली** लागू करना।
- **जन जागरूकता:** स्कूलों और कॉलेजों में **डिजिटल साक्षरता कार्यक्रमों को** लागू करना ताकि **सोशल मीडिया का ज़िम्मेदारी से उपयोग करना सिखाया जा सके** एवं **फर्जी खबरों, घृणा फैलाने वाले आख्यानों व षड्यंत्र के सिद्धांतों को खारिज किया जा सके।**
    - सकारात्मक व्यवहार को बढ़ावा देने के साथ प्रभावशाली व्यक्तियों तथा मीडिया के माध्यम से **सांप्रदायिक एवं लैंगिक दुर्व्यवहार** का मुकाबला करने के क्रम में ट्रोलिंग विरोधी अभियान शुरू किये जाने चाहिये।
- **कॉर्पोरेट उत्तरदायित्व: प्लेटफार्मों को घृणा के एल्गोरिदमिक प्रवर्द्धन को रोककर और अपमानजनक कंटेंट** निर्माताओं को विमुद्रीकृत करके **नैतिक मुद्रीकरण नीतियों** को अपनाना चाहिये।
    - सोशल मीडिया कंपनियों को **ऑनलाइन दुर्व्यवहार** की कड़ी निगरानी (जैसा कि **अमेरिका** और **यूरोप** में किया गया है) करनी चाहिये।

निष्कर्ष

ऑनलाइन दुर्व्यवहार को रोकने के क्रम में **कानूनों के बेहतर प्रवर्तन के साथ तकनीकी नवाचार एवं सामाजिक परिवर्तन** की आवश्यकता है। **अभिव्यक्ति की स्वतंत्रता** का सम्मान किया जाना चाहिये लेकिन **संगठित उत्पीड़न, हेट स्पीच और निंदा के उल्लंघन** के संदर्भ में कोई समझौता नहीं किया जा सकता है। डिजिटल युग में साइबरबुलिंग, डॉक्सिंग और हेट स्पीच का मुकाबला करने के क्रम में एक संतुलित दृष्टिकोण अपनाने के साथ पीड़ितों की सुरक्षा करते हुए अभिव्यक्ति की स्वतंत्रता का सम्मान करना आवश्यक है।

दृष्टि मुख्य परीक्षा प्रश्न:

प्रश्न: भारत में साइबर उत्पीड़न और ऑनलाइन ट्रोलिंग का मुकाबला करने के क्रम में समर्पित विधि की आवश्यकता का विश्लेषण कीजिये।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ)

??????????

प्रश्न: भारत में, किसी व्यक्ति के साइबर बीमा कराने पर, निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त, सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

1. यदि कोई मैलवेयर कंप्यूटर तक उसकी पहुँच बाधित कर देता है, तो कंप्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1, 2 और 4
(b) केवल 1, 3 और 4
(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (B)

प्रश्न: भारत में, साइबर सुरक्षा घटनाओं पर रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है/हैं ? (2017)

1. सेवा प्रदाता (सर्विस प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट निकाय (बॉडी कॉर्पोरेट)

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1,2 और 3

उत्तर: (D)

?????

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने किस हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/tackling-online-abuse