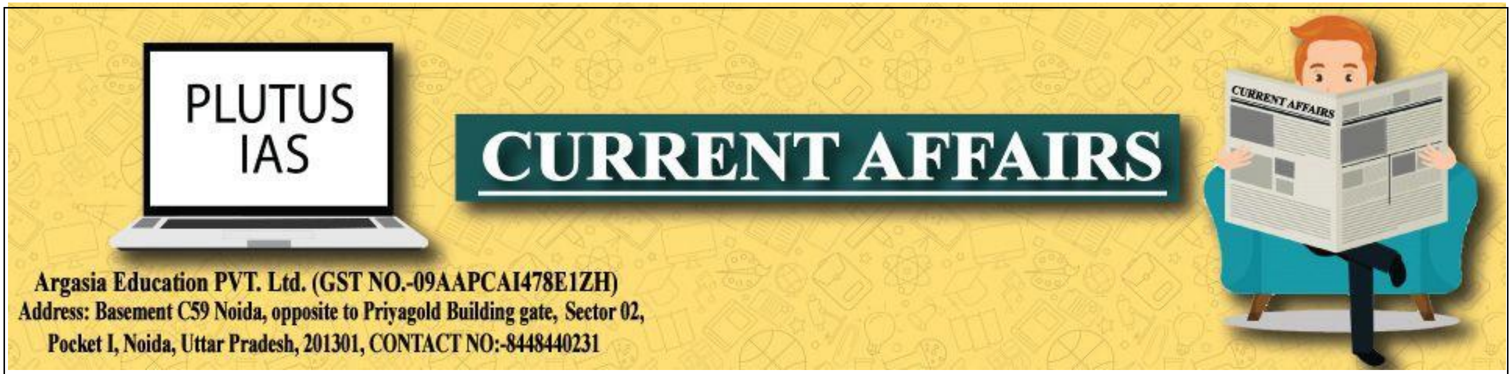

Date – 16 July 2024

डार्क नेट बनाम भारत में डेटा संरक्षण कानून एवं निजता का अधिकार

(यह लेख यूपीएससी सिविल सेवा परीक्षा के मुख्य परीक्षा के सामान्य अध्ययन प्रश्न पत्र – 3 के अंतर्गत ‘ साइबर सुरक्षा , सूचना प्रौद्योगिकी और कंप्यूटर , साइबर युद्ध , डार्क वेब की सीमापारीय प्रकृति ’ खंड से और यूपीएससी के प्रारंभिक परीक्षा के अंतर्गत ‘ डार्क वेब, डार्क नेट के संभावित खतरे , चाइल्ड पोर्नोग्राफी , निजता का अधिकार , डिजिटल इंडिया ’ खंड से संबंधित है। इसमें PLUTUS IAS टीम के सुझाव भी शामिल हैं। यह लेख ‘ दैनिक करेंट,अफेयर्स ’ के अंतर्गत ‘ डार्क नेट बनाम भारत में डेटा संरक्षण कानून एवं निजता का अधिकार ’ खंड से संबंधित है।)

खबरों में क्यों ?

- हाल ही में, राष्ट्रीय पात्रता प्रवेश परीक्षा (NEET-UG) और विश्वविद्यालय अनुदान आयोग-राष्ट्रीय पात्रता परीक्षा (UGC-NET) के पेपर परीक्षा से पूर्व ही डार्क वेब पर लीक हो गए।
- इस घटना से विभिन्न राज्यों में राष्ट्रीय स्तर पर वर्तमान सरकार के खिलाफ विरोध – प्रदर्शन और अनेक प्रकार की गंभीर समस्याएँ उत्पन्न हुई हैं।

डार्क नेट :

- डार्क नेट इंटरनेट का एक छिपा हुआ भाग है जो नियमित सर्च इंजन की पहुँच से बाहर या अदृश्य होता है।
- प्रारंभ में इसे मूल रूप से केवल सरकारी और सैन्य उपयोग के लिए सुरक्षित और गोपनीय संचार की सुविधा प्रदान करने के उद्देश्य से विकसित किया गया था।
- हाल के समय में यह अवैध हथियारों और ड्रग्स की बिक्री जैसी आपराधिक गतिविधियों के साथ भी जुड़ गया है।
- डार्क नेट पर संचार एन्क्रिप्टेड होता है, जिससे प्रेषक और प्राप्तकर्ता के बीच संचार का कोई संकेत बचा नहीं रहता है। अतः इसमें उपयोगकर्ताओं की गोपनीयता और निजता को उच्च स्तर तक सुनिश्चित किया जाता है।

क्या भारत में डार्क वेब तक पहुंच कानूनन वैध है ?

- भारत में डार्क वेब तक पहुंचना कानूनी है।
- भारत सरकार इसे अवैध गतिविधि के रूप में नहीं मानती है।
- हालाँकि, इसका मतलब यह नहीं है कि कोई भी व्यक्ति जो चाहे वह कर सकता है।
- बाल पोर्नोग्राफी, बंदूकें, पिस्तौलें, राइफलें, ड्रग्स आदि खरीदने जैसी गतिविधियाँ अवैध मानी जाती हैं। इसलिए, डार्क वेब खुद अवैध नहीं है, लेकिन इसका उपयोग करते समय किसी व्यक्ति की गतिविधि या इरादे को ध्यान में रखा जाता है।
- भारतीय कानून के अनुसार डार्क वेब के उपयोग या पहुंच को दंडनीय नहीं माना गया है, क्योंकि भारत में इसका उपयोग वैध है।
- अवैध उद्देश्यों के लिए इसका उपयोग करना भारत के कानून के तहत दंडनीय है।

भारत में डार्क वेब को विनियमित करने में नियामक चुनौतियाँ :

भारत में डार्क वेब को विनियमित करने में प्रमुख चुनौतियाँ निम्नलिखित है –

1. **एन्क्रिप्शन तकनीक और गुमनामी :** डार्क वेब की सबसे बड़ी चुनौती इसकी मजबूत एन्क्रिप्शन तकनीकों और उपयोगकर्ताओं की गुमनामी में निहित है।

2. **क्रिप्टोकरेंसी में लेनदेन :** डार्क वेब पर अधिकांश वित्तीय लेनदेन क्रिप्टोकरेंसी में किए जाते हैं, जो अतिरिक्त गुमनामी प्रदान करते हैं और लेनदेन को ट्रेस करना कठिन बना देते हैं।
3. **सीमापारीय प्रकृति :** डार्क वेब की सीमापारीय प्रकृति मामले को और जटिल बना देती है, क्योंकि इसमें विभिन्न देशों के उपयोगकर्ता शामिल होते हैं, जिससे अंतरराष्ट्रीय सहयोग की आवश्यकता पड़ती है।
4. **सूचना की स्वतंत्रता और ऑनलाइन गोपनीयता के अधिकार को सुनिश्चित करना :** डार्क वेब पर पनप रही अवैध गतिविधियों को समाप्त करना और साथ ही सूचना की स्वतंत्रता और ऑनलाइन गोपनीयता के अधिकार को सुनिश्चित करना भी एक बड़ी चुनौती है।

डार्क नेट के संभावित खतरे :

1. **पहचान का दुरुपयोग :** डार्कनेट पर लॉग-इन विवरण और अन्य व्यक्तिगत जानकारी की खरीददारी की जाती है, जिसका दुरुपयोग नकली पहचान बनाने, वित्तीय धोखाधड़ी और अन्य अपराधों के लिए किया जाता है। इसके अलावा, डार्कनेट पर ऐसे डेटा की उपलब्धता हो सकती है जो अन्य प्रथाओं में भी उपयोग हो सकता है।
2. **मैलवेयर और रैनसमवेयर :** डार्क नेट का एक और खतरा मैलवेयर और रैनसमवेयर है। ज़्यादातर मैलवेयर डार्क नेट पर प्रसारित होते हैं और फिर सार्वजनिक एक्सेस वाली वेबसाइटों पर इस्तेमाल किए जाते हैं, इसलिए डार्कनेट पर होने से मैलवेयर या रैनसमवेयर के संपर्क में आने का ख़तरा हो सकता है जो किसी व्यवसाय को नुकसान पहुंचा सकता है या किसी की पहचान चुरा सकता है।
3. **ड्रग तस्करी :** डार्कनेट ड्रग डीलरों के लिए एक प्रमुख आश्रय स्थल है, जो बेधड़क डार्कनेट पर मादक पदार्थों को बेचते हैं। डार्कनेट पर ड्रग्स और अन्य अवैध सामग्री की वितरण की जानकारी भी उपलब्ध हो सकती है।
4. **आतंकवाद :** डार्कनेट आतंकवादियों के लिए एक स्थान हो सकता है जहां वे जानकारी बांट सकते हैं, आतंकवादियों की भर्ती कर सकते हैं और आतंकवादी गतिविधियों और अन्य अपराधों के लिए योजना बना सकते हैं। आतंकवादी बिटकॉइन और अन्य क्रिप्टो-मुद्राओं का उपयोग करके विस्फोटक और हथियारों की अवैध खरीद के लिए भी डार्कनेट का उपयोग करते हैं।
5. **चाइल्ड पोर्नोग्राफी :** डार्कनेट का इस्तेमाल तस्करी, चाइल्ड पोर्नोग्राफी और अन्य अपराधों के लिए किया जाता रहा है। डार्क वेब चाइल्ड पोर्नोग्राफी वेबसाइट के उपयोगकर्ताओं का पता लगाने के लिए हुए एक अंतरराष्ट्रीय जांच में अमेरिका में तक़रीबन 337 लोगों की गिरफ्तारियाँ हुई हैं।

PLUTUS IAS

भारत में डेटा संरक्षण कानून की आवश्यकता :

1. **साइबर अपराध में वृद्धि :** भारत में बढ़ते डिजिटलीकरण और डिजिटल जटिलताओं के कारण, डेटा सुरक्षा कानून की जरूरत है। भारत में सरकारी वेबसाइट से आधार नंबर डाउनलोड करने से लेकर मतदाता सूची को बड़ी मात्रा में डाउनलोड करने तक सार्वजनिक डेटा का लीक होना आम बात है। व्हाट्सएप, पेगासस घोटाले जैसे अपराधों में हाल में हुई वृद्धि के कारण डेटा सुरक्षा कानून की अत्यंत आवश्यकता है।
2. **डेटा चोरी से सुरक्षा :** भारत में अभी भी डेटा गोपनीयता की सुरक्षा के लिए एक व्यापक कानूनी ढांचे का अभाव है। यूरोपीय संघ और अमेरिका में लागू डेटा सुरक्षा नियमों के विपरीत, भारत में डेटा सुरक्षा कानून की आवश्यकता है, ताकि सार्वजनिक और निजी संस्थाओं द्वारा संग्रहीत और उपयोग किए जाने वाले डेटा का दुरुपयोग न हो।

3. **निजता का अधिकार :** न्यायमूर्ति केएस पुट्टस्वामी बनाम भारत संघ मामले में सर्वोच्च न्यायालय (एससी) ने घोषित किया कि भारतीय संविधान के अनुच्छेद 21 के तहत निजता का अधिकार मौलिक अधिकार है, और कानून के माध्यम से इसे सुरक्षित किया जाना चाहिए। इस प्रकार, कानून के माध्यम से व्यक्ति की निजता की रक्षा करना राज्य का मुख्य कर्तव्य है।
4. **कंपनियों को विनियमित करना :** राज्य और निजी कंपनियों द्वारा व्यक्तिगत डेटा का उपयोग पारदर्शी और नियमित ढंग से होना चाहिए। डेटा के अनियमित और मनमाने उपयोग से बचने के लिए, एक स्पष्ट कानूनी ढांचा होना अत्यंत आवश्यक है।
5. **डिजिटल इंडिया :** भारत दुनिया में दूसरा सबसे बड़ा इंटरनेट उपयोगकर्ता आधार वाला देश है। इसलिए, सरकार को नागरिकों के डेटा की सुरक्षा सुनिश्चित करने के लिए विशेष ध्यान देना चाहिए। भारत में 450 मिलियन इंटरनेट उपयोगकर्ता हैं। अतः डिजिटल इंडिया पर जोर देते हुए, सरकार को नागरिकों के डेटा की सुरक्षा सुनिश्चित करनी चाहिए।
6. डिजिटल युग में डेटा सुरक्षा बहुत ज़रूरी है। राज्य को डिजिटल अपराधों को रोकना और उनकी जाँच करनी चाहिए, डेटा के दुरुपयोग को रोकना चाहिए और कानून के माध्यम से डेटा सुरक्षा को प्रोत्साहित करना चाहिए।

समाधान या आगे की राह :

1. **सूचना प्रौद्योगिकी अधिनियम, 2000 :** भारतीय संसद द्वारा पारित यह अधिनियम सूचना प्रौद्योगिकी के कई पहलुओं को जैसे कि इलेक्ट्रॉनिक दस्तावेजों को कानूनी मान्यता प्रदान करना , डिजिटल हस्ताक्षर को कानूनी मान्यता देना , साइबर अपराधों के लिए न्याय व्यवस्था के इतिहास का अध्ययन करना और सूचना तकनीक के विकास जैसे मुद्दों को संबोधित करता है।
2. **चीन मॉडल को अपनाने की दिशा में विचार करने की आवश्यकता :** चीन की नई आर्थिक नीतियां लोगों के बीच संपत्ति की बढ़ती खाई को कम करने के इरादे से बनाई गई हैं। यह उनकी आर्थिक विकास के अनुकूल है, लेकिन आलोचकों का कहना है कि यह व्यवसाय और समाज को अधिक नियंत्रित कर सकती है। भारत को भी चीन मॉडल को अपनाने की दिशा में विचार करने की आवश्यकता हो सकती है, जिसमें फ़ायरवॉल और टोर ट्रैफ़िक को अवरुद्ध किया जाता है।
3. **डार्क वेब की सुरक्षा :** डार्क वेब की सीमापार प्रकृति की चुनौतियों से निपटने के लिए भारत को बहुपक्षीय आदान-प्रदान को बढ़ावा देना चाहिए। इसके लिए नए एन्क्रिप्टिंग टूल और अन्य तकनीकी चुनौतियों का सामना करने में मदद मिलेगी।
4. **वीपीएन पंजीकरण :** वीपीएन पंजीकरण का मतलब होता है कि व्यक्ति या संगठन एक वीपीएन (Virtual Private Network) का उपयोग करने के लिए सरकार द्वारा निर्धारित पंजीकरण प्रक्रिया को पूरा करते हैं। यह एक सुरक्षा की प्रक्रिया होती है जिसमें वीपीएन सेवा प्रदाता से उपयोगकर्ता का पहचान और सर्वर कनेक्शन सुनिश्चित किया जाता है। इस प्रक्रिया के माध्यम से सरकार वीपीएन के उपयोग को नियंत्रित कर सकती है और सुरक्षा संबंधित नियमों का पालन सुनिश्चित कर सकती है। इसके तहत भारत का अतुल्य फ़ायरवॉल फलते-फूलते डार्कनेट अपराध पर गहरा प्रहार और आघात कर सकता है ।

स्रोत – टाइम्स ऑफ इंडिया एवं पीआईबी।

प्रारंभिक परीक्षा के लिए अभ्यास प्रश्न :

Q.1. डार्क वेब के संबंध में निम्नलिखित कथनों पर विचार करें।

1. डार्क वेब प्रकृति में अवैध है।

PLUTUS IAS

2. डार्क वेब तक आपके सामान्य ब्राउज़रों के माध्यम से नहीं पहुंचा जा सकता है और इसे केवल एक विशेष, अनाम ब्राउज़र, जैसे कि टोर या इनविजिबल इंटरनेट प्रोजेक्ट (I2P) के साथ ही पहुँचा जा सकता है।

उपरोक्त कथन / कथनों में से कौन सा कथन सत्य है?

A. केवल 1

B. केवल 2

C. कथन 1 और 2 दोनों ।

D. उपरोक्त में से कोई नहीं।

उत्तर – A

मुख्य परीक्षा के लिए अभ्यास प्रश्न :

Q.1. चर्चा कीजिए कि भारत में डार्क वेब को विनियमित करने की राह में प्रमुख चुनौतियाँ क्या है और उसका समाधान कैसे किया जा सकता है ? (UPSC – 2019 शब्द सीमा – 250 अंक – 15)

Dr. Akhilesh Kumar Shrivastava