Result Mitra Daily Magazine

संयुक्त राष्ट्र साइबर अपराध संधि

➢ **हालिया संदर्भ :**

- साइबर अपराध से निपटने के लिए कानून बनाने की वैश्विक प्रयास की दिशा में संयुक्त राष्ट्र साइबर सम्मेलन में ऐतिहासिक निर्णय लिया गया।
- यह सम्मेलन मुख्यतः साइबर मसौदा पर आयोजित की गई थी, जिसमें ऐसे वैश्विक कानून प्रस्ताव को यूएन सदस्यों द्वारा सर्वसम्पति से अनुमोदित किया गया।
- हालांकि तकनीकी कंपनियों, उद्योग संगठनों, शैक्षणिक संस्थनों, मानवाधिकार संगठनों एवं अन्य हितधारकों ने ऐसे मसौदे का विरोध किया।

➢ **विशेषता :**

- यह 41 पेज लंबी मसौदा है, जो संयुक्त राष्ट्र साइबर अपराध संधि से संबंधित है।
- यह मसौदा कानून प्रवर्तन एजेंसियों के बीच अंतर्राष्ट्रीय सहयोग को बढ़ावा देने और साइबर अपराध से निपटने के लिए पर्याप्त बुनियादी ढाँचा वाले देश को तकनीकी सहायता देने के लिए एक कानूनी ढांचे का समर्थन करता है।
- इस मसौदे में अवैध अवरोधन, मनी लॉन्ड्रिंग, हैकिंग एवं ऑनलाइन बाल यौन शोषण सामग्रियों से भी निपटने के लिए प्रावधान किए गए हैं।
- यूएन कार्यालय के अनुसार यह 20 वर्षों में पहली बहुपक्षीय अपराध-विरोधी संधि है और साइबर अपराध के विरूद्ध यूएन का पहला सम्मेलन है।

➢ आगे की संभावना :

- इस मसौदे को संयुक्त राष्ट्र महासभा में मतदान के लिए भेजा जाएगा, जो अगले महीने प्रस्तावित है।
- यदि यूएनजीए द्वारा इसे अपनाया जाता है तो न्यूनतम 40 देशों द्वारा इस मसौदे को अनुसमर्थित और हस्ताक्षरित करने से यह प्रभावी हो जाएगा।
- यह कानूनी रूप से बाध्यकारी प्रावधान होंगें और यही कारण है कि विरोधी गुट यूएन सदस्यों से इस मसौदे को न मानने के लिए अनुरोध कर रहे हैं।

➢ मसौदे में शामिल तत्व :

- मसौदे के अनुसार, जो भी देश इस पर हस्ताक्षर करेंगें, उन्हें अपने देश में एक कानून बनाने की आवश्यकता होगी, जो किसी विशेष साइबर अपराध को आपराधिक श्रेणी में लाएगा।
- हस्ताक्षर करने वाले देश, एक ऐसा कानून बनाने पर सहमत होंगें, जो गैर-सार्वजनिक डेटा-ट्रांसमिशन को अवैध बनाता है।
- इसके अलावा ऐसे कानूनी उपाय में डेटा को अनाधिकृत तरीके से नुकसान पहुंचाने, हटाने, खराब करने या बदलने के लिए किए ग्नए प्रयास को अवैध करार दिए जाने का मार्ग प्रशस्त करता है।
- यह संधि मुख्य रूस से साइबर अपराध करने के लिए बनाए उपकरणों के उत्पादन, आयात, निर्यात, बिक्री एवं खरीद को प्रतिबंधित करता है।
- इसके अलावा यह सूचना एवं संचार प्रौद्योगिकी प्रणालियों को हैक करने के लिए पासवर्ड एवं लॉगिन प्रणाली की बिक्री एवं खरीद को भी अवैध घोषित करता है।
- संधि में शामिल सरकारों को अनिवार्य रूप से बाल यौन शोषण को फैलाने, संग्रहित करने या देखने के लिए किसी भी प्रयास को साइबर अपराध के रूप में वर्गीकृत करना होगा।
- बाल यौन शोषण को लिखित, ऑडियो या दृश्य सामग्री के रूप में परिभाषित किया गया है, जो 18 वर्ष से कम उम्र के किसी भी व्यक्ति की वास्तविक या नकली/आभासी यौन गतिविधि में संलग्न होने का प्रतिनिधित्व करता है।
- संधि के अनुसार, किसी बच्चे के खिलाफ यौन अपराध करने के लिए ऑनलाइन व्यवस्था करना एवं व्यक्ति की सहमति के बिना उसकी अश्लील/अंतरंग छवियों या वीडियो को ऑनलाइन साझा करना भी साइबर अपराध माना जाएगा।

➢ प्राधिकारें को प्रस्तावित शक्तियाँ :

- संधि का अनुच्छेद-24 में निर्धारित शर्तों एवं सुरक्षा उपायों के अनुसार, सरकारों को यह सुनिश्चित करने का दायित्व है कि कानून प्रवर्तन एजेंसियों को दी गई शक्तियां अंतर्राष्ट्रीय मानवाधिकारों के अनुसार हों।
- इसके तहत अधिकारियों को डेटा को संरक्षित रखने की शक्तियां होंगी, यदि उन्हें ऐसा लगता है कि डेटा को संशोधित या किसी के द्वारा चुराया जा सकता है।
- लोगों के पास 90 दिनों तक डेटा को संरक्षित रखने का अधिकार होगा एवं संचार सेवा प्रदाताओं को पर्याप्त ट्रैफिक डेटा साझा करना आवश्यक होगा ताकि प्रेसित संचार के मार्ग का पता लगाया जा सकना कानून प्रवर्तन एजेंसियों के लिए आसान होगा।

➢ ट्रैफिक डेटा एवं सामग्री डेटा :

- ट्रैफिक डेटा को किसी संचार एवं सूचना प्रौद्योगिकी प्रणाली के किसी भी डेटा के रूप में परिभाषित किया जाता है, जो संचार की उत्पत्ति, गंतव्य, मार्ग, समय, तिथि, आकार, अवधि एवं अंतर्निहित सेवा के रूप में होता है।
- सामग्री डेटा के तहत एमेजेस, पाठ संदेश, ध्वनि संदेश, ऑडियो रिकार्डिंग, वीडियो रिकार्डिंग जैसे डेटा को शामिल किया जाता है।
- ग्राहक जानकारी में ऐसी जानकारियां शामिल होती है, जो किसी सेवा प्रदाता द्वारा अपनी सेवाओं के ग्राहकों से संबंधित होती है।
- अनुच्छेद-30 (संधि) में सरकारों को गंभीर आपराधिक अपराधों की एक श्रृंखला के संबंध में सामग्री डेटा को एकत्र करने के लिए कानून प्रवर्तन अधिकारियों की शक्ति देने का प्रस्ताव हैं
- यह संधि गंभीर अपराध को कम से कम 4 साल की अधिकतम स्वंतत्रता से वंचित करने के रूप में परिभाषित करता है।
- अनुच्छेद-36 का संबंध व्यक्तिगत डेटा-सुरक्षा से संबंधित है, जिसमें कहा गया है कि सरकार को व्यक्तिगत डेटा किसी अन्य देश को तभी हस्तांतरित करना आवश्यक होगा, जब वह घरेलू कानूनों के अनुसार हो।

➢ संबंधित चिंताएं :

- कई डिजिटल समूहों का मानना है कि इस संधि में साइबर अपराधों की व्यापक परिभाषाएं हैं, जो वैध ऑनलाइन गतिविधि को भी अवैध बना देता है।

- विशेषज्ञों के अनुसार संधि में बहुत सारी कमियां हैं, जो सरकारों को कई गतिविधियों की पूरी श्रृंखला को साइबर अपराध घोषित करने की शक्ति देता है। ऐसी गतिविधियों में पत्रकारिता या वैध सुरक्षा अनुसंधान साइबर अपराधियों के लिए संरक्षित क्षेत्र बन जाऐंगें।
- यह संधि डिजिटल युग में निजता की रक्षा करने वाले मानकों को भी कमजोर बनाता है, जो भारतीय संविधान में एक मूल अधिकार (पुट्टुस्वामी मामले 2017) के रूप में भारतीय सर्वोच्च न्यायालय द्वारा संरक्षित है।
- विशेषज्ञ इस बात से भी चिंतित हैं कि यह संधि सीमा-पार निगरानी को भी सक्षम बना सकती है, जिसका प्रयोग सत्तावादी शासन द्वारा मानवाधिकार के हनन के लिए किया जा सकता है।

➢ बुडापेस्ट कन्वेंशन :

- साइबर अपराध पर पहली अंतर्राष्ट्रीय संधि
- काउंसिल ऑफ यूरोप कन्वेंशन के रूप में लोकप्रिय
- 2001 में हस्ताक्षर के लिए रखा गया एवं 1 जुलाई 2004 को लागू हुआ।
- इसमें तीन पक्षों पर जो दिया गया था-1 जांच तकनीकों में सुधार, 2- राष्ट्रों के बीच सहयोग में वृद्धि, 3- राष्ट्रीय कानूनों में सामंजस्य लाना।
- इस संधि पर हस्ताक्षर करने वाले देशों को अपने यहां निर्दिष्ट साइबर-संबंधी अपराधों को गैर-कानूनी घोषित करने के लिए कानून बनाने की आवश्यकता थी।
- इस संधि पर 64 देशों ने समर्थन दिया, जिसमें, फ्रांस, यूएसए, कनाडा, जापान, फिलीपिंस, दक्षिण अफ्रीका आदि प्रमुख थे।
- इसमें डेटा-हस्तक्षेप, उपकरणों का दुरूपयोग, साइबर जालसाजी, बाल पोर्नोग्राफी एवं अवैध अवरोधन को साइबर अपराध के रूप में वर्गीकृत किया गया था।
- भारत ने इस संधि पर हस्ताक्षर नहीं किए थे।

➢ भारत की स्थिति :

- चुनावी रैली के दौरान गृहमंत्री अमित शाह के वीडियो को डीप-फेक वीडियो में बदलकर उनके भाषण को गलत तरीके से वायरल किया गया, जिसके बाद भारत में साइबर क्राइम के चिंताजनक हो रहे हालात पर ध्यान दिया गया।
- इसके अलावा, एक रिपोर्ट के अनुसार 2023-24 वित्तीय वर्ष में भारत में 7488 करोड़ का साइबर-फ्रॉड किया गया।

➢ साइबर सुरक्षित भारत के लिए प्रयास :

- साइबर अपराधों के प्रसार को देखते हुए कई मंत्रालयों विभागों एवं एजेंसियों को मिलाकर बहुआयामी संस्थागत ढांचा स्थापित किया गया है।
- भारत में इलेक्ट्रॉनिक एवं सूचना प्रौद्योगिकी मंत्रालय साइबर कानूनों सहित आईटी, इलेक्ट्रॉनिक्स एवं इंटरनेट से संबंधित नीतियों की देखरेख के लिए जिम्मेदार है।
- गृह मंत्रालय साइबर सुरक्षा सहित आंतरिक सुरक्षा के लिए जिम्मेदार है, जिसने साइबर और सूचना प्रभाग की स्थापना की है, जिसमे साइबर अपराध एवं साइबर सुरक्षा शाखा एवं निगरानी इकाई शामिल है।
- 2020 में गृह मंत्रालय ने भारतीय साइबर अपराध समन्वय केन्द्र स्थापित किया।

➢ नए आपराधिक कानूनों की भूमिका :

- भारतीय नागरिक सुरक्षा संहिता, भारतीय न्याय संहिता एवं भारतीय साक्ष्य अधिनियम 1 जुलाई 2024 से लागू हो गया।
- तीनों कानून इलेक्ट्रॉनिक्स एफआईआर का प्रावधान करते हैं। और इलेक्ट्रॉनिक साक्ष्य को प्राथमिक सबूत के रूप में मान्यता देते हैं।
- बीएनएसएस के तहत अपराधियों की पहचान के लिए डेटा संग्रह की अनुमति है। साथ ही इसमें प्रावधान है कि सभी परीक्षण, पूछताछ एवं कार्यवाही इलेक्ट्रॉनिक मोड में की जा सकती हैं
- बीएसए इलेक्ट्रॉनिक रिकॉर्ड की दस्तावेजों के रूप में वर्गीकृत करता है।

➢ बढ़ते मामले :

- एनसीआरबी की रिपोर्ट के अनुसार 2016 में पंजीकृत साइबर अपराधों की संख्या 12317 थी, जो 2020 में बढ़कर 50035 एवं 2021 में बढ़कर 52975 हो गया।
- 2022 में 2021 की तुलना में साइबर क्राइम में 24 प्रतिशत की वृद्धि हुई।

➢ सूचना प्रौद्योगिकी अधिनियम, 2000 :

- यह 17 अक्टूबर 2000 को लागू हुआ,
- शामिल अपराध निम्न हैं-

1. धारा-65 - कंप्यूटर स्रोत के दस्तावेजों के साथ छेड़-छाड़
2. धारा 66 - हैकिंग
3. धारा 66बी - चोरी हुए कंप्यूटर या किसी संचार उपकरण को प्राप्त करना
4. धारा 66सी- किसी दूसरे व्यक्ति के पासवर्ड का प्रयोग करना।

5. 66 डी- कंप्यूटर प्रणाली के प्रयोग से किसी के साथ धोखा
6. 66 ई - दूसरे व्यक्ति की निजी तस्वीरें प्रकाशित करना,
7. 66 एफ - साइबर आतंकवाद से संबंधित
8. 67 - इलेक्ट्रॉनिक मोड में अश्लील जानकारी का प्रकाशन
9. 67 ए - यौन कृत्यों वाली एमेज/वीडियो का प्रकाशन
10. 67 बी - बाल अश्लीलता
11. 67 सी - संबंधित सेवा प्रदाता द्वारा रिकॉर्ड सुरक्षित रखने में विफलता