डीप फेक और साइबर सुरक्षा की चुनौतियाँ

इस Editorial में The Hindu, The Indian Express, Business Line आदि में प्रकाशित लेखों का विश्लेषण किया गया है। इस लेख में डीप फेक' (Deep Fake) और सोशल मीडिया पर दुष्प्रचार की चुनौतियों व उससे संबंधित विभिन्न पहलुओं पर चर्चा की गई है। आवश्यकतानुसार, यथास्थान टीम दृष्टि के इनपुट भी शामिल किये गए हैं।

संदर्भ:

पिछले दो दशकों में सूचना प्रौद्योगिकी और इंटरनेट के विस्तार ने स्वास्थ्य, शिक्षा, रक्षा आदि क्षेत्रों के साथ हमारे दैनिक जीवन के हर पहलू में बड़े बदलाव किये हैं। सूचना प्रौद्योगिकी के क्षेत्र में तेज़ी से हो रहे नए प्रयोगों ने आधुनिकीकरण की गति में एक उत्प्रेरक का काम किया है, साथ ही इसकी वजह से समाज के हर वर्ग तक मूलभूत सुविधाओं की पहुँच को सुनिश्चित करना भी संभव हो सका है। हालाँकि किसी भी अन्य क्षेत्र की तरह इस क्षेत्र में विकसित तकनीकों के अनियंत्रित प्रयोग के कारण इसके दुरुपयोग की संभावनाएँ बढ़ गई हैं। दुष्प्रचार और अफवाहों की समस्या अब मात्र झुंझलाहट का एक कारण न होकर समाज में तनाव और ध्रुवीकरण बढ़ाने के साथ कई मामलों में चुनावी परिणामों को प्रभावित करने की क्षमता सहित एक बड़ी चुनौती बन गई है। इसी कड़ी में 'डीप फेक' (Deep Fake) दुष्प्रचार और अफवाहों को तेज़ी से तथा एक वृहद् पैमाने पर फैलाने का नया विकल्प बनकर उभरा है। सूचना प्रौद्योगिकी और मीडिया क्षेत्र अपेक्षाकृत नया होने के कारण इस क्षेत्र के अपराधों की निगरानी करना तथा उन्हें नियंत्रित कर पाना सुरक्षा एजेंसियों के लिये एक बड़ी चुनौती बन गया है।

डीप फेक (Deep Fake):

- डीप फेक, 'डीप लर्निंग' और 'फेक' का सम्मिश्रण है। इसके तहत डीप लर्निंग नामक एक कृत्रिम बुद्धिमत्ता या आर्टफिशियिल इंटेलिजेंस (आर्टफिशियिल इंटेलिजेंस-AI) सॉफ्टवेयर का उपयोग कर एक मौजूदा मीडिया फाइल (फोटो, वीडियो या ऑडियो) की नकली प्रतिकृति तैयार की जाती है।
- आर्टफिशियिल इंटेलिजेंस के एल्गोरिदम का प्रयोग कर किसी व्यक्ति द्वारा बोले गए शब्दों, शरीर की गतिविधि या अभिव्यक्ति को दूसरे व्यक्ति पर इस सहजता के साथ स्थानांतरित किया जाता है कि यह पता करना बहुत ही कठिन हो जाता है कि प्रस्तुत फोटो/वीडियो असली है या डीप फेक।
- डीप फेक का मामला सबसे पहले वर्ष 2017 में सामने आया जब सोशल मीडिया साइट 'रेडिट' (Reddit) पर 'डीप फेक' नाम के एक अकाउंट पर इसके एक उपयोगकर्त्ता द्वारा कई मशहूर हस्तियों की आपत्तिजनक डीप फेक तस्वीरें पोस्ट की गईं। इस घटना के बाद से डीप फेक के कई अन्य मामले भी सामने आए हैं।

डीप फेक के दुष्प्रभाव:

- डीप फेक के माध्यम से किसी व्यक्ति, संस्थान, व्यवसाय और यहाँ तक कि एक लोकतांत्रिक व्यवस्था को भी कई प्रकार से क्षति पहुँचाई जा सकती है।
- डीप फेक के माध्यम से मीडिया फाइल में व्यापक हस्तक्षेप (जैसे-चेहरे बदलना, लिप सिंकिंग या अन्य शारीरिक गतिविधि) किया जा सकता है और इससे जुड़े अधिकांश मामलों में लोगों की पूर्व अनुमति नहीं ली जाती, जो मनोवैज्ञानिक, सुरक्षा, राजनीतिक अस्थिरता और व्यावसायिक व्यवधान का खतरा उत्पन्न करता है।

महिला सुरक्षा:

- डीप फेक का दुरुपयोग बड़े पैमाने पर पोर्नोग्राफी के मामलों में देखा गया है जो भावनात्मक और व्यक्तिगत प्रतिष्ठा को क्षति पहुँचाने के साथ कुछ मामलों में व्यक्तिगत हिंसा को भी बढ़ावा देता है।
- डीप फेक पोर्नोग्राफी के अधिकांश मामलों में अपराधियों का लक्ष्य महिलाएँ ही रही हैं, ऐसे में डीप फेक पीड़ित व्यक्ति को धमकाने, डराने और मनोवैज्ञानिक क्षति पहुँचाने हेतु प्रयोग किये जाने के साथ यह किसी महिला को यौन उपभोग की वस्तु के रूप में प्रस्तुत करता है।

राजनीतिक और सामाजिक चुनौतियाँ:

- डीप फेक जैसी तकनीकों के दुरुपयोग से राजनीतिक और सामाजिक अस्थिरता के साथ राष्ट्रीय सुरक्षा के लिये बड़ा खतरा उत्पन्न हो सकता है।
- सत्ता में सर्वोच्च पदों पर बैठे लोगों, भू-राजनीतिक आकांक्षा रखने वाले लोगों, हिंसक अतिवादियों या आर्थिक हितों से प्रेरित लोगों द्वारा डीप फेक के माध्यम से सार्वजनिक रूप से उपलब्ध सूचनाओं में हेर-फेर कर और गलत सूचनाओं के प्रसार से बड़े पैमाने पर अस्थिरता उत्पन्न की जा सकती है।
    - उदाहरण के लिये वर्ष 2019 में अफ्रीकी देश 'गैबॉन गणराज्य' (Gabon Republic) में राजनीतिक और सैन्य तख्तापलट के एक प्रयास में डीप फेक के माध्यम से गलत सूचनाओं को फैलाया गया, इसी प्रकार 'मलेशिया' में भी कुछ लोगों द्वारा विरोधी राजनेताओं की छवि खराब करने के लिये डीप फेक का प्रयोग देखा गया।
- आतंकवादी या चरमपंथी समूहों द्वारा डीप फेक का प्रयोग राष्ट्र-विरोधी भावना फैलाने के लिये किया जा सकता है।

लोकतंत्र के लिये खतरा:

- डीप फेक लोकतांत्रिक संवाद को बदलने और महत्त्वपूर्ण संस्थानों के प्रति लोगों में अविश्वास फैलाने के साथ लोकतंत्र को कमज़ोर करने के प्रयासों को बढ़ावा दे सकता है।
- डीप फेक का प्रयोग चुनावों में जातिगत द्वेष, चुनाव परिणामों की अस्वीकार्यता या अन्य प्रकार की गलत सूचनाओं के लिये किया जा सकता है, जो एक लोकतांत्रिक व्यवस्था के लिये बड़ी चुनौती बन सकता है।
- इसके माध्यम से चुनावी प्रक्रिया शुरू होने के कुछ ही समय/दिन पहले विपक्षी दल या चुनावी प्रक्रिया के बारे में गलत सूचना फैलाई जा सकती है, जिसे समय रहते नियंत्रित करना और सभी लोगों तक सही सूचना पहुँचना बड़ी चुनौती होगी।
    - गौरतलब है कि ब्रिटेन के पिछले प्रधानमंत्री पद के चुनाव में लेबर पार्टी और कंज़रवेटिव पार्टी के उम्मीदवारों का एक डीप फेक वीडियो सामने आया जिसमें वे एक-दूसरे का समर्थन करते दिखाई दिये, इसी प्रकार भारत में भी 2019 के लोकसभा चुनावों में कुछ राजनेताओं के डीप फेक वीडियो सोशल मीडिया पर वायरल हुए थे जिसे बाद में हटा दिया गया।
- डीप फेक तथ्यात्मक सापेक्षवाद (Factual Relativism) को बढ़ावा देता है तथा यह किसी अधिनायकवादी शासक को सत्ता में बने रहने, लोगों के दमन को सही ठहराने और उन्हें उनके अधिकारों से वंचित रखने में सहायक हो सकता है।

व्यक्तिगत प्रतिष्ठा और पहचान को क्षति:

- डीप फेक का इस्तेमाल किसी व्यक्ति या संस्थान की पहचान और प्रतिष्ठा को क्षति पहुँचाने के लिये किया जा सकता है।
- ऐसे मामलों में यदि पीड़ित व्यक्ति फेक मीडिया को हटाने या स्थिति को स्पष्ट करने में सफल रहता है तब भी इसके कारण हुई शुरुआती क्षति को कम नहीं किया जा सकेगा।
- डीप फेक का प्रयोग कई तरह के अपराधों जैसे- धन उगाही, निजी अथवा संवेदनशील जानकारी एकत्र करने या किसी अन्य हित को अनधिकृत तरीके से पूरा करने के लिये किया जा सकता है।
- एक अध्ययन के अनुसार, प्रतिवर्ष विभिन्न व्यवसायों के खिलाफ प्रसारित गलत सूचनाओं और फेक न्यूज़ के कारण वैश्विक अर्थव्यवस्था को लगभग 78 बिलियन अमेरिकी डॉलर की क्षति होती है।

डीप फेक के मामलों में वृद्धि:

- हाल ही में जारी एक रिपोर्ट के अनुसार, पिछले एक वर्ष के दौरान विश्व भर में डीप फेक से जुड़े आपराधिक मामलों में तीव्र वृद्धि देखी गई है।
- जनवरी-जून 2020 के दौरान एशिया में डीप फेक के मामलों में पिछले 6 माह की तुलना में दोगुनी वृद्धि देखी गई।
- डीप फेक की पहचान करने वाली एक तकनीकी कंपनी डीप फेक लैब के आँकड़ों के अनुसार, जनवरी-जून 2020 के बीच एशिया में डीप फेक से बने वीडियो के लगभग 49,081 मामले देखने को मिले।
- डीप फेक लैब द्वारा जुलाई 2019 के बाद से चिह्नित डीप फेक वीडियोज़ में से 95% मामलों में फिल्म, खेल, फैशन या मीडिया क्षेत्र से जुड़े लोगों को लक्षित किया गया था।

भारत पर प्रभाव:

- **वर्तमान में डीप फेक के रूप में चिह्नित अधिकांश मामले (लगभग 61%) अमेरिका और यूनाइटेड किंगडम से संबंधित हैं, परंतु पिछले कुछ समय से दक्षिण कोरिया, जापान और भारत में भी ऐसे मामलों में तीव्र वृद्धि देखी गई है।**
- पिछले कुछ वर्षों में भारत (विशेषकर ग्रामीण क्षेत्रों में) में सूचना प्रौद्योगिकी के क्षेत्र में हुए व्यापक सुधार के कारण इंटरनेट और सोशल मीडिया से जुड़ने वाले लोगों की संख्या में तीव्र वृद्धि हुई है। वर्ष 2019 में भारत के ग्रामीण क्षेत्रों में इंटरनेट पहुँच में 45% की वृद्धि देखी गई, जबकि शहरी क्षेत्रों में यह वृद्धि मात्र 11% ही रही।
    - मई 2020 के एक अनुमान के अनुसार, भारत में मासिक रूप से सक्रिय कुल इंटरनेट उपयोगकर्त्ताओं की संख्या लगभग 574 मिलियन बताई गई थी, दिसंबर 2020 तक यह आँकड़ा बढ़कर 639 मिलियन तक पहुँच जाने का अनुमान है।
- हालाँकि देश की एक बड़ी आबादी के बीच इंटरनेट और साइबर सुरक्षा संबंधी जागरूकता का अभाव ऐसे लोगों को साइबर अपराधों के प्रति अत्यधिक सुभेद्य बनता है।
- साथ ही भारत में डेटा सुरक्षा के मामले में कानून का अभाव भी इस चुनौती को और अधिक बढ़ा देता है।

कानूनी प्रावधान:

- देश में साइबर अपराधों के मामलों में वर्ष 2000 में पारित 'सूचना प्रौद्योगिकी अधिनियम-2000' तथा भारतीय दंड संहिता के प्रावधानों के तहत कार्रवाई की जा सकती है।
- साइबर अपराधों से निपटने के लिये वर्ष 2018 में केंद्रीय गृह मंत्रालय के तहत 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-I4C) की स्थापना की गई।
- साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिये 'केंद्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय' (Ministry of Electronics and Information Technology-MeitY) के तहत 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है।
- नागरिकों के व्यक्तिगत डेटा को सुरक्षा प्रदान करने के लिये दिसंबर 2019 में 'व्यक्तिगत डेटा संरक्षण विधेयक, 2019' (Personal Data Protection Bill, 2019) लोकसभा में प्रस्तुत किया गया था जिसके बाद इसे स्थायी समिति के पास भेज दिया गया है।

समाधान:

- **नीति निर्माण:** डीप फेक मीडिया सामग्री के निर्माण और इसके वितरण की चुनौती से निपटने के लिये सूचना प्रौद्योगिकी क्षेत्र की कंपनियों, नागरिक समाज, नीतिनिर्माताओं तथा अन्य हितधारकों को चर्चा के माध्यम से इंटरनेट एवं सोशल मीडिया की विनियमन नीति की एक व्यापक रूपरेखा तैयार की जानी चाहिये।
- **तकनीकी का प्रयोग: डीप फेक मीडिया सामग्री की पहचान करने, इसे प्रमाणित करने और इसके आधिकारिक स्रोतों तक पहुँच को सुलभ बनाने के लिये आसानी से उपलब्ध तथा उपयोग किये जा सकने वाले तकनीकी आधारित समाधान के विकल्पों को बढ़ावा दिया जाना चाहिये।**
    - हाल ही में स्टैनफोर्ड यूनिवर्सिटी और यूसी बर्कले के शोधकर्त्ताओं ने एक प्रोग्राम तैयार किया है जो कृत्रिम बुद्धिमत्ता का उपयोग कर डीप फेक वीडियो की पहचान कर सकता है। 'डिटेक्टिंग डीप-फेक वीडियोज़ फ्रॉम फेनोम-विसिम मिसमैच' (Detecting Deep-Fake Videos from Phoneme-Viseme Mismatches) नामक शीर्षक से प्रकाशित एक शोध के अनुसार, यह प्रोग्राम किसी मीडिया फाइल में लोगों की आवाज़ और उनके मुँह के आकार में सूक्ष्म भिन्नताओं के माध्यम से 80% मामलों में डीप फेक वीडियो की पहचान करने में सफल रहा।

- **साक्षरता और जागरूकता: उपभोक्ताओं और पत्रकारों के लिये मीडिया जागरूकता को बढ़ाना गलत सूचनाओं तथा डीप फेक जैसी चुनौतियों से निपटने का सबसे प्रभावी साधन/विकल्प है।**
  - **वर्तमान समय में मीडिया साक्षरता एक विवेकशील समाज के लिये बहुत ही आवश्यक है। एक मीडिया उपभोक्ता के रूप में हमारे पास उपलब्ध सूचना को पढ़ने, समझने और उसका उपयोग करने की क्षमता अवश्य की होनी चाहिये।**
  - मीडिया और इंटरनेट को बेहतर ढंग से समझने और इसके सुरक्षित प्रयोग को बढ़ावा देने का एक छोटा हस्तक्षेप भी इससे होने वाले नुकसान को कम करने में सहायक हो सकता है।

निष्कर्ष:

सूचना प्रौद्योगिकी के क्षेत्र में हुई प्रगति के माध्यम से जहाँ संचार, शिक्षा स्वास्थ्य के क्षेत्र में व्याप्त सामाजिक असमानता को दूर करने में सहायता प्राप्त हुई है, वहीं इसने डीप फेक और साइबर सुरक्षा से जुड़ी कई अन्य चुनौतियों को जन्म दिया है। डीप फेक और दुष्प्रचार जैसी चुनौतियों से निपटते हुए अभिव्यक्ति की स्वतंत्रता को सुरक्षित रखने हेतु सभी हितधारकों के साथ मिलकर एक बहुपक्षीय दृष्टिकोण को अपनाना बहुत ही आवश्यक है। विधायी नियमों, प्लेटफॉर्म नीतियों, प्रौद्योगिकी हस्तक्षेप और मीडिया साक्षरता के क्षेत्र में साझा प्रयास डीप फेक के खतरे को कम करने के लिये नैतिक एवं प्रभावी समाधान प्रदान कर सकता है।

अभ्यास प्रश्न: डीप फेक से आप क्या समझते हैं? भारत में डिज़िटिल साक्षरता और मज़बूत डेटा सुरक्षा कानूनों के अभाव में डीप फेक की चुनौतियों और इसके दुष्प्रभावों की समीक्षा कीजिये।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/countering-deep-fakes-the-most-serious-ai-threat