राजस्थान उच्च न्यायालय

<u>जयपुर बेंच</u>

विषय: 'डिजिटल गिरफ्तारी घोटाले', साइबर अपराध के मुद्दे से निपटने और निर्दोष लोगों को अपना पैसा और जीवन खोने से बचाने के मामले में।

जस्टिस अनूप कुमार ढंड

<u>आदेश</u>

22/01/2025

<u>रिपोर्टयोग्य</u>

<u>न्यायालय द्वारा:</u>

1. इस न्यायालय द्वारा प्रतिदिन प्रकाशित अनेक इलेक्ट्रॉनिक, प्रिंट और सोशल मीडिया रिपोर्टों में यह देखा गया है कि पिछले कुछ वर्षों में, साइबर अपराध और 'डिजिटल गिरफ्तारी' जैसे अपराध दुनिया भर में बढ़े हैं और हमारे देश में भी हज़ारों निर्दोष लोग इसके जाल में फँसकर अपनी गाढ़ी कमाई का एक बड़ा हिस्सा गँवा चुके हैं और अपनी जान भी गँवा चुके हैं। 'डिजिटल गिरफ्तारी' के बढ़ते मामलों ने इस बात को उजागर किया है कि जीवन के हर क्षेत्र के लोगों को निशाना बनाने वाले ऐसे घोटालों में कितनी तेज़ी से वृद्धि हो रही है।

2. 'डिजिटल गिरफ्तारी' धोखेबाजों/साइबर अपराधियों द्वारा भोले-भाले पीड़ितों को ठगने और उनसे पैसे ऐंठने के लिए इस्तेमाल की जाने वाली एक नई और

अभिनव रणनीति है। इस साइबर अपराध पद्धति में धोखेबाज पुलिस, प्रवर्तन निदेशालय, सीबीआई आदि जैसे कानून प्रवर्तन अधिकारियों के रूप में खुद को पेश करते हैं और उन्हें यह विश्वास दिलाते हैं कि उन्होंने कोई गंभीर अपराध किया है।

3. घोटालेबाज पीड़ित को यह विश्वास दिलाकर धोखा देते हैं कि उसे 'डिजिटल अरेस्ट' कर लिया गया है और अगर वह घोटालेबाजों द्वारा मांगी गई रकम का भुगतान नहीं करता है, तो उसके खिलाफ मुकदमा चलाया जाएगा। साइबर विशेषज्ञों के अनुसार, इस रणनीति में धोखेबाज पीड़ितों के खिलाफ डर और जल्दबाजी का इस्तेमाल करते हैं और यह सुनिश्चित करते हैं कि वे धोखाधड़ी का एहसास होने से पहले ही अपना पैसा दे दें। साइबर अपराधी/घोटालेबाज अक्सर पीड़ितों से पैसे ऐंठने के लिए उनके प्रियजनों और परिवार के सदस्यों की आवाज़ की नकल करके उन्हें डराने के लिए आर्टिफिशियल इंटेलिजेंस (एआई) का इस्तेमाल करते हैं।

4. वे अक्सर भोले-भाले पीड़ितों को आत्म-गिरफ्तार करने या स्वयं को पृथक रखने के लिए मजबूर करते हैं, उन्हें यह विश्वास दिलाकर कि उन्हें 'डिजिटल गिरफ्तारी' में डाल दिया गया है और जब तक वे मांगी गई राशि का भुगतान नहीं करते, वे अपना घर नहीं छोड़ सकते।

5. तेज़ी से डिजिटल विकास के इस दौर में, डिजिटल गिरफ्तारी घोटाले साइबर अपराध के सबसे घातक रूपों में से एक बनकर उभरे हैं। घोटालेबाज़ अक्सर

डिजिटल स्पेस की कमज़ोरियों का फ़ायदा उठाते हैं, और अधिकार, तात्कालिकता और डर का इस्तेमाल करके पीड़ितों को अपनी निजी जानकारी देने या पैसे ट्रांसफर करने के लिए उकसाते हैं। अलग-अलग देशों ने इस बढ़ते खतरे से निपटने के लिए अलग-अलग स्तर की सफलता के साथ कई तरीके अपनाए हैं।

6. 'डिजिटल गिरफ्तारी' शब्द साइबर धोखाधड़ी के एक परिष्कृत और भ्रामक रूप को संदर्भित करता है, जिसमें अपराधी खुद को कानून प्रवर्तन अधिकारी या सरकारी अधिकारी बताकर निर्दोष व्यक्तियों से पैसे ऐंठते हैं। ये घोटाले छलपूर्ण मनोवैज्ञानिक युक्तियों का इस्तेमाल करते हैं, जिससे अक्सर पीड़ितों को यह विश्वास हो जाता है कि उन्हें गंभीर आपराधिक गतिविधियों में फंसाया गया है। धमकियों और डराने-धमकाने के दबाव में, पीड़ितों को अक्सर गिरफ्तारी या कारावास जैसे गंभीर परिणामों से बचने के लिए भारी रकम देने के लिए मजबूर किया जाता है।

यह ध्यान रखना ज़रूरी है कि भारत में 'डिजिटल गिरफ्तारी' का कोई कानूनी आधार नहीं है। डिजिटल गिरफ्तारी एक बेहद जटिल ठगी है जो पढ़े-लिखे लोगों को भी अपनी गिरफ़्त में ले सकता है।

7. डिजिटल गिरफ्तारी किसी व्यक्ति में भय और आतंक पैदा करने की क्रिया है, तथा उसके बाद झूठे बहाने से उससे पैसे ऐंठ लिए जाते हैं, जिससे अंततः ऐसे व्यक्ति साइबर अपराध का शिकार बन जाते हैं।

8. डिजिटल गिरफ्तारी घोटाले आमतौर पर एक व्यवस्थित तरीके से होते हैं, जिसमें धोखेबाज़ फ़ोन कॉल, ईमेल या वीडियो कॉन्फ्रेंसिंग जैसे विभिन्न माध्यमों से पीड़ितों तक पहुँचते हैं। ये घोटाले आमतौर पर कैसे काम करते हैं, इसका विवरण इस प्रकार है:

1. संपर्क शुरू करना: घोटालेबाज़ पीड़ितों पर नशीले पदार्थों की तस्करी या धन शोधन जैसे गंभीर अपराधों में उनकी प्रत्यक्ष संलिप्तता का आरोप लगाते हैं, जिससे पीड़ितों के मन में तुरंत डर पैदा हो जाता है।

2. डर पैदा करना: पीड़ितों को उनकी माँगें पूरी न करने पर गिरफ़्तारी की धमकी देकर, घोटालेबाज़ उनकी भावनाओं का प्रभावी ढंग से दुरुपयोग करते हैं, और उनमें तात्कालिकता और भय का भाव पैदा करते हैं।

3. वैधता का दिखावा: अपने दावों को विश्वसनीय बनाने के लिए, धोखेबाज़ हद से ज़्यादा कोशिश करते हैं। वे नकली वर्दी, जाली पहचान पत्र और जाली दस्तावेज़ों का इस्तेमाल करते हैं। कुछ मामलों में, वे नकली सरकारी कार्यालय के माहौल से काम करते हैं, जिससे पीड़ितों को अपनी असली होने का और भी ज़्यादा यकीन हो जाता है।

4. अलग-थलग करने की रणनीति: पीड़ितों को अक्सर घोटाले की पूरी प्रक्रिया के दौरान अपने कैमरे और माइक्रोफ़ोन "ऑन" मोड में रखने का निर्देश दिया जाता है, जिससे पीड़ितों के लिए किसी से मदद लेना या किसी से भी स्थिति पर चर्चा करना मुश्किल हो जाता है। यह रणनीति घोटालेबाजों की रणनीति का मूल है, क्योंकि यह पीड़ितों को अलग-थलग कर देती है, जिससे उनमें डर और अनुपालन बढ़ता है।

9. जब दुनिया डिजिटल इंटरैक्शन पर तेज़ी से निर्भर होती जा रही है, ऐसे खतरों से खुद को बचाने के लिए डिजिटल गिरफ्तारी घोटालों के पीछे के तंत्र को समझना ज़रूरी है। ऐसे हमलों के संकेतों को पहचानने के लिए जागरूकता और शिक्षा बेहद ज़रूरी है, ताकि लोग सतर्क और सूचित रहें, जिससे इन घोटालों का शिकार होने की संभावना कम हो।

10. **डिजिटल गिरफ्तारी घोटालों पर अंतर्राष्ट्रीय प्रतिक्रियाएँ**

1. कानून और नियामक उपाय

कई देशों ने डिजिटल गिरफ्तारी घोटालों से निपटने के लिए अपने कानूनी ढाँचों को मज़बूत किया है। उदाहरण के लिए, **ऑस्ट्रेलिया** ने ऐसे कानून बनाए हैं जो पहचान की चोरी और साइबर अपराध के लिए दंड बढ़ाने पर केंद्रित हैं। दूरसंचार धोखाधड़ी घोटालों के लिए

दंड बढ़ाने के लिए साइबर अपराध अधिनियम में संशोधन किया गया है, जिससे अधिकारियों को घोटालेबाजों के खिलाफ अधिक प्रभावी ढंग से कार्रवाई करने में मदद मिलती है। उल्लेखनीय है कि 2021 में, ऑस्ट्रेलियाई अधिकारियों ने ऐसे व्यक्तियों के एक समूह को गिरफ्तार किया था जो एक बड़े पैमाने पर घोटाले की योजना बना रहे थे, जिसमें पीड़ितों से 3 मिलियन ऑस्ट्रेलियाई डॉलर से अधिक की ठगी की गई थी, जिससे प्रभावी कानूनी हस्तक्षेप की आवश्यकता का पता चलता है।

2. **<u>जन जागरूकता अभियान</u>**

जनता में जागरूकता पैदा करना डिजिटल घोटालों से निपटने का एक महत्वपूर्ण आधार है। संयुक्त राज्य अमेरिका ने संघीय व्यापार आयोग (एफटीसी)और फिर इंटरनेट अपराध शिकायत केंद्र (आईसी3) के माध्यम से व्यापक अभियान चलाए हैं। ये अभियान नागरिकों को घोटालों के स्पष्ट संकेतों को पहचानने, व्यक्तिगत जानकारी की सुरक्षा के महत्व और ऐसे घोटालों की रिपोर्ट करने के बारे में शिक्षित करते हैं। हाल ही में, एफटीसी ने स्थानीय कानून प्रवर्तन एजेंसियों के सहयोग से कार्यशालाओं और वेबिनारों का आयोजन किया, जिसके परिणामस्वरूप नागरिकों द्वारा घोटालों के

बारे में रिपोर्टिंग में वृद्धि हुई, जिससे कई घोटालों का पता लगाने और उन्हें समाप्त करने में मदद मिली।

3. **<u>एजेंसियों के बीच सहयोगात्मक प्रयास</u>**

डिजिटल घोटालों से प्रभावी ढंग से निपटने के लिए सरकारी एजेंसियों और निजी कंपनियों के बीच सहयोग आवश्यक है।

4. **<u>तकनीकी समाधान</u>**

डिजिटल गिरफ्तारी घोटालों से निपटने में तकनीकी प्रगति भी महत्वपूर्ण भूमिका निभा सकती है। सिंगापुर ने साइबर सुरक्षा एजेंसी (सीएसए) द्वारा संचालित एआई-संचालित समाधानों को लागू किया है ताकि संभावित पीड़ितों तक पहुँचने से पहले ही घोटाले की कॉल का पता लगाया जा सके और उन्हें ब्लॉक किया जा सके। यह प्रणाली ऐतिहासिक घोटाले के आंकड़ों के आधार पर पैटर्न की पहचान करने के लिए मशीन लर्निंग एल्गोरिदम का उपयोग करती है। 2023 में, सिंगापुर के गृह मंत्रालय ने इन तकनीकी उपायों के लागू होने के बाद घोटाले के मामलों में 25% की कमी दर्ज की।

5. **<u>हॉटलाइन और रिपोर्टिंग प्लेटफॉर्म</u>**

समर्पित हॉटलाइन और ऑनलाइन रिपोर्टिंग प्लेटफ़ॉर्म स्थापित करने से पीड़ित घटनाओं की तुरंत रिपोर्ट कर सकते हैं, जिससे अधिकारियों को घोटाले के रुझानों पर नज़र रखने और हॉटस्पॉट की पहचान करने में मदद मिलती है। कनाडा ने कैनेडियन एंटी-फ्रॉड सेंटर की स्थापना की है, जो घोटालों की रिपोर्ट करने के लिए एक टोल-फ्री हॉटलाइन प्रदान करता है। उदाहरण के लिए, 2022 में, डिजिटल गिरफ्तारी घोटालों में वृद्धि देखी गई, जिसके कारण केंद्र ने एक आपातकालीन संचार रणनीति शुरू की, जिसके परिणामस्वरूप विभिन्न प्रांतों में सक्रिय घोटालेबाजों को लक्षित करने के समन्वित प्रयास में कई व्यक्तियों की गिरफ्तारी हुई।

6. **<u>अंतर्राष्ट्रीय सहयोग</u>**

डिजिटल घोटाले अक्सर सीमाओं को पार कर जाते हैं, जिससे अंतर्राष्ट्रीय सहयोग महत्वपूर्ण हो जाता है। इंटरपोल और यूरोपोल जैसे संगठनों ने टास्क फोर्स बनाए हैं जो सूचनाओं के आदान-प्रदान और संयुक्त अभियानों को सुगम बनाते हैं। 2023 में, एशिया और यूरोप में डिजिटल गिरफ्तारी घोटालों में शामिल एक गिरोह के खिलाफ इंटरपोल के नेतृत्व में एक बहुराष्ट्रीय अभियान के

परिणामस्वरूप 80 व्यक्तियों की गिरफ्तारी हुई और लाखों की संपत्ति जब्त की गई।

11. राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) की रिपोर्ट अपने प्रकाशन "भारत में अपराध" में अपराधों के सांख्यिकीय आंकड़ों का संकलन और प्रकाशन करती है। वर्ष 2022 में प्रकाशित अंतिम रिपोर्ट से पता चलता है कि देश भर में साइबर अपराध से संबंधित लगभग 65,893 मामले दर्ज किए गए और राजस्थान में लगभग 1,833 मामले दर्ज किए गए। इन अपराधों में 'डिजिटल गिरफ्तारी' का नया अपराध भी शामिल हो गया है और यह संख्या दिन-प्रतिदिन बढ़ रही है।

12. इस नए अपराध 'डिजिटल गिरफ्तारी' पर अंकुश लगाने के लिए सरकारी स्तर पर कई परामर्श जारी किए गए हैं और कुछ कदम भी उठाए गए हैं।

13. गृह मंत्रालय (एमएचए) के अंतर्गत भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) देश में साइबर अपराध से निपटने से संबंधित गतिविधियों का समन्वय करता है। गृह मंत्रालय इन धोखाधड़ी से निपटने के लिए अन्य मंत्रालयों और उनकी एजेंसियों जैसे आरबीआई और अन्य संगठनों के साथ मिलकर काम कर रहा है। आई4सी राज्यों/केंद्र शासित प्रदेशों के पुलिस अधिकारियों को मामलों की पहचान और जाँच के लिए इनपुट और तकनीकी सहायता भी प्रदान कर रहा है। डिजिटल गिरफ्तारी के मामलों में वृद्धि के बीच आई4सी ने सभी राज्यों और केंद्र शासित प्रदेशों की पुलिस को अलर्ट जारी किया है।”

14. आई4सी के तहत मेवात, जामताड़ा, अहमदाबाद, हैदराबाद, चंडीगढ़, विशाखापत्तनम और गुवाहाटी के लिए सात संयुक्त साइबर समन्वय दल (जेसीसीटी) गठित किए गए हैं, जो राज्यों/संघ शासित प्रदेशों की कानून प्रवर्तन एजेंसियों के बीच समन्वय ढांचे को बढ़ाने के लिए राज्यों/संघ शासित प्रदेशों को शामिल करके साइबर अपराध हॉटस्पॉट/बहु-क्षेत्राधिकार संबंधी मुद्दों वाले क्षेत्रों के आधार पर पूरे देश को कवर करते हैं। 2023 में हैदराबाद, अहमदाबाद, गुवाहाटी, विशाखापत्तनम, लखनऊ, रांची और चंडीगढ़ में जेसीसीटी के लिए सात कार्यशालाएँ आयोजित की गईं

आई4सी ने माइक्रोसॉफ्ट के साथ मिलकर ऐसी गतिविधियों में शामिल 1,000 से ज़्यादा स्काइप आईडी भी ब्लॉक कर दी हैं। यह ऐसे धोखेबाज़ों/स्कैमर्स द्वारा इस्तेमाल किए जाने वाले सिम कार्ड, मोबाइल डिवाइस और म्यूल अकाउंट को ब्लॉक करने में भी मदद कर रहा है। आई4सी ने अपने सोशल मीडिया प्लेटफॉर्म 'साइबरदोस्त' पर इन्फोग्राफिक्स और वीडियो के ज़रिए कई अलर्ट भी जारी किए हैं।

15. गृह मंत्रालय की साइबर शाखा ने ऐसे मामलों की सूचना देने और साइबर अपराध के नए खतरे के बारे में अधिक जानकारी प्राप्त करने के लिए एक हेल्पलाइन नंबर भी शुरू किया है। पीड़ितों से अनुरोध किया गया है कि वे 1930 पर कॉल करें और तुरंत आई4सी शाखा को ऐसी धोखाधड़ी की सूचना दें।

16. आई 4 सी के एक भाग के रूप में, राज्य/संघ राज्य क्षेत्र पुलिस के जांच अधिकारियों (आईओ) को प्रारंभिक साइबर फोरेंसिक सहायता प्रदान करने के लिए नई दिल्ली में राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला (जांच) की स्थापना की गई है। अब तक, राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला (जांच) ने साइबर अपराधों से संबंधित मामलों की जांच में मदद करने के लिए मोबाइल फोरेंसिक, मेमोरी फोरेंसिक, कॉल डेटा रिकॉर्ड (सीडीआर) विश्लेषण आदि जैसे लगभग 9,000 साइबर फोरेंसिक में राज्य कानून प्रवर्तन एजेंसियों को अपनी सेवाएं प्रदान की हैं। **राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला (साक्ष्य)** हैदराबाद में स्थापित की गई है। इस प्रयोगशाला की स्थापना साइबर अपराध से संबंधित साक्ष्य के मामलों में आवश्यक फोरेंसिक सहायता प्रदान करती है, सूचना और प्रौद्योगिकी अधिनियम और साक्ष्य अधिनियम के प्रावधानों के अनुरूप साक्ष्य और उसके विश्लेषण को संरक्षित करती है,तथा निस्तारण समय में कमी करती है।

17. इसके अतिरिक्त, आई 4 सी के अंतर्गत '**साइट्रेन**' नामक एक व्यापक मुक्त ऑनलाइन पाठ्यक्रम (एमओओसी) प्लेटफ़ॉर्म विकसित किया गया है, जिसका उद्देश्य साइबर अपराध जाँच, फोरेंसिक, अभियोजन आदि के महत्वपूर्ण पहलुओं पर ऑनलाइन पाठ्यक्रम के माध्यम से पुलिस अधिकारियों/न्यायिक अधिकारियों की क्षमता निर्माण और प्रमाणन प्रदान करना है। राज्यों/केंद्र शासित प्रदेशों के

76,000 से अधिक पुलिस अधिकारी पंजीकृत हैं और पोर्टल के माध्यम से 53,000 से अधिक प्रमाण पत्र जारी किए जा चुके हैं।

18. गृह मंत्रालय ने '**महिलाओं और बच्चों के विरुद्ध साइबर अपराध रोकथाम (सीसीपीडब्ल्यूसी)'** योजना के अंतर्गत राज्यों/केंद्र शासित प्रदेशों को साइबर फोरेंसिक-सह-प्रशिक्षण प्रयोगशालाओं की स्थापना, कनिष्ठ साइबर सलाहकारों की नियुक्ति और कानून प्रवर्तन एजेंसियों के कर्मियों, लोक अभियोजकों और न्यायिक अधिकारियों के प्रशिक्षण जैसी क्षमता निर्माण गतिविधियों के लिए 131.60 करोड़ रुपये की वित्तीय सहायता भी प्रदान की है। 33 राज्यों/केंद्र शासित प्रदेशों में साइबर फोरेंसिक-सह-प्रशिक्षण प्रयोगशालाएँ स्थापित की जा चुकी हैं और जून 2024 तक, 24,600 से अधिक कानून प्रवर्तन एजेंसियों के कर्मियों, न्यायिक अधिकारियों और लोक अभियोजकों को साइबर अपराध जागरूकता, जाँच, फोरेंसिक आदि पर प्रशिक्षण प्रदान किया जा चुका है।

19. इसके अतिरिक्त, दूरसंचार विभाग (डी ओ टी)ने साइबर धोखाधड़ी के बढ़ते मामलों के मद्देनजर नागरिकों के लिए एक एडवाइजरी जारी की है, जिसमें नागरिकों से फर्जी फोन कॉल्स का जवाब न देने का आग्रह किया गया है। इसमें लोगों को सतर्क रहने और **संचार साथी पोर्टल (डब्ल्यूडब्ल्यूडब्ल्यू.संचारसाथी. जाओवी. इन/ एसएफसी)की 'चक्षु - संदिग्ध धोखाधड़ी संचार** की रिपोर्ट करें' सुविधा पर ऐसे धोखाधड़ी वाले संचारों की रिपोर्ट करने की सलाह दी गई है। दूरसंचार

विभाग नागरिकों को यह भी सलाह देता है कि यदि वे पहले से ही साइबर अपराध या वित्तीय धोखाधड़ी का शिकार हैं, तो वे साइबर अपराध हेल्पलाइन नंबर 1930 या डब्ल्यूडब्ल्यूडब्ल्यू. साइबर क्राइम.जाओवी. इन पर रिपोर्ट करें। नागरिक संचार साथी प्लेटफॉर्म पर उपलब्ध चक्षु सुविधा पर संदिग्ध धोखाधड़ी वाले कॉल, एसएमएस और व्हाट्सएप संदेशों के बारे में जानकारी, स्क्रीनशॉट, प्राप्ति का माध्यम, इच्छित धोखाधड़ी की श्रेणी, ऐसे संचार प्राप्त होने की तिथि और समय प्रदान करके ऐसी कॉल्स की रिपोर्ट कर सकते हैं। चक्षु सुविधा नागरिकों को साइबर धोखाधड़ी से बचाने की दिशा में उठाया गया एक महत्वपूर्ण कदम है। संदिग्ध गतिविधियों की रिपोर्ट करने के लिए एक सुव्यवस्थित प्रक्रिया प्रदान करके, यह संभावित धोखाधड़ी का शीघ्र पता लगाने और रोकथाम में मदद करता है, जिससे उपयोगकर्ताओं को वित्तीय और व्यक्तिगत नुकसान से बचाया जा सकता है।

20. इसके अलावा, उपरोक्त खतरे के तेज़ी से बढ़ते प्रभाव को देखते हुए, दूरसंचार विभाग ने दूरसंचार सेवा प्रदाताओं (टीएसपी) के साथ मिलकर एक उन्नत प्रणाली शुरू की है, जो आने वाली अंतरराष्ट्रीय नकली कॉलों की पहचान करके उन्हें भारतीय दूरसंचार ग्राहकों तक पहुँचने से पहले ही ब्लॉक कर देगी। इस प्रणाली को दो चरणों में लागू किया जा रहा है: पहला, टीएसपी स्तर पर, अपने ग्राहकों के

फ़ोन नंबरों से नकली कॉलों को रोकने के लिए; और दूसरा, केंद्रीय स्तर पर, अन्य टीएसपी के ग्राहकों के नंबरों से नकली कॉलों को रोकने के लिए।

अब तक सभी टीएसपी ने इस प्रणाली को सफलतापूर्वक लागू कर दिया है। कुल 45 लाख स्पूफ कॉल्स में से लगभग एक तिहाई को भारतीय दूरसंचार नेटवर्क में आने से रोका जा रहा है। अगले चरण में एक केंद्रीकृत प्रणाली शामिल होगी जो सभी टीएसपी में शेष स्पूफ्ड कॉलों को समाप्त कर देगी, तथा इसके शीघ्र ही चालू होने की उम्मीद है।

21. राजस्थान राज्य ने भी साइबर अपराध पर अंकुश लगाने के लिए कई कदम उठाए हैं, जिनमें **'ऑपरेशन एंटी-वायरस'** और **साइबर सुरक्षा केंद्र** की स्थापना शामिल है। ऑपरेशन एंटी-वायरस राजस्थान पुलिस, भारत सरकार और दूरसंचार विभाग के बीच एक सहयोग है। इसी कड़ी में, राजस्थान पुलिस ने पिछले साल 2024 में धोखाधड़ी की गतिविधियों में शामिल एक समूह को निशाना बनाकर यह अभियान चलाया था और इसके परिणामस्वरूप कई संदिग्धों को गिरफ्तार किया गया था। पुलिस ने कई संदिग्ध सिम और मोबाइल फोन ब्लॉक किए हैं और जबरन वसूली और फर्जी निवेश योजनाओं में शामिल साइबर अपराधियों को गिरफ्तार किया है।

22. इसके अलावा, राजस्थान सरकार ने जोधपुर में सरदार पटेल पुलिस विश्वविद्यालय में साइबर सुरक्षा केंद्र की स्थापना की है, जिसका उद्देश्य राजस्थान

राज्य के लिए सूचना सुरक्षा रोडमैप विकसित करना और बड़ी/मध्यम/लघु इकाइयों सहित राजस्थान सरकार के विभागों को सूचना सुरक्षा के कार्यान्वयन और जागरूकता सुनिश्चित करने में मदद करना, और साइबर सुरक्षा के क्षेत्र में उत्कृष्टता केंद्र विकसित करना और सूचना सुरक्षा के क्षेत्र में ऑनसाइट और ऑफसाइट कार्यशालाओं/सेमिनारों के माध्यम से सरकारी और गैर-सरकारी एजेंसियों को प्रशिक्षण प्रदान करना है।

23. डिजिटल गिरफ्तारी घोटाले हमारी परस्पर जुड़ी दुनिया में एक बड़ा खतरा पैदा करते हैं, और इनसे प्रभावी ढंग से निपटने के लिए एक बहुआयामी दृष्टिकोण की आवश्यकता है। विभिन्न देशों ने इन घोटालों से जुड़े जोखिमों को कम करने के लिए कानून, जन जागरूकता अभियान, तकनीकी नवाचार और सहयोगात्मक पहल अपनाई हैं। हालाँकि चुनौतियाँ बनी हुई हैं, स्थानीय, राष्ट्रीय और अंतर्राष्ट्रीय स्तर पर चल रहे प्रयास और प्रतिबद्धता डिजिटल गिरफ्तारी घोटालों की व्यापकता और प्रभाव को कम करने की दिशा में एक आशाजनक प्रगति का संकेत देते हैं। विभिन्न देशों के साझा अनुभव और रणनीतियाँ साइबर अपराध के खिलाफ इस जारी लड़ाई में महत्वपूर्ण सीख के रूप में काम करती हैं। अंततः, इस लड़ाई में ऐसे घोटालों का विरोध करने के लिए ज्ञान और उपकरणों से व्यक्तियों को सशक्त बनाना सर्वोपरि होगा।

24. यद्यपि सरकार के विभिन्न स्तरों पर कई कदम उठाए गए हैं, लेकिन वर्तमान और खतरनाक स्थिति को रोकने के लिए सभी हितधारकों द्वारा अधिक गंभीर कदम उठाए जाने की आवश्यकता है।

25. सरकार ने सोशल मीडिया प्लेटफॉर्म, ओवर-द-टॉप प्लेटफॉर्म और डिजिटल समाचार पोर्टलों की गतिविधियों को नियंत्रित करने के लिए प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 (संक्षेप में '2021 के नियम') लागू किए हैं। ये नियम हानिकारक सूचना के स्रोत का पता लगाते हैं। यह पाया गया है कि कुछ सोशल मीडिया कंपनियां डेटा बेचती हैं और इसका दुरुपयोग निर्दोष जनता के साथ ऐसे साइबर अपराध करने वाले आरोपियों द्वारा किया जाता है। हमारे देश की बढ़ती तकनीकी प्रगति और बढ़ती पहुँच देश में साइबर अपराध के बढ़ते मामलों में परिलक्षित होती है।

26. यह सही समय है कि प्रिंट, इलेक्ट्रॉनिक, सोशल मीडिया, टेलीविजन और एफएम रेडियो के माध्यम से हर घंटे और हर दिन एक सार्वजनिक अभियान फैलाया जाए ताकि आम जनता को पता चले कि कानून प्रवर्तन के लिए 'वीडियो कॉल या ऑनलाइन निगरानी के जरिए गिरफ्तारी' करने का कोई प्रावधान नहीं है। अगर जनता को ऐसे कॉल आते हैं, तो यह एक स्पष्ट ठगी है। वास्तव में, हाल ही में लागू नए आपराधिक कानून में डिजिटल गिरफ्तारी करने का कोई कानूनी प्रावधान नहीं है। भारतीय नागरिक सुरक्षा संहिता, 2023 (बीएनएसएस)धारा 63 के

तहत समन को इलेक्ट्रॉनिक रूप से तामील करने का प्रावधान करती है। यह धारा समन के स्वरूप को परिभाषित करती है। इसमें कहा गया है कि इलेक्ट्रॉनिक रूप से तामील किया गया प्रत्येक समन एन्क्रिप्टेड होगा और उस पर न्यायालय की छवि, मुहर और डिजिटल हस्ताक्षर होंगे। लोगों को इस तथ्य से अवगत कराया जाना चाहिए कि BNSS की धारा 35 और 36 के अनुसार गिरफ्तारी के समय उचित प्रक्रिया का पालन किया जाना चाहिए। गिरफ्तारी करने वाले पुलिस अधिकारी की पहचान स्पष्ट और स्पष्ट होनी चाहिए तथा गिरफ्तारी के समय फर्द गिरफ्तारी तैयार करना आवश्यक है, जिसे कम से कम एक गवाह द्वारा सत्यापित किया जाना चाहिए तथा गिरफ्तार किए जा रहे व्यक्ति द्वारा हस्ताक्षरित होना चाहिए।

27. भारतीय रिजर्व बैंक (आरबीआई) के स्तर पर कुछ गंभीर कदम उठाए जाने की आवश्यकता है, ताकि ऐसे जालसाजी वाले लेनदेन के पैसे को स्थानांतरित न किया जा सके या ऐसे धोखाधड़ी वाले लेनदेन के भुगतान को रोका जा सके, जहां पीड़ित/पीड़ित द्वारा शिकायत की गई हो।

28. आरबीआई और सरकार को पोर्टल या वेबसाइट या मोबाइल नंबर पर शिकायत निवारण समिति को शिकायत प्राप्त होने पर धोखाधड़ी करने वाले व्यक्ति को भुगतान रोकने का तंत्र विकसित करने की आवश्यकता है, ताकि निर्दोष लोगों का पैसा बचाया जा सके।

29. इस चिंताजनक स्थिति और इस नए साइबर अपराध में वृद्धि को गंभीरता से लेते हुए, इस न्यायालय द्वारा स्वतः संज्ञान लिया जाता है और इसे इस प्रकार पंजीकृत किया जाता है:-

स्वप्रेरणा: 'डिजिटल गिरफ्तारी घोटाले', साइबर अपराध के मुद्दे से निपटने और निर्दोष लोगों को अपना पैसा और जीवन खोने से बचाने के मामले में।

बनाम

1) भारत संघ, सचिव, जरिये गृह मंत्रालय, नई दिल्ली ।
2) राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला (जांच एवं साक्ष्य), जरिये निदेशक, नई दिल्ली ।
3) भारतीय रिजर्व बैंक, जरिये गवर्नर, नई दिल्ली ।
4) भारतीय राष्ट्रीय भुगतान निगम, जरिये निदेशक, नई दिल्ली ।
5) मुख्य सचिव, राजस्थान सरकार, सचिवालय, जयपुर।
6) पुलिस महानिदेशक, पुलिस मुख्यालय, जयपुर।
7) अतिरिक्त पुलिस महानिदेशक (साइबर अपराध), पुलिस मुख्यालय, जयपुर।

30. प्रतिवादियों को नोटिस जारी करें, जिससे नियम तीन सप्ताह के भीतर प्रत्यावर्तनीय किया जा सके।

31. मुख्य सचिव, राजस्थान सरकार, जयपुर; और सचिव, गृह मंत्रालय, नई दिल्ली को निर्देश दिया जाता है कि वे डिजिटल गिरफ्तारी और साइबर अपराध के इन

अपराधों से उत्पन्न स्थिति से निपटने के लिए राज्य और केंद्र सरकार द्वारा उठाए गए कदमों के संबंध में इस न्यायालय के समक्ष एक रिपोर्ट प्रस्तुत करें।

32. यह न्यायालय भारत के अतिरिक्त सॉलिसिटर जनरल श्री आर.डी. रस्तोगी, महाधिवक्ता श्री राजेंद्र प्रसाद और अधिवक्ता श्री अनुराग कलावतिया से अनुरोध करता है कि वे इस याचिका से संबंधित मुद्दे पर न्यायालय की सहायता करें। कार्यालय को निर्देश दिया जाता है कि वे इस आदेश की एक प्रति उन्हें उपलब्ध कराएँ।

33. कार्यालय को निर्देश दिया जाता है कि इस मामले को माननीय मुख्य न्यायाधीश के समक्ष प्रस्तुत किया जाए ताकि इसे उपयुक्त पीठ के समक्ष सूचीबद्ध किया जा सके।

(अनूप कुमार ढंड**),जे**

करण/

"अस्वीकरण- इस निर्णय का अनुवाद स्थानीय भाषा में किया जा रहा है, एवं इसका प्रयोग केवल पक्षकार इसको समझने के लिए उनकी भाशा में कर सकेगे एवं यह किसी अन्य प्रयोजन में काम नहीं ली जायेगी। सभी अधिकारिक एवं व्यवहारिक उद्देश्यों के लिए उक्त निर्णय का अंग्रेजी संस्करण ही विश्वसनीय माना जायेगा एवं निश्पादन एवं क्रियान्वयन में भी उसी को उपयोग में लिया जायेगा।"

Tarun Mehra

Advocate