sflc.in

मार्गदर्शिका

इलेक्ट्रॉनिक उपकरणों की तलाशी एवं ज़ब्ती

इलेक्ट्रॉनिक उपकरणों की तलाशी एवं ज़ब्ती पर मार्गदर्शिका, 2025
SFLC.in द्वारा UNESCO के सहयोग से

प्रकाशक: SFLC.in
K9, दूसरी मंज़िल, बीरबल रोड, जंगपुरा एक्सटेंशन, नई दिल्ली – 14, भारत.

ईमेल: mail@sflc.in

वेबसाइट: https://www.sflc.in

sflc.in unesco

अनुक्रमणिका

खंड 1

मूल जानकारी

क्या किसी ने आपकी तलाशी ली है?
क्या उन्होंने आपके शरीर, वाहन या घर की तलाशी ली?
क्या उन्होंने आपके उपकरण ज़ब्त किए?
यदि इनमें से किसी का भी उत्तर हाँ है...

तलाशी और ज़ब्ती विस्तृत विश्लेषण

तलाशी और ज़ब्ती: क्या, क्यों और कहाँ

'तलाशी' का अर्थ है किसी व्यक्ति या उसकी संपत्ति[1] में चल रही जाँच या न्यायिक कार्यवाही [2] के लिए सबूत खोजने के लिए देखना। यह वारंट के साथ [3] या बिना [4] किया जा सकता है।

'ज़ब्ती' का अर्थ है तलाशी पूरी होने के बाद उस संपत्ति का कब्ज़ा ना ताकि उसे सबूत के तौर पर या जाँच के लिए संबंधित संपत्ति के तौर पर इस्तेमाल किया जा सके।[5]

क्या: यह वह उपकरण है जिसका उपयोग कानून प्रवर्तन एजेंसियों द्वारा किसी मामले की जाँच करने के लिए किया जाता है।

क्यों: यह सबूत इकट्ठा करने, अपराध को रोकने और न्याय का उल्लंघन होने से बचाने के लिए किया जाता है।

कहाँ: वे स्थान जहाँ अपराध किया गया था, वे स्थान जहाँ अपराध में शामिल लोग छिपे हो सकते हैं, और वे स्थान जहाँ अपराध से संबंधित कोई भी सामग्री रखी जा सकती है।

तलाशी और ज़ब्ती के कारण

- यह सुनिश्चित करने के लिए किया जाता है ताकि किसी व्यक्ति के खिलाफ जाँच, पूछताछ या मुकदमे के लिए महत्वपूर्ण वस्तुएँ और दस्तावेज़, जिनमें इलेक्ट्रॉनिक और डिजिटल रिकॉर्ड भी शामिल हैं, किसी भी एजेंसी को उपलब्ध कराई जा सके।
- जाँच एजेंसियाँ/पुलिस तलाशी और ज़ब्त किए गए दस्तावेज़ों की सामग्री को अदालत में प्राथमिक या द्वितीयक साक्ष्य के माध्यम से साबित कर सकती हैं।

इन कार्रवाइयों को संचालित करने वाले कानून

तलाशी और ज़ब्ती की शक्ति विभिन्न कानूनों से प्राप्त होती है, जैसे कि [6]:

+ भारतीय नागरिक सुरक्षा संहिता, 2023 {The Bharatiya Nagarik Suraksha Sanhita, 2023} [7]
  + भारतीय साक्ष्य अधिनियम, 2023 {The Bharatiya Sakshya Adhiniyam, 2023} [8]
+ भारतीय न्याय संहिता, 2023 {The Bharatiya Nyaya Sanhita, 2023} [9]
  + आयकर अधिनियम, 1961 {The Income Tax Act, 1961}
+ गैरकानूनी गतिविधियाँ (रोकथाम) अधिनियम, 1967 {Unlawful Activities (Prevention) Act, 1967}
  + धन शोधन निवारण अधिनियम, 2002 {Prevention of Money Laundering Act, 2002}
+ सीबीआई मैनुअल, 2020 {CBI Manual of 2020}
  + सूचना प्रौद्योगिकी अधिनियम, 2000 {The Information Technology Act, 2000}
+ दूरसंचार अधिनियम, 2023 {The Telecommunications Act, 2023}
  + स्वापक औषधि और मनःप्रभावी पदार्थ अधिनियम, 1985 {The Narcotic Drugs And Psychotropic Substances Act, 1985}

पर्दे के पीछे: तलाशी और ज़ब्ती में कौन क्या करता है

तलाशी और ज़ब्ती करने का अधिकार विभिन्न कानूनों के अनुसार अलग-अलग होता है और जो आगे विस्तार से समझाया गया है। इस भाग का उद्देश्य यह सामान्य जानकारी देना है कि तलाशी को कौन अधिकृत कर सकता है और किसे इसे करने का अधिकार है। इसे पढ़ने से आपको जाँच अधिकारियों के साथ उचित प्रश्न पूछने में मदद मिलेगी।

विभिन्न कानून और परिस्थितियों के आधार पर तलाशी और ज़ब्ती की प्रक्रिया अलग-अलग हो सकती है।

I. तलाशी का आदेश जारी करने का अधिकार किसके पास होता है?

भारतीय नागरिक सुरक्षा संहिता, 2023 (BNSS)	एक न्यायाधीश (जिला मजिस्ट्रेट, उप-विभागीय मजिस्ट्रेट या प्रथम श्रेणी के मजिस्ट्रेट) एक पुलिस अधिकारी को, जो कांस्टेबल के पद से ऊपर का हो (केवल कोई भी अधिकारी नहीं), किसी स्थान की तलाशी लेने के लिए विशेष अनुमति दे सकता है यदि उन्हें लगता है कि वहाँ चोरी का सामान या खतरनाक चीजें छिपी हैं। यह अधिकारी आवश्यकता पड़ने पर दूसरों से भी सहायता ले सकता है।
आयकर अधिनियम, 1961 (ITA)	निदेशक/महानिदेशक/मुख्य आयुक्त/आयुक्त के पास तलाशी का आदेश जारी करने का अधिकार है।
गैरकानूनी गतिविधियाँ (रोकथाम) अधिनियम, 1967 (UAPA)	केंद्र सरकार/राज्य सरकार तलाशी के आदेश दे सकती है। हालाँकि, कानून यह स्पष्ट नहीं करता कि कौन सा विभाग/मंत्रालय (केंद्र/राज्य) इस आदेश को जारी करने के लिए अधिकृत है।
धन शोधन निवारण अधिनियम, 2002 (PMLA)	**सर्वेक्षण के लिए:** निर्णय देने वाली प्राधिकृत संस्था आदेश जारी कर सकती है। **ज़ब्ती के लिए:** निदेशक या कोई अन्य अधिकारी जो उप निदेशक के रैंक से नीचे न हो, आदेश जारी कर सकता है।
मा हि ती तंत्रज्ञा न का यदा , 2000 (IT Act)	केंद्र सरकार को केंद्र या राज्य सरकार के किसी भी अधिकारी को तलाशी का आदेश देने का अधिकार है। नियंत्रक भी कंप्यूटरों के भीतर डेटा तक पहुँचने के लिए तलाशी का आदेश दे सकता है।

पर्दे के पीछे: तलाशी और ज़ब्ती में कौन क्या करता है

तलाशी और ज़ब्ती करने का अधिकार विभिन्न कानूनों के अनुसार अलग-अलग होता है और जो आगे विस्तार से समझाया गया है। इस भाग का उद्देश्य यह सामान्य जानकारी देना है कि तलाशी को कौन अधिकृत कर सकता है और किसे इसे करने का अधिकार है। इसे पढ़ने से आपको जाँच अधिकारियों के साथ उचित प्रश्न पूछने में मदद मिलेगी।

विभिन्न कानून और परिस्थितियों के आधार पर तलाशी और ज़ब्ती की प्रक्रिया अलग-अलग हो सकती है।

II. तलाशी करने का अधिकार किसके पास है?

भारतीय नागरिक सुरक्षा संहिता, 2023 (BNSS)	तलाशी और जब्ती से संबंधित कानून कैसे काम करता है, इसका मूल विचार इस प्रकार है: स्टेशन हाउस ऑफिसर (SHO) या जाँच अधिकारी (IO) तलाशी और ज़ब्ती कर सकते हैं, और यदि ये मौजूद नहीं हैं, तो यह किसी भी अधिकारी द्वारा किया जा सकता है जिसे लिखित रूप में अधिकृत किया गया हो। **अगर कोई गिरफ्तार होता है:** पुलिस उस स्थान की तलाशी ले सकती है जहाँ उसे पकड़ा गया है और अपराध से संबंधित किसी भी वस्तु को ज़ब्त कर सकती है। यह केवल पुलिस ही कर सकती है, और यदि आवश्यकता हो तो वे दरवाजे या खिड़कियां तोड़ भी सकती हैं। **अगर कुछ संदिग्ध छुपाया गया हो:** एक न्यायाधीश (जिला मजिस्ट्रेट, उप-विभागीय मजिस्ट्रेट या प्रथम श्रेणी के मजिस्ट्रेट) एक पुलिस अधिकारी को, जो कांस्टेबल के पद से ऊपर का हो (केवल कोई भी अधिकारी नहीं), किसी स्थान की तलाशी लेने के लिए विशेष अनुमति दे सकता है यदि उन्हें लगता है कि वहाँ चोरी का सामान या खतरनाक चीजें छिपी हैं। यह अधिकारी आवश्यकता पड़ने पर दूसरों से भी सहायता ले सकता है। **धारा: 44 & 97**
गैरकानूनी गतिविधियाँ (रोकथाम) अधिनियम, 1967 (UAPA)	UAPA की जाँच का अधिकार विभिन्न शहरों में अलग-अलग होता है: **दिल्ली स्पेशल पुलिस एस्टैब्लिशमेंट:** उप-पुलिस अधीक्षक या समकक्ष। **मुंबई, कोलकाता, चेन्नई, अहमदाबाद और अधिसूचित क्षेत्रों के महानगरों में:** सहायक पुलिस आयुक्त और उससे उच्च पद। **अन्य मामलों में:** अधिकारी जो उप-पुलिस अधीक्षक या समकक्ष रैंक से नीचे न हो।

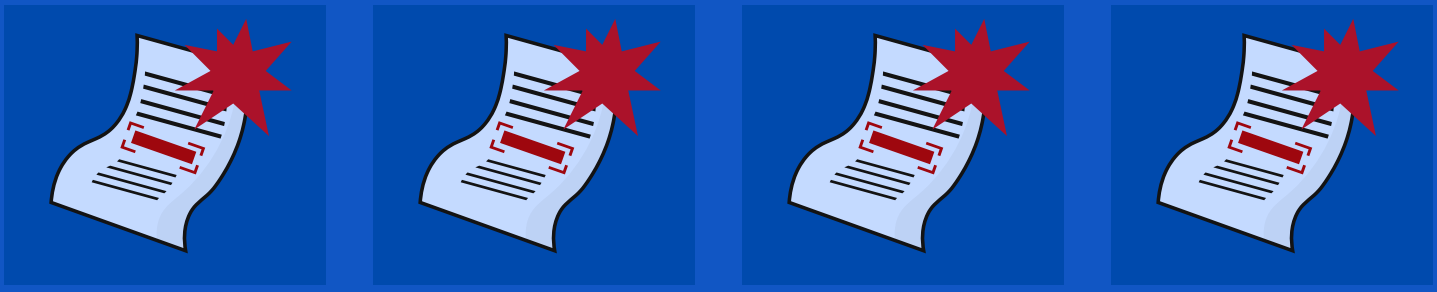
पर्दे के पीछे: तलाशी और ज़ब्ती में कौन क्या करता है

तलाशी और ज़ब्ती करने का अधिकार विभिन्न कानूनों के अनुसार अलग-अलग होता है और जो आगे विस्तार से समझाया गया है। इस भाग का उद्देश्य यह सामान्य जानकारी देना है कि तलाशी को कौन अधिकृत कर सकता है और किसे इसे करने का अधिकार है। इसे पढ़ने से आपको जाँच अधिकारियों के साथ उचित प्रश्न पूछने में मदद मिलेगी।

विभिन्न कानून और परिस्थितियों के आधार पर तलाशी और ज़ब्ती की प्रक्रिया अलग-अलग हो सकती है।

II. जाँच करने का अधिकार किसके पास है?

आयकर अधिनियम, 1961 (Income Tax Act)	केवल आयकर अधिकारी, जो सहायक आयुक्त या उससे उच्च रैंक के हो, जाँच कर सकते हैं।
धन शोधन निवारण अधिनियम, 2002 (PMLA)	निदेशक या कोई अन्य अधिकारी, जो उप निदेशक रैंक से नीचे न हो, के पास जाँच करने का अधिकार है।
सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act)	कोई भी पुलिस अधिकारी, जो निरीक्षक रैंक से नीचे न हो। इसके अतिरिक्त, केंद्रीय या राज्य सरकार का कोई अन्य अधिकारी जिसे केंद्रीय सरकार द्वारा जाँच करने के लिए अधिकृत किया गया हो, वह भी जाँच कर सकता है। नियंत्रक कंप्यूटरों के भीतर डेटा तक पहुँच प्राप्त करने के लिए तलाशी का आदेश भी दे सकता है।
दूरसंचार अधिनियम, 2023 (Telecommunications Act, 2023)	यह कानून केंद्रीय सरकार के एक अधिकृत अधिकारी को किसी भी स्थान की तलाशी लेने का अधिकार देता है, यदि उस अधिकारी को यह विश्वास हो कि कोई अनधिकृत दूरसंचार नेटवर्क या उपकरण रखा गया है या छुपाया गया है।



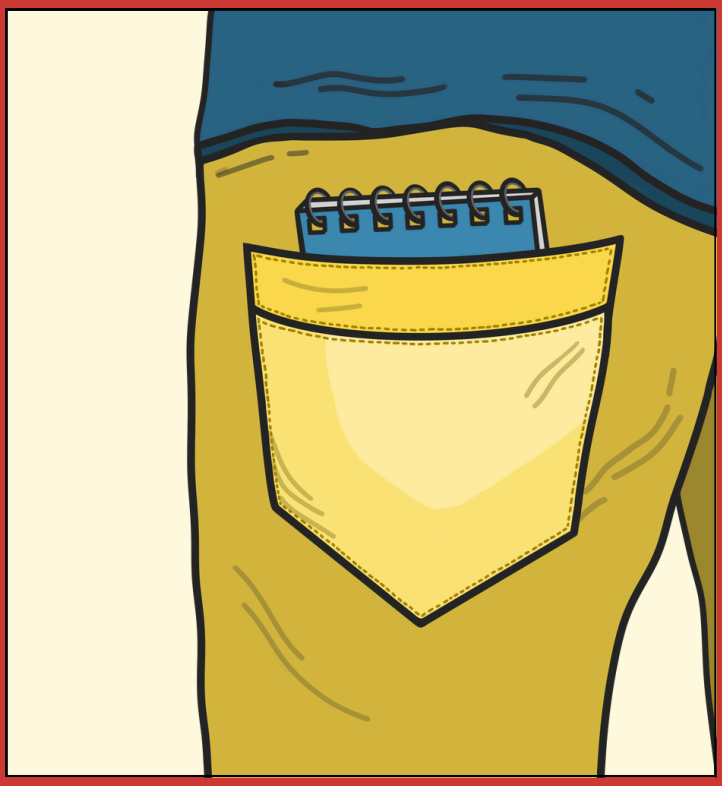
खंड 2

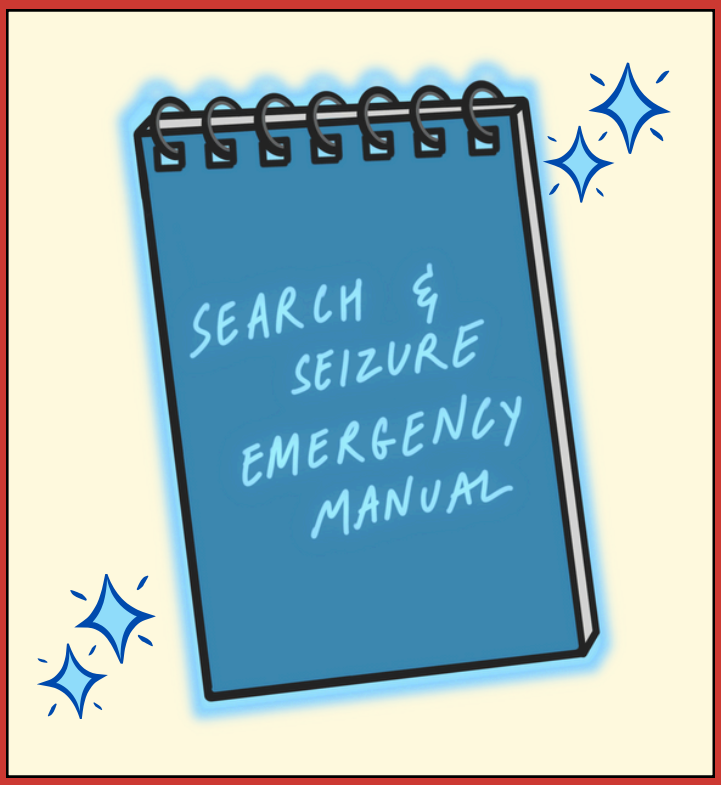
तलाशी के दौरान क्या करें?

किसी भी जाँच प्रक्रिया को अंजाम देना जटिल और चुनौतीपूर्ण हो सकता है।

इस प्रक्रिया को प्रभावी ढंग से समझने के लिए, इसमें शामिल प्रक्रियाओं और आवश्यक दस्तावेज़ीकरण को समझना ज़रूरी है।

एक जाँच अंततः एक मुकदमे का रूप ले सकती है, और ऐसे मामलों में, अदालत में आत्मरक्षा के लिए तलाशी प्रक्रियाओं और संबंधित प्रोटोकॉल की गहरी समझ महत्वपूर्ण है।





तलाशी की शुरुआत के दौरान, ये सवाल आपके काम आ सकते हैं:

1	**क्या आपके पास वारंट है?**
2	**क्या इसे इलेक्ट्रॉनिक रूप से भेजा गया है?**
3	**यदि हाँ, तो किस माध्यम से?**
4	**आप किस जाँच एजेंसी का प्रतिनिधित्व करते हैं?**
5	**आपका पद क्या है?**
6	**मेरे खिलाफ क्या आरोप हैं?**

यदि आपको लगता है कि आपके प्रश्नों का ठीक से उत्तर नहीं दिया जा रहा है, तो तुरंत एक वकील से संपर्क करें। यह सलाह दी जाती है कि जब तक आपका कानूनी प्रतिनिधि उपस्थित न हो, तब तक आप किसी भी आगे पूछे जाने वाले प्रश्न का उत्तर **न दें।**

अधिकारियों से प्रभावी ढंग से जानकारी निकालना।

- पुलिस आपके इलेक्ट्रॉनिक उपकरणों की तलाशी वारंट के साथ या बिना वारंट के ले सकती है। **हालाँकि, आपको हमेशा तलाशी और ज़ब्ती की प्रक्रिया की रिकॉर्डिंग की एक प्रति नजदीकी मजिस्ट्रेट से मांगनी चाहिए,**[11] **– जिसे पुलिस अधिकारी से ऐसी रिकॉर्डिंग प्राप्त हुई है।** [12]
- **आप अपने कब्जे में किसी अन्य व्यक्ति के इलेक्ट्रॉनिक रिकॉर्ड देने करने से भी इंकार कर सकते हैं, जब तक कि वही व्यक्ति इसके लिए सहमति न दे।**
- किसी भी जाँच में तलाशी और ज़ब्ती एक मानक प्रक्रिया है, केवल इसलिए कि आपके घर और उपकरणों की तलाशी ली जा रही है, **इसका मतलब यह नहीं है** कि आप दोषी हैं। यदि जाँच एजेंसियों के पास तलाशी लेने के लिए जरूरी दस्तावेज़ पूरे हैं, तो उन्हें अपना काम करने दें।
- अपने वकील से संपर्क करें क्योंकि भविष्य में आपको उनकी जरूरत पड़ सकती है। जाँच अधिकारी कभी-कभी आपके सवालों का जवाब नहीं दे सकते हैं। यह बेहतर होगा कि आप अपने प्रश्नों और प्रतिक्रियाओं को एक कागज पर लिख लें, ताकि इसका उपयोग आगे मुकदमे में किया जा सके।
- आप जाँच एजेंसियों को उनकी तलाशी में सहायता करने के लिए बाध्य नहीं हैं। हालाँकि, आपको प्रक्रिया में हस्तक्षेप भी नहीं करना चाहिए। इसका मतलब है, उदाहरण के लिए, उपकरण लेकर भागना या उपकरण तोड़ना।

जाँच स्थल पर तलाशी और ज़ब्ती के दौरान, विश्लेषण में एकत्रित साक्ष्यों की प्रासंगिकता और सत्यनिष्ठा सुनिश्चित करने के लिए तत्काल जाँच और मूल्यांकन शामिल होता है।

इसमें घटनास्थल पर पाए गए भौतिक वस्तुओं और डिजिटल उपकरणों की समीक्षा और दस्तावेज़ीकरण , डेटा निष्कर्षण और फोरेंसिक विश्लेषण करना शामिल है ताकि जानकारी को पुनर्प्राप्त और सत्यापित किया जा सके, और इस दौरान उपकरणों को छेड़छाड़ से बचाया जा सके। प्रमुख पैटर्न और कनेक्शन की पहचान की जाती है, और स्पष्ट ज़ब्ती श्रृंखला बनाए रखने के लिए विस्तृत नोट्स लिए जाते हैं।

1	**विश्लेषण के लिए उपयोग किए गए उपकरणों और खातों की एक सूची बनाए रखें:** अधिकारियों द्वारा बाद में एकत्रित किए गए सभी डेटा के क्रॉस-रेफरेंस को सुविधाजनक बनाने के लिए तलाशे गए उपकरणों के विश्लेषण के लिए उपयोग किए गए उपकरणों और खातों की एक सूची बनाए रखें।
2	**अपने उपकरणों पर फ़ाइलों के स्टोरेज स्थानों का खुलासा न करें:** जब अधिकारी तलाशी और ज़ब्ती करते हैं, तो अपनी गोपनीयता और प्रक्रिया की सत्यनिष्ठा की रक्षा के लिए अपने उपकरणों पर फ़ाइलों के स्टोरेज स्थानों का खुलासा न करना उचित है। फ़ाइलों के संग्रहीत होने के बारे में जानकारी प्रदान करने से अनजाने में तलाशी का दायरा कानूनी रूप से अनुमत से अधिक बढ़ सकता है, और संभावित रूप से संवेदनशील या अप्रासंगिक व्यक्तिगत जानकारी उजागर हो सकती है।
3	**विश्लेषण के लिए लिए गए सभी उपकरणों के सभी IMEI, सीरियल नंबर और विशिष्टताओं का ध्यान रखें:** यह उपकरण की पहचान को सत्यापित करने में मदद करता है, अन्य उपकरणों के साथ मिक्स-अप को रोकता है, और यह पुष्टि करके सबूत की सत्यनिष्ठा को बनाए रखता है कि सही आइटम का विश्लेषण किया जा रहा है या अदालत में प्रस्तुत किया जा रहा है।

खंड 3

इलेक्ट्रानिक्स उपकरण एवं कानून

भारत के (सर्वोच्च न्यायालय) ने *के.एस. पुट्टस्वामी* मामले में सूचनात्मक गोपनीयता सहित निजता को एक मौलिक अधिकार के रूप में मान्यता दी [13] - *वीरेंद्र खन्ना बनाम कर्नाटक राज्य में*, (कर्नाटक उच्च न्यायालय) ने इलेक्ट्रॉनिक उपकरणों की तलाशी और ज़ब्ती के संबंध में विशेष दिशानिर्देश निर्धारित किए। इस मामले में, न्यायालय ने फैसला सुनाया कि स्मार्टफोन या कंप्यूटर सिस्टम तक पहुँच प्रदान करने के लिए पासवर्ड, बायोमेट्रिक्स, पासकोड बताना किसी व्यक्ति के आत्म-अपराध के विरुद्ध मौलिक अधिकार का उल्लंघन नहीं करेगा [14]

हालाँकि, फाउंडेशन ऑफ मीडिया प्रोफेशनल्स ने सर्वोच्च न्यायालय में याचिका दायर की थी, जिसमें तर्क दिया गया था कि वर्तमान में कानून लोगों को आत्म-अपराध और निजता के विरुद्ध उनके मौलिक अधिकारों के उल्लंघन से बचाने में अपर्याप्त है - यह देखते हुए कि इलेक्ट्रॉनिक उपकरण किसी व्यक्ति के बड़ी मात्रा में व्यक्तिगत डेटा को संग्रहीत करते हैं [15]। जाँच एजेंसियों द्वारा इलेक्ट्रॉनिक उपकरणों की तलाशी और ज़ब्ती पर दिशानिर्देश विकसित करने के लिए एक समिति का गठन किया गया था [16]।

यदि आप जानना चाहते हैं कि विभिन्न कानूनों के तहत तलाशी और ज़ब्ती की प्रक्रिया कैसे संचालित की जाती है, तो कृपया परिशिष्ट देखें।

खंड 4

ज़ब्ती के बाद की प्रक्रिया:

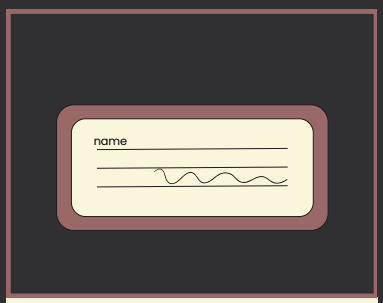
आपके उपकरण ज़ब्त होने के पश्चात क्या होता है?

ज़ब्त हुए उपकरणों के लिए जरूरी दस्तावेज़

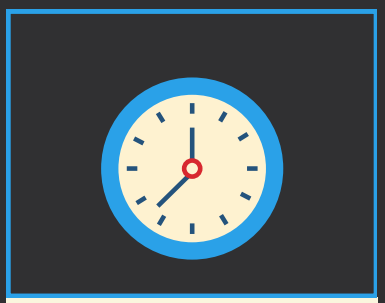
प्रमाण पत्र

(BSA की धारा 63(4)(c) के तहत प्रमाण पत्र)

किसी व्यक्ति जिसके **उपकरण तलाशे और ज़ब्त किए जा रहे हैं, और उस विशेषज्ञ द्वारा दाखिल किए जाने वाले प्रमाण पत्रों की प्रति का अनुरोध किया जा सकता है, जो प्रक्रिया का संचालन कर रहा है** [17][18] , जिसमें निम्नलिखित का विवरण होना चाहिए:



उस व्यक्ति का नाम जिसके उपकरण की तलाशी और ज़ब्ती की गई है और हस्ताक्षर।



ज़ब्ती की तारीख और समय

ज़ब्ती का स्थान

ज़ब्त किए गए उपकरणों का विवरण (निर्माता, मॉडल, सीरियल नंबर/आईएमईआई/ यूआईएन/यूआईडी/मैक)।

0000 1111
0000 2222

HASH संख्या (HASH रिपोर्ट के साथ)

विशेषज्ञ द्वारा दाखिल किया जाने वाला और सभी प्रासंगिक विवरणों के साथ विधिवत हस्ताक्षरित प्रमाण पत्र।

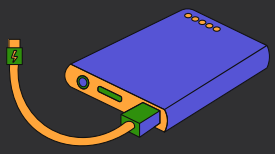
ज़ब्ती के दौरान मौजूद गवाहों के नाम

ज़ब्ती का कारण

तलाशी और ज़ब्ती की प्रक्रिया को कैमेरे या सबसे बेहतर मोबाइल फोन द्वारा रिकॉर्ड किये जाने का अनुरोध करें।

एक बार जब मजिस्ट्रेट के पास रिकॉर्डिंग आ जाए तो उसकी एक प्रति प्राप्त करने का अनुरोध करें।

सामान की सूची



ज़ब्त सामानों की विस्तृत सूची: ज़ब्त किए गए सभी **सामानों की विस्तृत सूची** [19] माँगे, जिसमें चार्जर या केस जैसे कोई भी अन्य सामान शामिल हों।

ज़ब्ती के कारण

स्पष्ट रूप से उन **विशेष कारणों** के बारे में पूछताछ करें जिनकी वजह से आपके उपकरण ज़ब्त किए गए थे और कानून के किन प्रावधानों के तहत ज़ब्ती की गई थी।

कानूनी सलाह तक पहुँच

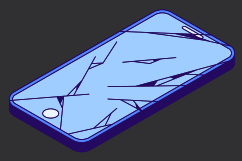
तलाशी के दौरान एक **वकील से परामर्श** करने के अपने अधिकार पर जोर दें।

वारंट/आदेशों की प्रतियां

यदि ज़ब्ती मजिस्ट्रेट के वारंट [20] या आदेश पर आधारित थी, तो ज़ब्ती को अधिकृत करने वाले **दस्तावेज़ों की प्रतियां** का अनुरोध करें। जाँचें कि क्या वारंट/आदेश में इच्छित व्यक्तियों का सही विवरण है, और क्या यह संबंधित अधिकृत अधिकारी द्वारा हस्ताक्षरित है।

ज़ब्ती की अनुमानित अवधि

उपकरणों को **कितने समय तक** रखा जाएगा और उनकी वापसी की प्रक्रिया के बारे में पूछताछ करें।



उपकरण स्थिति रिकॉर्ड

अपने उपकरण सौंपने से पहले, **उनकी स्थिति (जैसे, खरोंच या कुछ और) को तस्वीरों या वीडियो के साथ दस्तावेज़ित** करने के लिए कहें।

अतिरिक्त दस्तावेज़

परिस्थितियों के आधार पर, आप अतिरिक्त जानकारी का अनुरोध कर सकते हैं जैसे:

- प्रभारी जाँच अधिकारी का विवरण
- ज़ब्ती से संबंधित शिकायत या मामले के बारे में जानकारी जिसमें केस नंबर भी शामिल है
- अधिकारियों द्वारा पालन की गई किसी भी प्रासंगिक नीतियों या प्रक्रियाओं की प्रतियां

यदि आपका उपकरण लंबे समय तक वापस नहीं किया जाता है तो क्या करें?

- आपके उपकरण को वापस करने की प्रक्रिया इस बात पर निर्भर करेगी कि क्या इसे न्यायालय के समक्ष पेश किया गया था। मान लीजिए कि आपकी डिवाइस को जाँच या मुकदमे के दौरान न्यायालय के समक्ष पेश किया गया था। उस स्थिति में, न्यायालय जाँच या मुकदमे के समाप्त होने के बाद, BNSS, 2023 की धारा 497 और 503 के अनुसार, इसे वापस करने का आदेश दे सकता है। धारा 497 को अब विस्तृत किया गया है और इसमें एक समय-सीमा निर्दिष्ट की गई है।

- हालाँकि, यदि आपकी ज़ब्त की गई संपत्ति को न्यायालय के समक्ष पेश नहीं किया गया था और यदि मजिस्ट्रेट उचित समझते हैं, तो वे एक वापसी आदेश जारी करेंगे कि आपके उपकरण एकत्र करने के लिए तैयार हैं, जिसके लिए आपके पास दावा करने के लिए छह महीने का समय है। **[21]**

किसी भी स्थिति में, यह संभव है कि पुलिस द्वारा ज़ब्त की गई संपत्ति का दावा करने की प्रक्रिया आपके मामले की विशेष परिस्थितियों के आधार पर भिन्न हो सकती है। इन दोनों स्थितियों में, यदि आपका उपकरण एकत्र करने के लिए तैयार है और आपको ऐसा करने में समस्या आ रही है, तो याद रखें कि पुलिस द्वारा ज़ब्त की गई संपत्ति का दावा करने की प्रक्रिया आपके मामले की विशिष्ट परिस्थितियों के आधार पर भिन्न होती है। हालाँकि, यहाँ उन सभी कदमों का एक सामान्य अवलोकन दिया गया है जो आप उठा सकते हैं:

सूचना एकत्र करें: ज़ब्त किए गए विशिष्ट सामानों की एक सूची बनाएं, जिसमें सीरियल नंबर, विवरण, विशिष्टताएँ आदि जैसी कोई भी पहचान संबंधी जानकारी और संपत्ति के आपके स्वामित्व को साबित करने वाले कोई भी दस्तावेज़, जैसे खरीद रसीदें, बिल या पंजीकरण प्रमाण पत्र शामिल हों।

पुलिस स्टेशन से संपर्क करें: एक बार जब आप आवश्यक जानकारी एकत्र कर लें, तो निकटतम पुलिस स्टेशन पर जाएँ, या तो जहाँ मामला दर्ज किया गया है या जहाँ आपकी संपत्ति ज़ब्त की गई है। प्रभारी अधिकारी, या जाँच अधिकारी या संपत्ति विभाग के किसी भी कर्मचारी से बात करें। अपनी स्थिति स्पष्ट करें और अपनी संपत्ति वापस करने का अनुरोध करें। धैर्य रखें, विनम्र और सहयोगी बनें, और अपने पास मौजूद सभी प्रासंगिक दस्तावेज़ प्रस्तुत करें।

कानूनी सहायता लें: यदि पुलिस सहयोग नहीं कर रही है या प्रक्रिया जटिल लगती है, तो एक वकील से कानूनी सहायता लेने पर विचार करें।

उपकरण वापसी के बाद की चेकलिस्ट

1. सामान्य निरीक्षण

उपकरण और सेवाएँ	अधिकारियों से उन सभी उपकरणों की विस्तृत सूची प्राप्त करें जिनका उन्होंने विश्लेषण या ज़ब्त किया है, साथ ही जाँच की गई सेवाओं, जैसे ईमेल, चैट आदि की भी सूची प्राप्त करें ताकि आप अपनी ज़ब्ती-पूर्व डेटाबेस से मिलान कर सकें।
स्टार्टअप और कार्यक्षमता	डिवाइस को पावर ऑन करें और सुनिश्चित करें कि यह सामान्य रूप से बूट हो रहा है। इंटरनेट कनेक्टिविटी, ऐप उपयोग, कैमरा आदि जैसे बुनियादी कार्यों और सुविधाओं का परीक्षण करें।
उपकरण वापसी	सुनिश्चित करें कि छापे के बाद, वे सभी उपकरण जो ज़ब्त नहीं किए गए थे, आपको वापस कर दिए जाएँ।
भौतिक स्थिति	डिवाइस पर किसी भी भौतिक क्षति की जाँच करें, जिसमें सील या स्क्रू के साथ छेड़छाड़ के संकेत भी शामिल हैं। दस्तावेज़ीकरण के लिए किसी भी संदिग्ध निशान की तस्वीरें लें।
सेटिंग और कॉन्फ़िगरेशन	जाँचें कि क्या कोई सेटिंग, एक्सेस कंट्रोल या कॉन्फ़िगरेशन बदल दिया गया है, खासकर सुरक्षा, गोपनीयता या स्थान सेवाओं में।

उपकरण वापसी के बाद की चेकलिस्ट

1. सामान्य निरीक्षण

इंस्टाल्ड सॉफ्टवेयर/ ऐप्स	जाँचें कि क्या आपके फोन पर कोई नया सॉफ्टवेयर या ऑपरेटिंग सिस्टम स्थापित किया गया है और ऐप्स की सूची की तुलना उस सूची से करें जो आपको ज़ब्ती से पहले याद थी। अज्ञात संदिग्ध एप्लिकेशन स्पाइवेयर और/या मैलवेयर के संकेत हो सकते हैं।
असामान्य गतिविधि	आपके डिवाइस के साथ कोई भी अवर्णनीय या असामान्य गतिविधि, जैसे अत्यधिक बैटरी का खत्म होना, डेटा का उपयोग, निष्क्रिय कार्यक्षमता आदि, स्पाइवेयर और/या मैलवेयर के संकेत हो सकते हैं।
ऑनलाइन खाते जाँचें	अपने ऑनलाइन खातों जैसे ईमेल, स्टोरेज, सोशल मीडिया आदि की जाँच करें ताकि यह देखा जा सके कि क्या कोई अन्य डिवाइस लॉग इन हैं जिनका उपयोग आप नहीं करते हैं। यदि आपको अपरिचित डिवाइस मिलते हैं, तो उन्हें हटाने और खाते को सुरक्षित करने के लिए तत्काल कार्रवाई करें। यह आमतौर पर खाते की सुरक्षा सेटिंग्स के माध्यम से किया जा सकता है।

उपकरण वापसी के बाद की चेकलिस्ट

2. डेटा सत्यनिष्ठा

डेटा सत्यापन	सत्यापित करें कि आपका सारा डेटा अक्षुण्ण है। फ़ाइलों, फ़ोटो, दस्तावेज़ों, मेटाडेटा और किसी भी अन्य डेटा की जाँच करें ताकि यह सुनिश्चित हो सके कि कुछ भी गुम या दूषित नहीं है।
फ़ाइल टाइमस्टैम्प	अपने डिवाइस पर महत्वपूर्ण फ़ाइलों और दस्तावेज़ों के टाइमस्टैम्प की जाँच करें क्योंकि छेड़छाड़ किए गए टाइमस्टैम्प अनधिकृत पहुँच या संशोधन की ओर इशारा कर सकते हैं।
फ़ाइल हैश	ज़ब्ती से पहले और बाद में महत्वपूर्ण फ़ाइलों के क्रिप्टोग्राफ़िक हैश उत्पन्न करें और उनकी तुलना करें। विसंगतियां फ़ाइल में बदलाव या प्रतिस्थापन का संकेत दे सकती हैं।
फोरेंसिक टूल स्कैन	छिपी हुई फ़ाइलों, स्पाइवेयर या रूटकिट के निशान के लिए अपने डिवाइस को स्कैन करने के लिए एंटी-मैलवेयर और फोरेंसिक सॉफ़्टवेयर का उपयोग करने पर विचार करें। ये उपकरण जटिल हो सकते हैं, इसलिए डेटा रिकवरी या साइबर सुरक्षा विशेषज्ञ से परामर्श करना सहायक हो सकता है।

उपकरण वापसी के बाद की चेकलिस्ट

3. अतिरिक्त सतर्कता

बैकअप लॉग	यदि आपके डिवाइस में यह सेवा है, तो जाँचें कि क्या कोई भी बैकअप या सिस्टम लॉग ज़ब्ती अवधि के दौरान कोई संदेहास्पद या अनधिकृत गतिविधि दिखाते हैं।
क्लाउड स्टोरेज	अनधिकृत पहुँच या परिवर्तनों के लिए डिवाइस से जुड़े अपने क्लाउड स्टोरेज खातों की समीक्षा करें।
दस्तावेज़ीकरण	अपनी तलाशी का विस्तृत रिकॉर्ड रखें, जिसमें टाइमस्टैम्प, स्क्रीनशॉट और किसी भी संदिग्ध गतिविधि पर नोट्स शामिल हों। यदि आपको कानूनी कार्रवाई करने की आवश्यकता है तो यह दस्तावेज़ीकरण महत्वपूर्ण हो सकता है।
पासवर्ड प्रबंधन	अपने डिवाइस और किसी भी ऑनलाइन खाते से जुड़े अपने सभी मौजूदा पासवर्ड बदलें क्योंकि अधिकारियों द्वारा आपके पासवर्ड की एक प्रति रखी जा सकती है।

खंड 5

तैयारी:

अपने उपकरणों की सुरक्षा

आज की डिजिटल दुनिया में, हमारे उपकरण और उनमें मौजूद डेटा भारी मात्रा में जानकारी रखते हैं।

यह सुनिश्चित करने के लिए उपकरणों की सुरक्षा करना महत्वपूर्ण है ताकि हमारा डेटा सुरक्षित रहे।

इन खतरों के लिए तैयार रहना सरल और महत्वपूर्ण है। कल्पना कीजिए कि यदि आपका फोन हैक हो जाए और आपके सभी संदेश उजागर हो जाएँ तो कितनी अराजकता होगी! मजबूत पासवर्ड का उपयोग करके, ऑनलाइन साझा की जाने वाली चीजों के बारे में सतर्क रहकर, और सॉफ्टवेयर को अप-टू-डेट रखकर, आप अपने सूटकेस के लिए एक मजबूत डिजिटल ताला बनाते हैं। याद रखें, थोड़ी सी सावधानी आपके ऑनलाइन जीवन को सुरक्षित रखने में बहुत मददगार साबित होती है। आपके डेटा को सुरक्षित रखने के कुछ अच्छे तरीके नीचे दिए गए हैं:

अपनी ऑनलाइन गतिविधि को सुरक्षित रखें | कैसे, यहाँ देखें:

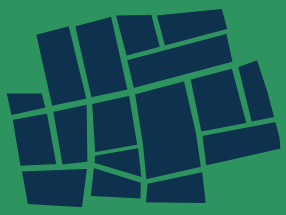
खुद को छिपाइए

आप वीपीएन और टॉर के उपयोग के माध्यम से अपनी ऑनलाइन गतिविधि को छिपा सकते हैं। यह उस तरह है जैसे एक गुप्त एजेंट एक गुप्त मिशन के दौरान एक छलावरण का उपयोग करता है।

वीपीएन

अपनी इंटरनेट गतिविधि के लिए एक सुरक्षित सुरंग की कल्पना करें। यह आपके वास्तविक स्थान को छुपाता है और आपके डेटा को एन्क्रिप्ट करता है, जिससे यह एक गुप्त कोड की तरह बन जाता है जिसे केवल आप और वीपीएन ही तोड़ सकते हैं। एक विश्वसनीय वीपीएन सेवा चुनें, जो आपकी गतिविधि को लॉग न करे।

टॉर



गुप्त रास्तों के एक भूलभुलैया की कल्पना करें। टॉर आपके इंटरनेट ट्रैफिक को एन्क्रिप्टेड रिले की परतों के माध्यम से बाउंस करता है, जिससे इसे ट्रैक करना लगभग असंभव हो जाता है। अतिरिक्त गोपनीयता के लिए टॉर ब्राउज़र डाउनलोड करें।

समझदारी से चुनाव करें

सभी सर्च इंजन समान नहीं बनाए गए हैं। कुछ, जैसे डकडकगो, गोपनीयता को प्राथमिकता देते हैं और आपकी सर्च को ट्रैक नहीं करते हैं। भले ही आपका ब्राउज़र इतिहास लॉग करता हो, पोस्ट अनुरोधों वाले सर्च इंजन का उपयोग करने से आपकी क्वेरी छिपी रहती हैं।

इन्कॉग्नी टो मोड़ में जाएँ

अपने ब्राउज़र में "इन्कॉग्नीटो मोड" को एक गुप्त एजेंट के मुखौटे की तरह समझें। यह आपके ब्राउज़िंग हिस्ट्री, कुकीज़ और फ़ॉर्म डेटा को सेव करने से रोकता है, जिससे किसी के लिए भी आपके ऑनलाइन कारनामों पर जासूसी करना मुश्किल हो जाता है।

सतर्क रहें

याद रखें, इन उपकरणों के साथ भी पूर्ण गोपनीयता एक मिथक है। जिन वेबसाइटों पर आप जाते हैं, उनके बारे में सावधान रहें, हमेशा सुरक्षित कनेक्शनों को प्राथमिकता दें (लॉक आइकन देखें!), और जब तक बिल्कुल आवश्यक न हो, ऑनलाइन व्यक्तिगत विवरण साझा करने से बचें।

गति बनाम गोपनीयता

एन्क्रिप्शन और रीरूटिंग के कारण वीपीएन और टॉर आपकी इंटरनेट गति को थोड़ा धीमा कर सकते हैं। यह एक समझौता है: अधिक गोपनीयता के लिए थोड़ी कम गति। आपके लिए जो सबसे बेहतर काम करता है, उसका चुनाव करें।

बोनस टिप: हमेशा किसी भी उपकरण की गोपनीयता नीतियों और सेवा की शर्तों की जाँच करें जिसका आप उपयोग करते हैं ताकि यह समझ सकें कि वे आपके डेटा को कैसे संभालते हैं। इन सरल चरणों का पालन करके, आप अपनी ऑनलाइन गोपनीयता पर नियंत्रण रख सकते हैं और अपने डिजिटल जीवन को अपने नियंत्रण में रख सकते हैं। याद रखें, जेम्स बॉन्ड को भी कभी-कभी अच्छे छलावरण की आवश्यकता होती है!

कार्य उपकरण बनाम व्यक्तिगत उपकरण

कल्पना कीजिए कि आपके पास दो सूटकेस हैं: एक आपके कार्यालय जीवन के लिए और दूसरा आपके व्यक्तिगत रोमांच के लिए। अपने कार्य लैपटॉप और फोन को अलग रखना उन अलग-अलग सूटकेसों की तरह है - यह आपको व्यवस्थित रहने और आपकी पेशेवर और व्यक्तिगत दोनों दुनियाओं की सुरक्षा करने में मदद करता है।

अपने व्यक्तिगत और व्यावसायिक जीवन के लिए अलग-अलग उपकरण रखने का प्रयास करें।

A. Data Detective: अलग-अलग उपकरणों का उपयोग करके, आप व्यक्तिगत और व्यावसायिक डेटा के आपस में मिलने के जोखिम को कम करते हैं, जिससे सुरक्षा बढ़ती है और दोनों के लिए गोपनीयता सुनिश्चित होती है। काम और व्यक्तिगत चीजों के लिए अलग-अलग उपकरणों का उपयोग करना मूल रूप से एक डेटा जासूस होने जैसा है! आप अपनी कार्य फ़ाइलों को अपनी व्यक्तिगत तस्वीरों में और इसके विपरीत चुपके से आने से रोकते हैं। यह सब कुछ सुरक्षित और निजी रखता है, जैसे अलग-अलग चाबियों वाले दो बंद सूटकेस।

B. अधिकार नियंत्रण निंजा: स्पष्ट विभाजन संवेदनशील कार्य-संबंधी जानकारी तक पहुँच को नियंत्रित करने में मदद करता है, जिससे आकस्मिक प्रकटीकरण या डेटा उल्लंघनों का जोखिम कम होता है। अपने कार्य और व्यक्तिगत उपकरणों को अलग रखना आपके कार्यालय के सूटकेस के लिए एक गुप्त कोड रखने जैसा है। केवल अधिकृत लोग (जैसे आप और आपके बॉस) ही आपके काम तक पहुँच सकते हैं, जबकि आपका व्यक्तिगत सूटकेस केवल आपके निजी उपयोग के लिए रहता है। यह आकस्मिक लीक या चोरी-छिपे ताका-झाँकी को रोकने में मदद करता है, जिससे आपका कार्य जीवन सुरक्षित और व्यवस्थित रहता है।

C. जिम्मेदारी का विजेता: उपकरणों को अलग करने से कार्य-संबंधी गतिविधियों और डेटा के लिए स्पष्ट स्वामित्व और जवाबदेही सुनिश्चित होती है। अलग-अलग उपकरण होने से यह स्पष्ट हो जाता है कि किसके लिए क्या जिम्मेदारी है। यह आपके सूटकेस को लेबल करने जैसा है - हर कोई जानता है कि कार्यालय में कार्य सूटकेस आपका है, और व्यक्तिगत सूटकेस आपका है जिसे आप अपनी पसंद के अनुसार पैक कर सकते हैं। इससे आपके और आपके सहकर्मियों दोनों के लिए कार्यों को ट्रैक करना और चीजों को जवाबदेह रखना आसान हो जाता है।

याद रखें, अपने कार्य और व्यक्तिगत उपकरणों को अलग रखना सिर्फ दो गैजेट रखने के बारे में नहीं है - यह आपकी गोपनीयता की रक्षा करने, व्यवस्थित रहने और अपने जीवन को आसान बनाने के बारे में है। तो आगे बढ़ें, एक डेटा जासूस बनें, एक पहुँच नियंत्रण निंजा बनें, और एक जिम्मेदारी चैंपियन बनें! और अपने सूटकेस को लेबल करना न भूलें!

बोनस टिप: अलग-अलग उपकरणों के साथ भी, आप ऑनलाइन क्या साझा करते हैं और आप किसे एक्सेस देते हैं, इसके बारे में हमेशा सावधान रहें। कोई भी सिस्टम पूर्णतया सुरक्षित नहीं है, इसलिए सतर्क रहें और अपने डिजिटल दुनिया का आनंद लें!

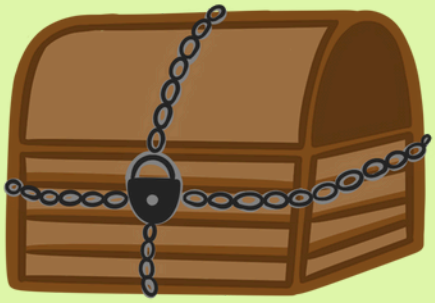
अपने डेटा को खजाने की तरह सुरक्षित रखें: एन्क्रिप्शन परतों के लिए एक गाइड

।कल्पना कीजिए कि आपका डेटा कीमती रहस्यों से भरा एक खजाना है। उन रहस्यों को सुरक्षित रखने के लिए, आपको कई तालों की आवश्यकता होगी, है ना?

यहीं पर एन्क्रिप्शन परतें काम आती हैं!

पूरे संदूक का ताला (FDE):

- अपनी पूरी हार्ड ड्राइव को एन्क्रिप्ट करें, जैसे पूरे खजाने के संदूक पर एक बड़ा, मजबूत ताला लगाना।
- बिटलॉकर (विंडोज), फाइलवॉल्ट (मैकओएस), या वेराक्रिप्ट (थर्ड-पार्टी) जैसे उपकरणों का उपयोग करें।

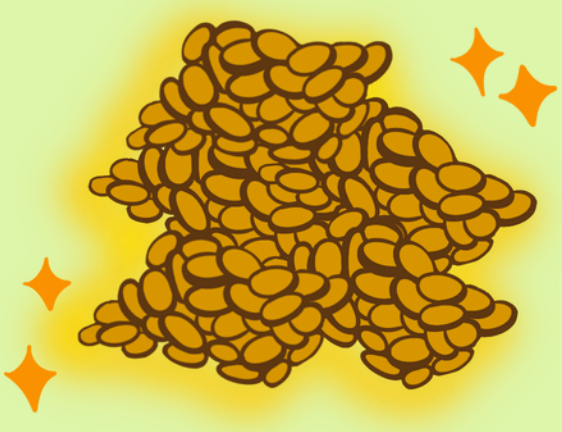


गुप्त डिब्बे के ताले (ओएस-स्तर):

- मैकओएस पर एन्क्रिप्टेड डिस्क इमेज (जैसे संदूक के भीतर गुप्त बक्से) बनाएं।
- कुछ ओएस पर एन्क्रिप्टेड फ़ाइल सिस्टम (जैसे छिपे हुए डिब्बे) का उपयोग करें।

व्यक्तिगत रत्न पाउच (ऐप-स्तर)

- अंतर्निहित एन्क्रिप्शन वाले ऐप्स के साथ विशिष्ट रत्नों (पासवर्ड, नोट्स, संदेश) की सुरक्षा करें।
- पासवर्ड मैनेजर, सुरक्षित नोट लेने वाले ऐप्स और एंड-टू-एंड एन्क्रिप्शन वाले मैसेजिंग ऐप्स (जैसे, सिग्नल, व्हाट्सएप) के बारे में सोचें।



ध्यान देने योग्य बातें:

- प्रत्येक ताले (एन्क्रिप्शन परत) के लिए मजबूत, अद्वितीय पासवर्ड या चाभियों का उपयोग करें।
- तालों को चमकदार और सुरक्षित रखने के लिए अपने सॉफ़्टवेयर को नियमित रूप से अपडेट करें।
- अपने एन्क्रिप्टेड डेटा (खजाने के नक्शे!) का बैकअप लें यदि आपको इसे भविष्य में फिर से ढूंढने की आवश्यकता हो।

इन एन्क्रिप्शन तालों को कई परत में करके, आप अपने डेटा के लिए एक किला बनाएंगे, जिससे किसी के लिए भी आपके डिजिटल खजाने को चुराना बहुत मुश्किल हो जाएगा!

गोपनीयता और साइबर सुरक्षा सुनिश्चित करना: ऑनलाइन और ऑफलाइन

- गायब होने वाली मैसेजिंग सेवाओं या उन एप्लिकेशन का उपयोग करें जो भेजे गए संदेशों को देखने के बाद या पूर्वनिर्धारित अवधि के बाद स्वचालित रूप से हटा देते हैं। सिग्नल, टेलीग्राम और व्हाट्सएप आदि जैसे ऐप गायब होने वाले संदेशों की सुविधाएँ प्रदान करते हैं, यह सुनिश्चित करते हुए कि संचार अस्थायी रहता है और पढ़े जाने या निर्दिष्ट समय सीमा के बाद चैट या इतिहास में बना नहीं रहता है।

- फ़िंगरप्रिंट या चेहरे की पहचान के बजाय प्रमाणीकरण उद्देश्यों के लिए पासवर्ड या पिन का उपयोग करें, क्योंकि इन तरीकों के लिए सचेत मानसिक ध्यान या स्पष्ट सहमति की आवश्यकता नहीं होती है। पासवर्ड या पिन का उपयोग यह सुनिश्चित करता है कि संवेदनशील जानकारी या उपकरणों तक पहुँच पूरी तरह से उपयोगकर्ता द्वारा दर्ज किए गए ज्ञान पर निर्भर करती है, प्रमाणीकरण के लिए जानबूझकर कार्यवाई और सचेत सहमति की आवश्यकता के द्वारा नियंत्रण और सुरक्षा बढ़ जाती है।

- अपने पासवर्ड के एक हिस्से को संग्रहीत करने के लिए पासवर्ड मैनेजर का उपयोग करना और शेष को याद रखना सुरक्षा बढ़ाने के लिए एक अच्छी रणनीति है। पासवर्ड के एक हिस्से को एक सुरक्षित प्रबंधक में संग्रहीत करके और शेष को स्मृति में रखकर, आप एक 2FA बनाते हैं जो आपके खातों की समग्र सुरक्षा को मजबूत करता है।

- उदाहरण के लिए, "fdsjrie" जैसे एक भाग को सुरक्षित रूप से संग्रहीत करने के लिए एक पासवर्ड मैनेजर का उपयोग करना और दूसरे भाग, जैसे "12345 ," को याद रखना आपको पूर्ण पासवर्ड "fdsjrie12345" बनाने में सक्षम बनाता है। यह विधि पासवर्ड मैनेजर के एन्क्रिप्शन के लाभों और एक अद्वितीय भाग को याद करने की आपकी क्षमता को मिलाकर सुरक्षा और सुविधा को संतुलित करने में मदद करती है, जिससे अनधिकृत उपयोगकर्ताओं के लिए आपके खातों तक पहुँच प्राप्त करना अधिक चुनौतीपूर्ण हो जाता है।

- 2FA (टू-फैक्टर ऑथेंटिकेशन) लागू करने से खाते की सुरक्षा काफी बढ़ जाती है। एसएमएस या ईमेल आधारित 2FA की तुलना में TOTP (टाइम-बेस्ड वन-टाइम पासवर्ड) आधारित 2FA का चयन करना बेहतर है क्योंकि इसकी सुरक्षा का स्तर अधिक होता है। TOTP एक अद्वितीय कोड उत्पन्न करता है जो नियमित अंतराल पर बदलता रहता है, आमतौर पर हर 30 सेकंड में, अनधिकृत पहुँच के खिलाफ सुरक्षा की एक अतिरिक्त परत प्रदान करता है।

- Google ऑथेंटिकेटर, ऑथी या माइक्रोसॉफ्ट ऑथेंटिकेटर जैसे ऑथेंटिकेटर ऐप्स का उपयोग करना, जो TOTP कोड उत्पन्न करते हैं, एक अधिक सुरक्षित विकल्प है। ये ऐप्स समय-संवेदनशील कोड बनाते हैं जो आपके खातों से जुड़े होते हैं और एसएमएस या ईमेल जैसे संचार चैनलों पर निर्भर नहीं होते हैं, जिससे इंटरसेप्शन या सिम स्वैपिंग हमलों का खतरा कम हो जाता है जो एसएमएस-आधारित 2FA से समझौता कर सकते हैं।

- TOTP-आधारित 2FA का लाभ उठाकर, आप सुरक्षा की एक अतिरिक्त परत जोड़ते हैं जो आपके खातों तक अनधिकृत पहुँच की संभावना को काफी कम कर देता है और विभिन्न साइबर खतरों के खिलाफ अधिक मजबूत सुरक्षा प्रदान करता है।

- फ़ाइलों को हटाना वास्तव में आपकी गोपनीयता की रक्षा करने के लिए पर्याप्त नहीं है! केवल "Delete" पर क्लिक करने से वे हमेशा के लिए गायब नहीं हो जाती हैं। वे अभी भी आपके डिवाइस पर छिपी हुई हैं, विशेष उपकरणों से पाए जाने की प्रतीक्षा कर रही हैं। वास्तव में चीजों को निजी रखने के लिए, आपको उन फ़ाइलों को श्रेड करने की आवश्यकता है। इसे कागजी दस्तावेज़ों को श्रेड करने की तरह समझें - उन्हें वापस एक साथ रखना लगभग असंभव है! श्रेडिंग सॉफ़्टवेयर आपकी फ़ाइलों को बेतरतीब अक्षरों और संख्याओं से ओवरराइट करता है, जिससे वे अस्त-व्यस्त और अपठनीय हो जाती हैं। यह श्रेड किए गए कागज को फेंकने और उसे जमीन में गहराई से दफनाने जैसा है। कोई भी उसे खोदकर आपके रहस्य नहीं पढ़ सकता है! इसलिए, अगली बार जब आप कुछ संवेदनशील हटाना चाहें, तो "Delete" बटन छोड़ दें और कुछ श्रेडिंग सॉफ़्टवेयर इस्तेमाल करें। यह आपके डिजिटल जीवन को निजी और सुरक्षित रखने का सबसे अच्छा तरीका है।

- टॉर के माध्यम से वेबसाइटों तक पहुँचने से बढ़ी हुई गोपनीयता और सुरक्षा सुनिश्चित होती है। उदाहरण के लिए, अतिरिक्त अज्ञात होने के लिए आप टॉर का उपयोग करके द गार्जियन जैसी समाचार साइटों या ट्विटर जैसे सोशल मीडिया प्लेटफॉर्म पर जा सकते हैं।

चीजें छिपाना: ऑनलाइन और ऑफलाइन

ऑनलाइन:

- **Crypt.ee**: अज्ञात साइन अप, एंड-टू-एंड एन्क्रिप्शन और अतिरिक्त गोपनीयता के लिए छिपे हुए फ़ोल्डर बनाने की अनुमति देता है।
- **Cryptomator**: व्यक्तिगत सर्वर पर एन्क्रिप्टेड फ़ाइलों को संग्रहीत करता है, जिससे ऐप अनइंस्टॉल करने के बाद फ़ाइल स्थानों का पता लगाना मुश्किल हो जाता है।

ऑफलाइन:

- **Veracrypt**: ड्राइव या स्टोरेज डिवाइस पर डेटा सुरक्षित करने के लिए छिपे हुए विभाजन बनाएँ।
- **Secret Compartments**: फर्नीचर या वस्तुओं के भीतर छिपे हुए डिब्बों में कीमती सामान छुपाएँ।
- **Cipher Systems**: लिखित जानकारी या सामान को एन्क्रिप्ट और सुरक्षित करने के लिए व्यक्तिगत कोड या सायफर विकसित करें।

ये तरीके दोनों, डिजिटल और भौतिक स्थानों में, अतिरिक्त गोपनीयता और सुरक्षा प्रदान करते हैं और संवेदनशील जानकारी की सुरक्षा के अलग-अलग तरीके प्रदान करते हैं।

कभी-कभार इस्तेमाल होने वाली फ़ाइलों को एक सुरक्षित सुरक्षित स्थान (एन्क्रिप्टेड ड्राइव या क्लाउड) में स्टोर करें और नियमित रूप से अपने डिजिटल डेस्क को साफ करें। केवल वही सूचना रखें जिसकी आपको अभी आवश्यकता है। प्रतियाँ बनाने के बजाय पुराने संस्करणों को संग्रहीत करें, जिससे आपका डिजिटल जीवन व्यवस्थित और सुरक्षित रहे।

अपनी डिजिटल पदचिन्ह छोड़े बिना किसी साइट से जुड़ना चाहते हैं? ऐसे डिजिटल उत्पाद चुनें जो:

- कम से कम जानकारी माँगें: सिर्फ एक उपयोगकर्ता नाम और शायद एक ईमेल, जैसे चुपके से हैंडशेक।
- आपको अदृश्य रहने दें: कोई नाम नहीं? कोई चिंता नहीं! कुछ साइटें आपको यह बताए बिना साइन अप करने देती हैं कि आप कौन हैं।
- नकली ईमेल प्रदान करें: जुड़ने के लिए एक "यूज एण्ड थ्रो योग्य" ईमेल का उपयोग करें, जिससे आपका असली ईमेल निजी रहे।

शब्दावली:

ऑडियो-वीडियो इलेक्ट्रॉनिक साधन: इसका अर्थ है वीडियो कॉन्फ्रेंसिंग, पहचान प्रक्रियाओं की रिकॉर्डिंग, तलाशी और ज़ब्ती, सबूत इकट्ठा करना, इलेक्ट्रॉनिक संचार संचारित करना और राज्य सरकार के नियमों द्वारा निर्दिष्ट अन्य उपयोगों के लिए कोई भी संचार उपकरण।

गिरफ्तारी: जब किसी व्यक्ति को कानूनी हिरासत में लिया जाता है और उसे हिरासत में रखा जाता है/सीमित किया जाता है, भले ही कोई आरोप या अभिकथन मौजूद हो या न हो कि उन्होंने कोई अपराध किया है, तो उन्हें गिरफ्तार कहा जाता है। किसी व्यक्ति को बिना किसी आरोप के दायर किए या बिना वारंट के भी गिरफ्तार किया जा सकता है (संज्ञेय अपराध देखें)।

जमानती अपराध: ऐसे अपराध जो प्रकृति में बहुत गंभीर या जघन्य नहीं हैं, जिसके लिए एक आरोपी/गिरफ्तार व्यक्ति को जमानत मांगने का अधिकार है, जमानती अपराध हैं।[22] एक जाँच अधिकारी को जमानती अपराधों के लिए जमानत बांड जमा करने की शर्त पर आमतौर पर जमानत देनी आवश्यक है। हालाँकि, जमानत देने का मतलब यह नहीं है कि आरोपी मुक्त है क्योंकि उसे अभी भी न्यायिक मुकदमे से गुजरना होगा।

आरोप: आरोप एक औपचारिक आरोप है कि किसी व्यक्ति ने कोई अपराध किया है, जो या तो एक अभियोजक या एक पुलिस/जाँच कार्यालय द्वारा लगाया गया है।[23] इसके लिए एक व्यक्ति को उनके खिलाफ लगाए गए आरोप/आरोपों के आधारों के बारे में सूचित करने की आवश्यकता होती है।

संज्ञेय अपराध: ऐसे अपराध जिनके लिए एक पुलिस अधिकारी बिना वारंट या मजिस्ट्रेट से पूर्व अनुमति के गिरफ्तार कर सकता है, संज्ञेय अपराध हैं। [24] यह तब होता है जब एफआईआर (प्रथम सूचना रिपोर्ट) दर्ज की जाती है या नहीं और आमतौर पर प्रकृति में अधिक गंभीर या जघन्य अपराधों के लिए लागू होता है।

कंप्यूटर: इसका अर्थ है कोई भी इलेक्ट्रॉनिक, चुंबकीय, ऑप्टिकल या अन्य उच्च गति वाला डेटा प्रोसेसिंग उपकरण या प्रणाली जो इलेक्ट्रॉनिक, चुंबकीय या ऑप्टिकल आवेगों के हेरफेर द्वारा तार्किक, अंकगणितीय और मेमोरी फ़ंक्शन करती है, और इसमें सभी इनपुट, आउटपुट, प्रोसेसिंग, स्टोरेज, कंप्यूटर सॉफ़्टवेयर या संचार सुविधाएं शामिल हैं जो कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क में कंप्यूटर से जुड़ी या संबंधित हैं।

संचार उपकरण: यह एक सेल फोन, व्यक्तिगत डिजिटल सहायता के लिए एक उपकरण या दोनों का संयोजन या कोई अन्य उपकरण हो सकता है जिसका उपयोग किसी भी पाठ, वीडियो, ऑडियो या छवि को संवाद करने, भेजने या प्रसारित करने के लिए किया जाता है।

कुकीज़: सूचना/डेटा की छोटी फाइलें जो वेब ब्राउज़र में आपकी गतिविधि को ट्रैक और रिकॉर्ड करती हैं, कुकीज़ कहलाती हैं। इनका उपयोग विज्ञापन और विश्लेषण सेवाओं द्वारा उपयोगकर्ता गतिविधि रिकॉर्ड करने के लिए किया जा सकता है। कुकीज़ में उपयोगकर्ताओं के बारे में व्यक्तिगत जानकारी हो सकती है, जैसे उनका उपयोगकर्ता नाम और पासवर्ड, अनुकूलित प्राथमिकताएं, वेब गतिविधि आदि, और यदि वे सुरक्षित नहीं हैं, तो वे उपयोगकर्ताओं के लिए संभावित सुरक्षा और गोपनीयता जोखिम हो सकते हैं।

शब्दावली:

इलेक्ट्रॉनिक संचार: यह इलेक्ट्रॉनिक रूप से साझा की गई किसी भी लिखित, मौखिक, चित्रमय या वीडियो जानकारी को संदर्भित करता है, चाहे लोगों या उपकरणों के बीच, फोन, कंप्यूटर, ऑडियो-वीडियो प्लेयर, कैमरे या अन्य इलेक्ट्रॉनिक उपकरणों का उपयोग करके, या केंद्र सरकार द्वारा निर्दिष्ट किसी अन्य इलेक्ट्रॉनिक रूप में।

एन्क्रिप्शन: वह प्रक्रिया जो व्यक्तिगत या संवेदनशील डेटा को एक गुप्त/कोड रूप में संग्रहीत करती है जिसे केवल डिक्रिप्शन कुंजी तक पहुँच रखने वाले व्यक्ति द्वारा ही डिक्रिप्ट/डिकोड किया जा सकता है, एन्क्रिप्शन कहलाती है। यह व्यक्तिगत और संवेदनशील जानकारी को संसाधित करने, संग्रहीत करने और स्थानांतरित करने को अधिक सुरक्षित और संरक्षित बनाता है क्योंकि यह किसी भी अनधिकृत व्यक्ति को डेटा तक पहुँचने या समझने से रोकता है।

सबूत: सबूत कोई भी बयान है, जो मौखिक या दस्तावेज़ी रूप में (लिखित या इलेक्ट्रॉनिक और इसमें डिजिटल उपकरण भी शामिल हैं) हो सकता है, जो किसी जाँच या अन्वेषण से संबंधित हो सकता है, ऐसे दस्तावेज़ों को दस्तावेज़ी सबूत कहा जाता है। सबूत प्रमाण से अलग है क्योंकि यह आवश्यक रूप से निर्णायक नहीं है और न्यायालय के विवेक के अधीन है।

जाँच अधिकारी (IO): एक पुलिस अधिकारी जिसे किसी अपराध की जाँच करने के लिए सौंपा गया है।

चल संपत्ति: जबकि BNS केवल चल संपत्ति को परिभाषित करता है, जिसका अर्थ है, खिड़की, दरवाजा, पेड़ आदि जैसी हर विवरण की संपत्ति, इसमें वे चीजें शामिल नहीं हैं जो पृथ्वी से जुड़ी हैं या स्थायी रूप से किसी भी चीज से जुड़ी हैं जो पृथ्वी से जुड़ी है। चल संपत्ति में सभी इलेक्ट्रॉनिक्स और डिजिटल उपकरण भी शामिल होंगे जो पृथ्वी से जुड़े नहीं हैं। [25]

गैर-जमानती अपराध: ऐसे अपराध जो प्रकृति में अधिक गंभीर या जघन्य हैं, जिसके लिए एक आरोपी/गिरफ्तार व्यक्ति को जमानत मांगने का अधिकार नहीं है, जमानती अपराध कहलाते हैं। इसके बावजूद कि उनके पास अधिकार नहीं है, न्यायालय अभी भी आरोपी के भागने, कानूनी कार्यवाही में सहयोग न करने आदि के जोखिम के आधार पर अपने विवेक पर उन्हें जमानत दे सकता है।

गैर-संज्ञेय अपराध: ऐसे अपराध जिनके लिए एक पुलिस अधिकारी बिना वारंट या मजिस्ट्रेट से पूर्व अनुमति के गिरफ्तार नहीं कर सकता है, गैर-संज्ञेय अपराध कहलाते हैं। यह एफआईआर (प्रथम सूचना रिपोर्ट) दर्ज होने और वारंट प्राप्त होने के बाद होता है और आमतौर पर प्रकृति में कम गंभीर या जघन्य अपराधों के लिए लागू होता है।

स्थान: BNSS के तहत, एक स्थान एक घर, भवन, तंबू, वाहन और पोत हो सकता है। [27]

सार्वजनिक स्थान: इसका अर्थ है सार्वजनिक वाहन, होटल, दुकानें या कोई अन्य स्थान जो जनता द्वारा उपयोग या पहुँच के लिए हो। [28]

शब्दावली:

ज़ब्ती पत्र: यदि किसी आरोपी व्यक्ति से किसी जाँच अधिकारी द्वारा जाँच के प्रयोजनों के लिए कोई संपत्ति (मूल्यवान या अमूल्य) ज़ब्त की जाती है, तो उसे ज़ब्ती ज्ञापन में पंजीकृत और दर्ज किया जाता है। इसमें संपत्ति के विवरण/विशेषताओं/जानकारी, स्टोरेज का स्थान, उस मामले का विवरण जिससे ज़ब्ती जुड़ी हुई है, आदि का सभी विवरण होता है।

वारंट: वारंट एक न्यायाधीश द्वारा हस्ताक्षरित एक दस्तावेज़ है जो पुलिस को या तो आपको गिरफ्तार करने या आपकी संपत्ति की तलाशी लेने और उस संपत्ति से कुछ सामान लेने की अनुमति देता है। आपको वारंट देखने का अधिकार है और आपको यह जाँचना चाहिए कि यह वैध है या नहीं।

परिशिष्ट:

तलाशी और ज़ब्ती पर कुछ नोट्स:

1. पहले, अदालतों ने फैसला सुनाया था कि अवैध और अनुचित साधनों से प्राप्त साक्ष्य स्वीकार्य हो सकते हैं। हालाँकि, ऐसे साक्ष्यों को प्रकृति में वास्तविक और छेड़छाड़ रहित साबित करना होगा। स्वीकार्यता का निर्धारण केवल अदालतों द्वारा किया जा सकता है - प्रत्येक मामले के तथ्यों और परिस्थितियों के आधार पर। *[उमेश कुमार बनाम आंध्र प्रदेश राज्य, (2013) 10 एससीसी 169]*

2. हालाँकि, केरल उच्च न्यायालय ने फैसला सुनाया था कि एक पुलिस अधिकारी सीआरपीसी (अब BNSS) के भीतर स्थापित प्रक्रिया का पालन किए बिना एक पत्रकार का मोबाइल फोन ज़ब्त नहीं कर सकता है। यदि ऐसा उपकरण किसी अपराध की जाँच के लिए आवश्यक है, तो ऐसे पुलिस अधिकारियों को उपकरण की उचित तलाशी और ज़ब्ती के लिए सीआरपीसी (अब BNSS) का पालन करना होगा। **[29]**

3. दिल्ली उच्च न्यायालय ने भी फैसला सुनाया है कि भारत के संविधान के अनुच्छेद 20(3) में आत्म-अभिशंसन से सुरक्षा को देखते हुए किसी व्यक्ति को पासवर्ड (या कोई अन्य विवरण) प्रदान करने के लिए मजबूर नहीं किया जा सकता है। **[30]**

4. इसी तरह, दिल्ली के राउज एवेन्यू जिला न्यायालय की एक विशेष सीबीआई अदालत ने फैसला सुनाया कि आरोपी को ऐसी जानकारी देने के लिए मजबूर नहीं किया जा सकता है और इस संबंध में वह भारत के संविधान के अनुच्छेद 20(3) के साथ-साथ BNSS की धारा 180(2) द्वारा संरक्षित है। **[31]**

5. तलाशी और जब्ती की प्रक्रियाओं को समझना न केवल आपको ऐसी तनावपूर्ण स्थितियों में घबराने से बचा सकता है, बल्कि अधिकारियों के साथ बेहतर सहयोग करने में भी मदद करता है। इसके अलावा, इन प्रक्रियाओं की जानकारी व्यक्ति को कानून और व्यवस्था बनाए रखने वाले अधिकारियों द्वारा की जाने वाली किसी भी प्रकार की अनुचित कार्रवाई से भी बचा सकती है।

इलेक्ट्रॉनिक उपकरण और कानून

इस मामले पर न्यायिक स्थिति अभी भी अनिश्चित है। हालाँकि, BNSS, BSA, UAPA, Income Tax Act, PMLA और IT Act के भीतर तलाशी और ज़ब्ती के संबंध में सामान्य दिशानिर्देश हैं। यह ध्यान दिया जाना चाहिए कि इन कानूनों में तलाशी और ज़ब्ती की प्रक्रियाएं अलग-अलग हैं और वे इस प्रकार हैं:

परिशिष्ट:

भारतीय नागरिक सुरक्षा संहिता (BNSS) *वारंट के साथ*	**धारा 96-** इस प्रावधान के तहत यह आवश्यक है कि एक पुलिस अधिकारी न्यायालय से विशेष अनुमति ले। जब न्यायालय के पास यह मानने का कारण हो कि तलाशी की जानी चाहिए, तो न्यायालय उन शर्तों को निर्दिष्ट करता है जिनके तहत तलाशी वारंट जारी किया जा सकता है। तलाशी/ज़ब्ती के प्रभारी अधिकारी को उस विशिष्ट क्षेत्र तक ही सीमित रहना चाहिए जिसके लिए वारंट जारी किया गया है। **धारा 103-** यह संपत्ति की तलाशी और ज़ब्ती के लिए एक बुनियादी प्रावधान है। जब भी पुलिस संपत्ति की तलाशी या ज़ब्ती कर रही हो, तो उसे इन नियमों का पालन करने की आवश्यकता होती है।
भारतीय नागरिक सुरक्षा संहिता (BNSS) *बिना वारंट के*	**धारा 185-** पुलिस विशेष अनुमति (वारंट) प्राप्त किए बिना किसी स्थान में प्रवेश कर सकती है और तलाशी ले सकती है यदि उन्हें लगता है कि कोई अपराध जल्द ही हो सकता है या यदि यह उनकी जाँच के लिए महत्वपूर्ण है। इसके अलावा, इस प्रावधान के तहत अब यह अनिवार्य है कि तलाशी करने वाले पुलिस अधिकारी को प्रक्रिया रिकॉर्ड करनी होगी। यदि कोई अधिकारी तलाशी करने में असमर्थ है, तो वह लिखित में कारण दर्ज करने के बाद अपने अधीनस्थ को ऐसा करने के लिए कह सकता है। ऐसी तलाशी के रिकॉर्ड की प्रतियां अड़तालीस घंटे के भीतर निकटतम मजिस्ट्रेट को भेजी जाएँगी। **जाँच के दौरान बयान:** ऐसे प्रावधान हैं (**धारा 180 और 181** में) जो कहते हैं कि किसी व्यक्ति को जाँच के दौरान दिए गए किसी भी बयान की पुष्टि करने की आवश्यकता नहीं है। साथ ही, लोगों को ऐसी बातें न कहने का अधिकार है जो उन्हें दोषी ठहरा सकती हैं, जो भारतीय संविधान द्वारा संरक्षित है।[32] **बिना वारंट गिरफ्तारी: धारा 35** के अनुसार, पुलिस बिना वारंट के भी किसी को गिरफ्तार कर सकती है यदि उन्हें लगता है कि वह व्यक्ति किसी गंभीर अपराध में शामिल था, यदि उनके खिलाफ कोई शिकायत है, या यदि यह मानने का कारण है कि वे किसी अपराध में शामिल हैं। हालाँकि, एक दुर्बल व्यक्ति या साठ वर्ष से अधिक आयु के व्यक्ति को डीएसपी की पूर्व अनुमति के बिना गिरफ्तार किया जाएगा यदि अपराध तीन वर्ष से कम कारावास से दंडनीय है।
	धारा 105- यह एक नया जोड़ा गया प्रावधान है जो अब यह अनिवार्य करता है कि पुलिस अधिकारी तलाशी और ज़ब्ती की कार्यवाही को अधिमानतः मोबाइल फोन के माध्यम से रिकॉर्ड करेगा। इसमें यह भी आवश्यक है कि ज़ब्त की गई वस्तुओं की एक सूची, गवाहों द्वारा हस्ताक्षरित, तैयार की जाए और उसे तुरंत जिला मजिस्ट्रेट, या प्रथम श्रेणी के न्यायिक मजिस्ट्रेट को भेजा जाए। **धारा 106: धारा 106** के तहत पुलिस के पास किसी भी ऐसी संपत्ति को लेने/ज़ब्त करने की शक्ति है जिसे वे चोरी हुई मान सकते हैं। कभी-कभी, इस प्रावधान का दुरुपयोग सामान्य तलाशी के लिए किया जाता है, जिसमें उन्हें मिलने वाली हर चीज शामिल होती है। यह किसी भी पुलिस अधिकारी को किसी भी ऐसी संपत्ति को ज़ब्त करने का अधिकार देता है जिस पर चोरी होने या अपराध के कमीशन से जुड़े होने का संदेह हो। पुलिस अधिकारी को ज़ब्ती की रिपोर्ट स्थानीय मजिस्ट्रेट को करनी होगी और उसकी हिरासत जिम्मेदार व्यक्ति को भी दी जा सकती है, यदि वह अदालत में आवश्यकता पड़ने पर ज़ब्त की गई संपत्ति पेश करने के लिए बांड पर हस्ताक्षर करता है।

परिशिष्ट:

भारतीय साक्ष्य अधिनियम (BSA)	**धारा 168-** न्यायाधीश के पास निम्नलिखित अधिकार हैं - • किसी भी तरीके से तथ्यों से संबंधित प्रश्न पूछना, चाहे वे प्रासंगिक हों या अप्रासंगिक हों। • किसी भी समय किसी भी पक्ष और गवाह से प्रश्न पूछना। • सबूत के तौर पर किसी भी दस्तावेज़ या चीज़ की प्रस्तुति की मांग करना। महत्वपूर्ण रूप से, इस प्रावधान के तहत किसी भी व्यक्ति को न्यायाधीश के अनुरोधों या मांगों पर आपत्ति करने का अधिकार नहीं है। [यह तलाशी और ज़ब्ती से जुड़े मामलों में महत्वपूर्ण हो सकता है जहाँ विशिष्ट दस्तावेज़ या वस्तुएँ सबूत हो सकती हैं।]
PMLA	**धारा 16 और 17-** ये धाराएँ क्रमशः तलाशी या ज़ब्ती करने के नियमों को निर्धारित करती हैं। इनके लिए यह आवश्यक है कि तलाशी या ज़ब्ती क्यों हो रही है, इसका एक लिखित रिकॉर्ड हो और ज़ब्त की गई वस्तुओं की सूची वाली एक रिपोर्ट तैयार की जाए। [यह तलाशी और ज़ब्ती अभियान के दौरान आवश्यक प्रक्रिया और दस्तावेज़ीकरण के बीच एक संबंध स्थापित करता है।]
UAPA	**धारा 43ए- धारा 43ए** अधिकारियों को अधीनस्थ अधिकारियों को तलाशी अधिकृत करने की अनुमति देती है, और यह अनिवार्य करती है कि 'विश्वास करने के आधार' या तो व्यक्तिगत ज्ञान या किसी तीसरे पक्ष द्वारा प्रदान की गई लिखित जानकारी के कारण हों। **धारा 43बी- धारा 43बी** तलाशी या ज़ब्त किए जा रहे व्यक्ति के अधिकारों का विवरण देती है। ये धाराएँ सुनिश्चित करती हैं कि तलाशी या ज़ब्ती के दौरान, तलाशी किए जा रहे व्यक्ति को उसकी तलाशी के आधारों से अवगत कराया जाना चाहिए और ली गई चीजों को निकटतम पुलिस स्टेशन ले जाना होगा। वहाँ के प्रभारी अधिकारी को सीआरपीसी (अब BNSS) में निर्धारित नियमों के अनुसार आवश्यक कार्रवाई करनी होगी।
Income Tax Act	**धारा 132-** यह धारा अधिकारियों को दस्तावेज़ों या वस्तुओं को ज़ब्त करने का अधिकार देती है यदि कोई व्यक्ति कानून द्वारा आवश्यक रूप से उन्हें प्रदान नहीं करता है। तलाशी और ज़ब्ती के संदर्भ में, यह धारा अधिकारियों को विशिष्ट दस्तावेज़ों या वस्तुओं को ज़ब्त करने के लिए कानूनी समर्थन देती है यदि वे जाँच या कानूनी कार्यवाही के दौरान स्वेच्छा से प्रस्तुत नहीं किए जाते हैं। यह धारा अभियुक्त व्यक्तियों को पर्याप्त सुरक्षा उपाय भी प्रदान करती है, जिसमें यह आवश्यक है कि अभियुक्त को ज़ब्त की गई वस्तुओं के संबंध में अपने स्पष्टीकरण का समर्थन करने के लिए सबूत पेश करने का उचित अवसर दिया जाना चाहिए।
IT Act	**धारा 80- धारा 80 अधिकृत अधिकारियों** [33] को किसी भी सार्वजनिक स्थान की तलाशी लेने और बिना वारंट के गिरफ्तार करने का अधिकार देती है - वहाँ पाया गया कोई भी व्यक्ति जिस पर अतीत, वर्तमान या भविष्य में IT Act के तहत अपराध करने का उचित संदेह हो।

परिशिष्ट:

THE SCHEDULE

[*See* section 63(*4*)(*c*)]

CERTIFICATE

PART A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable)
and any other relevant information, if any, about the device/digital record____(specify).

The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business. If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____hours (In 24 hours format)

Place: _____

चित्र 1:
पक्ष द्वारा भरा जाने वाला प्रमाण पत्र

परिशिष्ट:

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)
and any other relevant information, if any, about the device/digital record _____ (specify).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

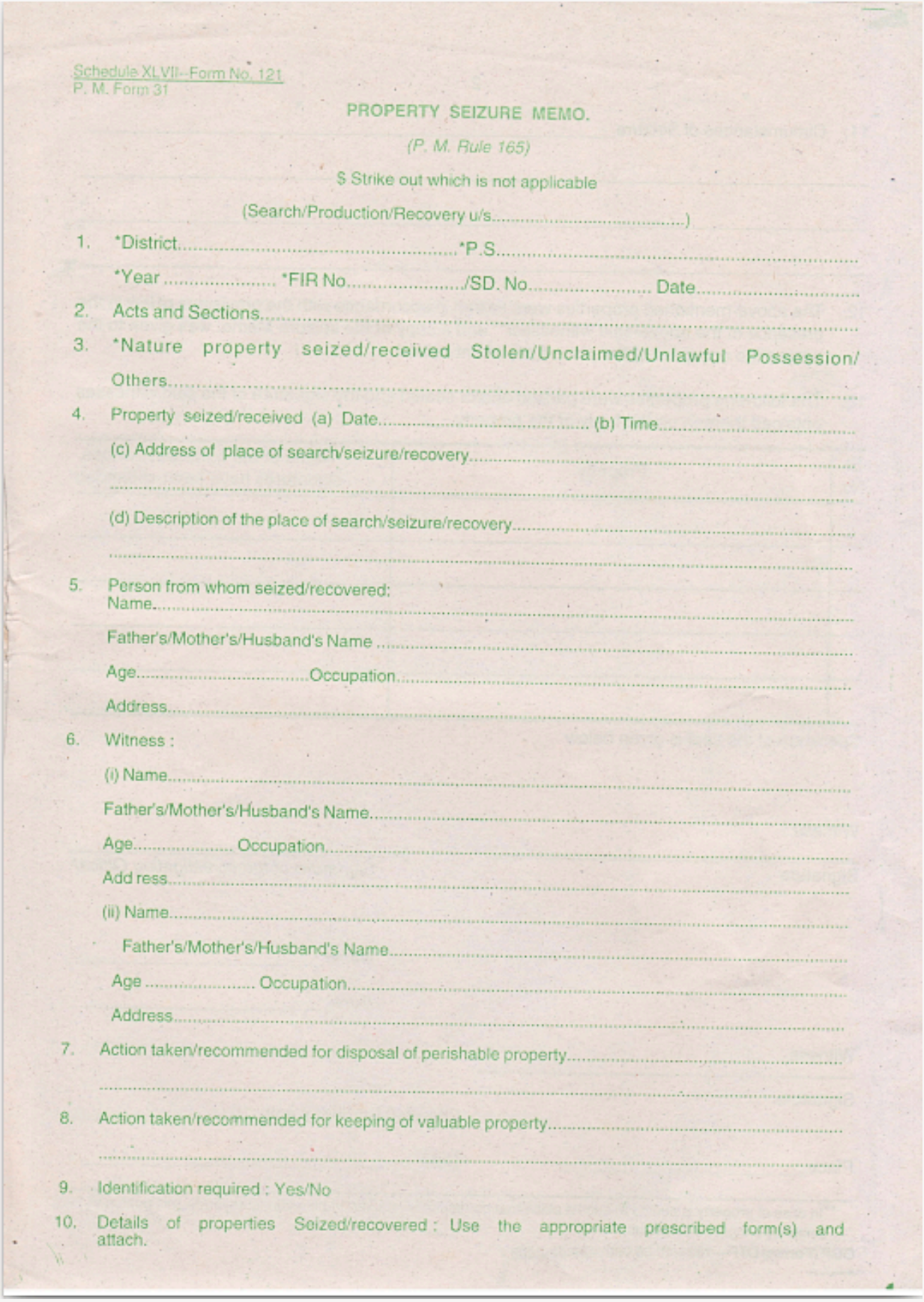
Place: _____

_____

DIWAKAR SINGH,
Joint Secretary & Legislative Counsel to the Govt. of India.

चित्र 2:
विशेषज्ञ द्वारा भरा जाने वाला प्रमाण पत्र

परिशिष्ट:



Schedule XLVII--Form No. 121
P. M. Form 31

PROPERTY SEIZURE MEMO.

(P. M. Rule 165)

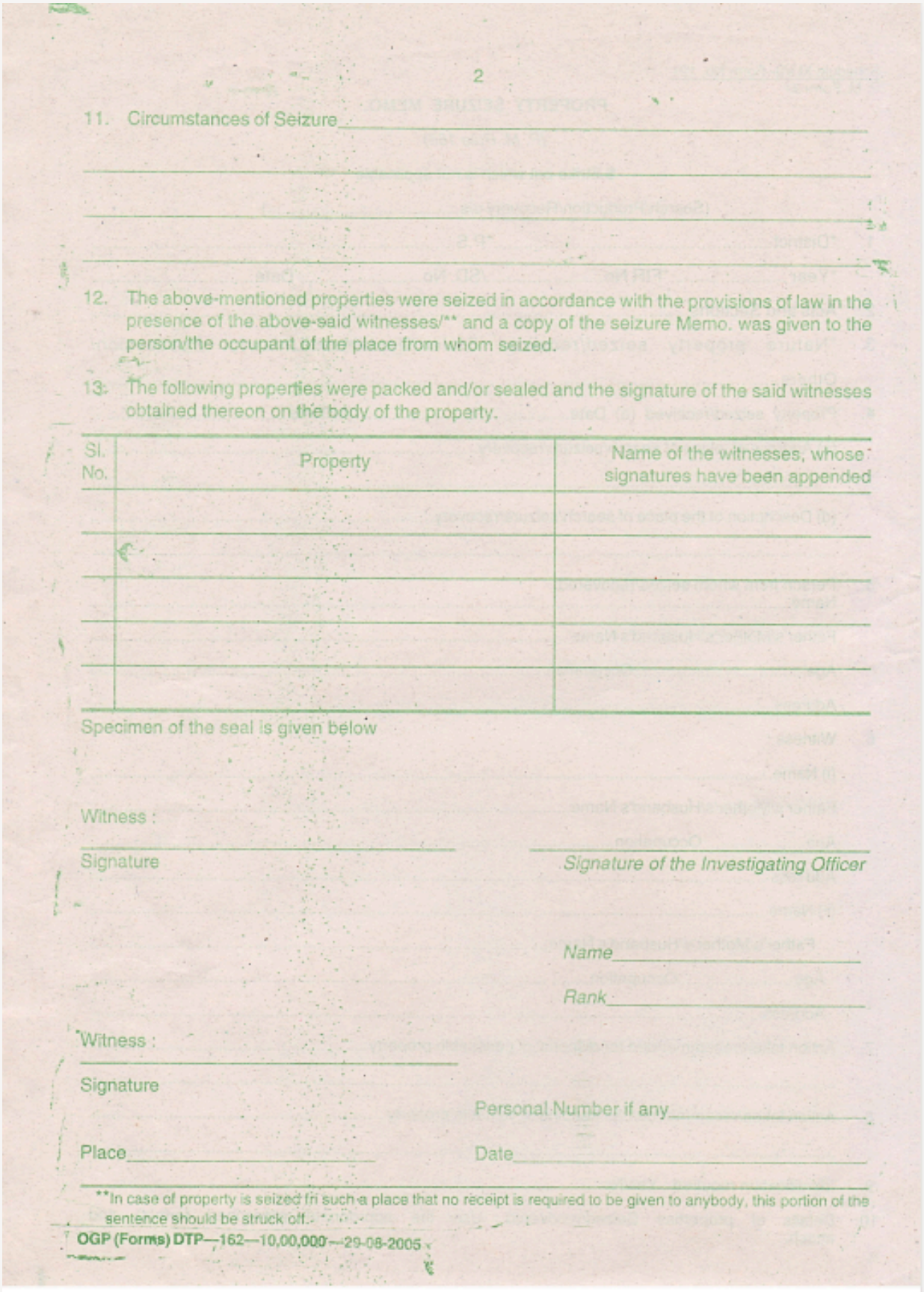
$ Strike out which is not applicable

(Search/Production/Recovery u/s.....)

1. *District.....*P.S.....
   *Year ..... *FIR No...../SD. No..... Date.....
2. Acts and Sections.....
3. *Nature property seized/received Stolen/Unclaimed/Unlawful Possession/ Others.....
4. Property seized/received (a) Date..... (b) Time.....
   (c) Address of place of search/seizure/recovery.....
   .....
   (d) Description of the place of search/seizure/recovery.....
   .....
5. Person from whom seized/recovered:
   Name.....
   Father's/Mother's/Husband's Name .....
   Age.....Occupation.....
   Address.....
6. Witness :
   (i) Name.....
   Father's/Mother's/Husband's Name.....
   Age..... Occupation.....
   Add ress.....
   (ii) Name.....
   Father's/Mother's/Husband's Name.....
   Age ..... Occupation.....
   Address.....
7. Action taken/recommended for disposal of perishable property.....
   .....
8. Action taken/recommended for keeping of valuable property.....
   .....
9. Identification required : Yes/No
10. Details of properties Seized/recovered : Use the appropriate prescribed form(s) and attach.

चित्र 3:
संपत्ति जब्ती ज्ञापन

परिशिष्ट:



2

11. Circumstances of Seizure _____

12. The above-mentioned properties were seized in accordance with the provisions of law in the presence of the above-said witnesses/** and a copy of the seizure Memo. was given to the person/the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the said witnesses obtained thereon on the body of the property.

Sl. No.	Property	Name of the witnesses, whose signatures have been appended

Specimen of the seal is given below

Witness :

Signature

Signature of the Investigating Officer

Name _____

Rank _____

Witness :

Signature

Personal Number if any _____

Place _____

Date _____

**In case of property is seized fri such a place that no receipt is required to be given to anybody, this portion of the sentence should be struck off.

OGP (Forms) DTP—162—10,00,000—29-08-2005

चित्र 3.1:
संपत्ति जब्ती ज्ञापन

परिशिष्ट:

SEIZURE LIST

Case Reference :

1. Date and Hours of Seizure :

2. Place of Seizure / Person from whom seized :

3. Name and Address of Witnesses :
   (i) (ii)

4. Description of articles seized :
   (Appropriate PF and / or space on reverse may be used)

5. Circumstances of Seizure :

6. Signature of Witnesses & Police Officer

चित्र 4:
जब्ती सूची

परिशिष्ट:

FORM No. 3

WARRANT OF ARREST

(*See* section 72)

To ..... (*name and designation of the person or persons who is or are to execute the warrant*).

WHEREAS (*name of accused*) of (*address*) stands charged with the offence of ..... (*state the offence*), you are hereby directed to arrest the said ....., and to produce him before me. Herein fail not.

Dated, this..... day of..... , 20 ..... .

(*Seal of the Court*) (*Signature*)

(*See* section 73)

This warrant may be endorsed as follows:—

If the said..... shall give bail himself in the sum of rupees..... with one surety in the sum of rupees..... (or two sureties each in the sum of rupees.....) to attend before me on the..... day of..... and to continue so to attend until otherwise directed by me, he may be released.

Dated, this..... day of..... , 20 ..... .

(*Seal of the Court*) (*Signature*)

चित्र 5:

गिरफ़्तारी वारंट प्रारूप

(बीएनएसएस की दूसरी अनुसूची में दिया गया है, जो अधिनियम के आधिकारिक राजपत्र अधिसूचना में पृष्ठ 192 पर प्रकाशित है)

संदर्भ:

[1] शब्द के अर्थ के लिए शब्दावली देखें।

[2] BNSS के भीतर तलाशी की व्याख्या के लिए धारा 49;97 देखें।

[3] BNSS की धारा 44

[4] BNSS की धारा 185(1)

[5] BNSS के भीतर ज़ब्ती की व्याख्या के लिए धारा 106, 117 देखें।

[6] लेकिन यह कानूनों की संपूर्ण सूची नहीं है। ऐसे अन्य कानून भी हैं जो तलाशी और ज़ब्ती का प्रावधान करते हैं।

[7] दंड प्रक्रिया संहिता, 1973 (CrPC).

[8] भारतीय साक्ष्य अधिनियम, 1872

[9] भारतीय दंड संहिता, 1860

[10] दूरसंचार अधिनियम, 2023 की धारा 42 और 43 देखें।

[11] कृपया ध्यान दें कि ऐसी रिकॉर्डिंग केवल प्रथम श्रेणी के न्यायिक मजिस्ट्रेट, जिला मजिस्ट्रेट और उप-विभागीय मजिस्ट्रेट को ही प्रदान की जा सकती है।

[12] BNSS, 2023 की धारा 94 और 185

[13] के.एस. पुट्टस्वामी बनाम भारत संघ (2017) 10 एससीसी 1।

[14] वीरेंद्र खन्ना बनाम कर्नाटक राज्य, रिट याचिका संख्या 11759 ऑफ 2020 (जीएम-आरईएस)।

[15] फाउंडेशन ऑफ मीडिया प्रोफेशनल्स बनाम भारत संघ, रिट याचिका (क्रिम) संख्या 395 ऑफ 2022, भारत का सर्वोच्च न्यायालय, पृष्ठ 1 ।

[16] अवस्थिका दास, डिजिटल उपकरणों की जब्ती के लिए दिशानिर्देश बनाने के लिए गठित समिति: केंद्र ने सुप्रीम कोर्ट को बताया, (6 दिसंबर, 2023 12:05 अपराह्न) https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831

[17] BSA, 2023 की धारा 63(4)(c) के तहत प्रमाण पत्र प्रदान किया गया है।

संदर्भ:

[18] ज़ब्ती ज्ञापन का एक नमूना परिशिष्ट में चित्र 3 और 3.1 के रूप में प्रदान किया गया है। इस नमूने का स्रोत https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf

[19] ऐसी एक सूची का नमूना (जिसे नीचे परिशिष्ट में चित्र 4 में जब्ती सूची के रूप में पहचाना जा सकता है) नीचे परिशिष्ट में प्रदान किया गया है।

[20] गिरफ्तारी वारंट का एक नमूना अनुलग्नक में चित्र 5 के रूप में प्रदान किया गया है।

[21] BNSS धारा 503(2).

[22] See BNSS धारा 2(c).

[23] BNSS की धारा 2(f) देखें, आरोप धारा 2(b) के तहत परिभाषित है; आरोप की सामग्री की बेहतर समझ के लिए धारा 234 भी देखें।

[24] BNSS, धारा 2(g) देखें। राजपत्र अधिसूचना में प्रकाशित अधिनियम के पृष्ठ 158 पर व्याख्यात्मक नोट्स का पहला शेड्यूल, बिंदु (2) भी देखें।

[25] BNS की धारा 2(21)।

[26] BNSS की धारा 2(o) देखें। राजपत्र अधिसूचना में प्रकाशित अधिनियम के पृष्ठ 158 पर व्याख्यात्मक नोट्स का पहला शेड्यूल, बिंदु (2) भी देखें।

[27] BNSS, धारा 2(s)।

[28] IT Act, धारा 80(1) की व्याख्या।

[29] जी. विशाकन बनाम केरल राज्य और अन्य, डब्ल्यूपी(सी) संख्या 22328 ऑफ 2023 (10.07.2023 - केईआरएचसी) : मनु/केई/1872/2023

[30] संकेत भद्रेश मोदी बनाम सीबीआई, बीए संख्या 3754/23।

[31] सीबीआई बनाम महेश कुमार शर्मा, सीबीआई 31/2021।

[32] यह अधिकार भारत के संविधान के भाग III के अनुच्छेद 20(3) के तहत निहित है।

[33] यहाँ अधिकृत अधिकारियों का अर्थ है या तो एक पुलिस अधिकारी (निरीक्षक से नीचे नहीं) या केंद्र सरकार द्वारा अधिकृत केंद्र या राज्य सरकार का कोई अन्य अधिकारी।

Email: mail@sflc.in

Website: https://www.sflc.in