sflc.in

इलेक्ट्रॉनिक साधनांची तपासणी व जप्ती कायद्याचे संपूर्ण मार्गदर्शन

इलेक्ट्रॉनिक साधनांच्या शोध व जप्तीवर मार्गदर्शक, २०२५
SFLC.in आणि UNESCO यांच्या सहकार्याने प्रकाशित

©Copyright 2024 SFLC.in | Creative Commons BY SA NC 4.0
अंतर्गत परवाना प्राप्त

प्रकाशक: SFLC.in
K9, दुसरा मजला, बीरबल रोड, जंगपूरा विस्तार, नवी दिल्ली – १४, भारत.

ईमेल: mail@sflc.in
वेबसाइट:https://www.sflc.in

अनुक्रमणिका

खंड 1

मूलभूत माहिती

तुमची कोणाकडून शोध तपासणी झाली आहे का?
तपासणी करताना त्यांनी तुमच्या शरीराचा,
वाहनाचा किंवा घराचा शोध घेतला का?
त्यांनी तुमची इलेक्ट्रॉनिक साधने जप्त केली का?
या प्रश्नांपैकी कोणत्याही प्रश्नाचे उत्तर "होय" असेल तर...

शोध आणि जप्ती डीकोड केली

शोध आणि जप्ती: काय, का आणि कुठे?

शोध (Search) म्हणजे एखाद्या व्यक्तीच्या संपत्तीची किंवा त्याच्या ठिकाणाची तपासणी करणे [1], जेणेकरून कोणत्याही गुन्ह्याच्या चौकशीसाठी किंवा कोर्टाशी संबंधित कार्यवाहीसाठी दाखला मिळू शकेल [2]. हा शोध वॉरंटसह [3] किंवा वॉरंटशिवाय [4] घेतला जाऊ शकतो.

जप्ती (Seizure) म्हणजे शोध घेतल्यानंतर मिळालेल्या संपत्तीचा ताबा घेणे, जेणेकरून तो दाखला म्हणून वापरता येईल किंवा चौकशीसाठी आवश्यक असलेली संपत्ती म्हणून जप्त करता येईल [5].

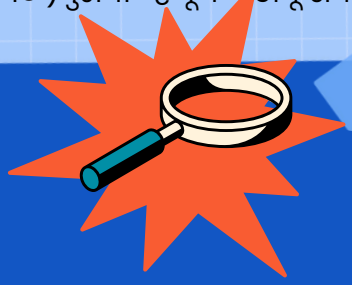
काय? - शोध आणि जप्ती म्हणजे पोलिस आणि तपास संस्थांकडून गुन्ह्याच्या चौकशीसाठी वापरले जाणारे पद्धत.

का? - पुरावे (एविडन्स) जमा करण्यासाठी, गुन्हे टाळण्यासाठी आणि अन्याय होऊ नये यासाठी.

कुठे? - जिथे गुन्हा घडला ते ठिकाण, गुन्ह्यात सहभागी असलेले लोक लपून बसण्याची शक्यता असलेली ठिकाणं आणि गुन्ह्याशी संबंधित वस्तू किंवा कागदपत्रं सापडू शकतील अशी ठिकाणं.

शोध आणि जप्ती का केली जाते?

- महत्त्वाचे पुरावे (एव्हिडन्स), कागदपत्रं आणि डिजिटल माहिती तपास संस्थांना { पोलिस विभाग, केंद्रीय अन्वेषण विभाग (CBI), अंमलबजावणी संचालनालय (ED), राज्य गुन्हे अन्वेषण विभाग (CID), महसूल गुप्तचर संचालनालय (DRI) } मिळावी, जेणेकरून चौकशी, तपास, किंवा कोर्टात वापर करता यावा.
- जप्त केलेल्या कागदपत्रांमधली माहिती तपास संस्था न्यायालयात (कोर्ट)पुरावा म्हणून दाखवू शकते.



शोध आणि जप्तीची कायदेशीर मुलतत्त्वे

शोध व जप्ती करण्याचे अधिकार खालील कायद्यांमधून मिळतात [6]:

- भारतीय नागरिक सुरक्षा संहिता, 2023 {Bhartiya Nagarik Suraksha Sanhita, 2023} [7]
  - भारतीय साक्ष्य अधिनियम, 2023 {Bharatiya Sakshya Adhiniyam, 2023} [8]
- भारतीय न्याय संहिता, 2023 {Bharatiya Nyaya Sanhita, 2023} [9]
  - आयकर कायदा, 1961 {Income Tax Act, 1961}
- बेकायदेशीर क्रियाकलाप (प्रतिबंध) अधिनियम, 1967 {Unlawful Activities (Prevention) Act, 1967}
  - मनी लॉंडरिंग प्रतिबंधक कायदा, 2002 {Prevention of Money Laundering Act, 2002}
- केंद्रीय अन्वेषण ब्युरो मार्गदर्शक, 2020 {CBI Manual of 2020}
  - माहिती तंत्रज्ञान कायदा, 2000 {Information Technology Act, 2000}
- दूरसंचार कायदा, 2023 {Telecommunications Act, 2023}
  - अंमली पदार्थ व मनोविकृती निर्माण करणारे पदार्थ कायदा, 1985 {Narcotic Drugs and Psychotropic Substances Act, 1985}

अंतर्गत प्रक्रिया (BTS): शोध आणि जप्तीमध्ये कोणाची भूमिका असते?

शोध आणि जप्ती करण्याचा अधिकार वेगवेगळ्या कायद्यांनुसार ठरतो आणि त्यामध्ये बदल होऊ शकतात.
हा विभाग प्रामुख्याने शोधाचे आदेश कोण देऊ शकतो याबाबत सामान्य माहिती देण्यासाठी आहे.
हे समजून घेतल्याने तुम्ही तपास अधिकाऱ्यांकडे योग्य पद्धतीने प्रश्न विचारू शकता.
वेगवेगळे कायदे आणि परिस्थितीनुसार शोध आणि जप्ती करण्याची प्रक्रिया बदलू शकते.

I. शोधाचा आदेश देण्याचा अधिकार कोणाकडे असतो?

भारतीय नागरिक सुरक्षा संहिता, 2023 (BNSS)	जिल्हा दंडाधिकारी, उपविभागीय दंडाधिकारी किंवा प्रथम श्रेणी न्यायाधीश विशेष परवानगी देऊ शकतात, ज्याद्वारे हवालदारपेक्षा उच्च पदाचा पोलीस अधिकारी (इतर कोणतेही अधिकारी नाही!) संशयित ठिकाणी शोध घेऊ शकतो. जर त्या ठिकाणी चोरीस गेलेली मालमत्ता किंवा धोकादायक वस्तू लपवलेल्या असल्याचा संशय असेल, तर न्यायाधीश हा आदेश देऊ शकतो. तसेच, गरज पडल्यास त्या अधिकाऱ्याला इतरांची मदत घेण्याची परवानगीही असते.
आयकर कायदा, 1961 (ITA)	डायरेक्टर/जनरल/चीफ कमिशनर/कमिशनर यांना शोधाचा आदेश देण्याचा अधिकार असतो.
बेकायदेशीर कृत्य प्रतिबंधक कायदा, 1967 (UAPA)	केंद्र सरकार/राज्य सरकार शोधाचा आदेश देऊ शकते. मात्र, कायद्यात स्पष्ट उल्लेख नाही की सरकारच्या (केंद्र/राज्य) कोणत्या विभाग/मंत्रालयाकडे हा आदेश देण्याचा अधिकार आहे.
मनी लॉंडरिंग प्रतिबंधक कायदा, 2002 (PMLA)	**सर्वेक्षणासाठी:** विवाचन प्राधिकरण (एडजुडिकेटिंग अथॉरिटी) आदेश देऊ शकते. **जप्तीसाठी:** संचालक (डायरेक्टर) किंवा उपसंचालक (डेप्युटी डायरेक्टर) पेक्षा कमी दर्जाचा नसलेला अधिकारी आदेश देऊ शकतो.
माहिती तंत्रज्ञान कायदा, 2000 (IT Act)	केंद्र सरकारला केंद्र किंवा राज्य सरकारमधील कोणत्याही अधिकाऱ्याला शोधाचा आदेश देण्याचा अधिकार आहे. कंट्रोलर संगणकातील डेटा मिळवण्यासाठी शोधाचा आदेश देऊ शकतो.

अंतर्गत प्रक्रिया (BTS): शोध आणि जप्तीमध्ये कोणाची भूमिका असते?

शोध आणि जप्ती करण्याचा अधिकार वेगवेगळ्या कायद्यांनुसार वेगवेगळ्या अधिकाऱ्यांकडे असतो. खाली त्याची महत्त्वाची माहिती दिली आहे. हा विभाग शोध करण्याचा अधिकार कोणाकडे असतो हे समजावण्यासाठी आहे. हे समजून घेतल्याने तपास अधिकाऱ्यांना योग्य प्रकारे प्रश्न विचारण्यास मदत होईल.

वेगवेगळ्या कायद्यांनुसार आणि परिस्थितीनुसार शोध आणि जप्ती करण्याची प्रक्रिया बदलू शकते.

II. शोध करण्याचा अधिकार कोणाकडे असतो?

भारतीय नागरिक सुरक्षा संहिता, 2023 (BNSS)	शोध आणि जप्तीबाबत कायदा कसा कार्य करतो याची साधी कल्पना: स्टेशन हाऊस ऑफिसर (SHO) किंवा तपास अधिकारी (IO) शोध आणि जप्ती करू शकतात. जर हे अधिकारी अनुपस्थित असतील, तर लिखित परवानगी असलेला कोणताही अधिकारी ही कारवाई करू शकतो. **कोणाला अटक झाल्यास:** पोलिस अटक झालेल्या ठिकाणी शोध घेऊ शकतात आणि गुन्ह्याशी संबंधित कोणतीही वस्तू ताब्यात घेऊ शकतात. हे फक्त पोलिसच करू शकतात, आणि गरज पडल्यास दरवाजे किंवा खिडक्या तोडूनही प्रवेश करू शकतात. **काही संशयास्पद लपवले असल्यास:** जिल्हा दंडाधिकारी, उपविभागीय दंडाधिकारी किंवा प्रथम श्रेणी न्यायाधीश हवालदाराच्या दर्जापेक्षा मोठ्या अधिकाऱ्याला विशेष परवानगी देऊ शकतात, जर त्यांना वाटले की त्या ठिकाणी चोरीच्या वस्तू किंवा धोकादायक साहित्य लपवले आहे. गरज असल्यास, हा अधिकारी इतर अधिकाऱ्यांची मदत घेऊ शकतो. **कलमे: 44 आणि 97**
बेकायदेशीर कृत्य प्रतिबंधक कायदा, 1967 (UAPA)	UAPA अंतर्गत तपास करण्याचा अधिकार वेगवेगळ्या शहरांमध्ये वेगवेगळ्या अधिकाऱ्यांकडे असतो: **दिल्ली स्पेशल पोलिस स्थापनामध्ये:** उप-अधीक्षक (Deputy Superintendent of Police) किंवा त्याच दर्जाचा अधिकारी. **मुंबई, कोलकाता, चेन्नई, अहमदाबाद आणि अधिसूचित क्षेत्रांमध्ये:** सहाय्यक पोलिस आयुक्त (Assistant Commissioner of Police) किंवा त्यापेक्षा वरिष्ठ अधिकारी. इतर प्रकरणांमध्ये: उप-अधीक्षक (Deputy Superintendent of Police) किंवा त्याच दर्जाच्या पेक्षा कमी नसलेले अधिकारी.

अंतर्गत प्रक्रिया (BTS): शोध आणि जप्तीमध्ये कोणाची भूमिका असते?

शोध आणि जप्ती करण्याचा अधिकार वेगवेगळ्या कायद्यांनुसार वेगवेगळ्या अधिकाऱ्यांकडे असतो. खाली त्याची महत्त्वाची माहिती दिली आहे. हा विभाग शोध करण्याचा अधिकार कोणाकडे असतो हे समजावण्यासाठी आहे. हे समजून घेतल्याने तपास अधिकाऱ्यांना योग्य प्रकारे प्रश्न विचारण्यास मदत होईल.

वेगवेगळ्या कायद्यांनुसार आणि परिस्थितीनुसार शोध आणि जप्ती करण्याची प्रक्रिया बदलू शकते.

II. शोध करण्याचा अधिकार कोणाकडे असतो?

आयकर कायदा, 1961 (Income Tax Act, 1961)	फक्त सहाय्यक आयुक्त (इनकम टॅक्स ऑफिसर) किंवा त्याहून मोठ्या पदावरचे इनकम टॅक्स अधिकारी तपास करू शकतात.
मनी लाँडरिंग प्रतिबंधक कायदा, 2002 (Prevention of Money Laundering Act, 2002)	डायरेक्टर किंवा डिप्टी डायरेक्टरच्या दर्जाच्या किंवा त्याहून मोठ्या पदावरचा कुठलाही अधिकारी तपास करू शकतो.
माहिती तंत्रज्ञान कायदा, 2000 (Information Technology Act, 2000)	इन्स्पेक्टरच्या दर्जाचा किंवा त्याहून मोठ्या पदाचा कुठलाही पोलिस अधिकारी तपास करू शकतो. त्याशिवाय, केंद्र सरकार राज्य किंवा केंद्र सरकारमधील इतर कोणत्याही अधिकाऱ्याला तपासासाठी अधिकृत करू शकतं. कंट्रोलर किंवा त्यांनी अधिकृत केलेला कुठलाही अधिकारीसुद्धा तपास करू शकतो.
दूरसंचार कायदा, 2023 (Telecommunications Act, 2023)	हा कायदा केंद्र सरकारच्या अधिकृत अधिकाऱ्याला कोणतीही जागा शोधण्याचा अधिकार देतो, जर त्या अधिकाऱ्याला विश्वास वाटत असेल की तिथे बेकायदेशीर टेलिकम्युनिकेशन नेटवर्क किंवा उपकरण लपवून ठेवले आहे. [10]



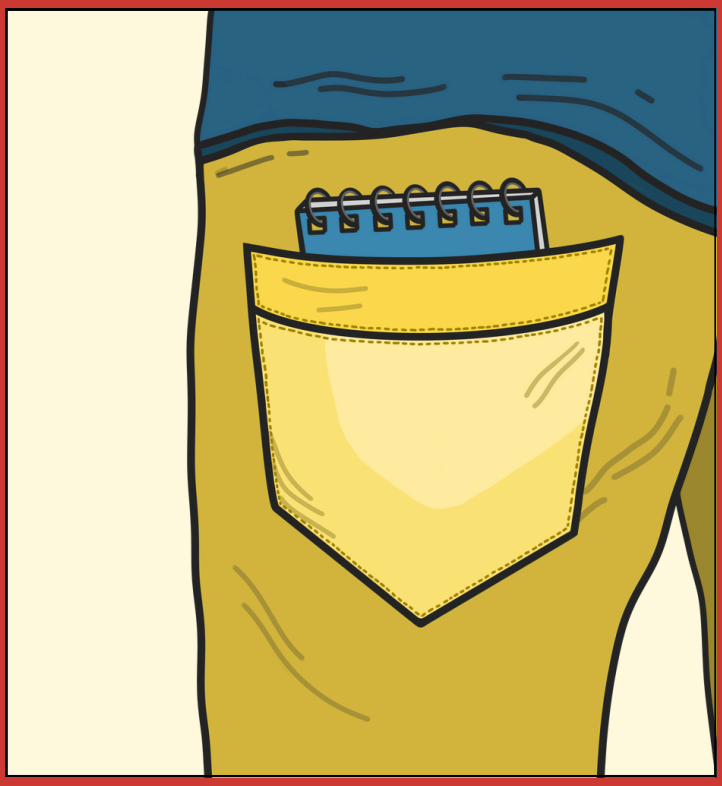

खंड 2

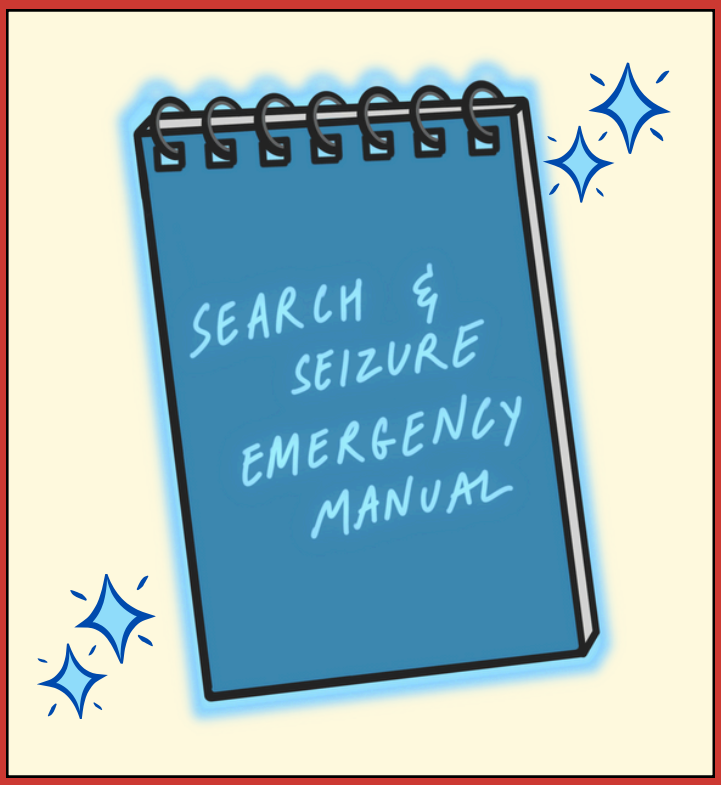
तपासाच्या वेळी काय करावे?

तपासाची प्रक्रिया कधी कधी गुंतागुंतीची आणि कठीण वाटू शकते.

ही प्रक्रिया नीट समजून घेण्यासाठी त्यामधील नियम आणि आवश्यक कागदपत्रांची माहिती असणे महत्त्वाचे आहे.

तपासाचा शेवटी केस कोर्टात जाऊ शकतो, आणि अशा वेळी शोध प्रक्रिया आणि संबंधित नियम प्रक्रिया (प्रोटोकॉल) यांचा नीट अभ्यास करणे कोर्टात स्वतःचा बचाव करण्यासाठी खूप उपयोगी ठरू शकते.





तपास सुरू होताना विचारायला उपयुक्त प्रश्न:

1	**तुमच्याकडे वॉरंट आहे का?**
2	**ते इलेक्ट्रॉनिक स्वरूपात दिले गेले आहे का?**
3	**होय असल्यास, कोणत्या माध्यमातून मिळाले आहे?**
4	**तुम्ही कोणत्या तपास यंत्रणेकडून आला आहात?**
5	**तुमची नेमकी पदवी/हुद्दा काय आहे?**
6	**माझ्यावर नक्की कोणते आरोप आहेत?**

यासोबत हे लक्षात ठेवा:

- जर तुम्हाला वाटत असेल की तुमच्या प्रश्नांची योग्य उत्तरे दिली जात नाहीत, तर ताबडतोब वकिलाशी संपर्क साधा.
- तुमच्या वकिलाच्या उपस्थितीशिवाय पुढील कोणत्याही प्रश्नांना उत्तर देऊ नका.

अधिकाऱ्यांकडून योग्य माहिती मिळवण्याचे उपाय:

- पोलिस, तपास आणि शोध प्रक्रिया - पोलिस [11] तुमची इलेक्ट्रॉनिक साधन वॉरंटसह किंवा त्याशिवायही तपासू शकतात. पण, तुम्ही शोध आणि जप्ती प्रक्रियेचा रेकॉर्ड मागू शकता. तो रेकॉर्ड पोलिसांनी जवळच्या दंडाधिकाऱ्याला (Magistrate)[12] दिलेला असतो.

- **तुमच्याकडे असलेल्या इतर कोणाच्याही इलेक्ट्रॉनिक नोंदी तुम्ही नाकारू शकता, जोपर्यंत त्या व्यक्तीची परवानगी नाही.**

- शोध आणि जप्ती ही तपासाची सामान्य प्रक्रिया आहे. त्यामुळे तुमच्या घराची किंवा साधनांची तपासणी होत असल्याने तुम्ही गुन्हेगार आहात असे होत नाही. जर तपास यंत्रणेकडे पूर्णपणे अधिकृत कागदपत्रे असतील, तर त्यांना त्यांचे काम करू द्या. पण, भविष्यात वकिलाची गरज लागू शकते, म्हणून त्यांच्याशी संपर्क ठेवा.

- काही वेळा तपास अधिकारी तुमच्या प्रश्नांना उत्तर देणार नाहीत. त्यामुळे तुमचे प्रश्न आणि मिळालेली उत्तरे एका कागदावर लिहून ठेवा, जे पुढील कोर्ट उपयोगी पडू शकते.

- तुम्हाला शोध प्रक्रियेला मदत करण्याची जबरदस्ती नाही, पण अडथळाही करू नये. उदा. इलेक्ट्रॉनिक डिव्हाइस घेऊन पळून जाणे किंवा तोडफोड करणे योग्य नाही. नेहमी शांत राहा, कायदेशीर सल्ला घ्या आणि तुमच्या हक्कांची जाणीव ठेवा.

शोध आणि जप्ती दरम्यान, मिळालेल्या पुराव्याची त्वरित परीक्षण आणि तपासणी केले जाते, जेणेकरून त्याची उपयुक्तता आणि विश्वासार्हता निश्चित करता येईल.

यामध्ये घटनास्थळी आढळलेली भौतिक साधने आणि डिजिटल साधनांची पाहणी आणि नोंद करणे समाविष्ट आहे. डेटा मिळवणे आणि फॉरेन्सिक विश्लेषण करून माहिती पुनर्प्राप्त व सत्यापित केली जाते, तसेच छेडछाड होण्यापासून संरक्षण केले जाते. महत्त्वाचे नमुने आणि संबंध शोधले जातात आणि प्रत्येक टप्प्यावर स्पष्ट नोंदी ठेवल्या जातात, जेणेकरून पुराव्याची साखळी व्यवस्थित राहील.

1	**विश्लेषणासाठी वापरलेल्या साधने आणि खात्यांची यादी ठेवा:** तपासासाठी वापरलेल्या साधने आणि खात्यांची यादी ठेवावी, त्यामुळे अधिकाऱ्यांनी गोळा केलेल्या सर्व डेटाचे नंतर क्रॉस-तपासणी करणे सोपे जाईल.
2	**साधनांवरील फाइल्स कुठे साठवलेल्या आहेत हे सांगू नका:** जेव्हा अधिकारी शोध आणि जप्ती करतात, तेव्हा तुमच्या गोपनीयतेचे आणि प्रक्रियेच्या विश्वासार्हतेचे संरक्षण करण्यासाठी फाइल्स कुठे साठवलेल्या आहेत हे सांगू नये. फाइल्सच्या स्थानाची माहिती दिल्यास शोधाचा कक्ष कायदेशीर मर्यादेपेक्षा वाढू शकतो आणि तुमची संवेदनशील किंवा गैरलागू वैयक्तिक माहिती उघड होऊ शकते.
3	**तपासासाठी घेतलेल्या साधनांचे आयएमईआय (IMEI), सिरियल नंबर आणि वैशिष्ट्ये नोंदवा:** हे केल्याने साधनाची ओळख निश्चित करता येते, इतर साधनांशी गडबड होण्यापासून संरक्षण मिळते आणि योग्य साधनच विश्लेषणासाठी वापरले जात आहे किंवा कोर्ट मध्ये सादर केले जात आहे, याची खात्री होते.

खंड 3

इलेक्ट्रॉनिक साधने आणि कायदा

भारताच्या सर्वोच्च न्यायालयाने (सुप्रिम कोर्ट ऑफ इंडिया) के. एस. पुट्टूस्वामी वि. युनियन ऑफ इंडिया (2017) या प्रकरणात खासगीपणा आणि माहितीविषयक खासगीपणा हा मूलभूत हक्क म्हणून मान्य केला.[13] - वीरेन्द्र खन्ना वि. स्टेट ऑफ कर्नाटका या प्रकरणात, कर्नाटक उच्च न्यायालयाने (कर्नाटका हाय कोर्ट) इलेक्ट्रॉनिक साधनांच्या शोध आणि जप्तीबाबत विस्तृत मार्गदर्शन दिलं. या प्रकरणात, कोर्ट ने असे ठरवले की स्मार्टफोन किंवाकंप्युटर सिस्टीमला प्रवेश देण्यासाठी पासवर्ड, बायोमेट्रिक्स किंवा पासकोड सांगणे हे कोणाच्याही स्वतःविरुद्ध साक्ष देण्याच्या मूलभूत अधिकाराचे उल्लंघन मानले जाणार नाही.[14]

मात्र, फाउंडेशन ऑफ मीडिया प्रोफेशनल्स संस्थेने सर्वोच्च न्यायालयात यासंदर्भात अर्ज दाखल केला. संस्थेने असा युक्तिवाद केला की सध्याच्या कायद्यांमध्ये इलेक्ट्रॉनिक साधनांमध्ये असलेल्या वैयक्तिक माहितीचे संरक्षण करण्यासाठी पर्याप्त व्यवस्था नाही. या साधनांमध्ये मोठ्या प्रमाणात खासगी माहिती साठवलेले असते, त्यामुळे अशा तपास प्रक्रियेमुळे लोकांच्या स्वतःविरुद्ध साक्ष न देण्याच्या आणि खासगीपणाच्या हक्काचे उल्लंघन होण्याची शक्यता असते. [15] त्यामुळे, शोध प्रक्रियेसाठी जबाबदार संस्थांकडून इलेक्ट्रॉनिक साधनांचा शोध आणि जप्ती कशी केली जावी यावर मार्गदर्शन विकसित करण्यासाठी एका कमीटीची स्थापना करण्यात आली.[16]

शोध आणि जप्तीची प्रक्रिया वेगवेगळ्या कायद्यांनुसार कशी केली जाते, हे जाणून घेण्यासाठी कृपया संदर्भ (Annexure) वाचा.

खंड 4

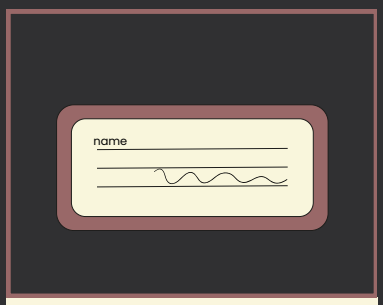
पोस्ट-सीझर प्रोटोकॉल:

जेव्हा तुमचं डिव्हाइस जप्त केलं जातं, तेव्हा काय होतं?

जप्त झालेल्या उपकरणांसाठी आवश्यक कागदपत्रे

आवश्यक प्रमाणपत्रे
(कलम 63(4)(क) अंतर्गत)

ज्या व्यक्तीचे साधन तपासले आणि जप्त केले आहे तसेच तपास करणाऱ्या तज्ज्ञाने भरलेले प्रमाणपत्र मिळवण्याची विनंती करता येते. या प्रमाणपत्रामध्ये पुढील तपशील [17] असणे आवश्यक आहे [18] :



ज्याचे साधन तपासले व जप्त केले आहे त्या व्यक्तीचे नाव व स्वाक्षरी

जप्तीची दिनांक व वेळ

जप्तीचे ठिकाण

जप्त केलेल्या साधनचे वर्णन (निर्माता, मॉडेल, अनुक्रमांक/ आय.एम.ई.आय/यू.आय.एन/ यू.आय.डी/एम.एसी)

0000 1111
0000 2222

हॅश मूल्य (हॅश रिपोर्ट सह)

तज्ज्ञाने (एक्सपर्ट) भरलेले आणि सर्व संबंधित तपशीलांसह स्वाक्षरी केलेले प्रमाणपत्र

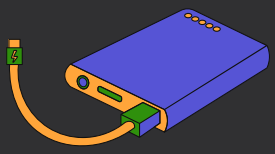
जप्ती दरम्यान उपस्थित असलेल्या साक्षीदारांची नावे

जप्तीचे कारण

शोध आणि जप्ती प्रक्रिया इलेक्ट्रॉनिक स्वरूपात किंवा शक्यतो मोबाइल फोनद्वारे रेकॉर्ड करण्याची विनंती

न्यायधीशकडे (मॅजिस्ट्रेट) नोंदणी झाल्यावर त्या नोंदीची एक कॉपी मागितली जावी

सूची:



संपूर्ण जप्त केलेल्या वस्तूंची तपशीलवार सूची मागितली [19] जावी, ज्यात चार्जर्स किंवा फोन कॅस सारखी कोणतीही साधने समाविष्ट असावीत.जप्ती का करण्यात आली याचे स्पष्ट कारण आणि कोणत्या कायद्याच्या तरतुदी अंतर्गत ही कारवाई झाली आहे हे विचारा

जप्तीचे कारण:

आपल्या उपकरणांची जप्ती का केली गेली आणि जप्ती कोणत्या कायदेशीर तरतुदीअंतर्गत केली गेली याबद्दल स्पष्टपणे चौकशी करा.

कायदेशीर सल्लागाराची उपलब्धता:

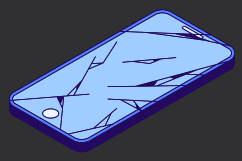
शोध घेत असताना वकीलाशी सल्ला घेण्याचा आपला हक्क ठामपणे व्यक्त करा.

वॉरंट/आदेशांची प्रती:

जर जप्ती न्यायाधीशाच्या वॉरंट [20] किंवा आदेशावर आधारित असेल, तर जप्तीला मान्यता देणाऱ्या दस्तऐवजांची प्रती मागितली जावी. वॉरंट/आदेशामध्ये उद्दिष्ट व्यक्तींच्या योग्य तपशीलांचा समावेश आहे का आणि ते संबंधित अधिकृत अधिकाऱ्यांद्वारे सही केले आहे का, याची तपासणी करा.

जप्तीची अंदाजित कालावधी:

उपकरणे किती काळ जप्त केली जातील आणि त्यांची परतफेड कशी होईल याबद्दल चौकशी करा.



स्थितीचा दस्तऐवजी करण:

आपली उपकरणे दिल्यापूर्वी, त्यांची स्थिती (उदाहरणार्थ, खुणा, डेंट्स) फोटो किंवा व्हिडिओद्वारे दस्तऐवजीकरण करण्याची मागणी करा.

अतिरिक्त कागदपत्रे:

परिस्थितीनुसार, खालील अतिरिक्त माहिती मागू शकता:

- तपास अधिकारी व त्यांची माहिती
- जप्तीशी संबंधित तक्रार किंवा प्रकरणाचा क्रमांक
- अधिकाऱ्यांनी कोणत्या धोरणांचे किंवा कार्यपद्धतींचे पालन केले त्याची प्रत.

तुमचे उपकरण परत मिळत नसेल तर काय करावे?

- तुमचे उपकरण परत मिळवण्याची प्रक्रिया न्यायालयीन सुनावणीवर अवलंबून असेल. जर तपास किंवा खटला (केस) चालू असताना तुमचे उपकरण न्यायालयात सादर केले गेले असेल, तर सुनावणी किंवा खटला पूर्ण झाल्यानंतर ते परत मिळू शकते.भारतीय नागरी सुरक्षा संहिता (बी.एन.एस.एस), 2023 मधील कलम 497 आणि 503 नुसार, न्यायालयाला यासंबंधी आदेश देण्याचा अधिकार आहे.कलम 497 मध्ये यासंदर्भात सविस्तर माहिती आणि वेळेचा उल्लेख करण्यात आला आहे.

- पण, जर तुमचं जप्त केलेलं मालमत्ता/संपत्ती कोर्टात सादर केली गेली नाही आणि मॅजिस्ट्रेटला योग्य वाटल्यास, ते एक रिटर्न ऑर्डर जारी करतील की तुमचं डिव्हाइस परत घेतासाठी तयार आहे, आणि त्यासाठी तुम्हाला ते मागवण्यासाठी सहा महिने वेळ दिला जातो. **[21]**

कुठल्या परिस्थितीतही, पोलिसांनी जप्त केलेली मालमत्ता/संपत्ती मागवण्यासाठीची प्रक्रिया तुमच्या प्रकरणाच्या विशेष परिस्थितीनुसार बदलू शकते. अशा परिस्थितीत, जर तुमचं डिव्हाइस परत घेण्यासाठी तयार असेल आणि तुम्हाला ते घेताना अडचणी येत असतील, तर लक्षात ठेवा की पोलिसांकडून जप्त केलेली मालमत्ता/संपत्ती मागवण्यासाठीची प्रक्रिया तुमच्या प्रकरणाच्या विशिष्ट परिस्थितीनुसार वेगळी असू शकते. तरीही, ह्याचं एक सामान्य आढावा पुढीलप्रमाणे आहे:

माहिती गोळा करा:

जप्त केलेल्या वस्तूंची एक यादी करा, ज्यात सीरियल नंबर, वर्णन, स्पेसिफिकेशनस आणि इतर ओळखपत्रांसह तुम्ही त्या वस्तूंचे मालक आहात हे सिद्ध करणारे कोणतेही कागदपत्र, जसं की खरेदी रशीद, विक्री बिल किंवा नोंदणी प्रमाणपत्र इत्यादी असू शकतात

पोलिस स्टेशनशी संपर्क करा:

आवश्यक माहिती गोळा केल्यानंतर, जवळच्या पोलिस स्टेशनला भेट द्या, जिथे प्रकरण नोंदवले गेले आहे किंवा जिथे तुमची मालमत्ता/संपत्ती जप्त केली गेली आहे. ऑफिसर-इन-चार्ज, किंवा तपास अधिकारी किंवा प्रॉपर्टी विभागातील कोणत्याही कर्मचाऱ्याशी बोला. तुमची परिस्थिती समजावून सांगा आणि तुमची मालमत्ता/संपत्ती परत मागण्याची विनंती करा. शांत, सभ्य आणि सहकार्यशील राहा आणि तुमच्याकडे असलेली संबंधित कागदपत्रे सादर करा.

कायदेशीर मदत घ्या:

जर पोलिस सहकार्य करत नसतील किंवा प्रक्रिया जटिल वाटत असेल, तर वकिलाची कायदेशीर मदत घेण्याचा विचार करा.

जप्त झाल्यानंतर तुमचं डिव्हाइस परत मिळाल्यावर काय करावं ?

1. सर्वसाधारण तपासणी

डिव्हाइस आणि सेवा:	पोलिसांकडून एक यादी घ्या ज्यात त्यांनी ज्या डिव्हाइसचा तपास केला किंवा जप्त केला, तसेच ज्या सेवांचा तपास केला, जसे की ईमेल, चॅट इत्यादी, त्यामुळे तुम्ही तुमच्या प्री-सीझर डेटाबेस सोबत त्याची क्रॉस-चेकिंग करु शकता.
स्टार्टअप आणि कार्यक्षमता:	डिव्हाइस पॉवर ऑन करा आणि ते सामान्यपणे बूट होते की नाही हे तपासा. मूलभूत कार्य आणि वैशिष्ट्ये जसे की इंटरनेट कनेक्टिविटी, ॲप वापर, कॅमेरा इत्यादी तपासा.
डिव्हाइस परतावा:	छापेमारीनंतर, ज्या डिव्हाइसवर जप्तीची कारवाई झाली नाही, ती तुमच्याकडे परत दिली आहे याची खात्री करा.
शारीरिक स्थिती:	डिव्हाइसवरील कोणत्याही शारीरिक नुकसानाची तपासणी करा, त्यात सील किंवा स्क्रू मध्ये बदल, नुकसान, किंवा इतर कोणतेही संशयास्पद चिन्ह असतील. डिव्हाइसवर असलेल्या कोणत्याही संशयास्पद मार्क किंवा नुकसानीची चित्रे/दस्तऐवज घ्या.
सेटिंग्ज आणि कॉन्फिगरेशन:	तपासा की कोणतीही सेटिंग्ज, ऍक्सेस कंट्रोल्स किंवा कॉन्फिगरेशन बदलली आहेत का, विशेषत: सुरक्षा, खाजगीपणा, किंवा स्थान सेवा.

जप्त झाल्यानंतर तुमचं डिव्हाइस परत मिळाल्यावर काय करावं ?

1. सर्वसाधारण तपासणी

इन्स्टॉल केलेली सॉफ्टवेअर/ ऍप्स:	तपासा की तुमच्या फोनवर नवीन सॉफ्टवेअर किंवा ऑपरेटिंग सिस्टिम इन्स्टॉल केली आहे का आणि जप्तीपूर्वी तुम्ही जो इन्स्टॉल केलेला ॲप्सचा लिस्ट होता, त्याची तुलना करा. अपरिचित किंवा संशयास्पद सॉफ्टवेअर किंवा ॲप्स स्पायवेअर आणि/किंवा मॅलवेअर असू शकतात.
असामान्य क्रियाकलाप:	तुमच्या डिव्हाइसवर काही असामान्य किंवा अज्ञात क्रियाकलाप असले, जसे की बॅटरीचा जास्त वापर, डेटा वापर, कार्यक्षमतेतील गडबड इत्यादी, तर हे स्पायवेअर आणि/किंवा मॅलवेअरचे संकेत असू शकतात.
ऑनलाइन अकाउंट्स:	जसे की ईमेल, ऑनलाइन स्टोरेज, सोशल मीडियाचे अकाउंट्स इत्यादी तपासा आणि पाहा की कोणत्याही इतर डिव्हायसवर तुमचं अकाउंट लॉगिन केलं आहे का, जे तुम्ही वापरत नाहीत. जर तुम्हाला कोणतेही अपरिचित डिव्हायस आढळले, तर ते तात्काळ काढून टाका, जेणेकरून तुमचं अकाउंट सुरक्षित होईल. हे सहसा अकाउंटच्या सुरक्षा सेटिंग्जद्वारे केलं जाऊ शकतं.

जप्त झाल्यानंतर तुमचं डिव्हाइस परत मिळाल्यावर काय करावं ?

2. डेटा इंटेग्रिटी

डेटा व्हेरिफिकेशन:	तुमचा सर्व डेटा पूर्णपिणे असलेला आहे का ते तपासा. फायली, फोटों, दस्तऐवज, मेटा डेटा आणि इतर कोणताही डेटा तपासा, जेणेकरून काहीही हरवलेले किंवा करप्ट झालेले नाही याची खात्री करा.
फाईल टाईमस्टॅम्प्स:	तुमच्या डिव्हाइसवरील महत्त्वाच्या फायली आणि दस्तऐवजांचे टाईमस्टॅम्प्स तपासा, कारण बदललेले टाईमस्टॅम्प्स अवैध प्रवेश किंवा बदल सूचित करू शकतात.
फाईल हॅशेस:	जप्तीपूर्वी आणि नंतर महत्त्वाच्या फायलींचे क्रिप्टोग्राफिक हॅशेस तयार करा आणि त्यांची तुलना करा. तफावत म्हणजे फाईलमध्ये बदल किंवा बदल केल्याचे संकेत असू शकतात.
फॉरेन्सिक टूल स्कॅन्स:	तुमच्या डिव्हाइसवर लपवलेली फायली, स्पायवेअरचे किंवा रूटकिटचे ट्रेसेस शोधण्यासाठी अँटी-मॅलवेअर आणि फॉरेन्सिक सॉफ्टवेअर वापरण्याचा विचार करा. हे टूल्स जटिल असू शकतात, त्यामुळे डेटा रिकव्हरी किंवा सायबर सुरक्षा तज्ञाची मदत घेणं उपयुक्त ठरू शकतं.

जप्त झाल्यानंतर तुमचं डिव्हाइस परत मिळाल्यावर काय करावं ?

3. अतिरिक्त गोष्टी:

बॅकअप लॉग्स:	जर तुमच्या डिव्हाइसला हे समर्थन असेल, तर तपासा की जप्तीच्या कालावधीत कोणत्याही बॅकअप लॉग्स किंवा सिस्टम लॉग्समध्ये असामान्य किंवा अवैध क्रियाकलाप दिसतात का.
क्लाऊड स्टोरेज:	तुमच्या डिव्हाइसशी संबंधित क्लाऊड स्टोरेज अकाउंट्स पुन्हा पाहणी करा आणि कोणत्याही अवैध प्रवेश किंवा बदलांचा तपास करा.
दस्तऐवजीकरण:	तुमच्या शोधांची तपशीलवार नोंद ठेवा, ज्यात टाईमस्टॅम्प्स, स्क्रीनशॉट्स, आणि संशयास्पद क्रियाकलापांची नोंद असू शकते. हे दस्तऐवजीकरण महत्त्वाचं ठरू शकतं, जर तुम्हाला कायदेशीर कारवाई करायची असेल तर.
पासवर्ड व्यवस्थापन:	तुमच्या डिव्हाइसशी संबंधित सर्व पासवर्ड्स आणि कोणत्याही ऑनलाइन अकाउंट्सचे पासवर्ड बदलून टाका, कारण तुमचे पासवर्ड्स कदाचित अधिकाऱ्यांनी जप्त केले असू शकतात.

खंड 5
प्रिपेअर्डनेस:
तुमच्या डिव्हायसचं संरक्षण

आजच्या डिजिटल जगात, आपले डिव्हायस आणि डेटा प्रचंड प्रमाणात माहिती साठवतात.

हे महत्त्वाचे आहे की आपले डिव्हायस सुरक्षित ठेवले जातील, जेणेकरून आपला डेटा सुरक्षित राहील.

या धमक्या विरुद्ध तयार राहणं साधं आणि अत्यंत महत्त्वाचं आहे. विचार करा, जर तुमचा फोन हॅक झाला आणि तुमच्या सर्व संदेश उघड झाले तर काय होईल! मजबूत पासवर्ड्स वापरून, ऑनलाईन काय शेअर करता ते लक्षात ठेवून, आणि सॉफ्टवेअर अपडेट ठेवून, तुम्ही तुमच्या डिजिटलीक सूटसाठी एक मजबूत लॉक तयार करता. लक्षात ठेवा, थोडी जागरूकता तुमच्या ऑनलाइन जीवनाला सुरक्षित ठेवण्यात खूप मदत करते. खाली दिलेल्या काही उत्तम पद्धती आहेत ज्यामुळे तुम्ही तुमचा डेटा सुरक्षित ठेवू शकता.

तुमच्या ऑनलाइन क्रियाकलापांना सुरक्षित ठेवा. | इथे कसं करायचं:

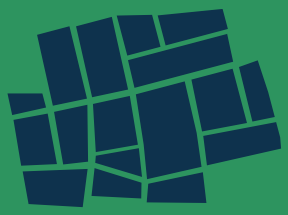
स्वत:ला लपवा:

तुम्ही VPNs आणि Tor चा वापर करून तुमच्या ऑनलाइन क्रियाकलापांना सुरक्षित करू शकता. हे अगदी जसं एक गुप्त एजंट त्याच्या गुप्त मिशनसाठी वेष बदलतो तसं आहे.

VPNs

तुमच्या इंटरनेट ट्रॅफिकसाठी एक सुरक्षित सुरंग समजा. हे तुमच्या वास्तविक स्थानाला लपवते आणि तुमचा डेटा एन्क्रिप्ट करते, ज्यामुळे तो गुप्त कोड होतो, जो फक्त तुम्ही आणि VPN उघडू शकता. एक विश्वासार्ह VPN सेवा निवडा जी तुमच्या क्रियाकलापांचा रेकॉर्ड ठेवत नाही.

Tor



एक गुप्त मार्गांच्या भूलभूलैयात समजा. Tor तुमच्या इंटरनेट ट्रॅफिकला एन्क्रिप्टेड रिलेच्या अनेक स्तरांमधून धक्का देतो, ज्यामुळे ट्रॅक करणे जवळपास अशक्य होईल. अतिरिक्त गोपनीयतेसाठी Tor ब्राउझर डाउनलोड करा.

समजून वापरा:

सर्व सर्च इंजिन समान नाहीत. काही, जसे DuckDuckGo, गोपनीयतेला प्राधान्य देतात आणि तुमच्या शोधांचा मागोवा घेत नाहीत. जरी तुमचा ब्राउझर इतिहास जतन करत असेल, तरीही POST रिक्वेस्टसह सर्च इंजिन वापरून तुमच्या शोधांना लपवता येईल.

इन्कॉग्निटो मोड वापरा:

तुमच्या ब्राउझरमधील "इन्कॉग्निटो मोड" ला गुप्त एजंटच्या मास्कसारखं समजा. हे तुमचा ब्राउझिंग इतिहास, कुकीज, आणि फॉर्म डेटा सेव्ह होऊ देत नाही, ज्यामुळे कोणालाही तुमच्या ऑनलाइन साहसांची पाहणी करणे कठीण होईल.

जागरूक रहा:

लक्षात ठेवा, या सर्व साधनांसह देखील, परिपूर्ण गोपनीयता एक आभास आहे. तुम्ही कोणती वेबसाइट्स भेट देता, त्यावर सावध रहा, नेहमी सुरक्षित कनेक्शनला प्राधान्य द्या (लॉक आयकॉन पाहा!), आणि आवश्यक नसल्यास ऑनलाइन वैयक्तिक माहिती शेअर करणं टाळा.

गती विरुद्ध गोपनीयता:

VPNs आणि Tor इंटरनेटचा वेग थोडा कमी करू शकतात कारण एन्क्रिप्शन आणि रीराउटिंग होते. हे एक समतोल आहे: थोडी कमी गती, पण खूप जास्त गोपनीयता. तुमच्यासाठी काय सर्वोत्तम काम करते ते निवडा.

बोनस टिप: तुम्ही वापरत असलेल्या कोणत्याही साधनाच्या गोपनीयता धोरणे आणि सेवा अटी तपासणे नेहमी महत्त्वाचे आहे, जेणेकरून तुम्हाला समजेल की ते तुमच्या डेटाशी कसं वागतात. या सोप्या पद्धती फॉलो करून, तुम्ही तुमच्या ऑनलाइन गोपनीयतेवर नियंत्रण ठेवू शकता आणि तुमचं डिजिटल जीवन तुमच्या स्वतःच्या लॉक आणि की वाट ठेवू शकता. लक्षात ठेवा, जेम्स बॉण्डला देखील कधी कधी चांगली गुप्तवेष लागते!

कामाच्या डिव्हायस आणि वैयक्तिक डिव्हायस

कल्पना करा, तुमच्याकडे दोन सूटकेस आहेत: एक तुमच्या ऑफिसच्या कामासाठी आणि दुसरं तुमच्या वैयक्तिक साहसांसाठी. तुमचं कामाचं लॅपटॉप आणि फोन वेगळं ठेवणं म्हणजे ते वेगळे सूटकेस असणं – हे तुम्हाला व्यवस्थित राहायला मदत करतं आणि तुमच्या व्यावसायिक आणि वैयक्तिक जीवनाचं संरक्षण करतं.

तुमच्या वैयक्तिक आणि व्यावसायिक जीवनासाठी वेगवेगळ्या डिव्हायसचा वापर करण्याचा विचार करा.

A. डेटा डिटेक्टिव्ह:
वेगवेगळ्या डिव्हायसचा वापर करून, तुम्ही तुमच्या वैयक्तिक आणि व्यावसायिक डेटाच्या मिसळण्याचा धोका कमी करतो, ज्यामुळे सुरक्षा वाढते आणि दोन्हीच्या गोपनीयतेचं संरक्षण होतं. कामासाठी आणि वैयक्तिक गोष्टींसाठी वेगवेगळे डिव्हायस वापरून, तुम्ही खरंतर डेटा डिटेक्टिव्ह बनता! तुम्ही तुमच्या कामाच्या फाईल्सला तुमच्या वैयक्तिक फोटोंमध्ये घुसण्यापासून थांबवता आणि उलट देखील. यामुळे सर्वकाही सुरक्षित आणि गोपनीय राहते, जणू दोन बंद सूटकेस आहेत आणि वेगवेगळ्या चावी सह लॉक केलेली आहेत.

B. ॲक्सेस कंट्रोल निंजा:
स्पष्ट विभाजन केल्यामुळे संवेदनशील कामाशी संबंधित माहितीवर ॲक्सेस नियंत्रित करणे सोपे जाते, त्यामुळे चुकून माहिती उघड होण्याचा किंवा डेटा लीक होण्याचा धोका कमी होतो. तुमच्या कामाच्या आणि वैयक्तिक डिव्हायसना वेगळं ठेवणं म्हणजे तुमच्या ऑफिस सूटकेससाठी गुप्त कोड ठेवणं. फक्त अधिकृत लोक (जसं की तुम्ही आणि तुमचा बॉस) च तुमच्या कामाच्या गोष्टींना ॲक्सेस करू शकतात, आणि तुमची वैयक्तिक सूटकेस तुमच्यासाठीच गोपनीय राहते. यामुळे चुकून लीक होणं किंवा गुपचूप पाहणं रोखता येतं, ज्यामुळे तुमचं काम सुरक्षित आणि व्यवस्थित राहातं.

C. जबाबदारी चॅम्पियन:
डिव्हायस वेगळं ठेवणं म्हणजे कामाशी संबंधित कार्यं आणि डेटासाठी स्पष्ट मालकी आणि उत्तरदायित्व ठरवणं. वेगवेगळे डिव्हायस असणं म्हणजे कोणाला काय जबाबदारी आहे हे स्पष्ट होतं. हे अगदी सूटकेस लेबल करण्यासारखं आहे – प्रत्येकाला माहित असतं की ऑफिसमधील सूटकेस तुम्हाला आहे, आणि वैयक्तिक सूटकेस तुम्ही त्यात तुमचं मनाप्रमाणे भरू शकता. यामुळे कार्य ट्रॅक करणं आणि जबाबदारी ठेवणं सोपं होतं, तुम्हाला आणि तुमच्या सहकाऱ्यांना.

लक्षात ठेवा: तुमच्या कामाच्या आणि वैयक्तिक डिव्हायसला वेगळं ठेवणं फक्त दोन गॅझेट्स असण्याबद्दल नाही – हे तुमच्या गोपनीयतेचं संरक्षण करणं, व्यवस्थित राहणं, आणि तुमचं जीवन सोपं करणं आहे. म्हणून, पुढे जा, डेटा डिटेक्टिव्ह, ॲक्सेस कंट्रोल निंजा, आणि जबाबदारी चॅम्पियन बन! आणि तुमच्या सूटकेसला लेबल लावायला विसरू नका!

बोनस टिप: वेगवेगळ्या डिव्हायससह देखील, ऑनलाइन काय शेअर करता आणि कोणाला ॲक्सेस देता, याबद्दल नेहमी जागरूक राहा. कोणतीही प्रणाली पूर्णपणे सुरक्षित नाही, त्यामुळे सतर्क रहा आणि तुमच्या डिजिटल साहसांचा आनंद घ्या!

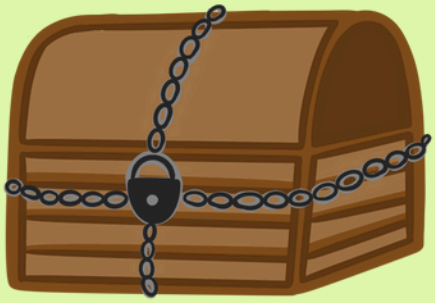
तुमच्या डेटाचं रक्षण करा जसं ते एक ठोस खजिना आहे: एन्क्रिप्शनच्या थरांची मार्गदर्शिका

तुमच्या डेटाला एक खजिना समजा जो महत्त्वाच्या गुप्त गोष्टींनी भरलेला आहे. त्या गुप्त गोष्टी सुरक्षित ठेवण्यासाठी, तुम्हाला अनेक लॉक्सची गरज आहे, नाही का?

इथे एन्क्रिप्शनचे थर कामाला येतात!

पूर्ण खजिना लॉक (FDE):

- तुमच्या संपूर्ण हार्ड ड्राइव्हला एन्क्रिप्ट करा, जसं तुमच्या संपूर्ण खजिन्याच्या पेटीवर एक मोठं, मजबूत लॉक लावणं.
- BitLocker (Windows), FileVault (macOS), किंवा VeraCrypt सारख्या साधनांचा वापर करा.

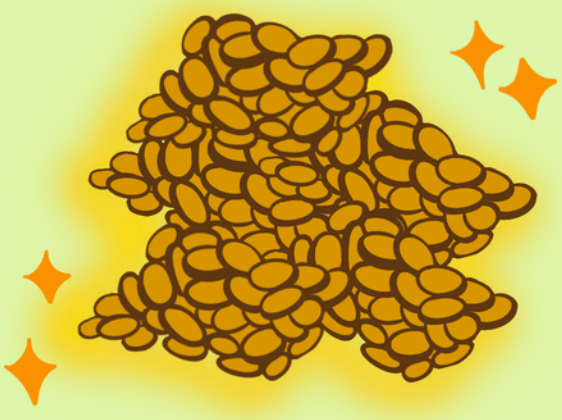


गुप्त कक्षाच्या लॉक्स (OS-स्तरीय):

- macOS वर गुप्त बॉक्ससारख्या एन्क्रिप्टेड डिस्क इमेजेस तयार करा.
- काही ऑपरेटिंग सिस्टम्सवर एन्क्रिप्टेड फाइल सिस्टम्सचा वापर करा (जसं गुप्त कक्ष).

वैयक्तिक रत्नाच्या पिशव्या (ॲप-स्तरीय):

- विशिष्ट रत्न (पासवर्ड्स, नोट्स, संदेश) ॲप्सच्या मदतीने सुरक्षित करा ज्यामध्ये बिल्ट-इन एन्क्रिप्शन आहे.
- पासवर्ड मॅनेजर्स, सुरक्षित नोट-टेकिंग ॲप्स, आणि एंड-टू-एंड एन्क्रिप्शन असलेली मेसेंजिंग ॲप्स (उदाहरणार्थ, Signal, WhatsApp) याचा विचार करा.



महत्वाच्या गोष्टी:

- प्रत्येक लॉक (एन्क्रिप्शन थर) साठी मजबूत, अद्वितीय पासवर्ड किंवा की वापरा.
- तुमचं सॉफ्टवेअर नियमितपणे अपडेट करा, जेणेकरून तुमचे लॉक चमचमीत आणि सुरक्षित राहतील.
- तुमचे एन्क्रिप्टेड डेटा (खजिन्याच्या नकाशा!) चं बॅकअप करा, कधीतरी तुम्हाला ते पुन्हा मिळवायचं असल्यास.

हे एन्क्रिप्शन लॉक लावून, तुम्ही तुमच्या डेटासाठी एक चावी तयार कराल, ज्यामुळे कोणालाही तुमचे डिजिटल खजिने चोरणे खूप कठीण होईल!

गोपनीयता आणि सायबरसुरक्षा सुनिश्चित करणे: ऑनलाइन आणि ऑफलाइन

- डिस्पीअरींग मेसेजिंग सेवा किंवा ॲप्सचा वापर करा, जे आपोआप पाठवलेले मेसेजेस त्यांचे वाचन झाल्यानंतर किंवा एक निश्चित कालावधीनंतर हटवतात. Signal, Telegram, WhatsApp अशा ॲप्समध्ये डिस्पीअरींग मेसेज फीचर्स असतात, ज्यामुळे संवाद तात्पुरता राहतो आणि वाचल्यानंतर किंवा निश्चित कालावधीनंतर ते चॅट्स किंवा इतिहासात राहत नाहीत.

- ओळख प्रमाणिकरणासाठी पासवर्ड किंवा PIN वापरा, फिंगरप्रिंट किंवा फेस ID ओळख वापरण्याऐवजी, कारण ह्या पद्धतींसाठी मानसिक ध्यान किंवा स्पष्ट सहमतीची आवश्यकता नाही. पासवर्ड किंवा PIN चा वापर केल्याने संवेदनशील माहिती किंवा डिव्हायसवर ॲक्सेस फक्त वापरकर्त्याद्वारे दिलेल्या माहितीवर अवलंबून राहतो, ज्यामुळे नियंत्रण आणि सुरक्षा वाढवते, आणि प्रमाणिकरणासाठी स्पष्ट क्रिया आणि सहमती आवश्यक ठरते.

- पासवर्ड मॅनेजरचा वापर करून तुमचे काही पासवर्ड सुरक्षितपणे साठवून, बाकीचे पासवर्ड लक्षात ठेवणे हे सुरक्षा वाढवण्यासाठी चांगली रणनीती आहे. पासवर्ड मॅनेजर मध्ये "12345" सारखा एक भाग सुरक्षितपणे साठवून आणि "fdsjrie" सारखा दुसरा भाग लक्षात ठेवून, तुम्ही संपूर्ण पासवर्ड "12345fdsjrie" तयार करू शकता. ह्या पद्धतीने सुरक्षा आणि सोयीचं संतुलन साधलं जातं, कारण तुम्ही पासवर्ड मॅनेजरच्या एन्क्रिप्शनच्या फायदे आणि तुमच्या स्मरणशक्तीच्या मदतीने एक अद्वितीय भाग लक्षात ठेवता, ज्यामुळे अवैध वापरकर्त्यांना तुमच्या खात्यांमध्ये प्रवेश मिळवणं खूप कठीण होतं.

- पासवर्ड मॅनेजर वापरून '12345' ह्या भागाला सुरक्षितपणे ठेवून आणि 'fdsjrie' ह्या दुसऱ्या भागाला लक्षात ठेवून तुम्ही पूर्ण पासवर्ड '12345fdsjrie' तयार करू शकता. ह्या पद्धतीने तुमच्या पासवर्डचा सुरक्षा आणि आराम दोन्ही साधता येतात, कारण पासवर्ड मॅनेजरच्या एन्क्रिप्शनचा (Encryption) फायदा आणि तुमचं लक्षात ठेवण्याची क्षमता दोन्ही वापरता येतात. यामुळे बिना परवानगी असलेल्या लोकांना तुमच्या खात्यात प्रवेश करणे कठीण होऊन जातं.

- 2FA (टू-फॅक्टर ऑथेंटिकेशन) लागू करणं तुमच्या खात्याच्या सुरक्षा वाढवण्यास मदत करतं. SMS किंवा Email आधारित 2FA पेक्षा TOTP (टाइम-बेस्ड वन-टाइम पासवर्ड) आधारित 2FA वापरणं जास्त सुरक्षित आहे. TOTP एक वेगळा कोड जनरेट करतं जो नियमित अंतराने बदलत राहतो, साधारणतः प्रत्येक 30 सेकंदांनी, ज्यामुळे बिना परवानगी असलेल्या लोकांकडून प्रवेश करण्यापासून तुमचं खातं अधिक सुरक्षित राहतं.

- गुगल ऑथेंटिकेटर, ऑथी, किंवा मायक्रोसॉफ्ट ऑथेंटिकेटर सारखी ऑथेंटिकेटर ॲप्स वापरणं, जे TOTP कोड्स जनरेट करतात, हे जास्त सुरक्षित पर्याय आहे. ह्या ॲप्स वेळेवर आधारित कोड तयार करतात जे तुमच्या खात्यांशी जोडलेले असतात आणि SMS किंवा ईमेल सारख्या संवाद माध्यमांवर अवलंबून नसतात, ज्यामुळे SMS आधारित 2FA मध्ये होणाऱ्या इंटरसेप्शन किंवा SIM स्वॅपिंग अटॅक्सचा धोका कमी होतो.

- TOTP आधारित 2FA वापरून, तुम्ही एक अतिरिक्त सुरक्षा स्तर जोडता, ज्यामुळे तुमच्या खात्यांमध्ये बिना परवानगी प्रवेश होण्याची शक्यता मोठ्या प्रमाणात कमी होते, आणि विविध सायबर धमक्यांपासून अधिक मजबूत संरक्षण मिळतं.

- फायली डिलीट करणं तुमची रहस्य खरंच सुरक्षित करण्यासाठी पुरेसं नाही! फक्त 'डिलीट' बटणावर क्लिक करणं म्हणजे त्या फायली कायमच्या नष्ट होणार नाहीत. त्या अजून तुमच्या डिव्हाइसवर लपलेल्या असतात, खास टूल्स वापरून त्या सापडू शकतात. खरंच गोपनीयता राखण्यासाठी, तुम्हाला त्या फायली नष्ट करण्याची गरज आहे. जसं कागदपत्र फाडणे - त्यांना पुन्हा जोडणं जवळपास अशक्य आहे! जस की शेडिंग सॉफ्टवेअर तुमच्या फायलींना रँडम अक्षरे आणि नंबर सह ओव्हरराइट करतं, ज्यामुळे त्या गोंधळलेल्या आणि वाचायला अशक्य होतात. हे असं मानू की शेड केलेल्या कागदाच्या तुकड्यांना फेकून, ते जमिनीत खोलवर गाडून टाकणं. कोणीही ते उकरून तुझं गुपित वाचू शकत नाही! त्यामुळे, पुढच्या वेळी जर तुम्हाला काही संवेदनशील डिलीट करायचं असेल, तर 'Delete' बटण वगळा आणि शेडिंग सॉफ्टवेअर वापरा. हे तुमचं डिजिटल जीवन सुरक्षित आणि गोपनीय ठेवण्याचा सर्वोत्तम मार्ग आहे.

- Tor वापरून वेबसाईट्स वापरणं तुमची गोपनीयता आणि सुरक्षा वाढवते. उदाहरणार्थ, तुम्ही Tor वापरून "द गार्डियन" (The Guardian) सारख्या न्यूज साईट्स किंवा Twitter सारख्या सोशल मीडिया साइट्सला भेट देऊ शकता, ज्यामुळे तुमचं नाव ओळखलं जाण्याची शक्यता कमी होते.

गोप्यापण ठेवणं: ऑनलाइन आणि ऑफलाइन

ऑनलाइन:

- **क्रिप्ट.ee:** हे ॲनॉनिमस साइन अप करण्याची, एंड-टू-एंड एन्क्रिप्शनची आणि अधिक गोपनीयतेसाठी लपवलेली फोल्डर्स तयार करण्याची सुविधा देते.
- **क्रिप्टोमेटर:** हे तुमच्या वैयक्तिक फाइल्सना एन्क्रिप्ट करून सुरक्षित ठेवतं.

ऑफलाइन:

- **वेराक्रिप्ट:** ड्राइव्ह्स किंवा स्टोरेज डिव्हाइसवर डेटा सुरक्षित करण्यासाठी लपवलेल्या पार्टिशन्स तयार करा.
- **सीक्रेट कंपार्टमेंट्स:** फर्निचर किंवा वस्तूंत लपवलेल्या कंपार्टमेंट्स मध्ये मौल्यवान वस्तू लपवा.
- **सायफर सिस्टिम:** वैयक्तिक कोड्स किंवा सायफर्स तयार करा जेणेकरून लिहिलेली माहिती किंवा मालमत्ता एन्क्रिप्ट आणि सुरक्षित केली जाऊ शकतील.

ही पद्धती डिजिटल आणि भौतिक दोन्ही ठिकाणी गोपनीयता आणि सुरक्षा वाढवतात, ज्यामुळे संवेदनशील माहितीचे संरक्षण करण्याचे मार्ग मिळतात.

जास्त वापरली जात नसलेली फायली सुरक्षित ठिकाणी (एन्क्रिप्टेड ड्राइव्ह किंवा क्लाऊड) संग्रहित करा आणि तुमचं डिजिटल डेस्क नियमितपणे स्वच्छ ठेवा, फक्त आज तुम्हाला लागणाऱ्या गोष्टी ठेवा. जुन्या आवृत्त्या कॉपी करणं सोडून, त्यांचा आर्काइव्ह करा, ज्यामुळे तुमचं डिजिटल जीवन सुव्यवस्थित आणि सुरक्षित राहील.

तुमचं डिजिटल ठसा न सोडता साइटमध्ये सामील होऊ इच्छिता का? अशी साइट्स निवडा जी:

- कमी माहिती मागतात: फक्त एक यूझरनेम आणि कदाचित ईमेल, जणू काही गुप्त हँडशेक.
- तुम्हाला अदृश्य होण्याची परवानगी देतात: नाव नाही? चिंता करू नका! काही साइट्स तुम्हाला तुमचं नाव न सांगता साइन अप करण्याची परवानगी देतात.
- बनावट ईमेल पत्ते देतात: "थ्रो-अवे" ईमेल वापरून सामील व्हा, तुमचं खरे ईमेल गुप्त ठेवून.

शब्दसूची

ऑडिओ-व्हिडिओ इलेक्ट्रॉनिक: याचा अर्थ म्हणजे कोणत्याही प्रकारच्या संवाद साधण्याच्या साधनांचा वापर, जसे व्हिडिओ कॉन्फरन्सिंग, ओळख प्रक्रियांची नोंद, शोध आणि जप्ती, पुरावे गोळा करणे, इलेक्ट्रॉनिक संवाद प्रसारित करणे, आणि राज्य सरकारच्या नियमांनुसार इतर वापर.

गिरफतारी: जेव्हा एखाद्या व्यक्तीला कायदेशीर ताब्यात घेतलं जातं आणि ती अटक केली जाते, हे त्या व्यक्तीवर कोणताही आरोप किंवा आरोप नसतानाही होऊ शकतं, त्याला अटक झालं असे म्हणतात. एखादी व्यक्ती आरोप दाखल न करता किंवा वॉरंटशिवायही अटक केली जाऊ शकते (संदर्भ घ्या: संज्ञेय अपराध).

जामिनार्ह अपराध: जे अपराध गंभीर किंवा गंभीर नसतात आणि ज्यासाठी आरोपी/गिरफतार केलेल्या व्यक्तीला जामिनाची मागणी करण्याचा हक्क असतो, त्यांना जामिनार्ह अपराध म्हणतात. एक तपास अधिकारी जामिनार्ह अपराधांसाठी जामीन मंजूर करण्याची जबाबदारी आहे, सामान्यत: जामिनाच्या बंधनामध्ये काही अटी ठरवून. तथापि, जामीन मंजूर करणं म्हणजे आरोपी स्वतंत्र झालं असं नाही, कारण त्यांना न्यायिक परीक्षण पार करावं लागेल.

आरोप: आरोप म्हणजे एक कायदेशीर आरोप की व्यक्तीने एखादा अपराध केला आहे, जो प्रॉसिक्युटर किंवा पोलिस/तपासणी अधिकारी यांच्याद्वारे केला जातो. [23] यासाठी व्यक्तीला त्यांच्यावर केलेल्या आरोपांची कारणे सांगणे आवश्यक असते.

संज्ञेय अपराध: असे अपराध ज्यासाठी पोलिस अधिकारी वॉरंट किंवा न्यायालयाच्या पूर्व परवानगीशिवाय अटक करू शकतात, ते संज्ञेय अपराध आहेत. [24] हे तेव्हा घडते जेव्हा FIR (प्रथम माहिती रिपोर्ट) दाखल केलेला असो किंवा नसो, आणि सामान्यत: हे अधिक गंभीर किंवा खूप गंभीर स्वरूपाच्या अपराधांसाठी लागू असते.

कंप्युटर: याचा अर्थ आहे, कोणताही इलेक्ट्रॉनिक, मॅग्नेटिक, ऑप्टिकल किंवा इतर उच्च-गती डेटा प्रोसेसिंग साधन किंवा सिस्टम, जो इलेक्ट्रॉनिक, मॅग्नेटिक किंवा ऑप्टिकल इम्पल्स वापरून लॉजिकल, अंकगणितीय आणि मेमोरीचे काम करतो, आणि यामध्ये सर्व इनपुट, आऊटपुट, प्रोसेसिंग, स्टोरेज, सॉफ्टवेअर किंवा संवाद साधण्याच्या साधनांचा समावेश असतो, जे कंप्युटर सिस्टम किंवा नेटवर्कमध्ये जोडलेले किंवा संबंधित असतात

संवाद साधण्याचे साधन: हे एक सेल फोन, व्यक्तिगत डिजिटल सहाय्यक साधन किंवा दोन्हींचे मिश्रण असू शकते, किंवा कोणतेही असे साधन जे संवाद साधण्यासाठी, लेख, व्हिडिओ, आवाज किंवा चित्र पाठवण्यासाठी किंवा प्रसारित करण्यासाठी वापरले जाते.

कुकीज: वेबसाईटवर तुमच्या क्रियाकलापांची माहिती/डेटा ट्रॅक करणारे छोटे फायली म्हणजे कुकीज. त्यांचा वापर जाहिराती आणि विश्लेषण सेवा साठी वापरला जातो, ज्यामुळे वापरकर्त्यांचे क्रियाकलाप नोंदवले जातात. कुकीजमध्ये वापरकर्त्यांची वैयक्तिक माहिती, जसे की त्यांचे यूझरनेम, पासवर्ड, कस्टमायझ्ड प्राधान्ये, वेब क्रियाकलाप इत्यादी असू शकतात आणि जर ती असुरक्षित असतील, तर त्या वापरकर्त्यांसाठी सुरक्षा आणि गोपनीयतेस धोका निर्माण करू शकतात.

शब्दसूची

इलेक्ट्रॉनिक संवाद: याचा अर्थ आहे कोणतीही लिखित, शब्द, चित्रात्मक, किंवा व्हिडिओ माहिती जी इलेक्ट्रॉनिकद्वारे शेअर केली जाते, मग ती लोकांमध्ये किंवा उपकरणांमध्ये असो, ज्यामध्ये फोन, कंप्युटर, ऑडिओ-व्हिडिओ प्लेअर, कॅमेरे, किंवा इतर इलेक्ट्रॉनिक उपकरणांचा वापर केला जातो, किंवा केंद्रीय सरकाराने दिलेल्या इतर कोणत्याही इलेक्ट्रॉनिक स्वरूपात.

एन्क्रिप्शन: ही एक प्रक्रिया आहे ज्यामध्ये वैयक्तिक किंवा संवेदनशील माहिती कोड किंवा गूढ स्वरूपात संग्रहित केली जाते, जी फक्त त्या व्यक्तीला डिक्रिप्शन चाबी वापरून उघडता येऊ शकते, ज्याच्याकडे त्या चाबीचा प्रवेश असतो. यामुळे वैयक्तिक आणि संवेदनशील माहितीचे प्रक्रिया, संग्रहण आणि हस्तांतरण अधिक सुरक्षित आणि संरक्षित होते, कारण हे कोणत्याही अनधिकृत व्यक्तीला डेटा ऍक्सेस किंवा समजून घेण्यापासून रोखते.

पुरावा: म्हणजे कोणतंही विधान, जे ओरल किंवा दस्तऐवजीक स्वरूपात (लिखित किंवा इलेक्ट्रॉनिक, आणि यामध्ये डिजिटल उपकरणं देखील समाविष्ट आहेत) असू शकतं, जे चौकशी किंवा तपासणीशी संबंधित असू शकतं. अशा दस्तऐवजांना दस्तऐवजी पुरावा म्हणतात. पुरावा आणि प्रमाण वेगळे आहेत, कारण पुरावा नक्कीच अंतिम ठरवणारा नसतो आणि तो न्यायालयाच्या निर्णयावर अवलंबून असतो.

तपासणी अधिकारी: एक पोलिस अधिकारी जो एखाद्या अपराधाची तपासणी करण्यासाठी नियुक्त केलेला असतो.

गत्यशील संपत्ती: बी.एन.एस.मध्ये गत्यशील संपत्ती अशी परिभाषित केली आहे, ज्यात प्रत्येक प्रकारच्या संपत्तीचा समावेश होतो, जसे की खिडक्या, दरवाजे, झाडे इत्यादी, परंतु यामध्ये पृथ्वीला जोडलेली किंवा पृथ्वीला जोडलेल्या कोणत्याही गोष्टीला स्थायीपणे बांधलेली वस्तू समाविष्ट नाही. गत्यशील संपत्ती यामध्ये सर्व इलेक्ट्रॉनिक आणि डिजिटल उपकरणांचा समावेश होईल, जे पृथ्वीला जोडलेले नाहीत. [25]

नॉन-बेलीयबल अपराध: असे अपराध जे अधिक गंभीर किंवा खूप गंभीर असतात आणि ज्यासाठी आरोपी/गिरफतार केलेल्या व्यक्तीला जामिनाची मागणी करण्याचा हक्क नसतो. असे अपराध जामिनार्ह नसतात. तरीही, न्यायालय त्याच्या निर्णयावरून जामीन मंजूर करू शकते, हे आरोपीच्या पळून जाण्याचा धोका, कायदेशीर प्रक्रिये मध्ये सहकार्य न करण्यासारख्या बाबींवर अवलंबून असते.

नॉन-संज्ञेय अपराध: असे अपराध ज्यासाठी पोलिस अधिकारी वॉरंट किंवा न्यायाधीशाची पूर्व परवानगी न घेता अटक करू शकत नाहीत, ते नॉन-संज्ञेय अपराध आहेत. [26] हे तेव्हा घडते जेव्हा FIR (प्रथम माहिती रिपोर्ट) दाखल केला जातो आणि वॉरंट मिळवला जातो, आणि सामान्यत: हे कमी गंभीर किंवा खूप गंभीर नसलेल्या अपराधांसाठी लागू असते.

ठिकाण: बी.एन.एस.एस अंतर्गत, ठिकाण म्हणजे घर, इमारत, तंबू, वाहन आणि जलयान. [27]

सार्वजनिक ठिकाण: { Public Place } यामध्ये सार्वजनिक वाहतूक, हॉटेल्स, दुकाने किंवा सार्वजनिक वापर किंवा प्रवेशासाठी असलेले इतर कोणतेही ठिकाण समाविष्ट आहे. [28]

शब्दसूची

जप्ती मेमो: जर तपासणी अधिकारी एखाद्या आरोपीकडून तपासणीसाठी कोणतीही संपत्ती (मूल्यवान किंवा अमूल्य) जप्त करतो, तर ती जप्ती मेमोत नोंदवली आणि रेकॉर्ड केली जाते. यामध्ये संपत्तीचे सर्व तपशील/विशेषत: तपशील, संग्रहणाचे ठिकाण, जप्ती संबंधित प्रकरणाचे तपशील इत्यादी असतात.

वॉरंट: वॉरंट हे एक दस्तऐवज असतो ज्यावर न्यायाधीशाचा सही असतो, ज्याद्वारे पोलिसांना तुम्हाला अटक करण्याची किंवा तुमच्या संपत्तीची तपासणी करून काही वस्तू घेण्याची परवानगी मिळते. तुम्हाला वॉरंट पाहण्याचा हक्क आहे आणि त्याची वैधता तपासणे आवश्यक आहे.

पूरक माहिती

शोध आणि जप्तीबद्दल काही नोट्स:

1. पूर्वी, न्यायालयांनी ठरवले होते की, अनधिकृत आणि चुकीच्या पद्धतीने मिळवलेला पुरावा admissible (स्वीकारायोग्य) असू शकतो. तथापि, अशा पुराव्याला खरे आणि न बदललेले असल्याचे सिद्ध करणे आवश्यक आहे. पुराव्याची स्वीकार्यता फक्त न्यायालयेच ठरवू शकतात - प्रत्येक प्रकरणाच्या तथ्यांवर आणि परिस्थितींवर आधारित. [उमेश कुमार वि. आंध्र प्रदेश राज्य, (2013) 10 SCC 169]

2. तथापि, केरळ उच्च न्यायालयाने ठरवले की, पोलिस अधिकारी पत्रकाराचा मोबाईल फोन त्याच्याशी संबंधित क्रिमिनल प्रक्रिया संहिता (आता बी.एन.एस.एस) मध्ये नमूद केलेल्या पद्धतींचे पालन न करता जप्त करू शकत नाहीत. जर अशा उपकरणाची आवश्यकता गुन्ह्याच्या तपासणीसाठी असेल, तर पोलिस अधिकाऱ्यांनी त्या उपकरणाच्या योग्य तपासणी आणि जप्तीसाठी क्रिमिनल प्रक्रिया संहिता (आता बी.एन.एस.एस) चे पालन करणे आवश्यक आहे. **[29]**

3. दिल्ली उच्च न्यायालयाने देखील ठरवले आहे की, कोणत्याही व्यक्तीला आपला पासवर्ड (किंवा अन्य कोणतेही तपशील) देण्यास बळजबरी केली जाऊ शकत नाही, कारण भारतीय संविधानाच्या अनुच्छेद 20(3) अंतर्गत आत्म-आपराध सिद्धीपासून संरक्षण आहे. **[30]**

4. त्याचप्रमाणे, दिल्लीतील रौझ अव्हेन्यू जिल्हा न्यायालयाच्या विशेष CBI न्यायालयाने ठरवले की, आरोपीला अशा माहिती देण्यासाठी बळजबरी केली जाऊ शकत नाही आणि याबाबतीत त्याला भारतीय संविधानाच्या अनुच्छेद 20(3) तसेच बीएनएसएसच्या कलम 180(2) ने संरक्षण मिळते. **[31]**

5. सर्च आणि जप्तीच्या प्रक्रियेची समजून घेणे केवळ अशा तीव्र परिस्थितींमध्ये गोंधळ टाळण्यात मदत करणार नाही, तर अधिकाऱ्यांशी चांगले सहकार्य करण्यास देखील मदत करेल. याव्यतिरिक्त, अशा प्रक्रिया जाणून घेणे व्यक्तींना कायदा आणि सुव्यवस्था राखण्याची जबाबदारी असलेल्या लोकांकडून होणाऱ्या वाईट वागणुकीपासून संरक्षण करू शकते.

इलेक्ट्रॉनिक उपकरणे आणि कायदा

या बाबतीत न्यायिक स्थिती अद्याप ठरलेली नाही. तथापि, बीएनएसएस, बीएसए, यूएपीए, आयकर अधिनियम, पीएमएलए आणि आयटी अधिनियम अंतर्गत सर्च आणि जप्तीच्या संदर्भात सामान्य मार्गदर्शक तत्त्वे आहेत. हे लक्षात घेतले पाहिजे की, सर्च आणि जप्तीची प्रक्रिया या कायद्यांमध्ये वेगवेगळी आहे आणि ती पुढील पृष्ठावर दिली आहे.

पूरक माहिती

भारतीय नागरिक सुरक्षा संहिता (बी.एन.एस.एस) (BNSS) वॉरंटसह	**कलम 96 –** या तरतुदीमध्ये पोलिस अधिकारी कोर्ट कडून विशेष परवानगी घेणे आवश्यक आहे. जेव्हा कोर्टाला असा विश्वास असतो की सर्च करणे आवश्यक आहे, तेव्हा कोर्ट सर्च वॉरंट जारी करण्याच्या अटी ठरवते. सर्च/जप्तीची जबाबदारी असलेल्या अधिकाऱ्याने फक्त त्या ठिकाणीच सर्च करणे आवश्यक आहे जिथे वॉरंट जारी करण्यात आले आहे. **कलम 103 –** हे संपत्तीची सर्च आणि जप्ती करण्यासाठी मूलभूत तरतुदी आहे. पोलिसांना संपत्ती सर्च किंवा जप्त करत असताना या नियमांचे पालन करणे आवश्यक आहे.
भारतीय नागरिक सुरक्षा संहिता (बीएनएसएस) (BNSS) वॉरंटशिवाय	**कलम 185 –** पोलिसांना विशेष परवानगी (वॉरंट) न घेताच एखाद्या ठिकाणी प्रवेश करून सर्च करण्याची परवानगी आहे, जर त्यांना असे वाटते की लवकरच गुन्हा होऊ शकतो किंवा त्यांच्या तपासणीसाठी ते महत्त्वाचे आहे. तसेच, या तरतुदीनुसार पोलिस अधिकाऱ्याने सर्च करताना त्या प्रक्रियेची नोंद ठेवणे आवश्यक आहे. जर एखादा अधिकारी सर्च करू शकत नसेल, तर तो त्याच्या कनिष्ठ अधिकारीला सर्च करण्याचे निर्देश देऊ शकतो, पण त्यासाठी तो कारणे लेखी नोंदवू लागेल. अशा सर्चची नोंद असलेल्या प्रती जवळच्या मॅजिस्ट्रेटकडे 48 तासांमध्ये पाठवली जाऊ शकतात. **तपासणी दरम्यानचे विधान - कलम 180** आणि **181** मध्ये असे नियम आहेत की, एखाद्या व्यक्तीस तपासणी दरम्यान केलेल्या कोणत्याही विधानावर सही करणे आवश्यक नाही. तसेच, लोकांना असे विधान न करणे हक्क आहे, ज्यामुळे ते दोषी दिसू शकतात, आणि हे भारतीय संविधानाने संरक्षित केले आहे. [32] **वॉरंटशिवाय अटक - कलम 35** नुसार, पोलिसांना वॉरंटशिवाय एखाद्याला अटक करण्याची परवानगी आहे, जर त्यांना असे वाटते की त्या व्यक्तीने गंभीर गुन्ह्यात भाग घेतला आहे, त्यांच्यावर तक्रार आहे, किंवा त्यांना विश्वास आहे की ती व्यक्ती गुन्ह्यात सामील आहे. तथापि, ज्येष्ठ वय असलेली व्यक्ती किंवा 60 वर्षांवरील व्यक्तीला तीन वर्षांपेक्षा कमी कारावासाच्या शिक्षेसाठी अटक करणे हे DSP च्या पूर्व परवानगीशिवाय केले जाऊ शकत नाही.
	कलम 105 - एक नवीन तरतुदीने आता पोलिसांना सर्च आणि जप्तीची प्रक्रिया मोबाइल फोनद्वारे नोंदवणे आवश्यक केले आहे. या तरतुदीनुसार, जप्त केलेल्या वस्तूंची यादी तयार करणे आवश्यक आहे, ज्यावर साक्षीदारांची सही असावी, आणि ती तत्काळ जिल्हा मॅजिस्ट्रेट किंवा प्रथम श्रेणी न्यायिक मॅजिस्ट्रेटकडे पाठवली जावी. **कलम 106 -** पोलिसांना त्यांना शंकेखाली चोरीस गेलेली असलेली कोणतीही संपत्ती जप्त करण्याची शक्ती दिली आहे. कधी कधी ही तरतुदी सामान्य सर्चेससाठी वापरली जाते, ज्यामध्ये ते जे काही सापडते ते सर्व जप्त करतात. या तरतुदीनुसार, कोणताही पोलिस अधिकारी चोरीस गेलेली किंवा गुन्ह्याशी संबंधित असलेली संपत्ती जप्त करू शकतो. पोलिस अधिकाऱ्याने जप्तीची माहिती स्थानिक मॅजिस्ट्रेटला कळवली पाहिजे, आणि त्याची देखरेख संबंधित व्यक्तीला त्याच्या सहीसह बंधपत्र देऊन कोर्टात त्याची उपस्थिती लागल्यास जप्त केलेली संपत्ती सादर करण्याची जबाबदारी सोपवली जाऊ शकते.

पूरक माहिती

भारतीय साक्ष्य अधिनियम (BSA)	**कलम 168 –** न्यायाधीशांना खालील अधिकार आहेत: • संबंधित किंवा संबंधित नसलेले तथ्य विचारण्यासाठी प्रश्न विचारण्याचा अधिकार. • कोणत्याही पक्षांसह आणि साक्षीदारांशी कोणत्याही वेळेस प्रश्न विचारण्याचा अधिकार. • कागदपत्रे किंवा वस्तूंचे उत्पादन प्रमाण म्हणून मागवण्याचा अधिकार. महत्त्वाचे म्हणजे, न्यायाधीशांच्या मागण्या किंवा. आदेशांवर कोणतीही व्यक्ती आक्षेप घेऊ शकत नाही, ही तरतूद दिली आहे. [हे विशेषतः सर्च आणि जप्तीच्या प्रकरणांमध्ये महत्त्वाचे ठरू शकते, जिथे विशिष्ट कागदपत्रे किंवा वस्तू साक्ष म्हणून महत्त्वाची असू शकतात.]
मनी लॉंडरिंग प्रतिबंधक कायदा, 2002 (PMLA)	**कलम 16 आणि 17 –** हे कलमे शोध किंवा जप्ती करण्याच्या नियमांची स्पष्टता देतात. यामध्ये शोध किंवा जप्ती का केली जात आहे याचे लेखी नोंद तयार करणे आवश्यक आहे आणि जप्त केलेल्या वस्तूंची यादी तयार करून त्याचा रिपोर्ट तयार करणे अनिवार्य आहे. [हे शोध आणि जप्ती प्रक्रियेतील आवश्यक कागदपत्रांची तयारी आणि दस्तऐवजीकरण यांना जोडते.]
बेकायदेशीर क्रियाकलाप (प्रतिबंध) अधिनियम, 1967 (UAPA)	**कलम 43A –** या कलमाअंतर्गत अधिकाऱ्यांना शोध करण्यासाठी त्यांचे कनिष्ठ अधिकारी नियुक्त करण्याचा अधिकार दिला जातो. तसेच, 'विश्वास ठेवण्याच्या कारणांचा' संदर्भ वैयक्तिक ज्ञान किंवा तिसऱ्या पक्षाने दिलेल्या लेखी माहितीवर आधारित असावा लागतो. **कलम 43B –** या कलमामध्ये शोध किंवा जप्ती होणाऱ्या व्यक्तीचे अधिकार स्पष्ट केले आहेत. यानुसार, शोध किंवा जप्ती करताना, त्या व्यक्तीला शोध घेतल्या जाणाऱ्या गोष्टींच्या कारणांची माहिती दिली पाहिजे आणि जप्त केलेल्या गोष्टी नजीकच्या पोलिस ठाण्यात नेऊन ठेवाव्यात. त्या ठाण्यातील अधिकारी आवश्यक त्या कारवायांसाठी CrPC (आता BNSS) मधील नियमांचे पालन करतात.
आयकर कायदा, 1961 (Income Tax Act)	**कलम 132 –** या कलमाअंतर्गत अधिकाऱ्यांना कागदपत्रे किंवा वस्तू जप्त करण्याचा अधिकार दिला जातो, जर कोणतीही व्यक्ती त्यांना कायद्यानुसार मागितल्याप्रमाणे पुरवठा करत नसेल. शोध आणि जप्ती संदर्भात, या कलमाने अधिकाऱ्यांना विशेष कागदपत्रे किंवा वस्तू जप्त करण्यासाठी कायदेशीर आधार दिला आहे, जर त्या वस्तू किंवा कागदपत्रांचे स्वेच्छेने उत्पादन केले जात नसेल. या कलमाने आरोपी व्यक्तींना योग्य सुरक्षा दिली आहे, कारण त्यांना जप्त केलेल्या वस्तूंबद्दल आपले स्पष्टीकरण देण्यासाठी पुरावा सादर करण्याची योग्य संधी दिली जाऊ शकते.
माहिती तंत्रज्ञान कायदा, 2000 (IT Act, 2000)	**कलम 80 –** या कलमाअंतर्गत अधिकृत अधिकारी [33] कोणत्याही सार्वजनिक ठिकाणी शोध घेण्याचा आणि त्याठिकाणी सापडलेल्या त्या व्यक्तीला अटक करण्याचा अधिकार असतो, ज्यावर माहिती असलेली आशंका असते की ती व्यक्ती आयटी कायद्यानुसार भूतकाळात, वर्तमानकाळात किंवा भविष्यकाळात कोणताही अपराध केलेला आहे.

पूरक माहिती

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: _____

आकृती १:
पक्षाने भरायचे प्रमाणपत्र

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)

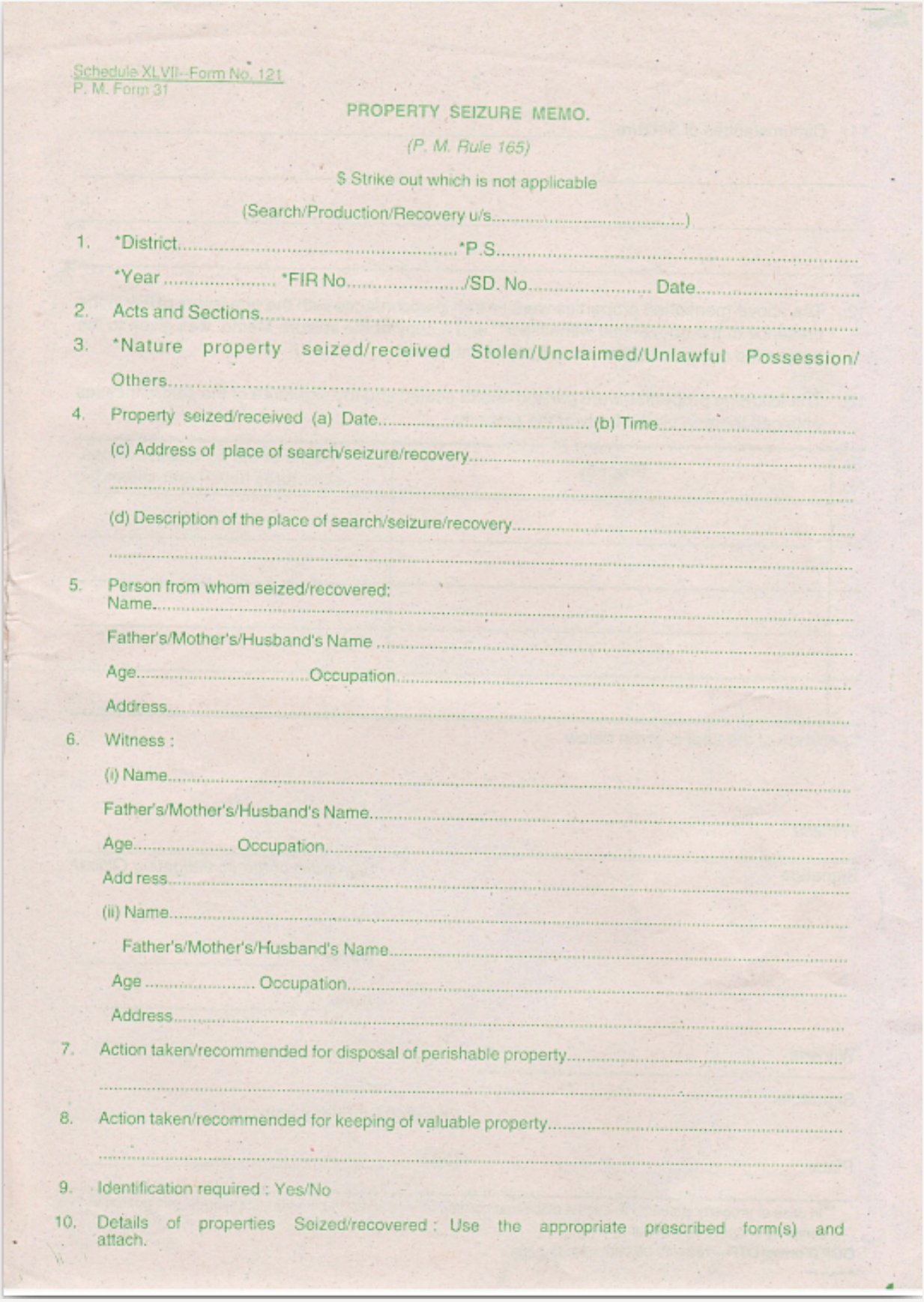
Place: _____

_____

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

आकृती 2:
तज्ञाने भरायचे प्रमाणपत्र

पूरक माहिती



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

PROPERTY SEIZURE MEMO.

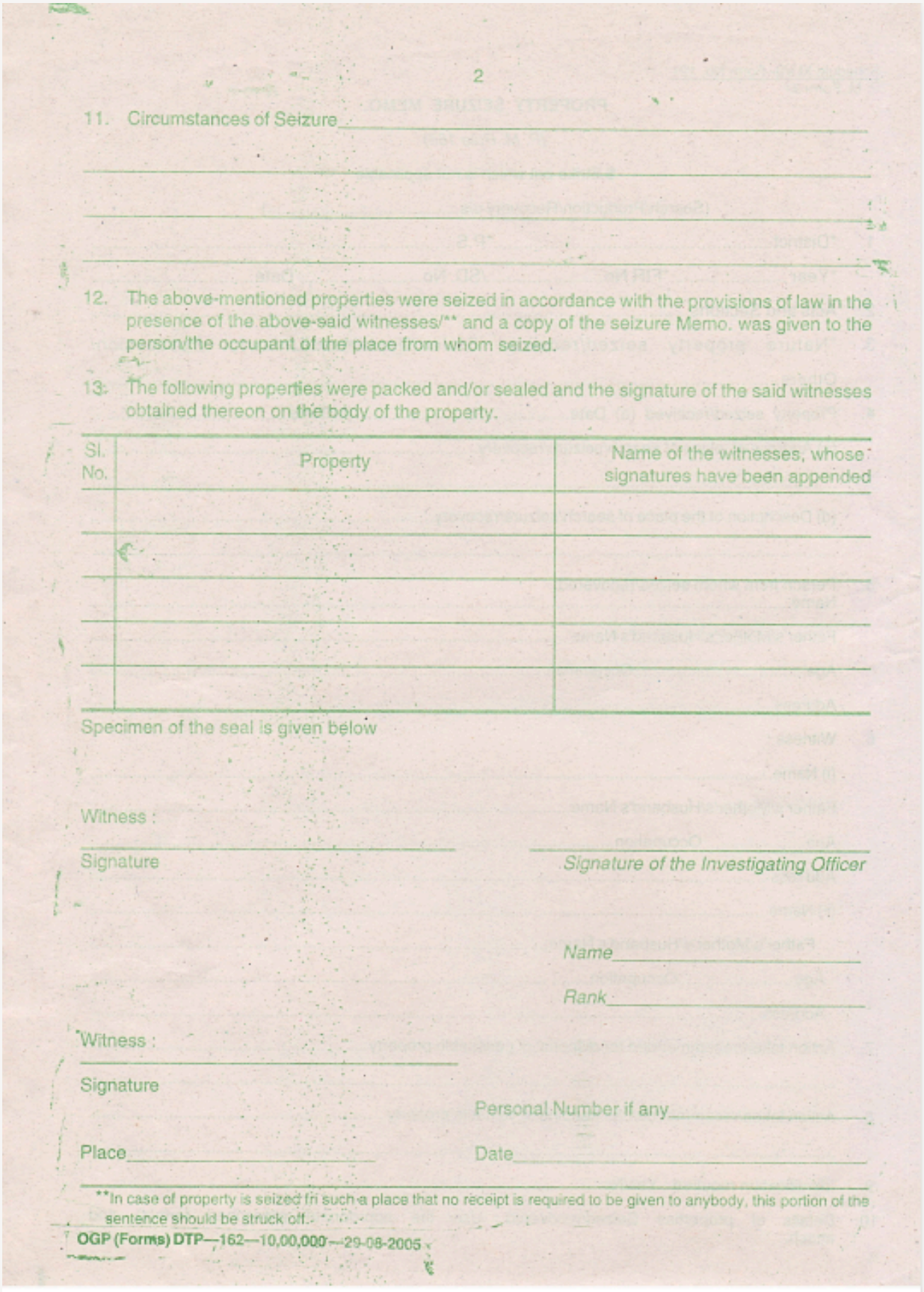
(P. M. Rule 165)

$ 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.

आकृती 3:
मालमत्ता जप्ती निवेदन



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

आकृती 3.1:
मालमत्ता जप्ती निवेदन

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

आकृती 4:
जप्त यादी

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*)

_____

आकृती 5:
अटक वॉरंट फॉरमॅट (अधिकृत राजपत्र अधिसूचनेत प्रकाशित झालेल्या कायद्याच्या पृष्ठ 192 वर बीएनएसएसच्या दुसऱ्या अनुसूचीमध्ये दिलेला)

संदर्भ

[1] शब्दाचा अर्थ समजण्यासाठी ग्लीसरीचा संदर्भ घ्या.

[2] बी.एन.एस.एस मध्ये शोध घेण्याबाबत स्पष्टीकरणासाठी, कलम 49; 97 पहा.

[3] बी.एन.एस.एस कलम 44.

[4] बी.एन.एस.एस कलम 185(1).

[5] बी.एन.एस.एस मध्ये जप्तीबाबत स्पष्टीकरणासाठी, कलम 106, 117 पहा.

[6] हे कायद्यांच्या सर्व समावेशक यादी नाही. शोध आणि जप्तीसाठी अन्य कायदे देखील आहेत.

[7] दंड प्रक्रिया संहिता, 1973 दंड प्रक्रिया संहिता, 1973 (सी.आर.पी.सी).

[8] भारतीय पुरावा कायदा, 1872.

[9] भारतीय दंड संहिता, 1860.

[10] दूरसंचार कायदा, 2023 च्या कलम 42 आणि 43 पहा.

[11] कृपया लक्षात घ्या की अशी रेकॉर्डिंग फक्त न्यायिक मजिस्ट्रेट ऑफ द फर्स्ट क्लास, जिल्हा मजिस्ट्रेट आणि उपविभागीय मजिस्ट्रेट यांना प्रदान केली जाऊ शकते.

[12] बी.एन.एस.एस, 2023 चे कलम 94, 185.

[13] के.एस. पुट्टुस्वामी विरुद्ध भारत संघ (2017) 10 एससीसी 1.

[14] वीरेंद्र खन्ना विरुद्ध कर्नाटका राज्य, रिट याचिका क्र. 11759 ऑफ 2020 (GM-RES).

[15] मीडिया व्यावसायिकांची संस्थाही भारत संघ, रिट याचिका (क्रिम) क्र. 395 ऑफ 2022, सर्वोच्च न्यायालय, पृष्ठ 1.

[16] अवस्तिका दास, डिजिटल डिव्हायस जप्तीसाठी मार्गदर्शक तत्वे तयार करण्यासाठी समिती गठित: केंद्र सर्वोच्च न्यायालयाला सांगते, (6 डिसेंबर 2023 12:05 PM)
https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831

[17] बी.एस.ए, 2023 च्या कलम 63(4)(c) अंतर्गत प्रमाणपत्र प्रदान केले गेले आहे.

संदर्भ

[18] जप्ती मेमोसाठी एक नमुना अनुबंधात, आकृती 3 आणि आकृती 3.1 म्हणून दिला आहे. या नमुन्याचा स्रोत: https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf

[19] अशा एक सूचीच्या नमुन्याचा (ज्याला जप्ती यादी म्हणून ओळखले जाऊ शकते, आकृती 4 मध्ये) अनुबंधामध्ये दिला आहे.

[20] अटक वॉरंटचा एक नमुना अनुबंधात, आकृती 5 म्हणून दिला आहे.

[21] बी.एन.एस.एस कलम 503(2).

[22] बी.एन.एस.एस कलम 2(क).

[23] बी.एन.एस.एस कलम 2(फ), आरोपाचे व्याख्याते कलम 2(ब) मध्ये; तसेच (आरोपाच्या घटकांचे चांगले समजून घेण्यासाठी) कलम 234 पहा.

[24] बी.एन.एस.एस, कलम 2(ग). तसेच पहा पहिला अनुसूची, स्पष्टीकरण नोट्सचे बिंदू (2), कायद्यात प्रसिद्ध केलेल्या गॅझेट नोटिफिकेशनवरील पृष्ठ 158.

[25] बी.एन.एस कलम 2(21).

[26] बी.एन.एस.एस कलम 2(0). तसेच पहा पहिला अनुसूची, स्पष्टीकरण नोट्सचे बिंदू (2), कायद्यात प्रसिद्ध केलेल्या गॅझेट नोटिफिकेशनवरील पृष्ठ 158.

[27] बी.एन.एस.एस, कलम 2(स).

[28] आयटी कायदा, कलम 80(1) चा स्पष्टीकरण.

[29] जी. विशालकान v. राज्य of केरळ व इतर, WP(C) क्र. 22328 ऑफ 2023 (10.07.2023 - KERHC) : MANU/KE/1872/2023.

[30] संकेत भद्रेश मोदी विरुद्ध CBI, BA क्र. 3754/23.

[31] CBI विरुद्ध महेश कुमार शर्मा, CBI 31/2021.

[32] हा अधिकार भारताच्या संविधानाच्या भाग III मध्ये, आर्ट. 20(3) अंतर्गत संरक्षित आहे.

[33] अधिकृत अधिकारी म्हणजे एक पोलिस अधिकारी (इंस्पेक्टरपेक्षा कमी नसलेला) किंवा केंद्रीय किंवा राज्य सरकारच्या इतर अधिकाऱ्यांना केंद्रीय सरकारने अधिकृत केलेले.

Email: mail@sflc.in

Website: https://www.sflc.in