

sflc.in

வழிகாட்டி

**மின்னணு கருவிகளை
சோதனை செய்வதற்கு
மற்றும் பறிமுதல்
செய்வதற்கான
வழிகாட்டி**

Guide on Search and Seizure of Electronic Devices, 2025

By SFLC.in in partnership with UNESCO

© Copyright 2024 SFLC.in Licensed under Creative Commons BY SA NC 4.0

Published by: SFLC.in

K9, 2nd Floor, Birbal Road, Jangpura Extension, New Delhi – 14, India.

Email: mail@sflc.in

Website: <https://www.sflc.in>



TABLE OF CONTENTS

01.	பிரிவு 1 அடிப்படைகள்	4
02.	பிரிவு 2 What to do during a search?	10
03.	பிரிவு 3 சோதனையிடும்போது என்ன செய்வது?	14
04.	பிரிவு 4 பறிமுதலுக்கு பிறகு நடைமுறை	16
05.	பிரிவு 5 தயார்நில	25
●	சொற்களின் சொற்களஞ்சியம்:	33
●	இணைப்பு	36
●	References	45

பிரிவு 1

அடிப்படைகள்

யாராவது உங்களை சோதனைக்கு உள்ளாக்கி உள்ளார்களா?
அவர்கள் உங்கள் உடல், வாகனம், வீட்டைத் சோதனைக்கு
உள்ளாக்கினார்களா?
அவர்கள் உங்கள் கருவிகளைப் பறிமுதல் செய்தார்களா?
இவற்றில் ஏதேனும் ஒன்றுக்கு பதில் ஆம் என்றால்...



எளிமைப்படுத்தப்பட்ட

சோதனை மற்றும் பறிமுதல்: என்ன, ஏன், எங்கே

‘சோதனை’ என்றால் ஒரு தனிநபர் அல்லது அவர்களின் சொத்தில் நடந்து கொண்டிருக்கும் விசாரணை அல்லது நீதித்துறை நடவடிக்கைகளுக்கான ஆதாரங்களைக் கண்டறியப் பார்ப்பது. [1] [2] இது வாரண்ட் உடனோ அல்லது இல்லாமலோ செய்யப்படலாம். [3][4]

‘பறிமுதல்’ என்றால் சோதனை முடிந்ததும் அந்தச் சொத்தை ஆதாரமாகவோ அல்லது விசாரணைக்கான சம்பந்தப்பட்ட சொத்தாகவோ பயன்படுத்திக் கொள்வது. [5]

என்ன: இது ஒரு வழக்கினை விசாரிக்க சட்ட அமலாக்க முகமைகளால் பயன்படுத்தப்படும் கருவியாகும்.

ஏன்: ஆதாரங்களைச் சேகரிக்கவும், குற்றத்தைத் தடுக்கவும், நீதியின் தவறான வழிகாட்டலைத் தடுக்கவும் இது செய்யப்படுகிறது.

எங்கே: குற்றம் நடந்த காட்சிகள், குற்றத்தில் ஈடுபட்டவர்கள் பதுங்கியிருக்கக்கூடிய இடங்கள் மற்றும் குற்றத்துடன் தொடர்புடைய எந்தவொரு பொருளும் வைக்கப்படக்கூடிய இடங்கள்.

சோதனையிடவும் மற்றும் பறிமுதல் செய்வதற்கான காரணங்கள்

- ஒரு நபருக்கு எதிரான விசாரணை, விசாரணை அல்லது விசாரணைக்காக முக்கியமான பொருள்கள் மற்றும் ஆவணங்கள், மின்னணு மற்றும் டிஜிட்டல் பதிவுகள் உட்பட எந்தவொரு நிறுவனத்திற்கும் கிடைக்கச் செய்யப்படுவதை உறுதி செய்வதற்காக இது செய்யப்படுகிறது.
- விசாரணை செய்யும் முகவர்/காவல்துறை தேடப்பட்ட மற்றும் பறிமுதல் செய்யப்பட்ட ஆவணங்களின் உள்ளடக்கங்களை முதன்மை அல்லது இரண்டாம் நிலை ஆதாரத்தின் மூலம் நீதிமன்றத்தில் நிரூபிக்க முடியும்.



இந்த நடவடிக்கைகளை இயக்கும் சட்ட அடித்தளங்கள்

சோதனை மற்றும் பறிமுதல் செய்வதற்கான அதிகாரம் பல்வேறு சட்டங்களிலிருந்து பெறப்பட்டது [6]:

- + பாரதிய நாகரிக் சுரக்ஷா சன்ஹிதா, 2023 (BNSS) [7]
- + பாரதிய சக்ஷயா அதினியம், 2023 (BSA) [8]
- + பாரதிய நியாய சன்ஹிதா, , 2023 (BNS) [9]
- + வருமான வரிச் சட்டம், 1961 (ITA)
- + சட்டவிரோத நடவடிக்கைகள் (தடுப்பு) சட்டம், 1967, மற்றும் (UAPA)
- + பணமோசடி தடுப்புச் சட்டம், 2002 (PMLA)
- + CBI கையேடு 2020
- + தகவல் தொழில்நுட்பச் சட்டம், 2000 (IT சட்டம்)
- + தொலைத்தொடர்புச் சட்டம், 2023
- + போதைப்பொருள் மற்றும் மனோவியல் பொருட்கள் சட்டம், 1985

திரைக்குப் பின்னால்: சோதனை மற்றும் பறிமுதல் நடவடிக்கையில் உள்ள முக்கிய அதிகாரிகள் மற்றும் அவர்களின் பொறுப்புகள் பற்றிய விளக்கம்

சோதனை மற்றும் பறிமுதல் செய்ய அதிகாரம் பெற்ற அதிகாரி சட்டத்தின்படி மாறுபடும் மற்றும் பின்வருமாறு உள்ளன. இந்த பிரிவின் நோக்கம், தேடலுக்கான உத்தரவை யார் பிறப்பிக்க அதிகாரம் உள்ளது என்பது பற்றிய பொதுவான தகவல்களை வழங்குவதாகும். இதை படித்துப் பார்ப்பதன் மூலம் சரியான கேள்விகளை அதிகாரிகளிடம் கேள்வி எழுப்ப உதவும்.

சோதனைகளும் மற்றும் பறிமுதல்களும் வெவ்வேறு சட்டங்களுக்கும் சூழ்நிலைகளுக்கும் ஏற்றவாறு நடத்தப்படுகின்றன.

I. சோதனைக்கான உத்தரவை யார் பிறப்பிக்க அதிகாரம் உள்ளது?	
BNSS	ஒரு நீதிபதி (மாவட்ட மாஜிஸ்திரேட், துணைப்பிரிவு மாஜிஸ்திரேட் அல்லது முதல் வகுப்பு மாஜிஸ்திரேட்) ஒரு போலீஸ் அதிகாரிக்கு, கான்ஸ்டபிள் தரத்திற்கு மேலே (எந்த அதிகாரியும் அல்ல!) ஒரு இடத்தை சோதனையிட சிறப்பு அனுமதி வழங்க முடியும், அவர்கள் திருடப்பட்ட பொருட்கள் அல்லது ஆபத்தான விஷயங்களை மறைத்து வைத்திருப்பதாக நினைத்தால், இந்த அதிகாரிக்கு தேவைப்பட்டால் மற்றவர்களிடமிருந்தும் உதவி பெறலாம்.
வருமான வரிச் சட்டம்	இயக்குனர்/பொது/தலைமை ஆணையர்/ஆணையர் தேடலுக்கான உத்தரவை பிறப்பிக்க அதிகாரம் உள்ளது.
UAPA	மத்திய அரசு/மாநில அரசு சோதனையிடுவதற்கான உத்தரவு பிறப்பிக்கலாம். இருப்பினும், எந்த பிரிவு/அமைச்சகம் (மத்திய/மாநில) இந்த உத்தரவை பிறப்பிக்க அதிகாரம் பெற்றுள்ளது என்று சட்டம் குறிப்பிடவில்லை.
PMLA	கணக்கெடுப்புகளுக்கு: தீர்ப்பளிக்கும் அதிகாரி உத்தரவு பிறப்பிக்கலாம். பறிமுதல்களுக்கு: இயக்குநர் அல்லது துணை இயக்குநருக்குக் குறையாத எந்த அதிகாரியும் உத்தரவு பிறப்பிக்கலாம்.
IT சட்டம்	மத்திய அல்லது மாநில அரசாங்கத்தின் எந்த அதிகாரிக்கும் சோதனை செய்ய மத்திய அரசுக்கு அதிகாரம் உள்ளது. கணினிகளுக்குள் இருக்கும் தரவை அணுகுவதற்கு கட்டுப்படுத்தி ஒரு தேடலுக்கு உத்தரவிடலாம்.

திரைக்குப் பின்னால்: சோதனை மற்றும் பறிமுதல் நடவடிக்கையில் உள்ள முக்கிய அதிகாரிகள் மற்றும் அவர்களின் பொறுப்புகள் பற்றிய விளக்கம்

சோதனை மற்றும் பறிமுதல் செய்ய அதிகாரம் பெற்ற அதிகாரி சட்டத்தின்படி மாறுபடும் மற்றும் பின்வருமாறு உள்ளன. இந்த பிரிவின் நோக்கம், தேடலுக்கான உத்தரவை யார் பிறப்பிக்க அதிகாரம் உள்ளது என்பது பற்றிய பொதுவான தகவல்களை வழங்குவதாகும். இதை படித்துப் பார்ப்பதன் மூலம் சரியான கேள்விகளை அதிகாரிகளிடம் கேள்வி எழுப்ப உதவும்.

சோதனைகளும் மற்றும் பறிமுதல்களும் வெவ்வேறு சட்டங்களுக்கும் சூழ்நிலைகளுக்கும் ஏற்றவாறு நடத்தப்படுகின்றன.

II. I.சோதனை நடத்த யாருக்கு அதிகாரம் உள்ளது?	
BNSS	சோதனைகளும் மற்றும் பறிமுதல்களும் வெவ்வேறு சட்டங்களுக்கும் சூழ்நிலைகளுக்கும் ஏற்றவாறு நடத்தப்படுகின்றன. நிலைய அதிகாரி (SHO) அல்லது விசாரணை அதிகாரி (IO) சோதனை மற்றும் பறிமுதல் செய்யலாம், அவர்கள் இல்லாத நிலையில், எழுத்துப்பூர்வமாக அங்கீகரிக்கப்பட்ட எந்த அதிகாரியாலும் அதை நடத்த முடியும். யாராவது கைது செய்யப்பட்டால்: குற்றவாளிகள் பிடிபட்ட இடத்தில் போலீசார் சோதனை செய்து, குற்றத்துடன் தொடர்புடைய எதையும் எடுத்துச் செல்லலாம். போலீசாரால் மட்டுமே இதைச் செய்ய முடியும், தேவைப்பட்டால் கதவுகள் அல்லது ஜன்னல்களைக் கூட உடைக்கலாம். சந்தேகத்திற்கிடமான ஒன்று மறைக்கப்பட்டிருந்தால்: ஒரு நீதிபதி (மாவட்ட மாஜிஸ்திரேட், துணைப்பிரிவு மாஜிஸ்திரேட் அல்லது முதல் வகுப்பு மாஜிஸ்திரேட்) ஒரு போலீஸ் அதிகாரிக்கு, கான்ஸ்டபிள் தரத்திற்கு மேலே (எந்த அதிகாரியும் அல்ல!) ஒரு இடத்தை சோதனையிட சிறப்பு அனுமதி வழங்க முடியும், அவர்கள் திருடப்பட்ட பொருட்கள் அல்லது ஆபத்தான விஷயங்களை மறைத்து வைத்திருப்பதாக நினைத்தால். இந்த அதிகாரிக்கு தேவைப்பட்டால் மற்றவர்களிடமிருந்தும் உதவி பெறலாம். பிரிவுகள்: 44 & 97
UAPA	வை விசாரிக்க அதிகாரம் ஒவ்வொரு நகரத்திலும் வேறுபடுகிறது: டெல்லி சிறப்பு காவல் அமைப்பு: துணை காவல் கண்காணிப்பாளர் அல்லது அதற்கு இணையானவர். மும்பை, கொல்கத்தா, சென்னை, அகமதாபாத் மற்றும் அறிவிக்கப்பட்ட பகுதிகளின் பெருநகர பகுதிகள்: உதவி காவல் ஆணையர் மற்றும் அதற்கு மேற்பட்டவர்கள். பிற வழக்குகள்: துணை காவல் கண்காணிப்பாளர் அல்லது அதற்கு இணையான பதவிக்குக் குறையாத அதிகாரிகள்.

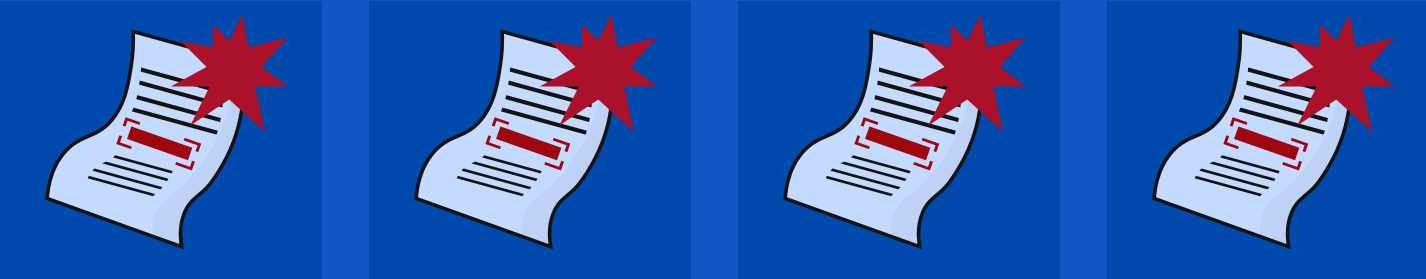
திரைக்குப் பின்னால்: சோதனை மற்றும் பறிமுதல் நடவடிக்கையில் உள்ள முக்கிய அதிகாரிகள் மற்றும் அவர்களின் பொறுப்புகள் பற்றிய விளக்கம்

சோதனை மற்றும் பறிமுதல் செய்ய அதிகாரம் பெற்ற அதிகாரி சட்டத்தின்படி மாறுபடும் மற்றும் பின்வருமாறு உள்ளன. இந்த பிரிவின் நோக்கம், தேடலுக்கான உத்தரவை யார் பிறப்பிக்க அதிகாரம் உள்ளது என்பது பற்றிய பொதுவான தகவல்களை வழங்குவதாகும். இதை படித்துப் பார்ப்பதன் மூலம் சரியான கேள்விகளை அதிகாரிகளிடம் கேள்வி எழுப்ப உதவும்.

சோதனைகளும் மற்றும் பறிமுதல்களும் வெவ்வேறு சட்டங்களுக்கும் சூழ்நிலைகளுக்கும் ஏற்றவாறு நடத்தப்படுகின்றன.

II. சோதனை நடத்த யாருக்கு அதிகாரம் உள்ளது?

வருமான வரிச் சட்டம்	உதவி ஆணையர்களுக்குக் குறையாத வருமான வரி அதிகாரிகள் மட்டுமே விசாரிக்க முடியும்.
PMLA	இயக்குனர் அல்லது துணை இயக்குனருக்குக் குறையாத வேறு எந்த அதிகாரியும் விசாரிக்க அதிகாரம் உண்டு.
IT சட்டம்	ஒரு ஆய்வாளருக்குக் குறையாத எந்த ஒரு காவல் அதிகாரியும். கூடுதலாக, மத்திய அல்லது மாநில அரசாங்கத்தின் வேறு எந்த அதிகாரியும் மத்திய அரசால் விசாரிக்க அங்கீகரிக்கப்படலாம். கட்டுப்பாட்டாளர் அல்லது அவர்களால் அங்கீகரிக்கப்பட்ட வேறு எந்த அதிகாரியும் விசாரிக்கலாம்.
தொலைத்தொடர்புச் சட்டம், 2023	இந்தச் சட்டம், அங்கீகரிக்கப்படாத தொலைத்தொடர்பு நெட்வொர்க் அல்லது உபகரணங்கள் ஏதேனும் வைக்கப்பட்டிருந்தால் அல்லது மறைத்து வைக்கப்பட்டிருந்தால், மத்திய அரசின் அங்கீகரிக்கப்பட்ட அதிகாரி எந்த இடத்தையும் தேட அதிகாரம் அளிக்கிறது. [10]



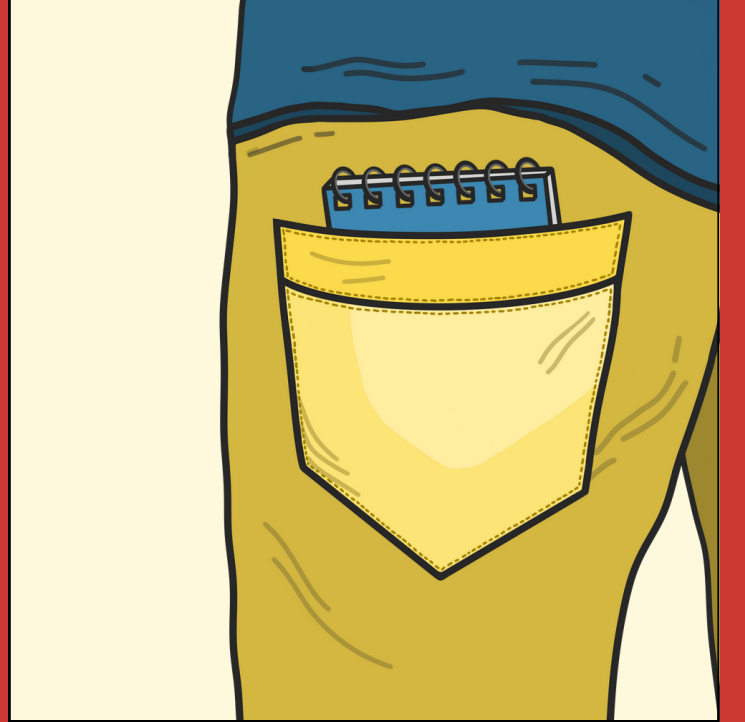
பிரிவு 2

சோதனையி
டும்போது
என்ன
செய்வது?

தடயவியல் விசாரணை நடைபெறும் செயல்முறை சிக்கலானதும், சில சமயங்களில் பயமுறுத்தக்கூடியதாகவும் இருக்கலாம்.

இந்தச் செயல்முறையை சிறப்பாக நெறிப்படுத்துவதற்காக, அதில் தொடர்புடைய நடைமுறைகள் மற்றும் தேவையான ஆவணங்களை புரிந்து கொள்வது மிகவும் அவசியம்.

ஒரு விசாரணை, இறுதியில் ஒரு வழக்குத் தீர்ப்புக்குச் செல்லக்கூடும். இத்தகைய நிலைமை ஏற்படும் போது, சோதனைகளின் நடைமுறை மற்றும் அதனுடன் தொடர்புடைய நெறிமுறைகள் குறித்து தெளிவான புரிதல் இருக்க வேண்டும். இது, நீதிமன்றத்தில் நம்மைக் காவல்படுத்தும் (self-defence) உரிமையில் முக்கியமானதாகும்.



சோதனையின் தொடக்கத்தில், இந்தக் கேள்விகள் கைகொடுக்கும்



1	உங்களிடம் வாரண்ட் இருக்கிறதா?
2	அது மின்னணு முறையில் வழங்கப்பட்டதா?
3	ஆம் எனில், எந்த ஊடகம் மூலம்?
4	நீங்கள் எந்த புலனாய்வு அமைப்பை பிரதிநிதித்துவப்படுத்துகிறீர்கள்?
5	உங்கள் பதவி என்ன?
6	எனக்கு எதிரான குற்றச்சாட்டுகள் என்ன?

கூடுதலாக, இதை மனதில் கொள்ளுங்கள் - உங்கள் கேள்விகளுக்குச் சரியாகப் பதிலளிக்கப்படவில்லை என்று நீங்கள் உணர்ந்தால், உடனடியாக ஒரு வழக்கறிஞரைத் தொடர்பு கொள்ளுங்கள். உங்கள் சட்டப் பிரதிநிதி இருக்கும் வரை நீங்கள் எந்தக் கேள்விக்கும் பதிலளிக்க வேண்டாம் என்று அறிவுறுத்தப்படுகிறது.

அதிகாரிகளிடமிருந்து தகவல்களை திறம்படப் பெறுதல்.

- காவல்துறை உங்கள் மின்னணு சாதனங்களைத் தேடலாம் - வாரண்ட் உடனோ அல்லது இல்லாமலோ. இருப்பினும், சோதனை மற்றும் பறிமுதல் நடைமுறையின் நகலை எப்போதும் அருகிலுள்ள மாஜிஸ்திரேட்டிடம் இருந்து கேட்க வேண்டும் [11] - அவர் காவல் அதிகாரியிடமிருந்து அத்தகைய பதிலைப் பெற்றவர்.[12]
- உங்களிடம் உள்ள வேறு எந்த நபரின் மின்னணு பதிவுகளையும் வழங்க நீங்கள் மறுக்கலாம், அதே நபர் அதற்கு ஒப்புதல் அளிக்காவிட்டால்.
- தேடல் மற்றும் பறிமுதல் என்பது எந்த விசாரணையிலும் ஒரு நிலையான நடைமுறையாகும், உங்கள் வீடு மற்றும் சாதனங்கள் தேடப்படுவதால் நீங்கள் குற்றவாளி என்று அர்த்தமல்ல. தேடலை நடத்த அங்கீகரிக்கும் முழுமையான ஆவணங்கள் புலனாய்வு அமைப்புகளிடம் இருந்தால், அவர்கள் தங்கள் வேலையைச் செய்யட்டும். எதிர்காலத்தில் உங்களுக்கு அவர் தேவைப்படலாம் என்பதால் உங்கள் வழக்கறிஞரைத் தொடர்பு கொள்ளுங்கள்.
- விசாரணை அதிகாரிகள் சில நேரங்களில் உங்கள் கேள்விகளுக்கு பதிலளிக்காமல் போகலாம், உங்கள் கேள்விகளையும் பதில்களையும் ஒரு காகிதத்தில் குறித்துக்கொள்வது நல்லது, எனவே அதை மேலும் ஒரு விசாரணையில் பயன்படுத்தலாம்.
- விசாரணை முகமைகளுக்கு அவர்களின் தேடலுக்கு உதவ நீங்கள் கடமைப்பட்டிருக்கவில்லை, இருப்பினும், நீங்கள் அந்த செயல்பாட்டில் தலையிடக்கூடாது. இதன் பொருள், உதாரணமாக, கருவியுடன் ஓடிப்போவது அல்லது கருவியை உடைப்பதாகும்.

தளத்தில் சோதனை மற்றும் பறிமுதல் செய்யும் போது, பகுப்பாய்வு என்பது சேகரிக்கப்பட்ட ஆதாரங்களின் பொருத்தத்தையும் ஒருமைப்பாட்டையும் உறுதி செய்வதற்காக உடனடியாக ஆய்வு செய்து மதிப்பீடு செய்வதை உள்ளடக்குகிறது.

காணப்படும் உடல் பொருட்கள் மற்றும் டிஜிட்டல் சாதனங்களை மதிப்பாய்வு செய்து ஆவணப்படுத்துவது, தரவு பிரித்தெடுத்தல் மற்றும் தடயவியல் பகுப்பாய்வு செய்து தகவல்களை மீட்டெடுப்பது மற்றும் சரிபார்ப்பது ஆகியவை இதில் அடங்கும், அதே நேரத்தில் சேதப்படுத்தாமல் தடுக்கிறது. முக்கிய வடிவங்கள் மற்றும் இணைப்புகள் அடையாளம் காணப்படுகின்றன, மேலும் தெளிவான பாதுகாப்புக் கோட்டை பராமரிக்க விரிவான குறிப்புகள் எடுக்கப்படுகின்றன.

1	பகுப்பாய்வுக்கு பயன்படுத்தப்படும் கருவிகள் மற்றும் கணக்குகளின் பட்டியலை வைத்திருங்கள்: தேடப்பட்ட சாதனங்களில் இருந்து சேகரிக்கப்பட்ட தரவுகளை பின்னர் ஒப்பிடுவதற்காக, விசாரணைக்காக பயன்படுத்தப்பட்ட அனைத்து கருவிகள் மற்றும் கணக்குகளின் பட்டியலை வைத்திருத்தல் அவசியமாகும்.
2	உங்கள் சாதனங்களில் உள்ள கோப்புகளின் சேமிப்பு இடங்களை வெளியிட வேண்டாம்: அதிகாரிகள் சோதனை மற்றும் பறிமுதல் நடத்தும் போது, உங்கள் தனியுரிமையை மற்றும் செயல்முறையின் முழுமையை பாதுகாக்க, உங்கள் கருவிகளில் உள்ள கோப்புகளின் சேமிப்பு இடங்களை வெளியிட வேண்டாம். கோப்புகள் எங்கு சேமிக்கப்படுகின்றன என்பதற்கான தகவல்களை வழங்குவது சட்டப்படி அனுமதிக்கப்படாத சோதனையின் அளவைக் கூடுதலாக விரிவாக்கலாம், மேலும் உணர்ச்சிமிக்க அல்லது தொடர்பில்லாத தனிப்பட்ட தகவல்களை வெளிப்படுத்தலாம்.
3	பகுப்பாய்வுக்கு எடுத்துக்கொள்ளப்பட்ட அனைத்து கருவிகளின் IMEI, தொடர் எண்கள் மற்றும் விவரங்களை குறித்துக்கொள்ளவும்: இது கருவியின் அடையாளத்தை உறுதிப்படுத்த உதவுகிறது, மற்ற சாதனங்களுடன் குழப்பங்களைத் தவிர்க்கிறது, மற்றும் சரியான உருப்படியை பகுப்பிக்க அல்லது நீதிமன்றத்தில் வழங்குவதன் மூலம் சான்றுகளின் முழுமையை பராமரிக்கிறது.

பிரிவு 3

மின்னணு
சாதனங்கள்
மற்றும் சட்டம்

இதேவேளை, Foundation of Media Professionals எனும் அமைப்பு, மின்னணு கருவிகளில் ஒருவரின் தனிப்பட்ட தகவல்கள் பெருமளவில் சேமிக்கப்பட்டிருப்பதை முன்னிட்டு, தற்காலிக சட்டங்கள் ஒருவர் தன்னையே குற்றவாளி என சாட்சியம் அளிக்க வேண்டாமை மற்றும் தனியுரிமை போன்ற அடிப்படை உரிமைகளை பாதுகாக்கப் போதுமானவை அல்ல என்று வாதாடி, இது தொடர்பாக வழக்கு தொடர்ந்தது.^[15] இதேவேளை, Foundation of Media Professionals எனும் அமைப்பு, மின்னணு கருவிகளில் ஒருவரின் தனிப்பட்ட தகவல்கள் பெருமளவில் சேமிக்கப்பட்டிருப்பதை முன்னிட்டு, தற்காலிக சட்டங்கள் ஒருவர் தன்னையே குற்றவாளி என சாட்சியம் அளிக்க வேண்டாமை மற்றும் தனியுரிமை போன்ற அடிப்படை உரிமைகளை பாதுகாக்கப் போதுமானவை அல்ல என்று வாதாடி, இது தொடர்பாக வழக்கு தொடர்ந்தது.^[16]

A collage of icons representing data privacy and security. The central element is a clipboard with a purple clip, featuring a handwritten checklist and a table. The checklist includes items like 'Review system logs', 'Check for updates', 'Test backup recovery', 'Verify access controls', and 'Conduct security audit'. The table has columns for 'Task', 'Status', 'Priority', and 'Due Date'. Surrounding the clipboard are various icons: a hand with a fingerprint, a smartphone with a lock, a login form with a password field and a lock icon, and a 'DATA PRIVACY' label with a question mark icon.

பிரிவு 4

பறிமுதலுக்
கு பிறகு

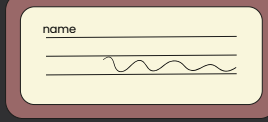
நடைமுறை:

உங்கள் கருவிகள்
பறிமுதல் செய்யப்பட்ட
பிறகு என்ன நடக்கிறது?

பறிமுதல் செய்யப்பட்ட கருவிகளுக்கு ஆவணங்கள் தேவை

சான்றிதழ்கள் [பிரிவு 63(4)(c) இன் கீழ்]

சோதனையிடப்படும் மற்றும்
பறிமுதல் செய்யப்படும்
நபரால் தாக்கல் செய்யப்படும்
சான்றிதழ்களின் நகலை
மற்றும் செயல்முறையை
நடத்தும் நிபுணரால் [17][18],
விவரிக்கப்பட வேண்டியது:



கருவியை
சோதனையிடப்பட்டு
பறிமுதல் செய்யப்பட்ட
நபரின் பெயர் மற்றும்
கையொப்பம்



பறிமுதல்
செய்யப்பட்ட தேதி
மற்றும் நேரம்



பறிமுதல்
செய்யப்பட்ட இடம்



பறிமுதல் செய்யப்பட்ட
சாதனங்களின்
விளக்கம் (உற்பத்தி,
மாதிரி, வரிசை
எண்/IMEI/UID/UID/MAC)

0000 1111
0000 2222

HASH மதிப்பு (Hash
அறிக்கையுடன்)



நிபுணரால் தாக்கல்
செய்யப்பட வேண்டிய
சான்றிதழ் மற்றும்
அனைத்து
தொடர்புடைய
விவரங்களுடன்
முறையாக
கையொப்பமிடப்பட்டது



பறிமுதல்
செய்யப்பட்டபோது
இருந்த
சாட்சிகளின்
பெயர்கள்



பறிமுதலுக்கா
ன காரணம்



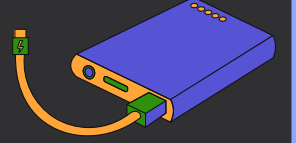
சோதனை மற்றும் பறிமுதல்
செயல்முறை மின்னணு முறையில்
அல்லது மொபைல் போன் மூலம் பதிவு
செய்யப்பட வேண்டும் என்று
கோரிக்கை வைக்கவும்.



நீதிபதி அதை
வைத்தவுடன் பதிவின்
நகலைக் கோரவும்.



சரக்கு பட்டியல்



சரக்கு பட்டியல் [19]: சார்ஜர்கள் அல்லது உறைகள் உட்பட
கைப்பற்றப்பட்ட அனைத்து பொருட்களின் விரிவான சரக்கு
பட்டியலைக் கேளுங்கள்.

கைப்பற்றுவதற் கான காரணங்கள்



உங்கள் கருவிகள் ஏன் கைப்பற்றப்பட்டன என்பதற்கான குறிப்பிட்ட
காரணங்கள் மற்றும் எந்த சட்டத்தின் கீழ் கைப்பற்றப்பட்டது என்பது
குறித்து தெளிவாக விசாரிக்கவும்.



சட்ட ஆலோசனைக்கான அணுகல்

சோதனை நடக்கும்போது ஒரு வழக்கறிஞரை அணுகுவதற்கான
உங்கள் உரிமையை வலியுறுத்துங்கள்.



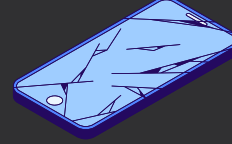
வாரண்ட்/ஆர்டர்களின் நகல்கள்:

பறிமுதல் ஒரு மாஜிஸ்திரேட்டின் வாரண்ட் அல்லது உத்தரவின் அடிப்படையில் நடந்திருந்தால் [20] பறிமுதல் செய்வதற்கு அங்கீகாரம் அளிக்கும் ஆவணங்களின் நகல்களைக் கோருங்கள். சம்பந்தப்பட்ட அங்கீகரிக்கப்பட்ட அதிகாரியால் கையொப்பமிடப்பட்டிருந்தால், வாரண்ட்/உத்தரவு நோக்கம் கொண்ட நபர்களின் சரியான விவரங்களைக் கொண்டிருக்கிறதா என்பதைச் சரிபார்க்கவும்.



கைப்பற்றலின் மதிப்பிடப்பட்ட காலம்

கருவிகள் எவ்வளவு காலம் வைத்திருக்கப்படும் மற்றும் அவற்றை திரும்பப் பெறுவதற்கான செயல்முறை பற்றி விசாரிக்கவும்.



நிபந்தனையின் ஆவணம்

உங்கள் சாதனங்களை ஒப்படைப்பதற்கு முன், அவற்றின் நிலையை (எ.கா., கீறல்கள், பற்கள்) புகைப்படங்கள் அல்லது வீடியோக்களுடன் ஆவணப்படுத்தக் கேளுங்கள்.

கூடுதல் ஆவணங்கள்



சூழ்நிலைகளைப் பொறுத்து, நீங்கள் கூடுதல் தகவல்களைக் கேட்கலாம்:

- பொறுப்பான விசாரணை அதிகாரியின் விவரங்கள்
- வழக்கு எண் உட்பட கைப்பற்றல் தொடர்பான புகார் அல்லது வழக்கு பற்றிய தகவல்
- அதிகாரிகள் பின்பற்றிய தொடர்புடைய கொள்கைகள் அல்லது நடைமுறைகளின் நகல்கள்

உங்கள் கருவியை நீண்ட காலமாக திரும்பப் பெறப்படாவிட்டால் என்ன செய்வது?

- * உங்கள் சாதனம் (device) எப்போது திருப்பிக் கொடுக்கப்படும் என்பதற்காக, அது நீதிமன்றத்தில் கொடுக்கப்பட்டதா என்பதைப் பொருத்தது. அது விசாரணை அல்லது வழக்கு நடக்கும் போது நீதிமன்றத்தில் கொடுக்கப்பட்டிருந்தால், அந்த வழக்கு முடிந்த பிறகு நீதிமன்றம் அதை திருப்பி கொடுக்க சொல்லலாம். BNSS 2023 என்ற சட்டத்தின் 497 மற்றும் 503 பிரிவுகளின் கீழ்தான் இது நடக்கும். இப்போது 497வது பிரிவில் இது பற்றி சற்று விளக்கம் கூட கொடுக்கப்பட்டுள்ளது, மேலும் எப்போது திருப்பிக்கொடுக்க வேண்டும் என்பதும் சொல்லப்பட்டுள்ளது.
- * ஆனால் உங்கள் பறிமுதல் செய்யப்பட்ட சொத்து (device) நீதிமன்றத்தில் சமர்ப்பிக்கப்படவில்லை என்றால், மகிஸ்திரேட் (Magistrate) தேவையாக இருக்கிறது என்று நினைத்தால், அதைப் பெறலாம் என்று உத்தரவு விடுவார். இதற்காக உங்களுக்கு 6 மாத காலம் வழங்கப்படும். [21]

எந்த சூழ்நிலையிலும், போலீசாரால் பறிமுதல் செய்யப்பட்ட சாதனங்களை திரும்ப பெறும் செயல்முறை உங்கள் வழக்கின் நிலைமைகளைப் பொறுத்து மாறுபடலாம். மேற்கண்ட எந்த ஒரு சூழ்நிலையிலும் உங்கள் சாதனம் பெற தயாராக இருந்தாலும், அதை எடுத்துக்கொள்வதில் சிக்கல்கள் ஏற்பட்டால், நினைவில் வைத்துக்கொள்ள வேண்டியது என்னவென்றால் – பறிமுதல் செய்யப்பட்ட சொத்துகளைத் திரும்ப பெறும் நடைமுறை உங்கள் வழக்கின் தனிப்பட்ட சூழ்நிலையைப் பொறுத்தே இருக்கும். இருப்பினும், நீங்கள் எடுக்கக்கூடிய அனைத்து நடவடிக்கைகளின் பொதுவான கண்ணோட்டம் கீழே கொடுக்கப்பட்டுள்ளன

தகவல்களைச் சேகரிக்கவும்: பறிமுதல் செய்யப்பட்ட குறிப்பிட்ட பொருட்களின் பட்டியலை உருவாக்கவும், வரிசை எண்கள், விளக்கங்கள், விவரக்குறிப்புகள் போன்ற அடையாளத் தகவல்கள் மற்றும் கொள்முதல் ரசீதுகள், விற்பனைப் பட்டியல்கள் அல்லது பதிவுச் சான்றிதழ்கள் போன்ற சொத்தின் உரிமையை நிரூபிக்கும் ஆவணங்கள் உட்பட.

காவல் நிலையத்தைத் தொடர்பு கொள்ளவும்: தேவையான தகவல்களைச் சேகரித்தவுடன், வழக்கு தாக்கல் செய்யப்பட்ட அல்லது உங்கள் சொத்து பறிமுதல் செய்யப்பட்ட அருகிலுள்ள காவல் நிலையத்திற்குச் செல்லவும். பொறுப்பிலுள்ள அதிகாரி, அல்லது விசாரணை அதிகாரி அல்லது சொத்துத் துறையில் உள்ள எந்தவொரு பணியாளரிடமும் பேசவும். உங்கள் சூழ்நிலையை விளக்கி, உங்கள் சொத்தை திரும்பப் பெறுமாறு கோருங்கள். பொறுமையாக, மரியாதையாக மற்றும் ஒத்துழைப்புடன் இருங்கள், உங்களிடம் உள்ள தொடர்புடைய ஆவணங்களை சமர்ப்பிக்கவும்.

சட்ட உதவியை நாடுங்கள்: காவல்துறையினர் ஒத்துழைக்கவில்லை என்றால் அல்லது செயல்முறை சிக்கலானதாகத் தோன்றினால், ஒரு வழக்கறிஞரிடம் சட்ட உதவியை நாடவும்.

உங்கள் சாதனம் திரும்பக் கிடைக்கும்போது பறிமுதல் செய்யப்பட்ட பிறகு சரிபார்க்க வேண்டிய பட்டியல்

1. பொது ஆய்வு

கருவிகள்
மற்றும்
சேவைகள்

மின்னஞ்சல், அரட்டை போன்ற அவர்கள் ஆய்வு செய்த அல்லது பறிமுதல் செய்த அனைத்து சாதனங்களையும், அவர்கள் பரிசோதித்த சேவைகளையும் விவரிக்கும் அதிகாரிகளிடமிருந்து ஒரு பட்டியலைப் பெறுங்கள், எனவே உங்கள் பறிமுதல் செய்யப்பட்ட தரவுத்தளத்துடன் நீங்கள் சரிபார்க்கலாம்.

தொடக்கம்
மற்றும்
செயல்பாடு

கருவியை ஆன் செய்து, அது சாதாரணமாக துவக்கப்படுவதை உறுதிப்படுத்தவும். இணைய இணைப்பு, app பயன்பாடு, கேமரா போன்ற அடிப்படை செயல்பாடுகள் மற்றும் அம்சங்களை சோதிக்கவும்.

கருவியை
திருப்பி
அனுப்புதல்

சோதனைக்குப் பிறகு, பறிமுதல் செய்யப்படாத அனைத்து கருவிகளையும் உங்களிடம் திருப்பி அனுப்பப்படுவதை உறுதிசெய்யவும்.

உடல்
நிலை

கருவியில் ஏதேனும் உடல் சேதம் உள்ளதா என்று சரிபார்க்கவும், சீல் அல்லது திருகுகளுடன் சேதப்படுத்தப்பட்ட அறிகுறிகள் உட்பட. சாதனத்தில் ஏதேனும் சந்தேகத்திற்கிடமான அடையாளங்கள் அல்லது சேதங்கள் இருந்தால் படங்கள்/ஆவணங்களாக எடுத்துவைக்கவேண்டும்

அமைப்புகள்
மற்றும்
உள்ளமைவு
கள்

ஏதேனும் அமைப்புகள், அணுகல் கட்டுப்பாடுகள் அல்லது உள்ளமைவுகள் மாற்றப்பட்டுள்ளதா என்று சரிபார்க்கவும், குறிப்பாக பாதுகாப்பு, தனியுரிமை அல்லது இருப்பிட(location) சேவைகளில் மாற்றம் உள்ளதா என்று சரிப்பார்க்கவும்.

உங்கள் சாதனம் திரும்பக் கிடைக்கும்போது பறிமுதல் செய்யப்பட்ட பிறகு சரிபார்க்க வேண்டிய பட்டியல்

1. பொது ஆய்வு

நிறுவப்பட்ட
மென்பொருள்/
பயன்பாடுகள்

உங்கள் தொலைபேசியில் ஏதேனும் புதிய மென்பொருள் அல்லது இயக்க முறைமை நிறுவப்பட்டுள்ளதா என்று சரிபார்த்து, அறியப்படாத அல்லது சந்தேகத்திற்கிடமான மென்பொருள் அல்லது பயன்பாடுகள் ஸ்பைவேர் மற்றும்/அல்லது தீம்பொருளின் அறிகுறிகளாக இருக்கலாம். அதனால் கைப்பற்றுவதற்கு முன்பு நீங்கள் நினைவில் வைத்திருந்த நிறுவப்பட்ட பயன்பாடுகளின் பட்டியலுடன் ஒப்பிடுக.

அசாதாரண
செயல்பாடு

உங்கள் சாதனத்தில் விவரிக்க முடியாத அல்லது அசாதாரண செயல்பாடு, அதிகப்படியான பேட்டரி வடிகால், தரவு பயன்பாடு, செயலிழந்த அம்சங்கள் போன்றவை ஸ்பைவேர் மற்றும்/அல்லது தீம்பொருளின் அறிகுறிகளாக இருக்கலாம்.

ஆன்லைன்
கணக்குகள்

மின்னஞ்சல், ஆன்லைன் சேமிப்பு, சமூக ஊடகங்கள் போன்றவை. உங்களால் பயன்படுத்தப்படாத வேறு ஏதேனும் சாதனங்கள் உள்நுழைந்துள்ளதா என்று பார்க்கவும். உங்களுக்குப் பழக்கமில்லாத சாதனங்கள் ஏதேனும் கண்டால், உங்கள் கணக்கைப் பாதுகாக்க அவற்றை அகற்ற உடனடியாக நடவடிக்கை எடுக்கவும். இதை வழக்கமாக கணக்கின் பாதுகாப்பு அமைப்புகள் மூலம் செய்யலாம்.

உங்கள் சாதனம் திரும்பக் கிடைக்கும்போது பறிமுதல் செய்யப்பட்ட பிறகு சரிபார்க்க வேண்டிய பட்டியல்

2. தரவு ஒருமைப்பாடு

தரவு சரிபார்ப்பு

உங்கள் தரவு அனைத்தும் அப்படியே உள்ளதா என்பதைச் சரிபார்க்கவும். எதுவும் காணாமல் போகவில்லை அல்லது சிதைந்துவிடவில்லை என்பதை உறுதிப்படுத்த கோப்புகள், புகைப்படங்கள், ஆவணங்கள், மெட்டாடேட்டா மற்ற அனைத்தையும் சரிபார்க்கவும்.

கோப்பு நேர முத்திரைகள்

உங்கள் சாதனத்தில் உள்ள முக்கியமான கோப்புகள் மற்றும் ஆவணங்களின் நேர முத்திரைகளை ஆராயுங்கள், ஏனெனில் சேதப்படுத்தப்பட்ட நேர முத்திரைகள் அங்கீகரிக்கப்படாத அணுகல் அல்லது மாற்றத்தைக் குறிக்கலாம்.

கோப்பு ஹாஷ்கள்

கைப்பற்றுவதற்கு முன்னும் பின்னும் முக்கியமான கோப்புகளின் கிரிப்டோகிராஃபிக் ஹாஷ்களை உருவாக்கி ஒப்பிடுக. முரண்பாடுகள் கோப்பு மாற்றம் அல்லது மாற்றத்தை சுட்டிக்காட்டலாம்.

தடயவியல் கருவி ஸ்கேன்கள்

மறைக்கப்பட்ட கோப்புகள், ஸ்பைவேரின் தடயங்கள் அல்லது ரூட்கிட்களுக்காக உங்கள் கருவியை ஸ்கேன் செய்ய தீம்பொருள் எதிர்ப்பு மற்றும் தடயவியல் மென்பொருளைப் பயன்படுத்த கருதுங்கள். இந்த கருவிகள் சிக்கலானதாக இருக்கலாம், எனவே தரவு மீட்பு அல்லது இணைய பாதுகாப்பு நிபுணரை அணுகுவது உதவியாக இருக்கும்.

உங்கள் சாதனம் திரும்பக் கிடைக்கும்போது பறிமுதல் செய்யப்பட்ட பிறகு சரிபார்க்க வேண்டிய பட்டியல்

3. கூடுதல் பரிசீலனைகள்

காப்புப் பிரதி பதிவுகள்

உங்கள் கருவி அதை ஆதரித்தால், பறிமுதல் காலத்தில் ஏதேனும் காப்புப் பிரதி பதிவுகள் அல்லது கணினி பதிவுகள் அசாதாரணமான அல்லது அங்கீகரிக்கப்படாத செயல்பாட்டைக் காட்டுகிறதா என்று சரிபார்க்கவும்.

கிளவுட் சேமிப்பகம்

அங்கீகரிக்கப்படாத அணுகல் அல்லது மாற்றங்களுக்கு கருவியுடன் தொடர்புடைய உங்கள் கிளவுட் சேமிப்பக கணக்குகளை மதிப்பாய்வு செய்யவும்.

ஆவணப் படுத்தல்

நேர முத்திரைகள், ஸ்கிரீன் ஷாட்கள் மற்றும் சந்தேகத்திற்கிடமான செயல்பாடு குறித்த குறிப்புகள் உட்பட உங்கள் கண்டுபிடிப்புகளின் விரிவான பதிவை வைத்திருங்கள். நீங்கள் சட்ட நடவடிக்கை எடுக்க வேண்டியிருந்தால் இந்த ஆவணம் முக்கியமானது.

கடவுச்சொல் மேலாண்மை

உங்கள் சாதனம் மற்றும் எந்தவொரு ஆன்லைன் கணக்குகளுடன் தொடர்புடைய உங்களிடம் இருக்கும் கடவுச்சொற்கள் அனைத்தையும் மாற்றவும், ஏனெனில் உங்கள் கடவுச்சொற்களின் நகலை அதிகாரிகள் வைத்திருக்க முடியும்.

பிரிவு 5

தயார்நில:

உங்கள் சாதனங்களைப்
பாதுகாத்தல்

இன்றைய டிஜிட்டல் உலகில், எங்கள் சாதனங்கள் மற்றும் தரவு ஏராளமான தரவுகளை எடுத்துச் செல்கின்றன.

எங்கள் தரவு பாதுகாப்பாக இருப்பதை உறுதி செய்வதற்காக சாதனங்களைப் பாதுகாப்பது முக்கியமானது.



pA*s*0*D

இந்த அச்சுறுத்தல்களுக்குத் தயாராவது எளிமையானது மற்றும் முக்கியமானது. உங்கள் தொலைபேசி ஹேக் செய்யப்பட்டு உங்கள் செய்திகள் அனைத்தும் வெளிப்பட்டால் ஏற்படும் குழப்பத்தை கற்பனை செய்து பாருங்கள்! வலுவான கடவுச்சொற்களைப் பயன்படுத்துவதன் மூலமும், நீங்கள் ஆன்லைனில் என்ன பகிர்கிறீர்கள் என்பதில் கவனமாக இருப்பதன் மூலமும், மென்பொருளைப் புதுப்பித்த நிலையில் வைத்திருப்பதன் மூலமும், உங்கள் சூட்கேஸுக்கு ஒரு உறுதியான டிஜிட்டல் பூட்டை உருவாக்குகிறீர்கள். உங்கள் ஆன்லைன் வாழ்க்கையைப் பாதுகாப்பாக வைத்திருக்க ஒரு சிறிய விழிப்புணர்வு நீண்ட தூரம் செல்லும் என்பதை நினைவில் கொள்ளுங்கள். உங்கள் தரவைப் பாதுகாப்பாக வைத்திருக்க சில நல்ல முறைகள் கீழே கொடுக்கப்பட்டுள்ளன.

உங்கள் ஆன்லைன் செயல்பாட்டைப் பாதுகாப்பாக வைத்திருங்கள்

இதோ எப்படி:

உங்களை மறைத்துக் கொள்ளுங்கள்



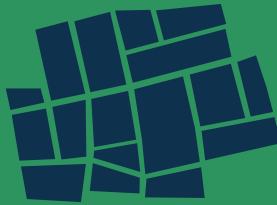
VPNகள் மற்றும் Tor ஐப் பயன்படுத்துவதன் மூலம் உங்கள் ஆன்லைன் செயல்பாட்டைப் பாதுகாக்கலாம். இது ஒரு ரகசிய உளவாளி ஒரு ரகசிய பணியின் போது மாறுவேடம் அணிவது போன்றது.

VPNகள்



உங்கள் இணைய போக்குவரத்துக்கு ஒரு பாதுகாப்பான சுரங்கப்பாதையை கற்பனை செய்து பாருங்கள். இது உங்கள் உண்மையான இருப்பிடத்தை மறைத்து, உங்கள் தரவை மறைக்கிறது, இது உங்களுக்கும் VPNக்கும் மட்டுமே உடைக்கக்கூடிய ஒரு ரகசிய குறியீடு போன்றது. உங்கள் செயல்பாட்டை பதிவு செய்யாத நம்பகமான VPN சேவையைத் தேர்ந்தெடுக்கவும்.

Tor



ரகசிய பாதைகளின் ஒரு பிரமை படத்தை கற்பனை செய்து பாருங்கள். Tor உங்கள் இணைய போக்குவரத்தை குறியாக்கம் செய்யப்பட்ட ரிலேகளின் அடுக்குகளின் மூலம் துள்ளுகிறது, இது கண்காணிக்க முடியாததாக ஆக்குகிறது. கூடுதல் தனியுரிமைக்கு Tor உலாவியைப் பதிவிறக்கவும்.

புத்திசாலித் தனமாகத் தேர்ந்தெடுக்கவும்



எல்லா தேடுபொறிகளும்(search engine) சமமாக உருவாக்கப்படவில்லை. சில, DuckDuckGo போன்றவை, தனியுரிமைக்கு முன்னுரிமை அளிக்கின்றன மற்றும் உங்கள் தேடல்களைக் கண்காணிக்காது. உங்கள் உலாவி வரலாற்றைப் பதிவு செய்தாலும், POST கோரிக்கைகளுடன் ஒரு தேடுபொறியைப் பயன்படுத்துவது உங்கள் கேள்விகளை மறைத்து வைக்கிறது.

மறைநிலை
க்குச்
(Incognito)செ
ல்லுங்கள்



உங்கள் உலாவியில் உள்ள "மறைநிலை பயன்முறையை" ஒரு ரகசிய முகவரின் முகமூடியாக நினைத்துப் பாருங்கள். இது உங்கள் உலாவல் வரலாறு, குக்கீகள் மற்றும் படிவத் தரவு சேமிக்கப்படுவதைத் தடுக்கிறது, இது உங்கள் ஆன்லைன் சாகசங்களை யாராவது உளவு பார்ப்பதை கடினமாக்குகிறது.

விழித்திரு
ங்கள்



இந்த கருவிகள் இருந்தும், சரியான தனியுரிமை ஒரு கட்டுக்கதை என்பதை நினைவில் கொள்ளுங்கள். நீங்கள் பார்வையிடும் வலைத்தளங்களைப் பற்றி எச்சரிக்கையாக இருங்கள், எப்போதும் பாதுகாப்பான இணைப்புகளை விரும்புங்கள் (பூட்டு ஐகானைத் தேடுங்கள்!), மேலும் முற்றிலும் அவசியம் இல்லாவிட்டால் ஆன்லைனில் தனிப்பட்ட விவரங்களைப் பகிர்வதைத் தவிர்க்கவும்.

வேகம் vs.
தனியுரிமை



VPNகள் மற்றும் Tor பயன்படுத்துவதனால் உங்கள் இணையத்தை சிறிது மெதுவாக்கலாம். இது ஒரு வர்த்தகம்: நிறைய தனியுரிமைக்கு கொஞ்சம் குறைவான வேகம். உங்களுக்கு எது சிறந்தது என்பதைத் தேர்ந்தெடுக்கவும்.

கூடுதல் உதவிக்குறிப்பு:

உங்கள் தரவை அவர்கள் எவ்வாறு கையாளுகிறார்கள் என்பதைப் புரிந்துகொள்ள, நீங்கள் பயன்படுத்தும் எந்தவொரு கருவியின் தனியுரிமைக் கொள்கைகள் மற்றும் சேவை விதிமுறைகளை எப்போதும் சரிபார்க்கவும். இந்த எளிய வழிமுறைகளைப் பின்பற்றுவதன் மூலம், உங்கள் ஆன்லைன் தனியுரிமையைக் கட்டுப்படுத்தலாம் மற்றும் உங்கள் டிஜிட்டல் வாழ்க்கையை உங்கள் சொந்த பூட்டு மற்றும் சாவியின் கீழ்

வேலை சாதனங்கள் VS. தனிப்பட்ட சாதனங்கள்

உங்களிடம் இரண்டு சூட்கேஸ்கள் இருப்பதாக கற்பனை செய்து பாருங்கள்: ஒன்று உங்கள் அலுவலக வாழ்க்கைக்கும் மற்றொன்று உங்கள் தனிப்பட்ட சாகசங்களுக்கும். உங்கள் வேலை மடிக்கணினி மற்றும் தொலைபேசியை தனித்தனியாக வைத்திருப்பது அந்த தனி சூட்கேஸ்களை வைத்திருப்பது போன்றது - இது உங்களை ஒழுங்காக வைத்திருக்கவும் உங்கள் தொழில் மற்றும் தனிப்பட்ட உலகங்களை பாதுகாக்கவும் உதவுகிறது.



உங்கள் தனிப்பட்ட மற்றும் தொழில் வாழ்க்கைக்கு வெவ்வேறு கருவிகள் வைத்திருப்பதைக் கவனியுங்கள்.



A. தரவு துப்பறியும் நிபுணர்: தனித்தனி கருவிகளைப் பயன்படுத்துவதன் மூலம், தனிப்பட்ட மற்றும் தொழில்முறை தரவுகள் ஒன்றோடொன்று கலக்கும் அபாயத்தைக் குறைத்து, பாதுகாப்பு மற்றும் தனியுரிமையை உறுதிப்படுத்தலாம். வேலை மற்றும் தனிப்பட்ட விஷயங்களுக்கு வெவ்வேறு சாதனங்களைப் பயன்படுத்துவதன் மூலம், நீங்கள் அடிப்படையில் ஒரு தரவு துப்பறியும் நிபுணர் ஆகிறீர்கள்! உங்கள் வேலை கோப்புகள் உங்கள் தனிப்பட்ட புகைப்படங்களில் நுழைவதையும், அதற்கு நேர்மாறாகவும் தடுக்கிறீர்கள். இது எல்லாவற்றையும் பாதுகாப்பாகவும், தனிப்பட்டதாகவும் வைத்திருக்கிறது, வெவ்வேறு சாவினைக் கொண்ட இரண்டு பூட்டிய பெட்டிகள் போன்றவை.

B. அணுகல் கட்டுப்பாட்டு நிபுணர்: தெளிவான பிரிப்பு முக்கியமான வேலை தொடர்பான தகவல்களுக்கான அணுகலைக் கட்டுப்படுத்த உதவுகிறது, தற்செயலான வெளிப்பாடு அல்லது தரவு மீறல்களின் அபாயத்தைக் குறைக்கிறது. உங்கள் வேலை மற்றும் தனிப்பட்ட சாதனங்களை தனித்தனியாக வைத்திருப்பது உங்கள் அலுவலக பெட்டிக்கான ஒரு ரகசிய குறியீட்டைப் போன்றது. அங்கீகரிக்கப்பட்ட நபர்கள் மட்டுமே (உங்களைப் போன்றவர்கள் மற்றும் உங்கள் முதலாளி) உங்கள் வேலை விஷயங்களை அணுக முடியும், அதே நேரத்தில் உங்கள் தனிப்பட்ட பெட்டி உங்கள் கண்களுக்கு மட்டுமே தனிப்பட்டதாக இருக்கும். இது தற்செயலான கசிவுகள் அல்லது திருட்டுத்தனமான பார்வைகளைத் தடுக்க உதவுகிறது, உங்கள் வேலை வாழ்க்கையை பாதுகாப்பாகவும் ஒழுங்கமைக்கப்பட்டதாகவும் வைத்திருக்கிறது.



C. பொறுப்பு சாம்பியன்: கருவிகளைப் பிரிப்பது வேலை தொடர்பான செயல்பாடுகள் மற்றும் தரவுகளுக்கான தெளிவான உரிமையை உறுதி செய்கிறது. தனித்தனி கருவிகள் வைத்திருப்பது யாருக்கு என்ன பொறுப்பு என்பதை தெளிவுபடுத்துகிறது. இது உங்கள் பெட்டிகளுக்கு லேபிளிடுவது போன்றது - அலுவலகத்தில் உள்ள வேலை பெட்டி உங்களுக்கு சொந்தமானது என்றும், தனிப்பட்ட பெட்டி நீங்கள் விரும்பும் எதையும் நிரப்ப உங்களுடையது என்றும் அனைவருக்கும் தெரியும். இது பணிகளைக் கண்காணிக்கவும், உங்களுக்கும் உங்கள் சக ஊழியர்களுக்கும் பொறுப்புக்கூறலை வைத்திருக்கவும் எளிதாக்குகிறது.

நினைவில் கொள்ளுங்கள், உங்கள் வேலை மற்றும் தனிப்பட்ட சாதனங்களை தனித்தனியாக வைத்திருப்பது இரண்டு கேஜெட்களை வைத்திருப்பது மட்டுமல்ல - இது உங்கள் தனியுரிமையைப் பாதுகாப்பது, ஒழுங்கமைப்பது மற்றும் உங்கள் வாழ்க்கையை எளிதாக்குவது பற்றியது. எனவே முன்னேறுங்கள், ஒரு தரவு துப்பறியும் நிபுணராகவும், அணுமதி கட்டுப்பாட்டு நிபுணராகவும், பொறுப்பு சாம்பியனாகவும் இருங்கள்! உங்கள் பெட்டிகளுக்கு லேபிளிடுவதை மறக்காதீர்கள்!

போனஸ் உதவிக்குறிப்பு: வித்தியாசமான சாதனங்களை பயன்படுத்தினாலும், நீங்கள் ஆன்லைனில் என்ன பகிர்கிறீர்கள், யாருக்கு அனுமதி அளிக்கிறீர்கள் என்பதில் எப்போதும் கவனமாக இருங்கள். எந்த சிஸ்டமும் 100% பாதுகாப்பானது இல்லை, எனவே எச்சரிக்கையுடன் இருங்கள் - இதன்மூலம் உங்கள் டிஜிட்டல் பயணத்தை மகிழ்ச்சியாக அனுபவிக்கலாம்!

உங்கள் தரவைப் பொக்கிஷமாகப் பாதுகாக்கவும்: மறையாக்கத்தின் அடுக்குகள் பற்றிய வழிகாட்டி

உங்கள் தரவை விலைமதிப்பற்ற ரகசியங்கள் நிறைந்த ஒரு புதையல் பெட்டியாக கற்பனை செய்து பாருங்கள். அந்த ரகசியங்களைப் பாதுகாப்பாக வைத்திருக்க, உங்களுக்கு பல பூட்டுகள் தேவை, இல்லையா?

குறியாக்க அடுக்குகள் இங்குதான் வருகின்றன!



முழு பெட்டி பூட்டு (FDE):

- El உங்கள் முழு ஹார்டு டிரைவையும் மறையாக்கம் செய்யுங்கள் – இது முழு புதையல் பெட்டியையே ஒரு பெரிய, வலிமையான பூட்டால் பூட்டுவது போல இருக்கிறது.
- BitLocker (Windows), FileVault (macOS) அல்லது VeraCrypt (மூன்றாம் தரப்பு) போன்ற கருவிகளைப் பயன்படுத்தவும்.



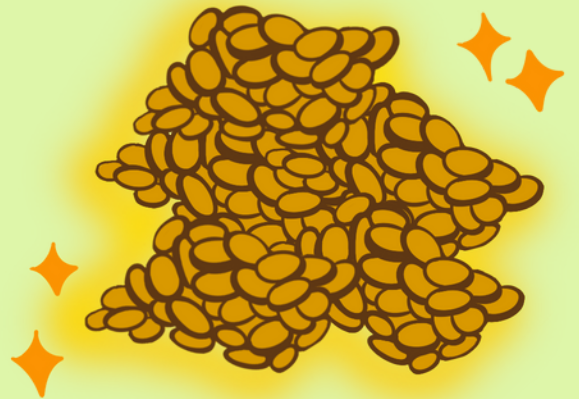
ரகசிய பெட்டகப் பூட்டுகள் (OS-நிலை):

- macOS-இல் மறையாக்கம் செய்யப்பட்ட டிஸ்க் படங்களை உருவாக்குங்கள் – இது புதையல் பெட்டிக்குள் இருக்கும் ரகசியப் பெட்டிகளைப் போலாகும்.
- சில OS களில் மறைகுறியாக்கப்பட்ட கோப்பு முறைமைகளைப் பயன்படுத்தவும் (மறைக்கப்பட்ட பெட்டிகள் போன்றவை).



தனிப்பட்ட ஜெம் பைகள் (ஆப்-நிலை)

- குறிப்புகள், கடவுச்சொற்கள், செய்திகள் போன்ற முக்கியமான ரத்தினங்களை, உட்பொதிந்த மறையாக்கம் கொண்ட செயலிகள் மூலம் பாதுகாக்கவும்.
- கடவுச்சொல் மேலாளர்கள், பாதுகாப்பான குறிப்பு எடுக்கும் பயன்பாடுகள் மற்றும் இறுதி முதல் இறுதி வரை மறைகுறியாக்கத்துடன் கூடிய செய்தி பயன்பாடுகளைப் பற்றி சிந்தியுங்கள் (எ.கா., சிக்னல், வாட்ஸ்அப்).



முக்கிய நினைவூட்டல்கள்:

- ஒவ்வொரு பூட்டுக்கும் வலிமையானதும், தனித்தன்மை கொண்டதும் ஆன கடவுச்சொற்கள் அல்லது சாவிகளை பயன்படுத்தவும்..
- பூட்டுகளை பளபளப்பாகவும் பாதுகாப்பாகவும் வைத்திருக்க உங்கள் மென்பொருளை தவறாமல் புதுப்பிக்கவும்.
- உங்கள் மறைகுறியாக்கப்பட்ட தரவை (புதையல் வரைபடங்கள்!) காப்புப் பிரதி எடுக்கவும், நீங்கள் அதை மீண்டும் கண்டுபிடிக்க வேண்டியிருந்தால்.



இந்த மறையாக்கப் பூட்டுகளை அடுக்குகளாக அமைப்பதன் மூலம், உங்கள் தரவுக்காக ஒரு கோட்டையை உருவாக்குகிறீர்கள் – இது யாராலும் உங்கள் டிஜிட்டல் புதையல்களை திருட கடினமாக்கும்!

தனியுரிமை மற்றும் சைபர் பாதுகாப்பு உறுதி செய்தல்: ஆன்லைன் மற்றும் ஆப்லைன்



காணாமல் போகும் செய்தி சேவைகள் அல்லது அனுப்பப்பட்ட செய்திகளைப் பார்த்த பிறகு அல்லது ஒரு குறிப்பிட்ட காலத்திற்குப் பிறகு தானாகவே நீக்கும் பயன்பாடுகளைப் பயன்படுத்தவும். சிக்னல், டெலிகிராம் மற்றும் வாட்ஸ்அப் போன்ற பயன்பாடுகள் காணாமல் போகும் செய்தி அம்சங்களை வழங்குகின்றன, இதன் மூலம் தகவல்தொடர்பு தற்காலிகமாக இருப்பதை உறுதிசெய்கிறது மற்றும் படிக்கப்பட்ட பிறகு அல்லது ஒரு குறிப்பிட்ட காலக்கெடுவுக்குப் பிறகு அரட்டைகள் அல்லது வரலாறுகளில் நிலைத்திருக்காது.



அடையாளம் உறுதி செய்ய (authentication) கடவுச்சொல் அல்லது பின் எண் (PIN) பயன்படுத்துவது சிறந்தது; காரணம், கைரேகை (fingerprint) அல்லது முகம் அடையாளம் காணும் (Face ID) முறைகள் பயனர் முழுமையான மன ஒப்புதலோ சிந்தனையோ இல்லாமலேயே செயல்படுகின்றன. ஆனால், கடவுச்சொல் அல்லது பின் எண் பயன்படுத்துவதால், அந்த கருவிகள் அல்லது தகவலுக்கு அணுகும் முழு கட்டுப்பாடும் பயனரின் அறிவார்ந்த செயல்பாட்டிலும் மன ஒப்புதலிலும் தங்கியிருக்கும். இது பாதுகாப்பையும், தனிநபர் கட்டுப்பாட்டையும் மேம்படுத்துகிறது.



பாதுகாப்பை மேம்படுத்த ஒரு நல்ல உத்தியாக, கடவுச்சொற்களின் ஒரு பகுதியை பாஸ்வேர்ட் மேனேஜரில் (Password Manager) சேமித்து, மீதியைக் நினைவில் வைத்துக்கொள்வது சிறந்தது. ஒரு பகுதியை பாதுகாப்பான மேனேஜரில் வைக்கும் முறையும், மற்றொரு பகுதியை நினைவில் வைத்திருக்கும் முறையும் சேர்ந்து, இரு நிலை அடையாள உறுதிப்படுத்தலை உருவாக்குகிறது. இது உங்கள் கணக்குகளின் பாதுகாப்பை வலுப்படுத்துகிறது.

உதாரணமாக, "12345" என்ற பகுதியை பாஸ்வேர்ட் மேனேஜரில் பாதுகாப்பாக வைத்திருக்கலாம், மேலும் "fdsjrie" என்ற மற்றொரு பகுதியை மனதில் வைத்திருக்கலாம். இதைப் பயன்படுத்தி முழு கடவுச்சொல்லை "12345fdsjrie" என உருவாக்கலாம். இந்த முறையால் பாதுகாப்பும் வசதியும் சமநிலையாகிறது – பாஸ்வேர்ட் மேனேஜரின் மறையாக்கம் வழங்கும் பாதுகாப்பையும், உங்கள் நினைவாற்றலின் தனிப்பட்ட பகுதியும் சேர்ந்து, அங்கீகரிக்கப்படாத நபர்கள் உங்களுடைய கணக்குகளுக்கு அணுகுவது கடினமாகிறது.

இரட்டை அடையாள உறுதிப்படுத்தலை (Two-Factor Authentication – 2FA) அமல்படுத்துவதன் மூலம், கணக்குகளின் பாதுகாப்பை பெரிதும் மேம்படுத்தும். இதற்காக, SMS அல்லது மின்னஞ்சல் அடிப்படையிலான 2FA முறைகளுக்குப் பதிலாக TOTP (Time-Based One-Time Password) அடிப்படையிலான 2FA முறையைத் தேர்ந்தெடுக்குவது மிகவும் பாதுகாப்பானதாகக் கருதப்படுகிறது. TOTP என்பது ஒவ்வொரு குறியீட்டின் நேர இடைவெளியிலும், பொதுவாக 30 விநாடிகளுக்கு ஒருமுறை, மாறிக்கொண்டிருக்கும் தனிப்பட்ட குறியீட்டை உருவாக்கும் முறை ஆகும். இது அனுமதியற்ற அணுகல்களைத் தடுக்கும் மேலதிக பாதுகாப்பு அடுக்காக செயல்படுகிறது.

TOTP குறியீடுகளை உருவாக்கும் Google Authenticator, Authy அல்லது Microsoft Authenticator போன்ற அங்கீகார பயன்பாடுகளைப் பயன்படுத்துவது மிகவும் பாதுகாப்பான விருப்பமாகும். இந்த பயன்பாடுகள் உங்கள் கணக்குகளுடன் இணைக்கப்பட்ட நேர உணர்திறன் குறியீடுகளை உருவாக்குகின்றன மற்றும் SMS அல்லது மின்னஞ்சல் போன்ற தகவல்தொடர்பு சேனல்களை நம்பவில்லை, இது SMS அடிப்படையிலான 2FA ஐ சமரசம் செய்யக்கூடிய இடைமறிப்பு அல்லது SIM மாற்றுதல் தாக்குதல்களின் அபாயத்தை குறைக்கிறது.

TOTP அடிப்படையிலான 2FA ஐப் பயன்படுத்துவதன் மூலம், உங்கள் கணக்குகளுக்கான அங்கீகரிக்கப்படாத அணுகலுக்கான வாய்ப்புகளை கணிசமாகக் குறைக்கும் கூடுதல் பாதுகாப்பைச் சேர்க்கிறீர்கள், இது பல்வேறு சைபர் அச்சுறுத்தல்களுக்கு எதிராக மிகவும் வலுவான பாதுகாப்பை வழங்குகிறது.

! கோப்புகளை நீக்குவது உங்கள் தனியுரிமையைப் பாதுகாக்க போதுமானதாக இல்லை! "நீக்கு" என்பதைக் கிளிக் செய்வது அவற்றை என்றென்றும் மறைந்துவிடச் செய்யாது. அவை இன்னும் உங்கள் கருவிகளில் மறைந்துள்ளன, சிறப்பு கருவிகளைக் கொண்டு கண்டுபிடிக்கக் காத்திருக்கின்றன. விஷயங்களை உண்மையிலேயே தனிப்பட்டதாக வைத்திருக்க, நீங்கள் அந்த கோப்புகளை துண்டாக்க வேண்டும். காகித ஆவணங்களைத் துண்டாக்குவது போல் நினைத்துப் பாருங்கள் – அவற்றை மீண்டும் ஒன்றாக இணைப்பது கிட்டத்தட்ட சாத்தியமற்றது! துண்டாக்கும் மென்பொருள் உங்கள் கோப்புகளை சீரற்ற எழுத்துக்கள் மற்றும் எண்களுடன் மேலெழுதும், அவற்றை சிதைத்து படிக்க முடியாததாக ஆக்குகிறது. அது துண்டாக்கப்பட்ட காகிதத்தை தூக்கி எறிந்து ஆழமாக நிலத்தடியில் புதைப்பது போன்றது. யாரும் அதைத் தோண்டி உங்கள் ரகசியங்களைப் படிக்க முடியாது! எனவே, அடுத்த முறை நீங்கள் முக்கியமான ஒன்றை நீக்க விரும்பினால், "நீக்கு" பொத்தானைத் தவிர்த்து, சில துண்டாக்கும் மென்பொருளைப் பிடிக்கவும். உங்கள் டிஜிட்டல் வாழ்க்கையை தனிப்பட்டதாகவும் பாதுகாப்பாகவும் வைத்திருக்க இதுவே சிறந்த வழி.

ITor மூலம் இணையதளங்களை அணுகுவது மேம்பட்ட தனியுரிமை மற்றும் பாதுகாப்பை உறுதி செய்கிறது. உதாரணமாக, கூடுதல் அநாமதேயத்திற்காக Tor ஐப் பயன்படுத்தி The Guardian போன்ற செய்தி தளங்கள் அல்லது Twitter போன்ற சமூக ஊடக தளங்களைப் பார்க்கலாம்.



பொருட்களை மறைத்தல்: ஆன்லைன் மற்றும் ஆப்லைன்

ஆன்லைன்:

- **Crypt.ee:** அடையாளம் தெரிவிக்காமல் பதிவு செய்யும் வசதி, முடிவிலிருந்து முடிவிற்கு மறையாக்கம் (End-to-End Encryption), மேலும் கூடுதல் தனியுரிமைக்காக மறைக்கப்பட்ட கோப்புறை உருவாக்கும் வசதியையும் வழங்குகிறது.
- **Cryptomator:** தனிப்பட்ட சேவையகங்களில் மறைகுறியாக்கப்பட்ட கோப்புகளை சேமிக்கிறது, பயன்பாட்டை நிறுவிய பின் கோப்பு இருப்பிடங்களை கண்டுபிடிக்க முடியாதபடி செய்கிறது.

ஆப்லைன்:

- **Veracrypt:** : டிரைவ்கள் அல்லது சேமிப்பக சாதனங்களில் தரவைப் பாதுகாக்க மறைக்கப்பட்ட பகிர்வுகளை உருவாக்கவும்.
- **ரகசிய பெட்டிகள்:** தளபாடங்கள் அல்லது பொருட்களுக்குள் மறைக்கப்பட்ட பெட்டிகளில் மதிப்புமிக்க பொருட்களை மறைக்கவும்.
- **குறியாக்க அமைப்புகள்:** உங்களது எழுத்துப்பூர்வமான தகவல்கள் அல்லது சொத்துகளை மறையாக்கம் செய்து பாதுகாக்க, தனிப்பட்ட குறியீடுகள் அல்லது சைபர்கள் (ciphers) உருவாக்குங்கள்.

இந்த முறைகள் மேம்பட்ட தனியுரிமை மற்றும் பாதுகாப்பை வழங்குகின்றன, டிஜிட்டல் மற்றும் கருவியின் தோற்றங்களிலும், முக்கியமான தகவல்களைப் பாதுகாக்க வழிகளை வழங்குகின்றன.



I அரிதாகப் பயன்படுத்தப்படும் கோப்புகளை பாதுகாப்பான இடத்தில் (மறைகுறியாக்கப்பட்ட டிரைவ் அல்லது கிளவுட்) சேமித்து, உங்கள் டிஜிட்டல் டெஸ்க்டாப்பை தவறாமல் ஒழுங்கமைத்து, உங்களுக்கு இப்போது தேவையானதை மட்டும் வைத்திருங்கள். நகல்களை உருவாக்குவதற்குப் பதிலாக பழைய பதிப்புகளை காப்பகப்படுத்துங்கள், உங்கள் டிஜிட்டல் வாழ்க்கையை ஒழுங்கமைத்து பாதுகாப்பாக வைத்திருங்கள்.



உங்கள் டிஜிட்டல் கைரேகைகளை விட்டுவிடாமல் ஒரு தளத்தில் சேர வேண்டுமா? பின்வருவனவற்றைத் தேர்ந்தெடுக்கவும்:

- குறைந்த தகவல்களைக் கேளுங்கள்: ஒரு பயனர் பெயர் மற்றும் ஒரு வேளை ஒரு மின்னஞ்சல், ஒரு ரகசிய கைகுலுக்கல் போன்றவை.
- உங்களை கண்ணுக்கு தெரியாதவராக ஆக்குங்கள்: பெயரில்லையா? கவலை வேண்டாம்! நீங்கள் யார் என்று சொல்லாமல் சில தளங்கள் உங்களை பதிவு செய்ய அனுமதிக்கின்றன.
- போலி மின்னஞ்சல் முகவரிகளை வழங்குங்கள்: சேர "தூக்கி எறியக்கூடிய" மின்னஞ்சலைப் பயன்படுத்தவும், உங்கள் உண்மையான மின்னஞ்சலை தனிப்பட்டதாக வைத்திருங்கள்.

சொற்களின் சொற்களஞ்சியம்:

ஆடியோ-வீடியோ மின்னணு சாதனங்கள்: இது, வீடியோ மாநாடுகள் நடத்தல், அடையாளம் நிரூபிக்கும் செயல்முறைகளை பதிவு செய்தல், சோதனை மற்றும் பரிமுதல் நடவடிக்கைகள், ஆதாரங்களை சேகரித்தல், மின்னணு தகவல்களை அனுப்புதல் மற்றும் மாநில அரசு விதிமுறைகளில் குறிப்பிடப்பட்டுள்ள பிற பயன்பாடுகளுக்காக பயன்படுத்தப்படும் எந்தவொரு தகவல் தொடர்பு சாதனத்தையும் குறிக்கிறது .

கைது: ஒரு நபர் சட்டப்பூர்வ காவலில் எடுக்கப்பட்டு தடுத்து வைக்கப்படும்போது / அடைக்கப்படும்போது, அவர்கள் ஒரு குற்றத்தைச் செய்ததாக எந்தவொரு குற்றச்சாட்டு அல்லது குற்றச்சாட்டு இருந்தாலும் இல்லாவிட்டாலும், அவர்கள் கைது செய்யப்பட்டதாகக் கூறப்படுகிறது. எந்த குற்றச்சாட்டுகளும் தாக்கல் செய்யப்படாமலோ அல்லது வாரண்ட் இல்லாமலோ ஒரு நபர் கைது செய்யப்படலாம் (அறியக்கூடிய குற்றங்களைப் பார்க்கவும்).

ஜாமினுக்குரிய குற்றங்கள்: அதிதீவிரமல்லாத அல்லது மிகுந்த பாளையமில்லாத குற்றங்கள் ஜாமினுக்குரிய குற்றங்களாக வகைப்படுத்தப்படுகின்றன. இந்தவகை குற்றங்களில், குற்றஞ்சாட்டப்பட்டவர் அல்லது கைது செய்யப்பட்டவர் ஜாமின் கோருவதற்கான உரிமையைக் கொண்டிருப்பார். இத்தகைய குற்றங்களில் விசாரணை அதிகாரி, வழக்கறிஞரால் நிர்ணயிக்கப்படும் ஜாமின் பத்திரம் தாக்கல் செய்யும் நிபந்தனையுடன், ஜாமினை வழங்க வேண்டிய கட்டாயம் உள்ளார். ஆனால், ஜாமின் வழங்கப்படுவது குற்றஞ்சாட்டப்பட்டவர் முற்றிலும் விடுவிக்கப்பட்டுவிட்டார் என்பதல்ல; அவர் நீதிமன்ற விசாரணை முடிவடையும் வரை நீதிமன்ற நடைமுறைகளுக்கு உட்பட்டவராகவே இருப்பார்.

குற்றச்சாட்டு: ஒரு நபர் குற்றம் செய்துள்ளார் என்று அரசியல் வழக்கறிஞர் (Prosecutor) அல்லது போலீஸ்/விசாரணை அதிகாரி ஆகியோரால் அதிகாரப்பூர்வமாக சாட்டப்படும் குற்றமாக இது விளக்கப்படுகிறது.[23] இதன் அடிப்படையில், குற்றச்சாட்டுகள் எதற்காக விதிக்கப்பட்டுள்ளன என்பது குற்றஞ்சாட்டப்பட்ட நபருக்கு தெளிவாக தெரிவிக்கப்பட வேண்டும்.

அறியக்கூடிய குற்றங்கள்: மஜிஸ்திரேட்டின் முன்அனுமதியோ அல்லது வாரண்ட் இல்லாமலே ஒரு போலீஸ் அதிகாரி கைது செய்யக்கூடிய குற்றங்கள் அறிவிக்கத்தக்க (Cognizable) குற்றங்கள் ஆகும். [24] இந்த நடவடிக்கை, முதல் தகவல் அறிக்கை (FIR) பதிவு செய்யப்பட்டதா இல்லையா என்பதைக் கருத்தில் கொள்ளாமல் நடைபெறலாம். இத்தகை குற்றங்கள் பொதுவாக மிக தீவிரமான அல்லது படுகாயம் விளைவிக்கும் குற்றங்களுக்கு நடைமுறையாகும்.

கணினி: மின்னணு, காந்த, ஒளி அல்லது வேறு அதிவேக தரவியல் செயலாக்க சாதனம் அல்லது அமைப்பை இது குறிக்கும். இது மின்னணு, காந்தம் அல்லது ஒளி இழைகள் (impulses) மூலம் தார்க்கிக் (logical), கணித (arithmetic) மற்றும் நினைவகச் செயல்பாடுகளை இயங்கச் செய்கிறது. இதில் உள்ளீடு (input), வெளியீடு (output), செயலாக்கம் (processing), சேமிப்பு (storage), கணினி மென்பொருள் (software), மற்றும் தகவல் தொடர்பு வசதிகள் (communication facilities) போன்றவை – அந்த கணினி, கணினி அமைப்பு (computer system) அல்லது கணினி வலையமைப்புடன் (computer network) இணைக்கப்பட்டவை அல்லது தொடர்புடையவை – அனைத்தும் அடங்கும்.

தகவல் தொடர்பு கருவி: இது ஒரு செல்பேசி, தனிப்பட்ட டிஜிட்டல் உதவியாளருக்கான கருவி (Personal Digital Assistant), அல்லது இந்த இரண்டும் இணைந்த ஒருங்கிணைந்த கருவியாகவும் இருக்கலாம். மேலும், உரை (text), வீடியோ (video), ஆடியோ (audio) அல்லது படம் (image) போன்றவற்றை தொடர்புகொள்க, அனுப்ப அல்லது ஒளிபரப்ப பயன்படுத்தப்படும் ஏதேனும் தகவல் தொடர்பு கருவியாகவும் இருக்கலாம்.

குக்கீகள்: வலை உலாவியில் உங்கள் செயல்பாட்டைக் கண்காணித்து பதிவு செய்யும் தகவல்/தரவின் சிறிய கோப்புகள் குக்கீகள் ஆகும். அவை விளம்பரம் மற்றும் பகுப்பாய்வு சேவைகளுக்காக பயனர் செயல்பாட்டைப் பதிவு செய்யப் பயன்படும். குக்கீகளில் பயனர்களின் பயனர் பெயர் மற்றும் கடவுச்சொல், விருப்பத்தேர்வுகள், வலைச் செயல்பாடு போன்ற தனிப்பட்ட தகவல்கள் இருக்கலாம். அவை பாதுகாக்கப்படாவிட்டால், அவை பயனர்களுக்கு சாத்தியமான பாதுகாப்பு மற்றும் தனியுரிமை ஆபத்தாக இருக்கலாம்.

சொற்களின் சொற்களஞ்சியம்:

மின்னணு தொடர்பு: இது தொலைபேசிகள், கணினிகள், ஆடியோ-வீடியோ பிளேயர்கள், கேமராக்கள் அல்லது பிற மின்னணு கருவிகள் அல்லது மத்திய அரசால் குறிப்பிடப்பட்ட வேறு எந்த மின்னணு வடிவம் ஆகியவற்றைப் பயன்படுத்தி, மக்கள் அல்லது கருவிகளுக்கு இடையே மின்னணு முறையில் பகிரப்படும் எந்தவொரு எழுதப்பட்ட, வாய்மொழி, சித்திர அல்லது வீடியோ தகவலையும் குறிக்கிறது.

மறையாக்கம்: தனிப்பட்ட அல்லது அதிக முக்கியத்துவம் வாய்ந்த தகவல்களை ஒரு குறியீட்டுப் பயன்முறை (code/cryptic form) மூலம் சேமிப்பதையே மறையாக்கம் என அழைக்கப்படுகிறது. இந்தத் தகவல்களை மீண்டும் வாசிக்கவோ புரிந்துகொள்வதற்கோ, அந்த தகவலுக்கு உரிய மறையீட்டு சாவி (decryption key) அவசியமாக இருக்க வேண்டும். இந்த முறையால், தகவல்களை செயலாக்கும், சேமிக்கும் மற்றும் பரிமாற்றும் செயல்கள் மேலும் பாதுகாப்புடன் நடைபெறும். இதனால், அனுமதியற்ற நபர்கள் அந்த தகவல்களை அணுகவோ அல்லது புரிந்துகொள்வதற்கோ முடியாது.

ஆதாரம்: ஆதாரம் என்பது, வாக்குமூலம் (தகவல் அல்லது பிரகடனம்) ஆக இருக்கக்கூடியது; இது வாய்மொழி அல்லது ஆவண வடிவில் இருக்கலாம் (எழுத்துப்பூர்வமாகவோ, மின்னணுவழியிலோ, டிஜிட்டல் சாதனங்களையும் உள்ளடக்கியதாகவோ). இது விசாரணை அல்லது தடயவியல் விசாரணைக்கு தொடர்புடையதாக இருக்கலாம். இவ்வகை ஆவணங்கள் ஆவண ஆதாரங்கள் (Documentary Evidence) என அழைக்கப்படுகின்றன. ஆதாரம் என்பது ஆண்மை (Proof) என்ற உறுதி செய்யப்பட்ட நிலையைவிட வேறுபட்டது. அது முடிவானதாக இருக்க வேண்டிய அவசியமில்லை, மேலும் அது நீதிமன்றத்தின் விருப்பத்திற்கும் (discretion) உட்பட்டதாகும்.

விசாரணை அதிகாரி (IO): ஒரு குற்றத்தை விசாரிக்க நியமிக்கப்பட்டுள்ள ஒரு போலீஸ் அதிகாரி.

கைமாறும் சொத்துகள்: BNS சட்டத்தில் கைமாறும் சொத்துகள் என்பது பல வகையான சொத்துகளைக் குறிக்கும்; உதாரணமாக ஜன்னல், கதவு, மரங்கள் போன்றவை. இதனால், பூமியுடன் நேரடியாக இணைக்கப்பட்டவையோ அல்லது பூமியுடன் இணைக்கப்பட்ட பொருள்களில் நிரந்தரமாக அடைக்கப்பட்டவையோ கைமாறும் சொத்துகளுக்குள் வராது. கைமாறும் சொத்துகளுக்கு பூமியுடன் இணைக்கப்படாத அனைத்து மின்னணு மற்றும் டிஜிட்டல் கருவிகளும் அடங்கும். [25]

ஜாமீனில் வெளிவர முடியாத குற்றங்கள்: மிக தீவிரமான அல்லது புணர்ச்சியான இயல்புடைய குற்றங்கள், அவற்றுக்கான குற்றஞ்சாட்டப்பட்டவருக்கு அல்லது கைது செய்யப்பட்டவருக்கு ஜாமின் கோர உரிமை இல்லை எனப்படும் குற்றங்கள். என்றாலும், குற்றஞ்சாட்டப்பட்டவர் ஓடிசெல்லும் அபாயம், நீதிமன்ற நடவடிக்கைகளுடன் ஒத்துழைக்காமை போன்ற காரணிகளின் அடிப்படையில், நீதிமன்றம் விருப்பப்படி ஜாமினை வழங்க முடியும்.

அறியப்படாத குற்றங்கள்: ஒரு போலீஸ் அதிகாரி, மஜிஸ்திரேட்டின் முன் அனுமதி அல்லது வாரண்ட் இல்லாமல் கைது செய்ய முடியாத குற்றங்களை அறிகுறாத குற்றங்கள் என கூறுகிறோம். [26] இத்தகைய நடவடிக்கைகள், முதலில் FIR (முதல் தகவல் அறிக்கை) பதிவு செய்யப்பட்ட பின்னர், மஜிஸ்திரேட்டிடமிருந்து வாரண்ட் பெற்ற பிறகு மட்டுமே நடக்கும். பொதுவாக, இவை குறைந்த தீவிரம் அல்லது சீர்கேடான இயல்புடைய குற்றங்களுக்கு பொருந்தும்.

இடம்: BNSS இன் கீழ், ஒரு இடம் ஒரு வீடு, கட்டிடம், கூடாரம், வாகனம் மற்றும் கப்பலாக இருக்கலாம். [27]

பொது இடம்: இது பொது போக்குவரத்து, ஹோட்டல்கள், கடைகள் அல்லது பொதுமக்களால் பயன்படுத்த அல்லது அணுகுவதற்காக உருவாக்கப்பட்ட வேறு எந்த இடத்தையும் உள்ளடக்கியது. [28]

சொற்களின் சொற்களஞ்சியம்:

கைப்பற்றல் குறிப்பு: விசாரணை நோக்கங்களுக்காக, ஒரு விசாரணை அதிகாரியால் குற்றம் சாட்டப்பட்ட ஒருவரிடமிருந்து ஏதேனும் சொத்து (மதிப்புமிக்க அல்லது விலைமதிப்பற்றது) கைப்பற்றப்பட்டால், அது ஒரு கைப்பற்றல் குறிப்பில் பதிவு செய்யப்பட்டு பதிவு செய்யப்படுகிறது. இதில் சொத்தின் விவரக்குறிப்புகள் / விவரங்கள் / விவரங்கள், சேமிப்பு இடம், கைப்பற்றல் இணைக்கப்பட்ட வழக்கின் விவரங்கள் போன்றவை உள்ளன.

வாரண்ட்: வாரண்ட் என்பது ஒரு நீதிபதி கையொப்பமிட்ட ஆவணமாகும், இது உங்களை கைது செய்யவோ அல்லது உங்கள் சொத்தை சோதனையிடவோ மற்றும் அந்த சொத்திலிருந்து சில பொருட்களை எடுக்கவோ போலீசாருக்கு அனுமதி வழங்குகிறது. வாரண்டைப் பார்க்க உங்களுக்கு உரிமை உண்டு, அது செல்லுபடியாகும் என்பதை உறுதிப்படுத்திக் கொள்ள வேண்டும்.

சோதனை மற்றும் பறிமுதல் பற்றிய சில குறிப்புகள்:

1. முன்னதாக, நீதிமன்றங்கள் சட்டவிரோதமான மற்றும் தவறான முறையில் பெறப்பட்ட ஆதாரங்களைச் சில சமயங்களில் ஏற்றுக்கொண்டிருக்கின்றன. இருப்பினும், அத்தகைய ஆதாரம் உண்மையானதாயும் மாற்றப்படாததாயும் இருப்பதை நிரூபிக்க வேண்டும். ஆதாரத்தின் ஏற்றுக் கொள்ளப்படுவதை பற்றிய தீர்மானம், ஒவ்வொரு வழக்கின் உண்மை நிலைகளும் சூழல்களும் அடிப்படையாகக் கொண்டு, நீதிமன்றங்கள் மட்டுமே செய்ய முடியும். [உமேஷ் குமார் v. ஆந்திரப் பிரதேசம், (2013) 10 SCC 169]
2. இருப்பினும், கேரள உயர் நீதிமன்றம், CrPC (இப்போது BNSS) இல் நிறுவப்பட்ட நடைமுறையைப் பின்பற்றாமல் ஒரு பத்திரிகையாளரின் மொபைல் போனை ஒரு போலீஸ் அதிகாரி பறிமுதல் செய்ய முடியாது என்று தீர்ப்பளித்தது. ஒரு குற்றத்தின் விசாரணைக்கு அத்தகைய சாதனம் அவசியமானால், அத்தகைய போலீஸ் அதிகாரிகள் சாதனத்தை முறையாகத் தேடி பறிமுதல் செய்வதற்கு CrPC (இப்போது BNSS) ஐப் பின்பற்ற வேண்டும். [29]
3. இந்திய அரசியலமைப்பின் 20(3) வது பிரிவில் சுய-குற்றச்சாட்டுக்கு எதிரான பாதுகாப்பைக் கருத்தில் கொண்டு, கடவுச்சொல்லை (அல்லது வேறு எந்த விவரங்களையும்) வழங்க ஒரு நபரை வற்புறுத்த முடியாது என்று டெல்லி உயர் நீதிமன்றம் தீர்ப்பளித்துள்ளது. [30]
4. அதேபோல், டெல்லியில் உள்ள ரவுஸ் அவென்யூ மாவட்ட நீதிமன்றத்தின் சிறப்பு சிபிஐ நீதிமன்றம், குற்றம் சாட்டப்பட்டவர் அத்தகைய தகவல்களை வழங்க கட்டாயப்படுத்த முடியாது என்றும், இந்த விஷயத்தில் அவர் இந்திய அரசியலமைப்பின் 20(3) வது பிரிவு மற்றும் BNSS இன் 180(2) வது பிரிவின் மூலம் பாதுகாக்கப்படுகிறார் என்றும் கூறியது. [31]
5. சோதனை மற்றும் பறிமுதல் நடைமுறைகளைப் புரிந்துகொள்வது, இதுபோன்ற தீவிரமான சூழ்நிலைகளில் நீங்கள் பீதியடைவதைத் தவிர்க்க உதவுவது மட்டுமல்லாமல், அதிகாரிகளுடன் சிறப்பாக ஒத்துழைக்கவும் உதவும். கூடுதலாக, இத்தகைய நடைமுறைகளை அறிவது சட்டம் ஒழுங்கை பராமரிக்கும் பொறுப்பில் உள்ளவர்களால் தவறாக நடத்தப்படுவதிலிருந்து தனிநபர்களைப் பாதுகாக்க முடியும்.

மின்னணு சாதனங்கள் மற்றும் சட்டம்

இந்த விஷயத்தில் நீதித்துறை நிலைப்பாடு இன்னும் தீர்க்கப்படவில்லை. இருப்பினும், BNSS, BSA, UAPA, வருமான வரிச் சட்டம், PMLA மற்றும் IT சட்டத்திற்குள் சோதனை மற்றும் பறிமுதல் தொடர்பாக பொதுவான வழிகாட்டுதல்கள் உள்ளன. இந்த சட்டங்கள் முழுவதும் சோதனை மற்றும் பறிமுதல் செயல்முறைகள் வேறுபடுகின்றன என்பதைக் கவனத்தில் கொள்ள வேண்டும், அவை பின்வருமாறு

பாரதிய நாகரிக சுரக்ஷா சன்ஹிதா வாரண்டுன்	பிரிவு 96- இந்த விதிமுறை, ஒரு காவல் அதிகாரி நீதிமன்றத்திடம் இருந்து ஒரு சிறப்பு அனுமதியைப் பெற வேண்டும் என்று கூறுகிறது. ஒரு சோதனை நடத்தப்பட வேண்டும் என்று நீதிமன்றம் நம்புவதற்கு ஒரு காரணம் இருந்தால், நீதிமன்றம் ஒரு சோதனைவாரண்ட் வழங்கப்படக்கூடிய நிபந்தனைகளை குறிப்பிடுகிறது. சோதனை / கைப்பற்றலுக்கு பொறுப்பான அதிகாரி, வாரண்ட் வழங்கப்பட்ட குறிப்பிட்ட பகுதிக்கு தன்னை கட்டுப்படுத்திக் கொள்ள வேண்டும். பிரிவு 103: இது சொத்துக்களைத் தேடுவதற்கும் கைப்பற்றுவதற்குமான ஒரு அடிப்படை விதிமுறை. காவல்துறையினர் சொத்துக்களைத் சோதனையிடும்போது அல்லது கைப்பற்றும்போதெல்லாம் இந்த விதிகளைப் பின்பற்ற வேண்டும்.
பாரதிய நாகரிக சுரக்ஷா சன்ஹிதா வாரண்டு இல்லாமல்	பிரிவு 185- ஒரு குற்றம் விரைவில் நடக்கக்கூடும் என்று அவர்கள் நினைத்தால் அல்லது அவர்களின் விசாரணைக்கு அது முக்கியமாக இருந்தால், காவல்துறையினர் சிறப்பு அனுமதி (வாரண்ட்) பெறாமல் ஒரு இடத்திற்குள் நுழைந்து சோதனையிடலாம். மேலும், ஒரு சோதனை நடத்தும் ஒரு காவல் அதிகாரி நடைமுறையைப் பதிவு செய்ய வேண்டும் என்று இப்போது விதிமுறை கட்டாயமாக்குகிறது. ஒரு அதிகாரி, சோதனை நடத்த முடியாவிட்டால், எழுத்துப்பூர்வமாக காரணங்களைப் பதிவு செய்த பிறகு, தனது கீழ்படிந்தவரை அவ்வாறு செய்யுமாறு கேட்கலாம். அத்தகைய சோதனையின் பதிவின் நகல்கள் நாற்பத்தெட்டு மணி நேரத்திற்குள் அருகிலுள்ள மாஜிஸ்திரேட்டுக்கு அனுப்பப்பட வேண்டும். விசாரணைகளின் போது அறிக்கைகள்: விசாரணையின் போது அவர்கள் செய்யும் எந்த அறிக்கையையும் ஒரு நபர் சான்றளிக்க வேண்டியதில்லை என்று கூறும் விதிகள் (பிரிவுகள் 180 மற்றும் 181 இல்) உள்ளன. மேலும், இந்திய அரசியலமைப்பால் பாதுகாக்கப்பட்ட, தங்களை குற்றவாளிகளாகக் காட்டக்கூடிய விஷயங்களைச் சொல்லாதிருக்க மக்களுக்கு உரிமை உண்டு.[32] வாரண்டுகள் இல்லாமல் கைதுகள்: பிரிவு 35 இன் படி, அந்த நபர் ஒரு தீவிர குற்றத்தில் ஈடுபட்டதாக அவர்கள் நினைத்தால், அவர்களுக்கு எதிராக ஒரு புகார் இருந்தால் அல்லது அவர்கள் ஒரு குற்றத்தில் ஈடுபட்டிருக்கிறார்கள் என்று நம்புவதற்கு ஒரு காரணம் இருந்தால், காவல்துறையினர் வாரண்ட் இல்லாமல் யாரையும் கைது செய்யலாம். இருப்பினும், ஒரு பலவீனமான நபர் அல்லது அறுபது வயதுக்கு மேற்பட்ட நபர் மூன்று வருடங்களுக்கு குறைவான சிறைத்தண்டனை விதிக்கக்கூடிய குற்றமாக இருந்தால், DSP இன் முன் அனுமதியின்றி கைது செய்யப்படக்கூடாது.
	பிரிவு 105 - என்பது புதிதாகச் சேர்க்கப்பட்ட ஒரு விதியாகும், இது இப்போது காவல் அதிகாரி சோதனை மற்றும் பறிமுதல் நடவடிக்கைகளை மொபைல் போன் மூலம் பதிவு செய்ய வேண்டும் என்று கூறுகிறது. சாட்சிகளால் கையொப்பமிடப்பட்ட பறிமுதல் செய்யப்பட்ட பொருட்களின் பட்டியலைத் தயாரிக்க வேண்டும் என்றும், அதை உடனடியாக மாவட்ட மாஜிஸ்திரேட் அல்லது முதல் வகுப்பு நீதித்துறை நடுவருக்கு அனுப்ப வேண்டும் என்றும் அது கூறுகிறது. பிரிவு 106ன் கீழ், ஒரு போலீஸ் அதிகாரி திருடப்பட்டதாக சந்தேகிக்கப்படும் எந்தவொரு சொத்தையும் பறிமுதல் செய்ய அதிகாரம் பெற்றிருப்பார். இத்தகைய விதிமுறை சில நேரங்களில் பொதுவான தேடல்களுக்காக தவறாக பயன்படுத்தப்படுகிறது, இதனால் அவர்கள் காணும் அனைத்து பொருட்களையும் கையகப்படுத்துகிறார்கள். இந்த பிரிவின் கீழ், குற்றம் நடத்தியதுடன் தொடர்புடையதாகவோ அல்லது திருடியதாகவோ சந்தேகிக்கப்படும் சொத்துகளை எந்த போலீஸ் அதிகாரியும் பறிமுதல் செய்யலாம். பறிமுதல் செய்யப்பட்ட சொத்துகள் குறித்த தகவல் அருகிலுள்ள மாஜிஸ்திரேட்டுக்கு போலீஸ் அதிகாரியால் அறிவிக்கப்பட வேண்டும். அவ்வாறு பறிமுதல் செய்யப்பட்ட சொத்துகளை, நீதிமன்றத்தில் தேவைப்படும் போதும் சமர்ப்பிக்கப்படும் என்பதற்கான பிணையெழுத்து மேற்கொண்டு, ஒரு நபரிடம் பாதுகாப்புக்காக ஒப்படைக்கும் உரிமை நீதிமன்றத்திற்கு உள்ளது.

பாரதிய சசுஷ்யா அதினியம்	பிரிவு 168- நீதிபதி பின்வருவனவற்றைச் செய்ய அதிகாரம் கொண்டுள்ளார் - • சம்பந்தப்பட்ட அல்லது தொடர்பில்லாதா உண்மைகள் தொடர்பான கேள்விகளைக் கேளுங்கள் - எந்த வகையிலும். • எந்த நேரத்திலும் எந்த தரப்பினருக்கும் சாட்சிகளுக்கும் கேள்விகளைக் கேளுங்கள். • எந்த ஆவணங்கள் அல்லது விஷயங்களையும் ஆதாரமாகத் தயாரிக்கக் கோருங்கள். முக்கியமாக, இந்த விதியின் கீழ் வழங்கப்பட்டுள்ளபடி, எந்தவொரு தனிநபரும் நீதிபதியின் கோரிக்கைகள் அல்லது தேவைகளுக்கு ஆட்சேபிக்க முடியாது. [குறிப்பிட்ட ஆவணங்கள் அல்லது பொருட்கள் ஆதாரமாக இருக்கக்கூடிய சோதனை மற்றும் பறிமுதல் தொடர்பான வழக்குகளில் இது முக்கியமாக இருக்கலாம்.]
PMLA	பிரிவுகள் 16 மற்றும் 17- இந்த பிரிவுகள் முறையே ஒரு சோதனை அல்லது பறிமுதல் நடத்துவதற்கான விதிகளை அமைக்கிறது. சோதனை அல்லது பறிமுதல் ஏன் நடக்கிறது என்பதற்கான எழுத்துப்பூர்வமான பதிவை அவை கோருகின்றன மற்றும் பறிமுதல் செய்யப்பட்ட பொருட்களின் பட்டியலுடன் ஒரு அறிக்கையைத் தயாரிக்க வேண்டும். [இது ஒரு சோதனை மற்றும் பறிமுதல் நடவடிக்கையின் போது தேவையான செயல்முறைக்கும் ஆவணத்திற்கும் இடையே ஒரு தொடர்பை உருவாக்குகிறது.]
UAPA	பிரிவு 43A - அதிகாரிகள் ஒரு சோதனை கீழ் அதிகாரிகளுக்கு அங்கீகரிக்க அனுமதிக்கிறது, மேலும் 'நம்பும் காரணங்கள்' தனிப்பட்ட அறிவு அல்லது மூன்றாம் தரப்பினரால் வழங்கப்பட்ட எழுத்துப்பூர்வ தகவல்களுக்கு காரணமாக இருக்க வேண்டும் என்று கட்டாயப்படுத்துகிறது. பிரிவு 43B - சோதனையிடப்படும் அல்லது பறிமுதல் செய்யப்படும் நபரின் உரிமைகளை விவரிக்கிறது. இந்த பிரிவுகள் ஒரு சோதனை அல்லது பறிமுதல் செய்யும் போது, சோதனையிடப்படும் நபருக்கு அவர்களின் தேடலுக்கான காரணங்கள் தெரிவிக்கப்பட வேண்டும் மற்றும் எடுக்கப்பட்ட விஷயங்கள் அருகிலுள்ள காவல் நிலையத்திற்கு கொண்டு வரப்பட வேண்டும் என்பதை உறுதி செய்கிறது. அங்குள்ள பொறுப்பிலுள்ள அதிகாரி CrPC (இப்போது BNSS) இல் குறிப்பிடப்பட்டுள்ள விதிகளைப் பின்பற்றி தேவையான நடவடிக்கைகளை எடுக்க வேண்டும்.
வருமான வரிச் சட்டம்	பிரிவு 132 - சட்டப்படி தேவைப்படும்போது யாராவது ஆவணங்கள் அல்லது பொருட்களை வழங்கவில்லை என்றால், இந்த பிரிவு ஆவணங்கள் அல்லது பொருட்களை பறிமுதல் செய்ய அதிகாரிகளுக்கு அதிகாரம் அளிக்கிறது. சோதனை மற்றும் பறிமுதல் குழுவில், ஒரு விசாரணை அல்லது சட்ட நடவடிக்கைகளின் போது குறிப்பிட்ட ஆவணங்கள் அல்லது பொருட்கள் தாமத முன்வந்து தயாரிக்கப்படாவிட்டால், அவற்றை பறிமுதல் செய்ய இந்த பிரிவு அதிகாரிகளுக்கு சட்டப்பூர்வ ஆதரவை அளிக்கிறது. பறிமுதல் செய்யப்பட்ட பொருட்கள் தொடர்பான அவர்களின் விளக்கத்தை ஆதரிக்க சான்றுகளை வழங்க குற்றம் சாட்டப்பட்ட நபர்களுக்கு நியாயமான வாய்ப்பு வழங்கப்பட வேண்டும் என்று கோருவதன் மூலம் இந்த பிரிவு குற்றம் சாட்டப்பட்ட நபர்களுக்கு போதுமான பாதுகாப்புகளை வழங்குகிறது.
IT சட்டம்	பிரிவு 80 - அங்கீகரிக்கப்பட்ட அதிகாரிகளுக்கு எந்தவொரு பொது இடத்தையும் சோதனையிடவும், பிடியாணை இல்லாமல் கைது செய்யவும் அதிகாரம் அளிக்கிறது - கடந்த காலத்திலோ, நிகழ்காலத்திலோ அல்லது எதிர்காலத்திலோ தகவல் தொழில்நுட்பச் சட்டத்தின் கீழ் குற்றம் செய்ததாக நியாயமான சந்தேகத்தின் பேரில் காணப்படும் எந்தவொரு நபரும் கைது செய்யப்படலாம்.

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: _____

படம் 1.
சான்றிதழ்

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.

படம் 2.

சான்றிதழ் (நிபுணரால் தாக்கல் செய்யப்பட வேண்டும்)

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.....
Address.....
(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.....

படம் 3.
பறிமுதல் பட்டியல்

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 from 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

படம் 3.1.
பறிமுதல் பட்டியல்

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

படம் 4.

கைது ஆணை

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)

படம் 5.

வடிவம் (BNSS இன் இரண்டாவது அட்டவணையில் அதிகாரப்பூர்வ கெஜட் அறிவிப்பில் வெளியிடப்பட்ட சட்டத்தின் 192 ஆம் பக்கத்தில் கொடுக்கப்பட்டுள்ளது)

REFERENCES:

- [1]** See glossary for the meaning of the word
- [2]** For explanation of search within the BNSS, see Section 49;97.
- [3]** Section 44 of the BNSS.
- [4]** Section 185(1) of the BNSS.
- [5]** For explanation of seizure within BNSS, see Sec 106, 117.
- [6]** This is not an exhaustive list of the laws. There are other laws as well which provide for search and seizure.
- [7]** Code of Criminal Procedure, 1973 (CrPC).
- [8]** Indian Evidence Act, 1872.
- [9]** Indian Penal Code, 1860
- [10]** See Section 42 and 43 of The Telecommunications Act, 2023
- [11]** Please note that such a recording can be provided to only Judicial Magistrate of the First Class, District Magistrate and Sub-divisional Magistrate.
- [12]** Sections 94, 185 of BNSS, 2023.
- [13]** K.S. Puttuswamy v Union of India (2017) 10 SCC 1.
- [14]** Virender Khanna v. State of Karnataka, Writ Petition No. 11759 of 2020 (GM-RES).
- [15]** Foundation of Media Professionals v. Union of India, Writ Petition (Crim) No, 395 of 2022, Supreme Court of India, pg 1.
- [16]** Awstika Das, Committee Constituted To Frame Guidelines For Seizure Of Digital Devices : Centre Tells Supreme Court, (December 6th, 2023 12:05 PM)
<https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831>
- [17]** Certificate has been provided under Section 63(4)(c) of BSA, 2023.

REFERENCES:

- [18]** A sample of the seizure memo is provided in the Annexure as Figure 3 & Figure 3.1. The source of this sample is <https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf>
- [19]** A sample of such an inventory list (can be identified as the seizure list in Figure 4) is provided in the Annexure below.
- [20]** A sample of the warrant of the arrest is provided in the Annexure as Figure 5.
- [21]** BNSS Section 503(2).
- [22]** See BNSS Section 2(c).
- [23]** See BNSS Section 2(f), charge is defined under Section 2(b); See also (for better understanding of the contents of a charge) Section. 234.
- [24]** See BNSS, Section 2(g). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.
- [25]** BNS Section 2(21).
- [26]** See BNSS Section 2(o). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.
- [27]** BNSS, Section 2(s).
- [28]** IT Act, Explanation to section 80(1).
- [29]** G. Vishakan v. State of Kerala & Ors., WP(C) No. 22328 of 2023 (10.07.2023 – KERHC) : MANU/KE/1872/2023.
- [30]** Sanket Bhadresh Modi vs CBI, BA No. 3754/23.
- [31]** CBI vs. Mahesh Kumar Sharma, CBI 31/2021
- [32]** This right is enshrined within Part III of the Constitution of India, under art. 20(3).
- [33]** Authorised officers here means either a police officer (not below Inspector) or any other officer of the Central or State Government authorised by the Central Government.

Email: mail@sflc.in

Website: <https://www.sflc.in>

sflc.in

