

sflc.in

માર્ગદર્શિકા

ઇલેક્ટ્રોનિક ઉપકરણોની તલાશી અને જાતી સંબંધિત

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.	ધારા 1 મૂળભૂત માહિતી	4
02.	ધારા 2 તલાશી દરમિયાન શું કરવું?	10
03.	ધારા 3 ઇલેક્ટ્રોનિક ઉપકરણો અને કાયદો	14
04.	ધારા 4 જપ્તી પછીની પ્રક્રિયા	16
05.	ધારા 5 તૈયારી	25
●	શબ્દાવલી	33
●	પરિશિષ્ટ	36
●	સંદર્ભો	45

ધારા 1

મૂળભૂત માહિતી

શું કોઈએ તમારી તલાશી લીધી છે?
શું તેમણે તમારા શરીર, વાહન અથવા ઘરની તલાશી લીધી?
શું તેમણે તમારા ઇલેક્ટ્રોનિક ઉપકરણ જપ્ત કર્યા?
જો ઉપરોક્ત પ્રશ્નોમાંથી કોઈનું ઉત્તર “હા” હોય, તો...



તલાશી અને જપ્તી :સરળ બનાવ્યું

તલાશી અને જપ્તી : શું, કેમ અને ક્યાં

‘તલાશી’ નો અર્થ એ છે કે કોઈ વ્યક્તિ અથવા તેની મિલ્કતની [1] તપાસ કરવામાં આવે જેથી ચાલતી તપાસ અથવા ન્યાયિક કાર્યવાહી માટે જરૂરી પુરાવા મેળવી શકાય [2]. આ વોરંટ સાથે અથવા વોરંટ વિના બંને રીતે કરી શકાય છે. [4]

‘જપ્તી’ નો અર્થ એ છે કે તલાશી બાદ તે મિલ્કતને અધિકૃત રીતે પોતાના કબજામાં લેવામાં આવે, જેથી તેને પુરાવા તરીકે અથવા તપાસ સંબંધિત મિલ્કત તરીકે ઉપયોગ કરી શકા. [5]

શું: આ કાયદો અમલમાં મુકનારી એજન્સીઓ દ્વારા કોઈ કેસની તપાસ કરવા માટે ઉપયોગ કરવામાં આવતી પ્રક્રિયા છે।

કેમ: પુરાવા એકત્ર કરવા, ગુનાને અટકાવવા અને ન્યાય પ્રક્રિયામાં વિશ્લેષ ન થાય તે માટે તલાશી અને જપ્તી કરવામાં આવે છે।

ક્યાં: તે સ્થળો જ્યાં ગુનો બન્યો છે, તે સ્થળો જ્યાં ગુનામાં સંકળાયેલા વ્યક્તિઓ છુપાયા હોઈ શકે, તેમજ તે સ્થળો જ્યાં ગુનાથી સંબંધિત સામગ્રી રાખવામાં આવી હોઈ શકે.

તલાશી અને જપ્તીના પાછળના હેતુઓ

- આનો હેતુ એ છે કે કોઈપણ વ્યક્તિની સામે ચાલતી તપાસ, પૂછપરછ અથવા ચકાસણી (ટ્રાયલ) માટે જરૂરી વસ્તુઓ, દસ્તાવેજો — જેમાં ઇલેક્ટ્રોનિક તથા ડિજિટલ રેકૉર્ડ પણ સામેલ છે — સંબંધિત એજન્સીને ઉપલબ્ધ થઈ શકે।
- તપાસ એજન્સીઓ/પોલીસ તલાશી અને જપ્તી દરમિયાન પ્રાપ્ત થયેલા દસ્તાવેજોની સામગ્રીને કોર્ટમાં પ્રાથમિક અથવા દ્વિતીયક પુરાવા તરીકે સાબિત કરી શકે છે।



આ કાર્યવાહીનો સંચાલન કરતી કાનૂની પાયો

તલાશી અને જપ્તીની સત્તા વિવિધ કાયદાઓમાંથી પ્રાપ્ત થાય છે, જેમાં મુખ્યત્વે નીચેના કાયદાઓનો સમાવેશ થાય છે [6]:

- + ભારતીય નાગરિક સુરક્ષા સંહિતા, 2023 (BNSS) [7]
- + ભારતીય સાક્ષ્ય અધિનિયમ, 2023 (BSA) [8]
- + ભારતીય ન્યાય સંહિતા, 2023 (BNS) [9]
- + આયકર અધિનિયમ, 1961 (ITA)
- + ગેરકાનૂની પ્રવૃત્તિઓ (પ્રતિબંધ) અધિનિયમ, 1967 (UAPA)
- + ધનશોધન નિવારણ અધિનિયમ, 2002 (PMLA)
- + સીબીઆઈ મેન્યુઅલ, 2020
- + માહિતી પ્રૌદ્યોગિકી અધિનિયમ, 2000 (આઈટી અધિનિયમ)
- + રસંચાર અધિનિયમ, 2023
- + માદક દ્રવ્યો અને માનસપ્રભાવક પદાર્થ અધિનિયમ, 1985 (NDPS Act)

પર્દા પાછળ : તલાશી અને જપ્તી કરવાનો અધિકાર ધરાવતા અધિકારીઓ

વિવિધ કાયદાઓ અનુસાર તલાશી અને જપ્તી કરવાની સત્તા ધરાવતા સક્ષમ અધિકારી ભિન્ન હોઈ શકે છે. આ વિભાગનો હેતુ એ છે કે તલાશીનો આદેશ જારી કરવાનો અધિકાર કોના પાસે હોય છે તેની સામાન્ય માહિતી આપવામાં આવે. આ વિગતોને સમજવાથી તમે તપાસ અધિકારીઓને યોગ્ય પ્રશ્નો પૂછી શકશો.

વિવિધ કાયદાઓ અને પરિસ્થિતિઓ અનુસાર તલાશી અને જપ્તીની પ્રક્રિયામાં ફેરફાર થઈ શકે છે.

I. તલાશીનો આદેશ જારી કરવાનો અધિકાર કોને છે ?

ભારતીય નાગરિક સુરક્ષા સંહિતા	જજ (જિલ્લા મેજિસ્ટ્રેટ, ઉપવિભાગીય મેજિસ્ટ્રેટ અથવા પ્રથમ શ્રેણીના મેજિસ્ટ્રેટ) કોઈ સ્થળ પર તલાશી કરવા માટે કૉન્સ્ટેબલ કરતાં ઉચ્ચ પદના પોલીસ અધિકારીને (માત્ર કોઈપણ અધિકારીને નહીં!) વિશેષ પરવાનગી આપી શકે છે, જો તેમને એવું લાગે કે ત્યાં ચોરાયેલા માલ અથવા ખતરનાક વસ્તુઓ છુપાવવામાં આવી છે. આ અધિકારી જરૂરી હોય ત્યારે અન્ય વ્યક્તિઓની મદદ પણ લઈ શકે છે, જો તેમને એવું લાગે કે ત્યાં ચોરાયેલા માલ અથવા ખતરનાક વસ્તુઓ છુપાવવામાં આવી છે. આ અધિકારી જરૂરી હોય ત્યારે અન્ય વ્યક્તિઓની મદદ પણ લઈ શકે છે.
આયકર અધિનિયમ	ડિરેક્ટર/જનરલ/ચીફ કમિશનર/ કમિશનર પાસે તલાશીનો આદેશ જારી કરવાની સત્તા હોય છે.
ગેરકાનૂની પ્રવૃત્તિઓ (પ્રતિબંધ) અધિનિયમ	કેન્દ્ર સરકાર/રાજ્ય સરકાર તલાશી કરવાનો આદેશ આપી શકે છે. પરંતુ કાયદો એ સ્પષ્ટ કરતો નથી કે સરકારના (કેન્દ્ર અથવા રાજ્ય) કયા વિભાગ/મંત્રાલયને આ આદેશ જારી કરવાની સત્તા પ્રાપ્ત છે.
ધનશોધન નિવારણ અધિનિયમ	સર્વે માટે: એડજ્યુડિકેટિંગ ઓથોરિટી તલાશીનો આદેશ જારી કરી શકે છે. જપ્તી માટે: ડિરેક્ટર અથવા ડેપ્યુટી ડિરેક્ટર કરતાં નીચા પદનો ન હોય એવો કોઈ અન્ય અધિકારી આ આદેશ જારી કરી શકે છે.
માહિતી પ્રૌદ્યોગિકી અધિનિયમ	The Central Government has the authority to order any officer of the Central or State Government to search. The Controller can also order a search to access data within computers.

પર્દા પાછળ : તલાશી અને જપ્તી કરવાનો અધિકાર ધરાવતા અધિકારીઓ

વિવિધ કાયદાઓ અનુસાર તલાશી અને જપ્તી કરવાની સત્તા ધરાવતા સક્ષમ અધિકારી ભિન્ન હોઈ શકે છે. આ વિભાગનો હેતુ એ છે કે તલાશીનો આદેશ જારી કરવાનો અધિકાર કોના પાસે હોય છે તેની સામાન્ય માહિતી આપવામાં આવે. આ વિગતોને સમજવાથી તમે તપાસ અધિકારીઓને યોગ્ય પ્રશ્નો પૂછી શકશો.

વિવિધ કાયદાઓ અને પરિસ્થિતિઓ અનુસાર તલાશી અને જપ્તીની પ્રક્રિયામાં ફેરફાર થઈ શકે છે.

II. તલાશી કરવાનો અધિકાર કોને છે ?

ભારતીય નાગરિક સુરક્ષા સંહિતા	તલાશી અને જપ્તી સંબંધિત કાયદાનું સંચાલન — મૂળભૂત સિદ્ધાંતો: તલાશી અને જપ્તીની કાર્યવાહી સામાન્ય રીતે થાણા પ્રભારી (SHO) અથવા તપાસ અધિકારી (IO) દ્વારા કરવામાં આવે છે. તેમના અભાવમાં, કોઈપણ એવો અધિકારી જેને લેખિત રૂપે અધિકૃત કરવામાં આવ્યો હોય, તે પણ આ કાર્યવાહી કરી શકે છે. જો કોઈ વ્યક્તિને ધરપકડ કરવામાં આવે: પોલીસ તે સ્થળની તલાશી લઈ શકે છે જ્યાં આરોપીને ઝડપવામાં આવ્યો હોય અને ગુનાથી સંબંધિત કોઈપણ વસ્તુ જપ્ત કરી શકે છે. આ સત્તા માત્ર પોલીસ પાસે જ હોય છે. જરૂર પડે ત્યારે પોલીસ દરવાજો, બારી અથવા અન્ય કોઈ અવરોધ તોડી પણ શકે છે. જો કોઈ સ્થળ પર શંકાસ્પદ વસ્તુઓ છુપાયેલી હોવાની શક્યતા હોય: જિલ્લા મેજિસ્ટ્રેટ, ઉપ-વિભાગીય મેજિસ્ટ્રેટ અથવા પ્રથમ શ્રેણીના મેજિસ્ટ્રેટ — કોઈ સ્થળની તલાશી માટે વિશેષ મંજૂરી આપી શકે છે. આ મંજૂરી માત્ર એ પોલીસ અધિકારીને આપવામાં આવે છે જે કૉન્સ્ટેબલ કરતાં ઉચ્ચ પદ પર હોય (અથવા કોઈ પણ સામાન્ય અધિકારીને નથી આપવામાં આવતી). આ રીતે અધિકૃત અધિકારી જરૂરી હોય તો અન્ય વ્યક્તિઓની મદદ પણ લઈ શકે છે. સંબંધિત કલમો: કલમ 44 અને કલમ 97
ગેરકાનૂની પ્રવૃત્તિઓ (પ્રતિબંધ) અધિનિયમ	UAPA હેઠળ તપાસ કરવા માટે સત્તાધિકૃત એજન્સીઓ વિવિધ શહેરોમાં અલગ હોય છે: દિલ્હી વિશેષ પોલીસ પ્રતિષ્ઠાન: ઉપ પોલીસ અધિક્ષક અથવા તેના સમકક્ષ અધિકારી. મુંબઈ, કોલકાતા, ચેન્નઈ, અમદાવાદ જેવા મહાનગર વિસ્તારો અને સૂચિત વિસ્તારોમાં: સહાયક પોલીસ આયોગ્ય અને તેનાથી ઉચ્ચ પદના અધિકારીઓ. અન્ય તમામ કેસોમાં: ઉપ પોલીસ અધિક્ષક અથવા તેના સમકક્ષથી નીચા પદનો કોઈપણ અધિકારી તપાસ કરવાની સત્તા ધરાવતો નથી.

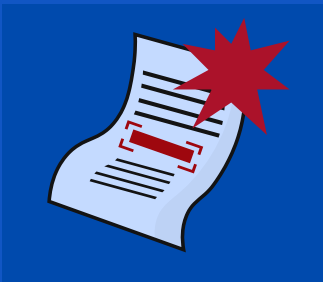
પર્દા પાછળ : તલાશી અને જપ્તી કરવાનો અધિકાર ધરાવતા અધિકારીઓ

વિવિધ કાયદાઓ અનુસાર તલાશી અને જપ્તી કરવાની સત્તા ધરાવતા સક્ષમ અધિકારી ભિન્ન હોઈ શકે છે. આ વિભાગનો હેતુ એ છે કે તલાશીનો આદેશ જારી કરવાનો અધિકાર કોના પાસે હોય છે તેની સામાન્ય માહિતી આપવામાં આવે. આ વિગતોને સમજવાથી તમે તપાસ અધિકારીઓને યોગ્ય પ્રશ્નો પૂછી શકશો.

વિવિધ કાયદાઓ અને પરિસ્થિતિઓ અનુસાર તલાશી અને જપ્તીની પ્રક્રિયામાં ફેરફાર થઈ શકે છે.

II. તલાશી કરવાનો અધિકાર કોને છે ?

આયકર અધિનિયમ	માત્ર આસિસ્ટન્ટ કમિશનર અથવા તેનાથી ઉચ્ચ પદના આયકર અધિકારીઓને જ તપાસ કરવાનો અધિકાર હોય છે.
ધનશોધન નિવારણ અધિનિયમ	ડિરેક્ટર અથવા ડેપુટી ડિરેક્ટર કરતાં નીચા ન હોય એવા કોઈપણ અન્ય અધિકારીને તપાસ કરવાનો અધિકાર હોય છે.
માહિતી પ્રૌદ્યોગિકી અધિનિયમ	કોઈપણ પોલીસ અધિકારી, જેનું પદ ઇન્સ્પેક્ટરથી નીચું ન હોય, તપાસ કરી શકે છે। આ ઉપરાંત, કેન્દ્ર સરકાર દ્વારા અધિકૃત કરવામાં આવે તો કેન્દ્ર અથવા રાજ્ય સરકારનો કોઈપણ અન્ય અધિકારી પણ તપાસ કરી શકે છે। કંટ્રોલર અથવા તેમના દ્વારા અધિકૃત કરવામાં આવેલ કોઈપણ અન્ય અધિકારી પણ તપાસ કરી શકે છે।
ટેલિકોમ્યુનિકેશન્સ અધિનિયમ, 2023	આ કાયદો કેન્દ્ર સરકારના અધિકૃત અધિકારીને એ સત્તા આપે છે કે જો અધિકારીને એવું માનવાનો કારણ હોય કે કોઈ અનધિકૃત ટેલિકોમ્યુનિકેશન નેટવર્ક અથવા સાધન રાખવામાં આવ્યું છે અથવા છુપાવવામાં આવ્યું છે, તો તે કોઈપણ સ્થળની તલાશી લઈ શકે છે। [10]



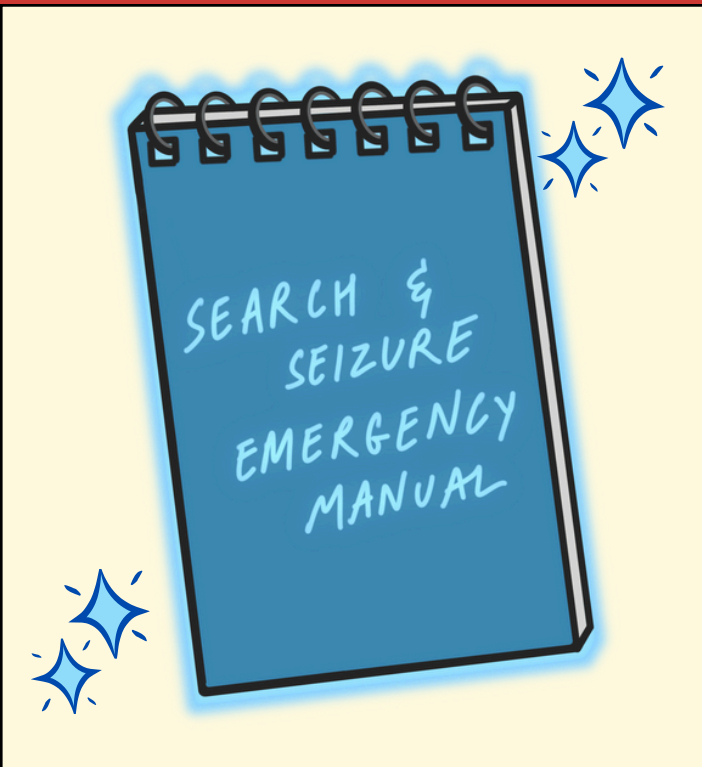
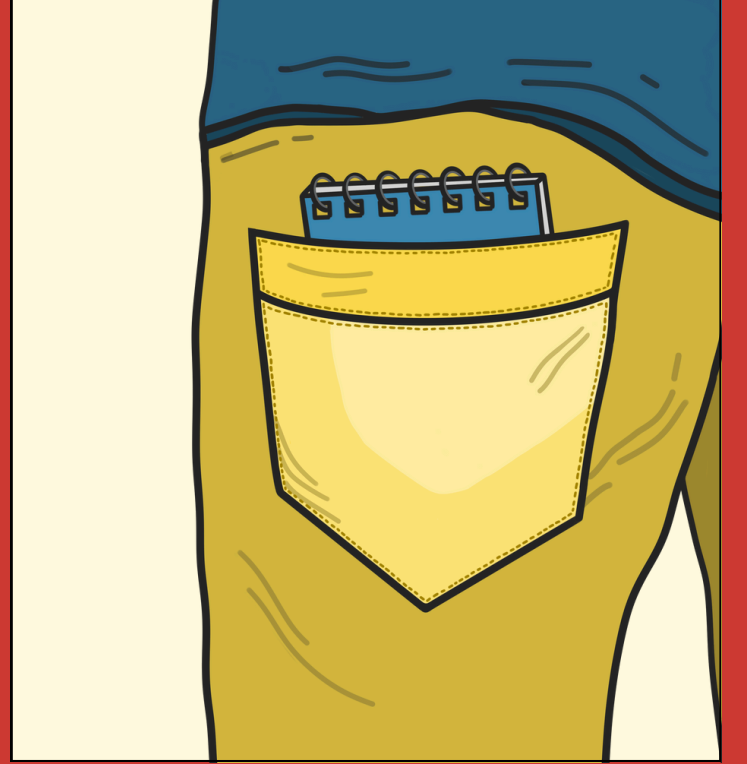
ધારા 2

તલાશી દરમિયાન
શું કરવું?

તપાસ કરવાની પ્રક્રિયા ઘણી વખત જટિલ અને ભયજનક થઈ શકે છે।

આ પ્રક્રિયા ને યોગ્ય રીતે સમજીને પાર પાડવા માટે, તેમાં સામેલ પ્રક્રિયાઓ અને જરૂરી દસ્તાવેજીકરણને સમજવું અત્યંત જરૂરી છે।

તપાસ અંતે ટ્રાયલ સુધી પહોંચી શકે છે, અને આવી પરિસ્થિતિમાં, તલાશીની પ્રક્રિયા અને સંબંધિત નિયમોની સંપૂર્ણ સમજ અદાલતમાં પોતાનું સંરક્ષણ કરવા માટે અત્યંત મહત્વપૂર્ણ બને છે।



તલાશી શરૂ થતી વખતે આ પ્રશ્નો ઉપયોગી સાબિત થઈ શકે છે:



1	શું તમારી પાસે વોરન્ટ છે?
2	શું તે ઇલેક્ટ્રોનિક રીતે સર્વ કરવામાં આવ્યું છે?
3	જો હા, તો કયા માધ્યમ દ્વારા?
4	તમે કઈ તપાસ એજન્સીનું પ્રતિનિધિત્વ કરો છો?
5	તમારો હોદ્દો શું છે?
6	મારા સામે કયા આક્ષેપો મૂકવામાં આવ્યા છે?

ઉપરાંત, કૃપા કરીને આ બાબતનું ધ્યાન રાખો — જો તમને લાગે કે તમારા પ્રશ્નોના યોગ્ય જવાબ આપવામાં આવી રહ્યા નથી, તો તરત જ કોઈ એડવોકેટનો સંપર્ક કરો. તમારા કાનૂની પ્રતિનિધિ હાજર ન થાય ત્યાં સુધી વધુ કોઈ પ્રશ્નનો જવાબ ન આપવા સલાહ આપવામાં આવે છે।

અધિકારીઓ પાસેથી માહિતી અસરકારક રીતે મેળવવી।

- પોલીસ તમારા ઇલેક્ટ્રોનિક ઉપકરણોની તલાશી વોરન્ટ સાથે અથવા વોરન્ટ વગર લઈ શકે છે। પરંતુ તમને હંમેશા નજીકના મેજિસ્ટ્રેટ પાસેથી તલાશી અને જપ્તીની પ્રક્રિયાની રેકૉર્ડિંગની નકલ માંગવી જોઈએ [11] – જેને પોલીસ અધિકારી પાસેથી આવી રેકૉર્ડિંગ પ્રાપ્ત થઈ હોય છે। [12]
- તમારા કબજામાં રહેલા અન્ય કોઈ વ્યક્તિના ઇલેક્ટ્રોનિક રેકૉર્ડ્સ તમે આપવા ઇનકાર કરી શકો છો, જો સુધી કે તે વ્યક્તિ તેની મંજૂરી ન આપે।
- તલાશી અને જપ્તી કોઈ પણ તપાસની માન્ય અને પ્રમાણભૂત પ્રક્રિયા છે। માત્ર તમારા ઘર અથવા ઉપકરણોની તલાશી લેવામાં આવે છે એટલે તેનાથી તમે દોષિત છો એવું માનવું યોગ્ય નથી। તપાસ એજન્સીઓ પાસે તલાશી કરવાનો અધિકૃત દસ્તાવેજ હોય, તો તેમને તેમનું કાર્ય કરવા દો। તમારા વકીલનો સંપર્ક કરો, કારણ કે ભવિષ્યમાં તમને તેની જરૂર પડી શકે છે।
- કેટલીક વખત તપાસ અધિકારીઓ તમારા પ્રશ્નોના જવાબ ન આપે। આવી સ્થિતિમાં, તમારા પ્રશ્નો અને પ્રાપ્ત થયેલા જવાબો તમે કાગળ પર નોંધતા જશો તો તે ટ્રાયલ દરમિયાન ઉપયોગી થઈ શકે છે।
- તમારું તપાસ એજન્સીઓને તેમની તલાશી દરમિયાન મદદ કરવાનો કોઈ કાનૂની ફરજિયાત ફરજ નથી, પરંતુ તમે પ્રક્રિયામાં અવરોધ પણ પેદા કરી શકતા નથી। આનો અર્થ એ છે કે તમે ઉપકરણ લઈને ભાગી નહીં શકો અથવા ઉપકરણને નુકસાન નહીં પહોંચાડી શકો।

સ્થળ પર શોધ અને જપ્તી દરમિયાન કરવામાં આવતું વિશ્લેષણ એ એકત્રિત થયેલા પુરાવાની તરત જ તપાસ અને મૂલ્યાંકન કરવાની પ્રક્રિયા છે, જેથી તેની પ્રાસંગિકતા અને અખંડિતતા સુનિશ્ચિત રહી શકે.

આ પ્રક્રિયામાં સ્થળ પરથી મળેલી ભૌતિક વસ્તુઓ અને ડિજિટલ ઉપકરણોની સમીક્ષા અને દસ્તાવેજીકરણ, ડેટા એક્સ્ટ્રેક્શન અને ફોરેન્સિક વિશ્લેષણ દ્વારા માહિતી મેળવવી અને તેની ચકાસણી કરવી—તેમજ કોઈપણ પ્રકારની છેડછાડ અટકાવવી—સમાવેશ થાય છે. મહત્વપૂર્ણ નમૂનાઓ અને જોડાણોની ઓળખ કરવામાં આવે છે અને ચેઇન ઓફ કસ્ટડી સ્પષ્ટ અને સતત જાળવાય તે માટે વિગતવાર નોંધો લેવામાં આવે છે.

1	વિશ્લેષણ માટે ઉપયોગમાં લેવાયેલા ઉપકરણો અને ખાતાઓની સૂચિ રાખો: શોધની પ્રક્રિયા દરમિયાન જે ઉપકરણો અને ખાતાઓનું વિશ્લેષણ કરવામાં આવે છે, તેની સૂચિ રાખવી અગત્યની છે. આથી અધિકારીઓ દ્વારા પાછળથી એકત્રિત કરાયેલા તમામ ડેટાના કોસ-રેફરન્સિંગમાં સરળતા થાય છે.
2	તમારા ઉપકરણોમાં ફાઇલ્સ ક્યાં સંગ્રહિત છે તેની માહિતી આપશો નહીં: જ્યારે સત્તાધિકારીઓ શોધ અને જપ્તી કરે છે, ત્યારે તમારા ઉપકરણોમાં ફાઇલ્સના સંગ્રહ સ્થાન વિશે માહિતી આપવી યોગ્ય નથી. આથી તમારી ગોપનીયતા સુરક્ષિત રહે છે અને કાનૂની પ્રક્રિયાની અખંડિતતા જાળવાઈ રહે છે. ફાઇલ્સનું સ્થાન જણાવવાથી શોધનો વિસ્તાર કાયદા હેઠળ નક્કી કરેલી સીમા બહાર વધી શકે છે અને સંવેદનશીલ અથવા અસંગત વ્યક્તિગત માહિતી બહાર આવી શકે છે.
3	વિશ્લેષણ માટે લેવામાં આવેલા તમામ ઉપકરણોના IMEI નંબર, સીરિયલ નંબર અને સ્પેસિફિકેશન નોંધો: આ નોંધ રાખવાથી ઉપકરણની ઓળખની પુષ્ટિ થાય છે, અન્ય ઉપકરણો સાથે ગડબડ થતી અટકે છે અને પુરાવાની અખંડિતતા જાળવવામાં મદદ મળે છે. આથી ખાતરી થાય છે કે કોર્ટમાં રજૂ કરવામાં આવતું ઉપકરણ એ જ છે જે જપ્ત કરવામાં આવ્યું હતું અને વિશ્લેષણ માટે લેવામાં આવ્યું હતું.

ધારા ૩

ઇલેક્ટ્રોનિક ઉપકરણો અને કાયદો

ભારતના સુપ્રીમ કોર્ટએ કે.એસ. પુટ્ટાસ્વામી કેસમાં ગોપનીયતાને — જેમાં માહિતીગત ગોપનીયતા (informational privacy) પણ સામેલ છે — મૂલભૂત અધિકાર તરીકે માન્યતા આપી છે. [13] - વીરેન્દ્ર ખન્ના V. સ્ટેટ ઓફ કર્ણાટક કેસમાં, કર્ણાટક હાઈકોર્ટે ઇલેક્ટ્રોનિક ઉપકરણોની શોધ અને જપ્તી અંગે વિશેષ માર્ગદર્શિકા નિર્ધારિત કરી હતી. આ કેસમાં કોર્ટએ નિર્ધારિત કર્યું કે: સ્માર્ટફોન અથવા કમ્પ્યુટર સિસ્ટમમાં પ્રવેશ આપવા માટે પાસવર્ડ, બાયોમેટ્રિક્સ અથવા પાસકોડ જાહેર કરવું, કોઈ વ્યક્તિના *સ્વ-અપરાધસ્વીકારના અધિકાર* નું ઉલ્લંઘન ગણાતું નથી. [14]

પરંતુ ફાઉન્ડેશન ઓફ મીડિયા પ્રોફેશનલ્સએ સુપ્રીમ કોર્ટનો દરવાજો ખખડાવ્યો હતો, દલીલ કરતા કે વર્તમાન કાયદો લોકોના સ્વ-અપરાધસ્વીકારના અધિકાર અને ગોપનીયતાના અધિકારના ભંગથી તેમને સુરક્ષિત રાખવા માટે પૂરતો નથી — ખાસ કરીને એ પરિસ્થિતિને ધ્યાનમાં લેતા કે ઇલેક્ટ્રોનિક ઉપકરણોમાં કોઈ વ્યક્તિનો અત્યંત ખાનગી અને વિશાળ પ્રમાણમાં ડેટા સંગ્રહિત હોય છે. [15] તપાસ એજન્સીઓ દ્વારા ઇલેક્ટ્રોનિક ઉપકરણોની શોધખોળ અને જપ્તી માટે માર્ગદર્શિકા તૈયાર કરવા એક સમિતિ રચવામાં આવી હતી. [16]

વિવિધ કાયદાઓ હેઠળ શોધખોળ અને જપ્તીની પ્રક્રિયા કેવી રીતે કરવામાં આવે છે તે જાણવા માટે કૃપા કરીને એનેક્સરોનો અભ્યાસ કરો.



ધારા 4

જપ્તી પછીની પ્રક્રિયા:

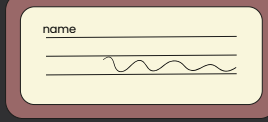
તમારું ઉપકરણ જપ્ત થયા પછી
શું થાય છે

જપ્ત કરાયેલા ઉપકરણો માટે જરૂરી દસ્તાવેજીકરણ

પ્રમાણપત્રો

[કલમ 63(4)(c) હેઠળ]

જે વ્યક્તિનું ઉપકરણ શોધવામાં અને જપ્ત કરવામાં આવ્યું છે અને જે નિષ્ણાત શોધ અને જપ્તની પ્રક્રિયા કરી રહ્યો છે, તેઓ દ્વારા ભરવાના પ્રમાણપત્રોની નકલ માંગવાનો અધિકાર વ્યક્તિને છે. [17] [18], આ પ્રમાણપત્રોમાં નીચેની વિગતો હોવી જોઈએ:



જે વ્યક્તિનું ઉપકરણ શોધખોળ અને જપ્ત થયું છે તેનું નામ અને હસ્તાક્ષર



જપ્તની તારીખ અને સમય



જપ્તનું સ્થળ



જપ્ત કરાયેલા ઉપકરણોની વિગત (બનાવટી કંપની, મોડેલ, સીરિયલ નંબર/IMEI/UIN/UID/MAC)

0000 1111
0000 2222

હેશ વેલ્યુ (હેશ રિપોર્ટ સાથે)



નિષ્ણાત દ્વારા ભરેલું પ્રમાણપત્ર, યોગ્ય વિગતો સાથે હસ્તાક્ષરિત



જપ્તી દરમિયાન હાજર સાક્ષીઓના નામ



જપ્તી કરવાનો કારણ



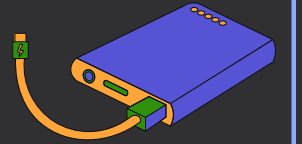
શોધ અને જપ્તીની પ્રક્રિયા ઇલેક્ટ્રોનિક રીતે, અથવા શ્રેષ્ઠ રીતે મોબાઇલ ફોનથી રેકૉર્ડ કરવામાં આવે તેવી વિનંતી



મેજિસ્ટ્રેટ પાસે રેકૉર્ડિંગ પહોંચ્યા બાદ તેની નકલ આપવા વિનંતી



ઈન્વેન્ટરી યાદી



બધા જપ્ત કરેલા આઇટમોની વિગતવાર યાદી માંગો [19] જેમાં ચાર્જર, કવર જેવા એસેસરીઝ પણ સમાવેશ થાય.

જપ્તીનું કારણ



તમારા ઉપકરણો કેમ જપ્ત કરવામાં આવ્યા છે અને કયા કાયદાની જોગવાઈઓ હેઠળ કરવામાં આવ્યા છે તેની સ્પષ્ટ માહિતી માંગો.



કાનૂની સલાહકારનો અધિકાર

શોધની પ્રક્રિયા દરમિયાન વકીલ સાથે સલાહ લેવા તમારા હક્કનો દાવો કરો.



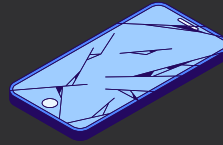
વૉરન્ટ/આદેશોની નકલ

જો જપ્તી વૉરન્ટ અથવા મેજિસ્ટ્રેટના આદેશ પર આધારિત હોય [20] તો તેની નકલ માંગો. તપાસો કે વૉરન્ટ/આદેશમાં યોગ્ય વિગતો છે કે નહીં અને તે અધિકૃત અધિકારી દ્વારા હસ્તાક્ષરિત છે કે નહીં.



જપ્તીનો અંદાજિત સમયગાળો

ઉપકરણો કેટલા સમય માટે રાખવામાં આવશે અને પરત કરવાની પ્રક્રિયા શું છે તે પૂછો.



ઉપકરણની સ્થિતિનું દસ્તાવેજીકરણ

ઉપકરણ સોંપતા પહેલાં તેની સ્થિતિ (જેમ કે સ્ક્રેચિસ, ડેન્ટ્સ) ફોટો અથવા વિડિયો દ્વારા દસ્તાવેજિત કરવાની વિનંતી કરો.

વધારાના દસ્તાવેજો



પરિસ્થિતિ પ્રમાણે તમે વધારાની માહિતી પણ માંગી શકો છો, જેમ કે:

- તપાસ અધિકારીની વિગત, જે જપ્તીની પ્રક્રિયાનું નેતૃત્વ કરી રહ્યા છે
- ફરિયાદ અથવા કેસ વિશેની માહિતી, જેમાં જપ્તી સંબંધિત કેસ નંબરનો સમાવેશ થાય છે
- સત્તાવાળાઓએ અનુસરેલી સંબંધિત નીતિઓ અથવા પ્રક્રિયાઓની નકલ

જો તમારું ઉપકરણ લાંબા સમય સુધી પાછું ન મળે તો શું?

- * તમારું ઉપકરણ કેવી રીતે પાછું આપવામાં આવશે તેની પ્રક્રિયા એ પર આધારિત રહેશે કે તે કોર્ટ સમક્ષ રજૂ કરવામાં આવ્યું હતું કે નહીં. જો તમારી ડિવાઇસ કોઈ પૂછપરછ અથવા ટ્રાયલ દરમિયાન કોર્ટમાં રજૂ કરવામાં આવી હોય, તો પૂછપરછ અથવા ટ્રાયલ પૂર્ણ થયા પછી કોર્ટ તેના પરત આપવાનો આદેશ આપી શકે છે — BNSS, 2023ની કલમ 497 અને 503 મુજબ. કલમ 497ને વિગતવાર સમજાવવામાં આવી છે અને હવે તેમાં સમયસીમા પણ નક્કી કરવામાં આવી છે.
- * પરંતુ, જો તમારી જપ્ત કરેલી સંપત્તિ કોર્ટ સમક્ષ રજૂ કરવામાં આવી ન હોય અને મેજિસ્ટ્રેટને યોગ્ય લાગે, તો તેઓ પરત આપવાનો આદેશ જારી કરશે કે તમારી ઉપકરણો લેવા માટે તૈયાર છે. આ ઉપકરણો છ માસની અંદર તમને દાવો કરવા પડશે. [21]

કોઈપણ પરિસ્થિતિમાં, પોલીસે જપ્ત કરેલી સંપત્તિ પાછી મેળવવાની પ્રક્રિયા તમારા કેસની ખાસ પરિસ્થિતિઓ પર આધારિત બદલાઈ શકે છે. ઉપરોક્ત બંને પરિસ્થિતિઓમાં, જો તમારું ઉપકરણ પરત મેળવવા માટે તૈયાર હોય અને તમને તેને મેળવવામાં મુશ્કેલી પડી રહી હોય, તો યાદ રાખો કે ઉપકરણનો દાવો કરવાની પોલીસ પ્રક્રિયા કેસની પરિસ્થિતિ પ્રમાણે અલગ હોઈ શકે છે. તેમ છતાં, તમે લઈ શકતાં પગલાંઓનો સામાન્ય સારાંશ નીચે મુજબ છે:

માહિતી એકત્ર કરો: જપ્ત કરાયેલી ચોક્કસ વસ્તુઓની યાદી બનાવો — જેમાં સિરિયલ નંબર, વર્ણન, સ્પેસિફિકેશન્સ જેવી ઓળખ વિગતો સામેલ કરો. ઉપરાંત, ખરીદીની રસીદ, વેચાણ બિલ અથવા રજિસ્ટ્રેશન સર્ટિફિકેટ જેવા માલિકી સાબિત કરતાં દસ્તાવેજો પણ એકત્રિત કરો.

પોલીસ સ્ટેશનનો સંપર્ક કરો: જરૂરી માહિતી એકત્રિત કર્યા પછી નજીકના પોલીસ સ્ટેશનમાં જાઓ — દાંતદ તો જ્યાં કેસ નોંધાયો છે અથવા જ્યાં તમારી સંપત્તિ જપ્ત કરવામાં આવી હતી. ઓફિસર-ઇન-ચાર્જ, તપાસ અધિકારી અથવા પ્રોપર્ટી વિભાગના કોઈ કર્મચારી સાથે વાત કરો. તમારી પરિસ્થિતિ સમજાવો અને તમારી સંપત્તિ પરત આપવા વિનંતી કરો. ધીરજ, શિસ્ત અને સહકાર રાખીને, તમારી પાસેના તમામ સંબંધિત દસ્તાવેજો રજૂ કરો.

કાનૂની સહાય લો: 1. જો પોલીસ સહકાર ન આપે અથવા પ્રક્રિયા જટિલ લાગે, તો વકીલ પાસેથી કાનૂની મદદ મેળવવા પર વિચાર કરો.

જખ્તી પછી – ઉપકરણ પરત મળે ત્યારે ચેકલિસ્ટ

1. સામાન્ય તપાસ

ઉપકરણો અને સેવાઓ

અધિકારીઓ પાસેથી એવી યાદી મેળવો જેમાં તેઓએ વિશ્લેષણ કરેલા અથવા જખ્ત કરેલા તમામ ઉપકરણો તથા તેઓએ ચકાસેલી સેવાઓ — જેમ કે ઇમેઈલ, ચેટ વગેરે — નો સમાવેશ થાય. જેથી તમે તેને તમારા જખ્તી પહેલાંના ડેટાબેસ સાથે ક્રોસ-ચેક કરી શકો.

સ્ટાર્ટઅપ અને કાર્યક્ષમતા

ઉપકરણ ચાલુ કરો અને તે સામાન્ય રીતે ચાલુ થાય છે કે નહીં તેની ખાતરી કરો. ઈન્ટરનેટ કનેક્ટિવિટી, એપ્લિકેશન ઉપયોગ, કેમેરા વગેરે જેવી મૂળભૂત સુવિધાઓનું પરીક્ષણ કરો.

ઉપકરણ પરત

રેડ (છાપો) પછી જે ઉપકરણો જખ્ત કરવામાં આવ્યા નહીં હોય, તે બધા તમને પરત આપવામાં આવ્યા છે તેની ખાતરી કરો.

ભૌતિક સ્થિતિ

ઉપકરણમાં કોઈ શારીરિક નુકસાન છે કે નહીં તે તપાસો — જેમ કે સીલ તોડવાના નિશાન, સ્ક્રૂ સાથે છેડછાડ વગેરે. કોઈપણ શંકાસ્પદ નિશાન અથવા નુકસાન જોવા મળે તો તેની તસવીરો/દસ્તાવેજીકરણ કરો.

સેટિંગ્સ અને કન્ફિગારેશન્સ

ખાસ કરીને સિક્યુરિટી, પ્રાઇવસી અથવા લોકેશન સર્વિસેસ સંબંધિત સેટિંગ્સમાં કોઈ ફેરફાર થયો છે કે નહીં તે તપાસો.

જાપ્તી પછી – ઉપકરણ પરત મળે ત્યારે ચેકલિસ્ટ

1. સામાન્ય તપાસ

સ્થાપિત સોફ્ટવેર/એપ્સ

તમારા ઉપકરણમાં કોઈ નવું સોફ્ટવેર અથવા ઓપરેટિંગ સિસ્ટમ ઇન્સ્ટોલ કરવામાં આવ્યું છે કે નહીં તે તપાસો. જાપ્તી પહેલાં ઇન્સ્ટોલ થયેલી એપ્સની સૂચિ સાથે હાલની સૂચિની સરખામણી કરો. અજાણી અથવા શંકાસ્પદ એપ્સ સ્પાયવેર અથવા મેલવેર હોવાની સંભાવના હોઈ શકે છે.

અસામાન્ય પ્રવર્તન

ઉપકરણમાં કોઈ અપ્રાકૃતિક અથવા અસામાન્ય પ્રવૃત્તિ — જેમ કે બેટરી ઝડપથી ઓછું થવું, વધારે ડેટાનો ઉપયોગ, સુવિધાઓ યોગ્ય રીતે ન ચાલવી — જોવા મળે તો તે સ્પાયવેર અથવા મેલવેરનું સૂચક હોઈ શકે છે.

ઓનલાઇન એકાઉન્ટ્સ

જેમ કે ઇમેઇલ, ક્લાઉડ સ્ટોરેજ, સોશિયલ મીડિયા વગેરેમાં ચકાસો કે કોઈ અજાણ્યા ઉપકરણો તમારા એકાઉન્ટમાં લૉગિન થયેલા તો નથી ને. જો કોઈ અજાણ્યું ઉપકરણ મળે તો તાત્કાલિક તેને રિમૂવ કરીને તમારું એકાઉન્ટ સુરક્ષિત કરો. આ સામાન્ય રીતે એકાઉન્ટના સિક્યુરિટી સેટિંગ્સ દ્વારા કરી શકાય છે.

જાપ્તી પછી – ઉપકરણ પરત મળે ત્યારે ચેકલિસ્ટ

2. ડેટાની અખંડિતતા

ડેટા ચકાસણી

તમારી બધી વિગતો (ડેટા) સંપૂર્ણ છે તેની ખાતરી કરો. ફાઇલ્સ, ફોટોગ્રાફ્સ, દસ્તાવેજો, મેટાડેટા અને અન્ય ડેટાની તપાસ કરો કે ક્યાંય કંઈ ગુમ થયું હોય અથવા ક્રશ્ટ થયું હોય તેવું નથી.

ફાઇલ ટાઈમસ્ટેમ્પ્સ

તમારા ઉપકરણ પર મહત્વપૂર્ણ ફાઇલ્સ અને દસ્તાવેજોના ટાઈમસ્ટેમ્પ્સ તપાસો. જો ટાઈમસ્ટેમ્પ બદલાયેલા હોય, તો તે અનધિકૃત ઍક્સેસ અથવા ફેરફારનું સંકેત હોઈ શકે છે.

ફાઇલ હેશેસ

મહત્વપૂર્ણ ફાઇલ્સના ક્રિપ્ટોગ્રાફિક હેશ બનાવો અને સીઝર પહેલાં અને પછી તેમના હેશ મૂલ્યો સરખાવો. જો હેશમાં તફાવત મળે, તો તે ફાઇલમાં ફેરફાર અથવા બદલાવનો પુરાવો હોઈ શકે છે.

ફોરેન્સિક ટૂલ સ્કેન

તમારા ઉપકરણને હિડન ફાઇલ્સ, સ્પાયવેર અથવા રૂટકિટ્સ માટે ચકાસવા એન્ટી-મેલવેર અને ફોરેન્સિક સોફ્ટવેરનો ઉપયોગ કરો. આ ટૂલ્સ કઠિન હોઈ શકે છે, તેથી ડેટા રિકવરી અથવા સાયબર સિક્યોરિટી નિષ્ણાતની સલાહ ઉપયોગી થઈ શકે છે.

જાપ્તી પછી – ઉપકરણ પરત મળે ત્યારે ચેકલિસ્ટ

૩. વધારાની બાબતો

બેકઅપ લોગ્સ

જો તમારું ઉપકરણ આ સુવિધાને સપોર્ટ કરતું હોય, તો સીઝર થયેલ સમયગાળા દરમિયાન કોઈ અનિયમિત અથવા અનધિકૃત પ્રવૃત્તિ દર્શાવતા બેકઅપ લોગ્સ અથવા સિસ્ટમ લોગ્સ તપાસો.

ક્લાઉડ સ્ટોરેજ

તમારા ઉપકરણ સાથે જોડાયેલા ક્લાઉડ સ્ટોરેજ એકાઉન્ટ્સમાં કોઈ અનધિકૃત ઍક્સેસ અથવા બદલાવ થયેલા છે કે નહીં તે સમીક્ષિત કરો.

દસ્તાવેજીકરણ

તમારા તમામ નિષ્કર્ષોનો વિગતવાર રેકૉર્ડ રાખો—જેમ કે ટાઈમસ્ટેમ્પ્સ, સ્ક્રીનશોટ્સ, અને શંકાસ્પદ પ્રવૃત્તિ વિશેની નોંધો. જો તમને આગળ જઈને કાનૂની કાર્યવાહી કરવાની જરૂર પડે, તો આ દસ્તાવેજો ખૂબ જ મહત્વપૂર્ણ બની શકે છે.

પાસવર્ડ મેનેજમેન્ટ

તમારા ઉપકરણ અને તેના સાથે સંબંધિત તમામ ઓનલાઈન એકાઉન્ટ્સના પાસવર્ડ બદલો, કારણ કે સત્તાવાળાઓ પાસે તમારા પાસવર્ડ્સની નકલ રહેલી હોવાની શક્યતા રહે છે.

ધારા 5

તૈયારી:

તમારા ઉપકરણોને સુરક્ષિત રાખવું

આજના ડિજિટલ વિશ્વમાં, અમારા ઉપકરણો અને તેમાં રહેલો ડેટા બહુ મોટું માહિતીનું પ્રમાણ ધરાવે છે.

અમારો ડેટા સુરક્ષિત રહે તે માટે ઉપકરણોને સુરક્ષિત રાખવું અત્યંત જરૂરી છે.



pa*s*o*d

ડિજિટલ જોખમો માટે તૈયાર રહેવું સરળ પણ જરૂરી છે. કલ્પના કરો કે તમારો ફોન હેક થઈ જાય અને તમારા બધા સંદેશાઓ બહાર આવી જાય—કેટલું મોટું ગડબડ સર્જાઈ શકે! મજબૂત પાસવર્ડનો ઉપયોગ કરવાથી, ઓનલાઇન શું શેર કરો છો તેની સાવધાની રાખવાથી અને સોફ્ટવેરને સમયસર અપડેટ રાખવાથી, તમે તમારા ડિજિટલ જીવનને સુરક્ષિત રાખવા માટે એક મજબૂત તાળું તૈયાર કરો છો. યાદ રાખો—થોડીક જાગરૂકતા તમારા ઓનલાઇન જીવનને સુરક્ષિત રાખવામાં લાંબો માર્ગ પસાર કરે છે. નીચે આપેલ છે તમારા ડેટાને સુરક્ષિત રાખવા માટેની કેટલીક અસરકારક પદ્ધતિઓ.

તમારી ઓનલાઇન પ્રવૃત્તિ સુરક્ષિત રાખો | આ રીતે:

પોતાને
ઢાંકી લો



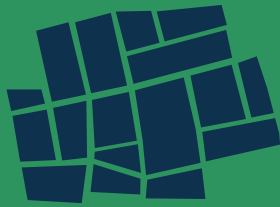
તમે VPN અને Tor નો ઉપયોગ કરીને તમારી ઓનલાઇન પ્રવૃત્તિને સુરક્ષિત રાખી શકો છો. આ એ જ રીતે છે જેમ કોઈ ગુપ્ત એજન્ટ ગુપ્ત મિશન દરમિયાન ભેસ ફેરવે છે.

VPNs



તમારા ઇન્ટરનેટ ટ્રાફિક માટે એક સુરક્ષિત ટનલ તરીકે કલ્પના કરો. તે તમારી વાસ્તવિક જગ્યાને છુપાવે છે અને તમારા ડેટાને એન્ક્રિપ્ટ કરે છે, જે તેને એક ગુપ્ત કોડ જેવું બનાવે છે જેને માત્ર તમે અને VPN જ સમજાવી શકો. એવી વિશ્વસનીય VPN સેવા પસંદ કરો જે તમારી પ્રવૃત્તિનો લોગ ન રાખે.

Tor



ગુપ્ત માર્ગોથી ભરેલા એક ભુલભુલૈયાની કલ્પના કરો. Tor તમારા ઇન્ટરનેટ ટ્રાફિકને એન્ક્રિપ્ટ થયેલા રિલેની અનેક સ્તરોમાંથી પસાર કરે છે, જેથી તેનો પીછો કરવો લગભગ અશક્ય બની જાય છે. વધારાની પ્રાઇવેસી માટે Tor બ્રાઉઝર ડાઉનલોડ કરો.

સમજદા
રીતી
પસંદ કરો



બધા સર્ચ એન્જિનો એકસરખા નથી. કેટલાક, જેમ કે DuckDuckGo, ગોપનીયતાને પ્રાથમિકતા આપે છે અને તમારી શોધને ટ્રેક કરતા નથી. ભલે તમારા બ્રાઉઝરમાં હિસ્ટરી સંગ્રહાય, પરંતુ POST રીક્વેસ્ટ વાપરતા સર્ચ એન્જિનનો ઉપયોગ કરો તો તમારી શોધ છુપાયેલી રહે છે.

ઇન્કોગ્નિટો થાઓ



તમારા બ્રાઉઝરમાં "Incognito Mode" ને એક ગુપ્ત એજન્ટના માસ્ક તરીકે માનો. તે તમારી બ્રાઉઝિંગ હિસ્ટરી, કૂકીઝ અને ફોર્મ ડેટા સેવ થવાથી રોકે છે, જેથી કોઈ તમારી ઓનલાઇન પ્રવૃત્તિને સહેલાઈથી ચકાસી ન શકે.

સાવચેત રહો



ધ્યાન રાખો, આ સાધનો હોવા છતાં સંપૂર્ણ ગોપનીયતા એક દંતકથાની જેમ છે. તમે કઈ વેબસાઇટ્સ ખોલો છો તે અંગે સાવચેત રહો, હંમેશા સુરક્ષિત કનેક્શન (લોક આઇકન શોધો!) પસંદ કરો, અને જરૂરી હોય ત્યારે જ વ્યક્તિગત વિગતો શેર કરો.

ઝડપ સામે ગોપનીયતા



VPNs અને Tor એન્ક્રિપ્શન અને રીરાઉટિંગને કારણે ઇન્ટરનેટની ઝડપ થોડું ધીમી કરી શકે છે. આ એક આપલેની બાબત છે — થોડું ઓછું સ્પીડ, પણ ઘણી વધારે ગોપનીયતા. તમારા માટે શું યોગ્ય છે તે મુજબ પસંદ કરો.

બોનસ ટિપ:

તમે જે કોઈ પણ ટૂલનો ઉપયોગ કરો છો, તેની પ્રાઇવસી પોલિસી અને સર્વિસની શરતો હંમેશા તપાસો, જેથી તમે સમજી શકો કે તેઓ તમારી માહિતી કેવી રીતે સંભાળે છે. આ સરળ પગલાંઓ અનુસરવાથી, તમે તમારી ઓનલાઇન પ્રાઇવસી પર નિયંત્રણ મેળવી શકો છો અને તમારી ડિજિટલ જિંદગી તમારી પોતાની સુરક્ષા હેઠળ રાખી શકો છો. યાદ રાખો, જેમ્સ બોન્ડને પણ ક્યારેક સારી છલાંગ લેવાની જરૂર પડે છે!

કામના ઉપકરણો વર્સસ વ્યક્તિગત ઉપકરણો

કલ્પના કરો કે તમારી પાસે બે સૂટકેસ છે: એક તમારા કાર્યસ્થળ જીવન માટે અને બીજું તમારા વ્યક્તિગત સાહસો માટે. તમારા વર્ક લેપટોપ અને ફોનને અલગ રાખવું એ એવું જ છે જેમ કે આ અલગ સૂટકેસ ધરાવવું — તે તમને વ્યવસ્થિત રહેવામાં મદદ કરે છે અને તમારા વ્યાવસાયિક અને વ્યક્તિગત દુનિયાઓ બંનેની સુરક્ષા કરે છે.



તમારા વ્યક્તિગત જીવન અને વ્યાવસાયિક જીવન માટે અલગ ઉપકરણો રાખવાનું વિચાર કરો.



A. ડેટા ડિટેક્ટિવ: અલગ ઉપકરણો વાપરવાથી, તમે વ્યક્તિગત અને વ્યાવસાયિક ડેટા મિક્સ થવાના જોખમને ઘટાડો છો, સુરક્ષા વધારશો અને બંને માટે પ્રાઇવસી સુનિશ્ચિત કરશો. કામ અને વ્યક્તિગત કામ માટે અલગ ઉપકરણો વાપરવાથી, તમે અસલમાં ડેટા ડિટેક્ટિવ બની જાઓ છો! તમે તમારી કાર્ય ફાઇલોને તમારી વ્યક્તિગત ફોટોમાં ચોરીથી જાળવે શકો છો અને આ વિલક્ષણ રીતે પ્રત્યેક માટે સુરક્ષિત રાખો છો, જેમ બે તાળાવાળા સૂટકેસ જુદા કી સાથે સુરક્ષિત હોય.



B. એક્સેસ કંટ્રોલ નિન્જા: સ્પષ્ટ અલગાવ સંવેદનશીલ કાર્ય સંબંધિત માહિતી પર એક્સેસ નિયંત્રિત કરવામાં મદદ કરે છે, આથી અચાનક પ્રકાશન અથવા ડેટા ભંગ થવાનો જોખમ ઘટે છે. તમારા કાર્ય અને વ્યક્તિગત ઉપકરણોને અલગ રાખવું એ એવું જ છે જેમ કે તમારા ઓફિસના સૂટકેસ માટે એક ગુપ્ત કોડ હોય. ફક્ત સત્તાધિકૃત લોકો (જેમ કે તમે અને તમારા બોસ) તમારા કાર્ય સંબંધિત વસ્તુઓ જોઈ શકે, જ્યારે તમારી વ્યક્તિગત સૂટકેસ માત્ર તમારી નજર માટે ખાનગી રહેશે. આ અચાનક લીક અથવા ચોરપટ્ટી અટકાવવા મદદ કરે છે અને તમારા કાર્યજીવનને સુરક્ષિત અને વ્યવસ્થિત રાખે છે.



C. જવાબદારી ચેમ્પિયન: ઉપકરણોને અલગ રાખવાથી કાર્ય સંબંધિત પ્રવૃત્તિઓ અને ડેટા માટે ownership અને જવાબદારી સ્પષ્ટ થાય છે. અલગ ઉપકરણો રાખવાથી એ સ્પષ્ટ થાય છે કે કોને કઈ જવાબદારી છે. આ એ રીતે છે જેમ તમે તમારા સૂટકેસ પર લેબલ લગાવો – દરેક જાણ જાણે કે કાર્ય સૂટકેસ ઓફિસમાં તમારો છે, અને વ્યક્તિગત સૂટકેસ તમારા પોતાના માટે છે જેને તમે જે ઇચ્છો તે ભરી શકો. આ ટાસ્ક ટ્રેક કરવી અને જવાબદારી રાખવી સરળ બનાવે છે, તમને અને તમારા સાથીદારો બંને માટે.

યાદ રાખો, તમારા કાર્ય અને વ્યક્તિગત ઉપકરણોને અલગ રાખવું માત્ર બે ગેજેટ્સ હોવા વિશે નથી – તે તમારી પ્રાઇવસીની સુરક્ષા, વ્યવસ્થા જાળવવી અને તમારી જિંદગીને સરળ બનાવવી વિશે છે. તેથી આગળ વધો, ડેટા ડિટેક્ટિવ, એક્સેસ કંટ્રોલ નિન્જા, અને જવાબદારી ચેમ્પિયન બનો! અને તમારા સૂટકેસ પર લેબલ લગાવવાનું ભૂલશો નહીં!

બોનસ ટિપ: અલગ ઉપકરણો હોવા છતાં, હંમેશા ધ્યાન રાખો કે તમે ઓનલાઈન શું શેર કરો છો અને કોને એક્સેસ આપો છો. કોઈ પણ સિસ્ટમ સંપૂર્ણ સુરક્ષિત નથી, તેથી ચુસ્ત રહો અને તમારા ડિજિટલ સાહસોનો આનંદ માણો!

તમારા ડેટાને ખજાનાની જેમ સુરક્ષિત રાખો: એન્ક્રિપ્શન સ્તરો માટે માર્ગદર્શિકા

તમારા ડેટાને એક ખજાનાની તસવીર તરીકે કલ્પના કરો, જે કિંમતી રહસ્યોથી ભરેલું છે. આ રહસ્યોને સુરક્ષિત રાખવા માટે, તમને બહુવિધ તાળા લગાવવાની જરૂર છે, બરાબર?

આ જ એન્ક્રિપ્શન સ્તરોનો ઉદ્દેશ્ય છે!



સંપૂર્ણ ખજાના તાળું (FDE):

- તમારી સમગ્ર હાર્ડ ડ્રાઈવને એન્ક્રિપ્ટ કરો, જેમ ખજાનાના સમગ્ર બક્ષને મજબૂત તાળાથી બંધ કરવું.
- BitLocker (Windows), FileVault (macOS), અથવા VeraCrypt (ત્રીજી પાર્ટી) જેવા સાધનોનો ઉપયોગ કરો.



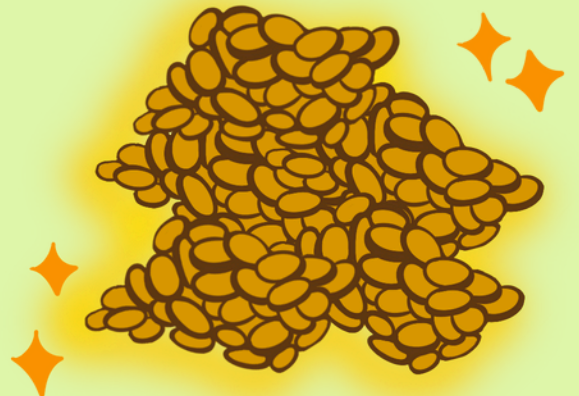
રહસ્ય વિભાગ તાળા (OS-સ્તર):

- macOS પર એન્ક્રિપ્ટ કરેલ ડિસ્ક ઈમેજ બનાવો (ખજાનામાં રહેલા ગુપ્ત બોક્સની જેમ).
- કેટલાક OS પર એન્ક્રિપ્ટ કરેલી ફાઈલ સિસ્ટમ્સનો ઉપયોગ કરો (લપાયેલ વિભાગોની જેમ).



વ્યક્તિગત રત્ન થેલી (એપ્લિકેશન-સ્તર)

- ખાસ રત્નો (પાસવર્ડ, નોટ્સ, સંદેશા)ને એન્ક્રિપ્ટ કરેલી એપ્લિકેશનો સાથે સુરક્ષિત રાખો.
- પાસવર્ડ મેનેજર, સુરક્ષિત નોટ-લેવાની એપ્સ, અને એન્ડ-ટુ-એન્ડ એન્ક્રિપ્શનવાળી મેસેજિંગ એપ્સ (જેમ કે Signal, WhatsApp) યાદ રાખો.



મુખ્યાં યાદગાર બાબતો:

- દરેક તાળા (એન્ક્રિપ્શન સ્ટર) માટે મજબૂત, અનન્ય પાસવર્ડ અથવા કીનો ઉપયોગ કરો.
- તમારું સોફ્ટવેર નિયમિત રીતે અપડેટ કરો જેથી તાળાઓ સુરક્ષિત અને તાજા રહે.
- તમારી એન્ક્રિપ્ટ કરેલી ડેટાનો બેકઅપ (ખજાનાના નકશા!) રાખો, જેથી તેને ફરી શોધવાની જરૂર પડે ત્યારે મદદ મળે.



આ એન્ક્રિપ્શન તાળાઓને સ્તરબદ્ધ કરીને, તમે તમારા ડેટા માટે એક કિલ્લો તૈયાર કરો છો, જેનાથી કોઈ પણ વ્યક્તિ તમારા ડિજિટલ ખજાનાને ચોરવી વધુ મુશ્કેલ બની જાય છે!

પ્રાઇવસી અને સાઇબરસુરક્ષા સુનિશ્ચિત કરવી: ઓનલાઇન અને ઓફલાઇન

- ➔ અલગ થઈ જતા મેસેજિંગ સર્વિસો અથવા એપ્લિકેશનોનો ઉપયોગ કરો, જે મોકલેલ મેસેજોને જ્યારે જોવામાં આવે છે અથવા પૂર્વનિર્ધારિત સમય બાદ સ્વયંલિત રીતે કાઢી દે છે. Signal, Telegram, WhatsApp વગેરે જેવી એપ્સ ડિસએપિયરિંગ મેસેજ ફીચર્સ પ્રદાન કરે છે, જે સુનિશ્ચિત કરે છે કે સંવાદ અસ્થાયી રહેશે અને વાંચ્યા પછી અથવા નિર્ધારિત સમય પછી ચેટ્સ અથવા હિસ્ટરીમાં રહેતો નહીં.
- ➔ પ્રમાણિકરણ માટે ફિંગરપ્રિન્ટ અથવા ફેસ ID ઓળખવાની જગ્યાએ પાસવર્ડ અથવા પિનનો ઉપયોગ કરો, કારણ કે આ રીતો ચેતન મગજની ધ્યાનશીલતા અથવા સ્પષ્ટ મંજૂરીની જરૂર નથી. પાસવર્ડ અથવા પિનનો ઉપયોગ સુનિશ્ચિત કરે છે કે સંવેદનશીલ માહિતી અથવા ઉપકરણો સુધી એક્સેસ માત્ર વપરાશકર્તા દ્વારા દાખલ કરવામાં આવેલી જાણકારી પર આધારિત છે, જે નિયંત્રણ અને સુરક્ષા વધારવા માટે વિશેષ ચેતન અને સંજ્ઞાત ક્રિયા જરૂરી બનાવે છે.
- ➔ તમારા પાસવર્ડનો એક ભાગ સ્ટોર કરવા માટે પાસવર્ડ મેનેજરનો ઉપયોગ કરવો અને બાકીનો ભાગ યાદ રાખવો સુરક્ષા વધારવા માટે સારી વ્યૂહરચના છે. પાસવર્ડનો એક ભાગ સુરક્ષિત મેનેજરમાં સંગ્રહિત કરીને અને બાકીના ભાગને યાદમાં રાખીને, તમે દ્વિભાગી પ્રમાણિકરણ બનાવો છો જે તમારા ખાતાઓની કુલ સુરક્ષા મજબૂત કરે છે.

- ઉદાહરણ તરીકે, પાસવર્ડ મેનેજરનો ઉપયોગ કરીને "12345" જેવા ભાગને સુરક્ષિત રીતે સંગ્રહિત કરો અને અનુરૂપ ભાગ, જેમ કે "fdsjrie," યાદ રાખો, જેથી સંપૂર્ણ પાસવર્ડ "12345fdsjrie" બને. આ પદ્ધતિ સુરક્ષા અને સુવિધાને સંતુલિત કરવામાં મદદ કરે છે, કારણ કે તે પાસવર્ડ મેનેજરની એન્ક્રિપ્શન ક્ષમતા અને તમારા વિશિષ્ટ ભાગને યાદ રાખવાની ક્ષમતા બંનેને જોડે છે, જે અનધિકૃત વપરાશકર્તાઓ માટે તમારા ખાતાઓમાં પ્રવેશ મેળવવો વધુ મુશ્કેલ બનાવે છે.
- 2FA (ટુ-ફેક્ટર ઓથેન્ટિકેશન) લાગુ કરવાથી ખાતાની સુરક્ષા નોંધપાત્ર રીતે વધે છે. SMS અથવા ઈમેઈલ આધારિત 2FAની જગ્યાએ TOTP (ટાઈમ-બેઝડ વન-ટાઈમ પાસવર્ડ) આધારિત 2FA પસંદ કરવી શ્રેષ્ઠ છે, કારણ કે તે વધુ ઊંચી સુરક્ષા પ્રદાન કરે છે. TOTP એક અનન્ય કોડ જનરેટ કરે છે જે નિયમિત અંતરાલ પર, સામાન્ય રીતે દરેક 30 સેકન્ડમાં, બદલાય છે અને અનધિકૃત એક્સેસ સામે વધારાની સુરક્ષા સ્તર પ્રદાન કરે છે.
- Google Authenticator, Authy, અથવા Microsoft Authenticator જેવા ઓથેન્ટિકેટર એપ્સનો ઉપયોગ કરવો, જે TOTP કોડ જનરેટ કરે છે, વધુ સુરક્ષિત વિકલ્પ છે. આ એપ્સ સમય સંવેદનશીલ કોડ બનાવે છે જે તમારા ખાતાઓ સાથે જોડાયેલા હોય છે અને SMS અથવા ઈમેઈલ જેવા સંચાર માધ્યમ પર નિર્ભર નથી, જે SMS આધારિત 2FAને જોખમરૂપ બનાવનારા ઇન્ટરસેપ્શન અથવા SIM સ્વેપિંગ હુમલાઓના જોખમને ઘટાડે છે.
- TOTP આધારિત 2FAનો ઉપયોગ કરીને, તમે સુરક્ષાનો વધારાનો સ્તર ઉમેરો છો જે તમારા ખાતાઓમાં અનધિકૃત એક્સેસની સંભાવના નોંધપાત્ર રીતે ઘટાડે છે અને વિવિધ સાઇબર જોખમો સામે વધુ મજબૂત સુરક્ષા પ્રદાન કરે છે.
- ફાઈલોને ફક્ત ડિલીટ કરવું તમારી પ્રાઇવસી સાચવવા માટે પૂરતું નથી! માત્ર "ડિલીટ" પર ક્લિક કરવાથી ફાઈલો કાયમ માટે મટતી નથી. તે હજુ પણ તમારા ઉપકરણમાં છુપાઈ રહે છે અને વિશેષ સાધનો દ્વારા શોધી શકાય છે. તમારી પ્રાઇવસી સાચી રીતે જાળવવા માટે, તમને તે ફાઈલો શ્રેડ (શ્રેડિંગ) કરવાની જરૂર છે. તેને કાગળના દસ્તાવેજોને શ્રેડ કરવા જેવી કલ્પના કરો – તેને ફરીથી એકત્રિત કરવું લગભગ અસંભવ છે! શ્રેડિંગ સોફ્ટવેર તમારી ફાઈલો પર રેન્ડમ અક્ષરો અને આંકડા લખી આપે છે, જે તેમને ગૂંચવાયેલ અને વાંચનયોગ્ય ન રાખે. એ એવું જ છે કે જેમ shredded કાગળને ફેંકી અને જમીન નીચે દફન કરી દેવું. કોઈ પણ વ્યક્તિ તેને ઉકાળી શકે નહીં અને તમારા રહસ્યો વાંચી શકે નહીં! તો, જ્યારે પણ તમે સંવેદનશીલ ફાઈલ ડિલીટ કરવી હોય, ત્યારે "ડિલીટ" બટન ટાળો અને શ્રેડિંગ સોફ્ટવેર વાપરો. તે તમારી ડિજિટલ જિંદગીને ખાનગી અને સુરક્ષિત રાખવાનો શ્રેષ્ઠ માર્ગ છે.
- Tor મારફતે વેબસાઇટ્સનો એક્સેસ લેવાથી વધારેલી પ્રાઇવસી અને સુરક્ષા સુનિશ્ચિત થાય છે. ઉદાહરણ તરીકે, તમે The Guardian જેવી ન્યૂઝ સાઇટ્સ અથવા Twitter જેવા સોશિયલ મીડિયા પ્લેટફોર્મ્સને Tor મારફતે મુલાકાત આપી વધારાની અવિનાશી ઓળખ સાથે બ્રાઉઝ કરી શકો છો.



વસ્તુઓ છુપાવવી: ઓનલાઇન અને ઓફલાઇન

ઓનલાઇન :

- **Crypt.ee:** અનામી સાઇન-અપ કરવાની સુવિધા આપે છે, એન્ડ-ટુ-એન્ડ એન્ક્રિપ્શન પ્રદાન કરે છે અને વધારાની પ્રાઇવસી માટે છુપાયેલા ફોલ્ડર્સ બનાવવાની મંજૂરી આપે છે.
- **Cryptomator:** વ્યક્તિગત સર્વિસ પર ફાઇલોને એન્ક્રિપ્ટ કરીને સંગ્રહિત કરે છે, જેના કારણે એપ્લિકેશન અનઇ-સ્ટોલ કર્યા પછી ફાઇલોના સ્થાનને ટ્રેસ કરવું અશક્ય બને છે.

ઓફલાઇન :

- **VeraCrypt:** ડ્રાઇવ્સ અથવા સ્ટોરેજ ડિવાઇસ પર ડેટાને સુરક્ષિત કરવા માટે છુપાયેલા પાર્ટિશન્સ બનાવો.
- **Secret Compartments:** ફર્નિચર અથવા વસ્તુઓમાં છુપાયેલા વિભાગોમાં કિંમતી વસ્તુઓ છુપાવો.
- **Cipher Systems:** લખાણ અથવા માલમત્તાને એન્ક્રિપ્ટ અને સુરક્ષિત કરવા માટે વ્યક્તિગત કોડ્સ અથવા સાઇફર્સ વિકસાવો.

આ પદ્ધતિઓ ડિજિટલ અને ભૌતિક બંને જગ્યાઓ પર વધારેલી પ્રાઇવસી અને સુરક્ષા પ્રદાન કરે છે, જે સંવેદનશીલ માહિતીને સુરક્ષિત રાખવાના વિશ્વસનીય માર્ગો આપે છે.



ઓછી ઉપયોગમાં આવતી ફાઇલોને સુરક્ષિત સ્થળે (એન્ક્રિપ્ટેડ ડ્રાઇવ અથવા ક્લાઉડમાં) સંગ્રહિત કરો અને તમારા ડિજિટલ કાર્યક્ષેત્રને નિયમિત રીતે ગોઠવો, જેથી હાલ જે જરૂરી છે તે જ રાખો. નકલો બનાવવા કરતાં જૂના સંસ્કરણોને આર્કાઇવ કરો, જે તમારા ડિજિટલ જીવનને વધુ વ્યવસ્થિત અને સુરક્ષિત બનાવે છે.



કોઈ સાઇટમાં જોડાવું છે પરંતુ તમારા ડિજિટલ ફિંગરપ્રિન્ટ પાછળ છોડવા નથી? તો એવી સાઇટ્સ પસંદ કરો જે:

- ઓછામાં ઓછી માહિતી માંગે: ફક્ત યુઝરનેમ અને કદાચ એક ઈમેઇલ — જાણે કોઈ ગુપ્ત હેન્ડશેક.
- તમને અદૃશ્ય રહેવા દે: નામ નથી? કોઈ સમસ્યા નથી! કેટલીક સાઇટ્સ તમને તમારી ઓળખ આપ્યા વગર સાઇન અપ કરવાની મંજૂરી આપે છે.
- નકલી ઈમેઇલ સરનામાં આપે: જોડાવવા માટે થ્રો-અવે ઈમેઇલનો ઉપયોગ કરો, જેથી તમારું સાચું ઈમેઇલ ખાનગી રહે.

શબ્દાવલી:

ઓડિયો-વિડિયો ઇલેક્ટ્રોનિક માધ્યમ: તે કોઈપણ સંચાર ઉપકરણ છે જે વિડિયો કોન્ફરન્સિંગ, ઓળખ પ્રક્રિયા રેકૉર્ડ કરવી, શોધ અને સીઝર, પુરાવા એકત્ર કરવું, ઇલેક્ટ્રોનિક સંચાર મોકલવું અને રાજ્ય સરકારના નિયમો મુજબ નિર્દિષ્ટ અન્ય ઉપયોગો માટે વપરાય છે.

ઘરપકડ: જ્યારે કોઈ વ્યક્તિને કાનૂની કસ્ટડીમાં લેવામાં આવે છે અને જેલ અથવા નિશ્ચિત સ્થળે બાંધી દેવામાં આવે છે, ભલે તે આરોપ છે કે નહીં, તેને ઘરપકડ કહેવાય છે. કોઈ પણ ચાર્જ દાખલ ન થયેલા અથવા વોરંટ વગર પણ વ્યક્તિને ઘરપકડ કરી શકાય છે (જુઓ: Cognizable Offences).

જામીનયોગ્ય ગુનાઓ: એવી ગુનાઓ જે ગંભીર કે ગંભીર સ્વભાવની નથી અને જેના માટે આરોપી/ઘરપકડ કરાયેલ વ્યક્તિને જામીન મેળવવાનો અધિકાર છે, તેમને જામીનયોગ્ય ગુનાઓ કહેવામાં આવે છે. ઇન્સ્પેક્ટિંગ ઓફિસર જામીન આપવામાં ફરજિયાત છે, સામાન્ય રીતે જામીન બોન્ડ સબમિટ કરવાની શરત સાથે. છતાં, જામીન મળવાથી આરોપી મુક્ત નથી, તેમને કોર્ટની કાર્યવાહી દ્વારા ટ્રાયલની શરત પૂર્ણ કરવી પડશે.

આરોપ: આરોપ એ અધિકૃત આરોપ છે કે કોઈ વ્યક્તિએ ગુના કર્યો છે, જે પ્રોસિક્યુટર અથવા પોલીસ/ઇન્સ્પેક્ટિંગ ઓફિસર દ્વારા કરવામાં આવે છે. [23] આમાં વ્યક્તિને તેમના વિરુદ્ધ આરોપના આધાર વિશે જાણ કરવી ફરજિયાત છે.

ઓળખાય તેવી ગુનાઓ: તે ગુનાઓ, જેના માટે પોલીસ અધિકારી વોરંટ કે મેજિસ્ટ્રેટની પૂર્વ મંજૂરી વગર ઘરપકડ કરી શકે છે. આ ત્યારે થાય છે, ભલે FIR દાખલ થયો હોય કે ન થયો હોય, અને સામાન્ય રીતે તે ગુનાઓ માટે લાગુ પડે છે જે વધુ ગંભીર અથવા ગંભીર સ્વભાવની હોય.

કમ્પ્યુટર: તે કોઈપણ ઇલેક્ટ્રોનિક, મેગ્નેટિક, ઓપ્ટિકલ અથવા અન્ય ઉચ્ચ-ગતિ ડેટા પ્રોસેસિંગ ઉપકરણ અથવા સિસ્ટમ છે, જે લોજિકલ, અંકગણિત અને મેમરી ફંક્શન્સ કરી શકે છે, અને તેમાં તમામ ઈનપુટ, આઉટપુટ, પ્રોસેસિંગ, સ્ટોરેજ, કમ્પ્યુટર સોફ્ટવેર અથવા કમ્પ્યુનિકેશન સુવિધાઓનો સમાવેશ થાય છે, જે કમ્પ્યુટર સિસ્ટમ અથવા નેટવર્કમાં જોડાયેલા છે.

સંચાર ઉપકરણ: આ કોઈ સેલ ફોન, પર્સનલ ડિજિટલ આસિસ્ટન્ટ ઉપકરણ અથવા બંનેનું સંયોજન અથવા કોઈપણ અન્ય ઉપકરણ હોઈ શકે છે, જેનો ઉપયોગ સંચાર, લખાણ, વિડિયો, ઓડિયો અથવા છબી મોકલવા માટે થાય છે.

ફૂકીઝ: વેબ બ્રાઉઝરમાં તમારી પ્રવૃત્તિને ટ્રેક અને રેકૉર્ડ કરવા માટે નાના માહિતી/ડેટા ફાઇલો ફૂકીઝ કહેવાય છે. તે જાહેરાત અને વિશ્લેષણ માટે વપરાય શકે છે. ફૂકીઝમાં વપરાશકર્તા વિશેની વ્યક્તિગત માહિતી હોઈ શકે છે જેમ કે યુઝરનેમ, પાસવર્ડ, કસ્ટમાઇઝ્ડ પસંદગીઓ, વેબ પ્રવૃત્તિ વગેરે, અને જો તે સુરક્ષિત ન હોય તો વપરાશકર્તાઓ માટે સુરક્ષા અને પ્રાઇવસી જોખમ હોઈ શકે છે.

ઇલેક્ટ્રોનિક સંચાર: તે કોઈપણ લેખિત, મૌખિક, છબી અથવા વિડિયો માહિતી માટે ઉપયોગ થાય છે, જે ઇલેક્ટ્રોનિક રીતે વહેંચવામાં આવે છે, લોકો કે ઉપકરણો વચ્ચે, ફોન, કમ્પ્યુટર, ઓડિયો-વિડિયો પ્લેયર, કેમેરા અથવા અન્ય ઇલેક્ટ્રોનિક ઉપકરણ દ્વારા, અથવા કેન્દ્ર સરકાર દ્વારા નિર્ધારિત અન્ય ઇલેક્ટ્રોનિક રૂપમાં.

એન્ક્રિપ્શન: તે પ્રક્રિયા છે જેમાં વ્યક્તિગત અથવા સંવેદનશીલ માહિતી એન્ક્રિપ્ટેડ/કોડ ફોર્મમાં સ્ટોર થાય છે અને માત્ર ડિક્રિપ્શન કી ધરાવતી વ્યક્તિ તેને ડિકોડ/ડિક્રિપ્ટ કરી શકે છે. આ ડેટાને અનધિકૃત વ્યક્તિઓના એક્સેસથી સુરક્ષિત રાખે છે.

શબ્દાવલી:

પુરાવો: પુરાવો એ કોઈ પણ નિવેદન છે, જે મૌખિક કે દસ્તાવેજરૂપ (લખાણ અથવા ઇલેક્ટ્રોનિક, જેમાં ડિજિટલ ઉપકરણોનો સમાવેશ થાય છે) હોઈ શકે છે, જે તપાસ અથવા અનુસંધાન સાથે સંબંધિત હોઈ શકે છે. દસ્તાવેજોને ડોક્યુમેન્ટરી પુરાવો કહેવામાં આવે છે. પુરાવો પ્રમાણ સાથે અલગ છે કારણ કે તે અનિવાર્ય રીતે નક્કી નથી અને કોર્ટની છૂટ પર આધારિત છે.

ઇન્સ્પેક્ટિંગ ઓફિસર: પોલીસ અધિકારી, જેને કોઈ ગુના તપાસવાની નિમણૂંક આપવામાં આવી છે.

ચલ મિલકત: BNS માત્ર ચલ મિલકત નિર્ધારિત કરે છે, જેમ કે દરવાજા, બારી, વૃક્ષો વગેરે, જે જમીન સાથે સ્થાયી રીતે જોડાયેલી નથી. ચલ મિલકતમાં બધા ઇલેક્ટ્રોનિક અને ડિજિટલ ઉપકરણોનો સમાવેશ થાય છે, જે જમીન સાથે જોડાયેલા નથી. [25]

અજામીનયોગ્ય ગુનાઓ: તે ગુનાઓ જે વધારે ગંભીર છે અને જેના માટે આરોપીને જામીન મેળવવાનો અધિકાર નથી, તેમને અજામીનયોગ્ય ગુનાઓ કહેવામાં આવે છે. છતાં, કોર્ટ પોતાના વિવેકબુદ્ધિ મુજબ જામીન આપી શકે છે, જેમ કે આરોપીની ભાગી જવાની શક્યતા, કાનૂની કાર્યવાહી સાથે સહયોગ ન આપવી વગેરે પર આધાર રાખીને.

અજાણ્યાતમુક્ત ગુનાઓ: તે ગુનાઓ, જેના માટે પોલીસ અધિકારી વોરંટ અથવા મેજિસ્ટ્રેટની પૂર્વ મંજૂરી વગર ઘરપકડ કરી શકે નહીં. આ FIR દાખલ કર્યા પછી અને વોરંટ મેળવ્યા પછી થાય છે અને સામાન્ય રીતે તે ગામભીર્ય અથવા ગંભીરતા ઘટાડેલી ગુનાઓ માટે લાગુ પડે છે.

સ્થળ: BNSS હેઠળ, સ્થાનમાં ઘર, બિલ્ડિંગ, ટેન્ટ, વાહન અથવા જહાજનો સમાવેશ થાય છે. [27]

જાહેર સ્થળ: આનો અર્થ તેવા કોઈપણ સ્થળ માટે છે, જે જાહેર પરિવહન, હોટલ, દુકાન અથવા જાહેર ઉપયોગ માટે ઉદ્દિષ્ટ હોય. [28]

સીઝર મેમો: જો કોઈ ઇન્સ્પેક્ટિંગ ઓફિસર દ્વારા આરોપી પાસેથી કોઈ સંપત્તિ (મૂલ્યવાન કે અમૂલ્ય) જપ્ત કરવામાં આવે, તો તે તપાસના હેતુ માટે સીઝર મેમોમાં નોંધાય છે. તેમાં સંપત્તિના તમામ વિગતવાર/વિશેષતાઓ, સંગ્રહનું સ્થાન, કિસ્સા સંબંધિત વિગતો વગેરે સમાવિષ્ટ હોય છે.

વોરંટ: વોરંટ એ એ જજ દ્વારા સહી કરાયેલ દસ્તાવેજ છે, જે પોલીસને તમે ઘરપકડ કે તમારી સંપત્તિ તપાસવા અને તેમાંની વસ્તુઓ લેનાં માટે અધિકાર આપે છે. તમને વોરંટ જોવા હક છે અને તેની માન્યતા તપાસવી જોઈએ.

પરિશિષ્ટ:

શોધ અને જપ્તી અંગે કેટલીક ટિપ્પણીઓ:

1. અગાઉ, અદાલતો એ ચુકાદા આપ્યા છે કે અવૈધ અને અનૈતિક માધ્યમ દ્વારા મેળવેલા પુરાવા કાયદેસર સ્વીકાર્ય હોઈ શકે છે. તેમ છતાં, આવા પુરાવાને વાસ્તવિક અને અનટેમ્પર્ડ સાબિત કરવું જરૂરી છે. સ્વીકાર્યતાનું નિર્ધારણ માત્ર અદાલતો કરી શકે છે – દરેક કેસના તથ્યો અને પરિસ્થિતિઓના આધારે. [Umesh Kumar v. State of A.P., (2013) 10 SCC 169]
2. હૈદરાબાદ હાઈકોર્ટ ઓફ કેરળએ ચુકાદું આપ્યું હતું કે પોલીસ અધિકારી કોઈ જર્નલિસ્ટનો મોબાઇલ ફોન CrPC (હવે BNSS) મુજબ નક્કી કરાયેલા પ્રક્રિયા અનુસાર પાલન કર્યા વિના જપ્ત કરી શકે નહીં. જો તે ઉપકરણ ગુનાની તપાસ માટે જરૂરી હોય, તો પોલીસ અધિકારીઓએ ઉપકરણની યોગ્ય તપાસ અને જપ્તી માટે CrPC (હવે BNSS)ના નિયમોનું પાલન કરવું ફરજિયાત છે. [29]
3. દિલ્હીની હાઈકોર્ટએ પણ ચુકાદું આપ્યું કે કોઈ વ્યક્તિને પાસવર્ડ (અથવા અન્ય વિગતો) આપવા માટે દબાણ કરી શકાતું નથી, કારણ કે આ ભારતના સંવિધાનના કલમ 20(3) હેઠળ સ્વયં-અપરાધ સંરક્ષણ હેઠળ આવે છે. [30]
4. એમ જ રીતે, દિલ્હી સ્થિત રાઉઝ એવન્યુ ડિસ્ટ્રિક્ટના વિશેષ CBI કોર્ટએ નિર્દેશ કર્યો કે આરોપીનો કોઈપણ પ્રકારની માહિતી આપવા માટે બળજબરી કરી શકાતી નથી, અને આ બાબતમાં તે ભારતના સંવિધાનના કલમ 20(3) અને BNSSના કલમ 180(2) હેઠળ સુરક્ષિત છે. [31]
5. શોધ અને જપ્તી પ્રક્રિયાઓને સમજવું માત્ર તીવ્ર પરિસ્થિતિઓમાં ઘબરમાં બચાવ નહીં કરે, પણ અધિકારીઓ સાથે સહયોગ આપવા માટે પણ મદદરૂપ થાય છે. ઉપરાંત, આવા નિયમોને જાણવું વ્યક્તિગત અત્યાચાર અને ગેરવર્તનથી રક્ષણ પ્રદાન કરી શકે છે, જે કાયદા અને નિયમો જાળવતા અધિકારીઓ દ્વારા થઈ શકે છે.

Electronic Devices and the Law

The judicial position on this matter remains unsettled. However, there are general guidelines with respect to search and seizure within the BNSS, BSA, UAPA, Income Tax Act, PMLA and IT Act. It must be noted that the processes of Search and Seizure differs across these legislations and are given on the following page.

પરિશિષ્ટ:

ભારતીય નાગરિક સુરક્ષા સંહિતા વોરન્ટ સાથે	Section 96- આ જોગવાઈ મુજબ પોલીસ અધિકારીએ શોધ (સર્ચ) માટે કોર્ટ પાસે વિશેષ અનુમતિ લેવી પડે છે. જ્યારે કોર્ટે એવું માનવાનો યોગ્ય આધાર મળે કે સર્ચ કરવું જરૂરી છે, ત્યારે કોર્ટ સર્ચ વોરન્ટ કઈ શરતો હેઠળ જારી કરવો તે સ્પષ્ટ કરે છે. સર્ચ/સીઝરનો જવાબદાર અધિકારી ફક્ત તે જ નિર્ધારિત વિસ્તારોમાં તપાસ કરી શકે છે, જે વોરન્ટમાં જણાવ્યા હોય. Section 103- આ મિલકતની શોધ અને જપ્તી (સીઝર) માટેની એક મૂળભૂત જોગવાઈ છે. જ્યારે પણ પોલીસ કોઈ મિલકતની શોધ કે જપ્તી કરે, ત્યારે તેમને આ નિયમોનું પાલન કરવું ફરજિયાત છે.
ભારતીય નાગરિક સુરક્ષા સંહિતા વોરન્ટ વગર	Section 185- પોલીસ કોઈપણ સ્થળમાં બિનવોરન્ટ પ્રવેશીને શોધ (સર્ચ) કરી શકે છે, જો તેમને લાગે કે ત્યાં ઝડપથી કોઈ ગુનો થઈ શકે છે, અથવા તેમની તપાસ માટે તે શોધ જરૂરી છે. આ જોગવાઈ હવે ફરજિયાત કરે છે કે સર્ચ conducting કરનાર પોલીસ અધિકારીએ આખી પ્રક્રિયાનું રેકોર્ડિંગ કરવું જોઈએ. જો અધિકારી પોતે શોધ ન કરી શકે, તો તે તેની અધિનસ્ત અધિકારીને સર્ચ સોંપી શકે છે—પણ તે પહેલાં લેખિતમાં કારણો નોંધવા પડશે. આ સર્ચનો રેકોર્ડ તૈયાર કર્યા બાદ તેની નકલ નજીકના મેજિસ્ટ્રેટને 48 કલાકની અંદર મોકલવી પડશે. Statements during Investigations: તપાસ દરમિયાન વ્યક્તિએ આપેલા નિવેદન પર હસ્તાક્ષર કરવાની ફરજ નથી. અને કોઈપણ વ્યક્તિને પોતે જ પોતાને દોષિત દર્શાવે તેવી વાત બોલવાની મજબૂરી નથી, કારણ કે ભારતીય બંધારણ તેઓને આ અધિકાર આપે છે. [32] પોલીસ કોઈ વ્યક્તિને બિનવોરન્ટ પણ ધરપકડ કરી શકે છે, જો: તેઓ માનતા હોય કે વ્યક્તિ ગંભીર ગુનામાં સંકળાયેલ છે, તેના વિરુદ્ધ ફરિયાદ છે, અથવા તેમને યોગ્ય કારણ હોય કે વ્યક્તિએ ગુનો કર્યો છે. પરંતુ જો વ્યક્તિ અશક્ત (infirm) હોય અથવા 60 વર્ષથી વધુ વય ધરાવતી હોય, તો અને જ્યારે ગુનાની સજા 3 વર્ષથી ઓછી હોય, ત્યારે તેની ધરપકડ માટે પહેલાથી DSPની મંજૂરી ફરજિયાત છે.
	Section 105- આ નવી ઉમેરાયેલી જોગવાઈ મુજબ, પોલીસ અધિકારીએ તપાસ અને જપ્તીની (search and seizure) પ્રક્રિયાનો રેકોર્ડ રાખવો ફરજિયાત છે, અને તે માટે મોબાઈલ ફોન દ્વારા રેકોર્ડિંગ કરવી પ્રાથમિકતા છે. તે ઉપરાંત, જપ્ત કરેલ વસ્તુઓની સૂચિ, જે સાક્ષીઓના હસ્તાક્ષરથી પ્રમાણિત હોય, તૈયાર કરવી જરૂરી છે. આ યાદી જિલ્લા મેજિસ્ટ્રેટ અથવા પ્રથમ વર્ગના ન્યાયિક મેજિસ્ટ્રેટને તરત જ મોકલવી જરૂરી છે. Section 106 આ કલમ હેઠળ, પોલીસને કોઈપણ એવી સંપત્તિ લઈ લેવાની અથવા જપ્ત કરવાની સત્તા છે, જેને તેઓ ચોરી થઈ હોવાની અથવા ગુના સાથે સંબંધિત હોવાની શંકા ધરાવે છે. ક્યારેક આ જોગવાઈનો દુરુપયોગ થાય છે અને સામાન્ય શોધખોળની આડમાં ઘણી વસ્તુઓ જપ્ત કરી લેવાય છે. આ કલમ દરેક પોલીસ અધિકારીને સત્તા આપે છે કે: ચોરીની શંકાસ્પદ અથવા ગુના સાથે જોડાયેલી કોઈપણ સંપત્તિ જપ્ત કરી શકે. જપ્તી અંગેની માહિતી સ્થાનિક મેજિસ્ટ્રેટને રિપોર્ટ કરવી જરૂરી છે. આ જપ્ત સંપત્તિની કસ્ટડી જવાબદાર વ્યક્તિને આપવામાં આવી શકે છે, શરતે કે તે વ્યક્તિ કોર્ટમાં જરૂરી વખતે તે વસ્તુઓ રજૂ કરવાની બોન્ડ પર હસ્તાક્ષર કરે.

પરિશિષ્ટ:

ભારતીય સાક્ષ્ય અધિનિયમ)	Section 168- ન્યાયાધીશને નીચે મુજબના અધિકારો પ્રાપ્ત છે - • સંબંધિત કે અસંબંધિત કોઈપણ હકીકતો અંગે — કોઈપણ રીતથી — પ્રશ્ન પૂછવાનો અધિકાર. • કોઈપણ પક્ષકાર અથવા સાક્ષીને — ક્યારેય પણ — પ્રશ્ન પૂછવાનો અધિકાર. • પુરાવા તરીકે જરૂરી કોઈપણ દસ્તાવેજો અથવા વસ્તુઓ રજૂ કરવાની માંગણી કરવાનો અધિકાર. મહત્વપૂર્ણ એ છે કે, આ જોગવાઈ અનુસાર, કોઈપણ વ્યક્તિ ન્યાયાધીશની માંગણી અથવા વિનંતીનો વિરોધ કરી શકતી નથી. [શોધ અને જપ્તી સંબંધિત કેસોમાં, ખાસ કરીને જ્યારે ચોક્કસ દસ્તાવેજો અથવા વસ્તુઓ પુરાવા તરીકે જરૂરી હોય, ત્યારે આ જોગવાઈ ખૂબ મહત્વપૂર્ણ બને છે.]
મની લોન્ડરિંગ અટકાવવાનો કાયદો	Sections 16 and 17- આ બંને કલમો અનુક્રમે શોધ (Search) અને જપ્તી (Seizure) કરવાની પ્રક્રિયાના નિયમો નિર્ધારિત કરે છે. આ જોગવાઈઓ મુજબ — શોધ અથવા જપ્તી શા માટે કરવામાં આવે છે તેનો લેખિત રેકૉર્ડ રાખવો ફરજિયાત છે. જપ્ત કરેલી તમામ વસ્તુઓની યાદી સાથેનો વિસ્તૃત અહેવાલ (report) તૈયાર કરવો આવશ્યક છે. [શોધ અને જપ્તીની પ્રક્રિયા તથા તે સંબંધિત જરૂરી દસ્તાવેજીકરણ — બંને વચ્ચેનો સીધો સંબંધ આ કલમો સ્પષ્ટ કરે છે.]
ગેરકાયદેસર પ્રવૃત્તિઓ (રોકથામ) અધિનિયમ	Section 43A- પોલીસ અધિકારીને પોતાના સહકર્મચારી (અધિનસ્ત અધિકારી)ને શોધ કરવાની મંજૂરી આપવાની સત્તા આપે છે. આ કલમ એ પણ નક્કી કરે છે કે 'વિશ્વાસ કરવાનો આધાર' દાંતદ તો અધિકારીના વ્યક્તિગત જ્ઞાન દ્વારા અથવા કોઈ ત્રીજા પક્ષ દ્વારા આપવામાં આવેલી લેખિત માહિતી દ્વારા હોઈ શકે. Section 43B- શોધ અથવા જપ્તી દરમિયાન જે વ્યક્તિની શોધ લેવામાં આવે છે તેની હક્કોની વિગત આપે છે. આ બંને કલમો એ ખાતરી આપે છે કે — શોધ અથવા જપ્તી દરમિયાન વ્યક્તિને શોધના કારણો સ્પષ્ટ રીતે જણાવવા ફરજિયાત છે. જપ્ત કરેલી વસ્તુઓને નજીકના પોલીસ સ્ટેશનમાં લઈ જવાની રહેશે. ત્યાંનો જવાબદાર અધિકારી પછી BNSS (પૂર્વે CrPC) માં નિર્ધારિત નિયમો અનુસાર જરૂરી કાર્યવાહી કરશે.
આવકવેરા અધિનિયમ	Section 132- આ કલમ સત્તાવાળાઓને સત્તા આપે છે કે જો કોઈ વ્યક્તિ કાયદા મુજબ આપવાની જરૂરી દસ્તાવેજો અથવા વસ્તુઓ સ્વેચ્છાએ ન આપે, તો અધિકારીઓ તે દસ્તાવેજો અથવા વસ્તુઓ જપ્ત કરી શકે. શોધ અને જપ્તીની પ્રક્રિયાના સંદર્ભમાં, આ કલમ અધિકારીઓને કાનૂની આધાર આપે છે કે તપાસ અથવા કાનૂની કાર્યવાહી દરમિયાન જરૂરિયાત મુજબની ચોક્કસ વસ્તુઓ અથવા દસ્તાવેજો વ્યક્તિ દ્વારા ન આપતાં હોય તો તેઓ તેને જપ્ત કરી શકે. આ કલમ આરોપી વ્યક્તિને પૂરતા સુરક્ષા ઉપાયો (safeguards) પણ આપે છે— અધિકારીઓએ જપ્ત કરેલી વસ્તુઓ વિશે આરોપીને તેમની તરફથી યોગ્ય સ્પષ્ટીકરણ અથવા પુરાવા રજૂ કરવાની ન્યાયપૂર્ણ તક આપવી આવશ્યક છે.
માહિતી ટેકનોલોજી અધિનિયમ	Section 80- આ કલમ મુજબ સત્તાધિકૃત અધિકારીઓને જાહેર સ્થળે શોધ (search) કરવાની અને વોરન્ટ વગર ધરપકડ કરવાની સત્તા આપવામાં આવે છે— એવા કોઈપણ વ્યક્તિની, જે જાહેર સ્થળે મળી આવે અને જે અંગે ભૂતકાળમાં, વર્તમાનમાં અથવા ભવિષ્યમાં IT Act હેઠળ ગુનો કર્યો હોવાનો યોગ્ય શંકા હોય.

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: _____

આકૃતિ 1:

પ્રમાણપત્ર (નિષ્ણાત દ્વારા ભરવાનું)

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.

આકૃતિ 2:

પ્રમાણપત્ર (નિષ્ણાત દ્વારા ભરવાનું)

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.

આકૃતિ ૩:
Property Seizure Memo

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

આકૃતિ 3.1:
Property Seizure Memo

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

આકૃતિ 4:
જપ્તી સૂચિ

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)

આકૃતિ 5:

ગ્રીફ્તારી વોરંટ ફોર્મેટ (સત્તાવાર રાજપત્રમાં પ્રકાશિત અધિનિયમના પૃષ્ઠ 192 પર BNSSની દ્વિતીય અનુસૂચિમાં આપવામાં આવેલ મુજબ)

સંદર્ભો:

- [1] શબ્દનો અર્થ જાણવા માટે શબ્દકોશ જુઓ.
- [2] BNSS હેઠળ “શોધ” નો અર્થ જાણવા માટે કલમ 49; 97 જુઓ.
- [3] BNSS ની કલમ 44.
- [4] BNSS ની કલમ 185(1).
- [5] BNSS હેઠળ “જપ્તી” વિશે સમજવા માટે કલમ 106, 117 જુઓ.
- [6] પરંતુ આ કાયદાઓની સંપૂર્ણ યાદી નથી. અન્ય ઘણા કાયદાઓ પણ છે જે શોધ અને જપ્તી માટે જોગવાઈ કરે છે.
- [7] ફોજદારી કાર્યવાહી સંહિતા, 1973 (CrPC).
- [8] ભારતીય પુરાવા અધિનિયમ, 1872.
- [9] ભારતીય દંડ સંહિતા, 1860.
- [10] ટેલિકોમ્યુનિકેશન્સ અધિનિયમ, 2023 ની કલમ 42 અને 43 જુઓ.
- [11] કૃપા કરી નોંધ લો કે આવી રેકોર્ડિંગ માત્ર પ્રથમ વર્ગના ન્યાયિક મેજિસ્ટ્રેટ, જિલ્લા મેજિસ્ટ્રેટ અને ઉપ-વિભાગીય મેજિસ્ટ્રેટને આપવામાં આવી શકે છે
- [12] BNSS, 2023 ની કલમ 94, 185.
- [13] K.S. પુત્તુસ્વામી વિ. ભારત સંઘ (2017) 10 SCC 1.
- [14] વિરેનદર ખન્ના વિ. કર્ણાટક રાજ્ય, રિટ પિટીશન નં. 11759 ઓફ 2020 (GM-RES).
- [15] ફાઉન્ડેશન ઓફ મીડિયા પ્રોફેશનલ્સ વિ. યુનિયન ઓફ ઈન્ડિયા, રિટ પિટીશન (ક્રિમિનલ) નં. 395 ઓફ 2022, ભારતનું સર્વોચ્ચ અદાલત, પૃષ્ઠ 1.
- [16] અવસ્ટિકા દાસ, Committee Constituted To Frame Guidelines For Seizure Of Digital Devices: Centre Tells Supreme Court, (6 ડિસેમ્બર 2023, 12:05 PM)
<https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831>
- [17] પ્રમાણપત્ર BSA, 2023 ની કલમ 63(4)(c) હેઠળ આપવામાં આવ્યું છે.

સંદર્ભો:

[18] જપ્તી મેમોનું એક નમૂનું અનુસૂચિમાં આકૃતિ 3 અને 3.1 તરીકે આપેલું છે. તેનું સ્ત્રોત:

<https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf>

[19] આવી એક ઈન્વેન્ટરી યાદી (જેને આકૃતિ 4 માં જપ્તી યાદી તરીકે ઓળખી શકાય)નું નમૂનું નીચેની અનુસૂચિમાં આપવામાં આવ્યું છે.

[20] ગ્રિફ્ટારી વોરંટનું એક નમૂનું અનુસૂચિમાં આકૃતિ 5 તરીકે આપેલું છે.

[21] BNSS, કલમ 503(2).

[22] BNSS, કલમ 2(c) જુઓ.

[23] BNSS કલમ 2(f) જુઓ. "ચાર્જ" કલમ 2(b) હેઠળ વ્યાખ્યાયિત છે; વધુ સમજૂતી માટે કલમ 234 પણ જુઓ.

[24] BNSS, કલમ 2(g) જુઓ. સત્તાવાર રાજપત્રમાં પ્રકાશિત અધિનિયમના પૃષ્ઠ 158 પર પ્રથમ અનુસૂચિના સ્પષ્ટીકરણ નોંધોના બિંદુ (2) નો પણ સંદર્ભ લો.

[25] BNS ની કલમ 2(21).

[26] BNSS કલમ 2(o) જુઓ. સત્તાવાર રાજપત્રમાં પ્રકાશિત અધિનિયમના પૃષ્ઠ 158 પર પ્રથમ અનુસૂચિના સ્પષ્ટીકરણ નોંધોના બિંદુ (2) નો પણ સંદર્ભ લો.

[27] BNSS, કલમ 2(s).

[28] આઈ.ટી. અધિનિયમ, કલમ 80(1) ની વ્યાખ્યા.

[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

