केवल जागरूकता के लिए

JUDICIAL ACADEMY
LEARNING
ENDURING JUSTICE

झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सब के लिए
JHARKHAND STATE LEGAL SERVICES AUTHORITY
ACCESS TO JUSTICE FOR ALL

साइबर अपराध

के अनुसंधान में बरती जाने वाली सावधानियाँ

साइबर अपराध के अनुसंधान में बरती जाने वाली सावधानियाँ

विवरणी 1

'संक्षिप्त विवरण'

'सुचना प्रौद्योगिकी' और 'इन्टरनेट' ने जन्म दिया है नए आयाम को जैसे रोजगार, विकास, आर्थिक वृद्धि, संपन्नता, संवाद का सरलीकरण आदि। इन नए आयामों के साथ 'अपराध' की प्रकृति में बदलाव का उद्‌भव हुआ। 'अपराधकर्ता' तकनीकी तौर पर प्रबुद्ध हुए, और अपनी तकनीक दक्षता से आम नागरिक तथा सरकारी और गैर सरकारी व्यवसायिक संस्थाओं को नुकसान पहुँचाना शुरू किया। विशेषज्ञों ने कम्प्यूटर जनित अपराधों कों 'साइबर अपराध' का नाम दिया है। 'साइबर अपराध' की व्यापकता का अंदाजा/आकलन इस बात से लगाया जा सकता है कि यदि दैनिक समाचार पत्रों पर एक सरसरी निगाह डालें तों साइबर अपराधियों के कुकृत्यों की दास्तां बयां करता दिखेगा, जिसके प्रभाव से आम नागरिक का जीवन 'त्रस्त' एवं आतंकित है। 'साइबर अपराध' को यदि 'परिभाषित' करने का प्रयास किया जाए तो हम यह कह सकते कि, ऐसी कोई आपराधिक गतिविधि, जहाँ 'कंप्यूटर' का प्रयोग 'अपराध' की निरन्तरता सुनिश्ति करने के लिए साधन अथवा साध्य के रूप में किया जाए उस गतिविधि को साइबर अपराध के दायरे में लाया जाता है।

भारत में 'साइबर अपराध' की संख्या में वृद्धि हुई है, और अपराधियों कि गिरफ्तारी भी हुई है।

❖ **सरकार एवं विधि प्रवर्तन द्वारा किए गए 'पहल'।**

'साइबर अपराध' मे घोर वृद्धि और उनके दुष्परिणाम की रोकथाम करने के लिए भारत सरकार ने पहल करते हुए, वर्तमान सूचना प्रौद्यौगिकी अधिनियम-2000 में व्यापक संशोधन करते हुए सूचना प्रौद्यौगिकी (संशोधित) अधिनियम-2008 पारित किया, संशोधित अधिनियम मे जहाँ electronic, दस्तावेज, digital हस्ताक्षर, और कम्प्यूटर और इन्टरनेट के माध्यम से किए गए लेन-देन को विधिक पहचान मिली वहीं 'साइबर अपराधों' को परिभाषित कर दोषियों के लिए पर्याप्त सजा के प्रावधान निहित किए गये। तमाम विधि प्रवर्तन मे शामिल संस्थाऐं जैसे C.B.I केन्द्रिय अन्वेषण ब्यूरो, राज्य पुलिस बल, ने 'साइबर अपराधों' के समुचित संचालन के लिए एक विशिष्ट 'साइबर इकाई' (Cyber Cell) का गठन किया है, यह 'इकाई' तकनीकी रूप से दक्ष एवं सक्षम होती है 'साइबर अपराधों' का सामना करने में।

❖ **साइबर अपराध के प्रकार**

'साइबर अपराध' स्वयं मे समाविष्ट करता है, उन तमाम अवैध गातिविधियों को जिसका क्रियान्वयन का मुख्य केन्द्र 'कम्प्यूटर' होता है, सूचना प्रौद्योगिकी (संशोधित) अधिनियम-2008 के धारा (66) 'साइबर अपराधों' का उल्लेख करते हुए उसमें 'सजा' का जिक्र है, यदि कोई गतिविधि सू०प्रा०अ० 2008 के अनुच्छेद (43) के विरूद्ध हो जहाँ कार्य कपटपूर्ण आश्य कि पूर्ति के लिए किया जाता है। धारा (66) सू०प्रा०अ० 2008 के अर्न्तगत उल्लेखित 'साइबर अपराध' में यह अवधारण (Notion) या पूर्वानुमान (Pre-supposition) निहित होता है कि ; समस्त 'कार्य' कपट पूर्ण और ठगी करने के दुराष्य से किए जाते है। अगर कपटपूर्ण या ठगी का आश्य न हो तो धारा 43 सु०प्रा०अ० 2008 आकृष्ट होता तदुपरान्त अनुच्छेद 46 में वर्णित निर्णायक पदाधिकारी (Adjudicating officer) विवाद का निबटारा करेगा।

वित्तिय जालसाजी (Financial fraud)

(भ०द०वि० के प्रावधान, सु०प्रा०सं०अ० धारा 66 अन्य प्रयुक्त विधि)

❖ वित्तीय जालसाजी - इन अपराधों के अर्न्तगत व्यवसायिक जालसाजी, निवेश जालसाजी, विदेशों में नौकरी देने के लालच, जैसे अपराध शामिल है, इन अपराधों में पीड़ित को प्रलोभन दे कर झाँसा दिया जाता है, झुठे वादे किए जाते है, तदोपरान्त उनसें पैसे की धोखाधड़ी की जाती है।

आँकड़ों मे विचलन (Data Modification)

(सु०प्रा०सं०अ० धारा 2008 के अर्न्तगत धारा-66, भा०द०वि० 1860 धारा 403,406,408,409)

- इस अपराध में अभियुक्त के सुरक्षित Computer System में प्रवेश कर, मौजुदा आंकड़ों/जानकारियों को परिवर्तित अथवा विचलित कर, व्यक्ति अथवा संस्था को नुकसान पहुँचाते है।

पहचान की चोरी और उसके दुरूपयोग (Identity theft)

(सु०प्रा०सं०अ० धारा 2008 के अर्न्तगत धारा 66C 66D प्रयुक्त होंगे।)

- यह नितांत निजी जानकारियों की जैसे जन्मदिन, नाम, PAN नम्बर, पासपोर्ट नम्बर, केडिट कार्ड नम्बर, ATM Pin no, ई.मेल Account details की चोरी, धोखाधड़ी के उद्देश्य से किया जाता है। अभियुक्त पीड़ित के इस अति संवेदनशील जानकारियों को विभिन्न तरीकों से प्राप्त करते है जैसे फिसिंग, पीड़ित के ईमेल पते पर संपदा भेजकर, जहाँ पीड़ित से उनकी गोपनीय सूचनाओं की माँग की जाती है।

साइबर स्टॉकिंग (Cyber Stalking)

(सु०प्रा०सं०अ० धारा 2008 के अन्तर्गत 66, भा०द०वि० 1860 के अन्तर्गत धारा 500, 506, 507, 508, 509 प्रयुक्त होंगे।)

- इस साइबर अपराध में सूचना और तकनीक का इस्तेमाल कर पीड़ित को धमकाया या डराया जाता है। पीड़ित को उनके मोबाइल पर तथा कम्प्यूटर के धमकी भरे मेल भेजकर तथा मोबाईल पर मैसेज अथवा कॉल करके, पीड़ित के Social Network Account पर आपत्तिजनक धमकी भरे मैसेज भेज कर पीड़ित को परेशान किया जाता है। स्टॉकिंग मे व्यक्ति को बार-बार उत्पीड़न का शिकार बना कर उसे मानसिक और शारीरिक रूप से हानि पहुँचाया जाता है। अपराधी पीड़ित को निजी हानि पहुँचाकर, पीड़ित का मानसिक दोहन कर अनुचित लाभ उठाने का उद्देश्य रखते है।

आँकड़ों की चोरी (Data theft)

(सु०प्रा०सं०अ० धारा 2008 के अन्तर्गत धारा 66, भा०द०वि० के अर्न्तगत धारा 379)

इस अपराध में बिना मालिक के अनुमति से किसी कम्प्यूर से संवेदनशील आंकड़ो तथा जानकारी की प्रतिलिपी तैयार करना उपरोक्त अपराध के दायरे में आता है। इन आंकड़ो में शामिल है, पीड़ित की निजी जानकारी जैसे नाम जन्मदिन, पता, संपर्क विवरणी, यूजर नाम पासवर्ड credit card/debit card number.

अश्लीलता (Pornography)

(सु०प्रा०सं०अ० धारा 2009 के अन्तर्गत धारा 67E, 67 and 67B, भा०दा०वि० 1860 के अन्तर्गत धारा 292)

ईमेल, website, chatting site, social network site के जरिए अश्लील संदेश विडीयो, फोटो आदि का प्रकाशन अश्लीलता अपराध की परिधि में आता है।

बौद्धिक संपदा एवं व्यापार के रहस्यों की चोरी

Theft of intellectual property and trade secret

(सु०प्रा०सं०अ० धारा 2008 के अर्न्तगत धारा 66, बौद्धिक संपदा अधिकार अधिनियम 1957, अन्य प्रयुक्त अधिनियम)

यह अपराध ज्ञान आधारित संपदा, व्यापार प्रारूप, विचार, नवीन्ता तथा प्रतिलिप्याधिकार (copy right) द्वारा सुरक्षित किसी व्यक्ति अथवा संस्था की अर्मूत संपदा की चोरी सम्मलित है।

बौद्धिक संपदा की software के माध्यम से चोरी की अपराध की संख्या बहुत ज्यादा है।

जासूसी (Esponiage)

(सु०प्रा०सं०अ० धारा 2008 के अन्तर्गत धारा 66, 70 एवं अन्य प्रयुक्त अधिनियम)

पड़ोसी तथा दुश्मन राष्ट्र के गुप्तचर अधिकारियों द्वारा किसी अन्य राष्ट्र के सरकारी संस्था के कम्प्यूटर सिस्टम के माध्यम से जासूसी गतिविधियों को अंजाम देते है, इस अपराध के अर्न्तगत संवेदनशील सरकारी दस्तावेज तक पहुँच बनाना है।

हैकिंग (Hacking)

(सु०प्रा०सं०अ० 2008 के अन्तर्गत धारा 66)

हैकिंग वह अपराध है जिसमें कम्प्यूटर के मालिक की अनुमति के बिना कंप्यूटर का किसी भी प्रकार से अवैध उपयोग किया जाता है। हैंकिग एक ऐसा अपराध है जिसमें कंप्यूटर प्रणाली में अवैध घुसपैठ करके उसको नुकसान पहुंचाया जाता है।

सलामी हमला (Salami Attack)

(सु०प्रा०सं०अ० 2008 के अन्तर्गत धारा 66)

यह एक वित्तीय अपराध है। ठगी इतनी छोटी होती है कि पकड़ पाना बहुत मुश्किल होता है, उदाहरण के लिए अगर कोई बैंक कर्मचारी इस प्रकार की धोखाधड़ी करें और वह हर खाताधारक के बैंक खाते से हर माह 5 रूपया काटे, तो कोई भी इतनी थोड़ी धनराशि के कटने को पकड़ नहीं पाएगा, पर अपराधी के पास महीने के अंत में काफी धन राशि इकठ्ठा हो जाएगी।

वायरस हमला (virus attack)

(सु०प्रा०सं०अ० 2008 के अन्तर्गत धारा 66 एवं 66F)

वायरस ऐसे प्रोग्राम को कहा जाता है जो कंप्यूटर के अन्य प्रोग्राम को संक्रमित करने की क्षमता रखते हैं अथवा अपनी प्रतियां बना कर दूसरे प्रोग्राम में फैल जाते हैं। यह दुर्भावनापूर्ण सॉफ्टवेयर होते हैं जो अपने आप को किसी दूसरे सॉफ्टवेयर से जोड़ लेते हैं अथवा कंप्यूटर को हानि पहुंचाते हैं।

साइबर आतंकवाद (cyber terrorism)

(सु०प्रा०सं०अ० 2008 के अन्तर्गत धारा 66 एवं 66F)

परमपरागत आतंकवाद के समनान्तर साइबर आतंवाद में तकनीक का प्रयोग बहुत होता है जैसे सैटेलाईट फोन सोशल नेटवर्क साईट ईमेल के जरिये आतंकवादी अपने विचार धारा का प्रचार प्रसार करते है और फंड रेजिन्ग का काम भी इन सोशल नेटवर्क साईट से करते है। साईबर आतंकवाद का एक और पहलू है कि वे सरकारी संस्थाओं के कंप्यूटर प्रणाली में बढ़े पैमाने पर घुसपैठ कर पुरी प्रणाली को ध्वस्त कर देते है।

स्पूफिंग (spoofing)

(सु०प्रा०सं०अ० धारा 2008 के अन्तर्गत धारा 66, 66D)

यह एक ऐसा अपराध है जिसमें पीडित को ईमेल भेजा जाता है, जो कि यह दावा करता है कि वह एक स्थापित उद्यम द्वारा भेजा गया है ताकि पीड़ित से गोपनीय निजी जानकारी निकलवा सके अथवा पीड़ित के खिलाफ, उसको आर्थिक नुकसान पहुंचाने के लिए इस्तेमाल की जा सके।

स्कीमिंग (skimming)

(सु०प्रा०सं०अ० 2008 के अन्तर्गत धारा 66C)

यह उपकरण के माध्यम से एटीएम धोखाधड़ी को अनजाम दिया जाता है, जिससे पीड़ित के संवेदनशील निजी जानकारियों को लिया जाता है।

पीड़ित के खिलाफ, उसको आर्थिक नुकसान पहुंचाने के लिए इस्तेमाल किया जाता है तथा फर्जी credit/debit card बनाये जाते है।

फारमिंग (Pharming)

(सु०प्रा०सं०अ० 2008 अन्तर्गत धारा 66D एवं 66D)

फारमिंग वह साईबर आक्रमण है जहाँ पीड़ित को धोखे में रखकर गोपनीय निजी जानकारी फर्जी वेबसाईट जो असली प्रतीत होता है उससे आसानी से लिया जाता है तत्पश्चात पीड़ित को आर्थिक नुकसान पहुंचाया जाता है।

❖ उक्त वर्णित अपराध दोनों विधियों में दर्ज होगा तथा trial भी चलाया जाएगा ।

विवरणी–2

❖ **'अनुसंधान' की मानक चलन प्रक्रिया (Standard Operating Procedure) साइबर जनित अपराधों के संदर्भ में :**

SOP की महत्ता 'अनुसंधान' के दौरान यह है कि, SOP हमारा मार्गदर्शन करता है crime scene को सुरक्षित करने और साक्ष्यों की पहचान तथा उन्हें एकत्रित करने में, साक्ष्य को न्यायालय में प्रस्तुत करने में।

Electronic/Digital साक्ष्यों की प्रकृति तथा उनकी वैधानिकता से यह स्पष्ट है कि, एक निष्पक्ष परिस्थिति में अनुसंधान की अनिवार्यता है 'अनुसंधान की मानक चलन प्रक्रिया का अक्षरसह अनुपालन निम्नलिखित कारणों से :

- साक्ष्यों का संग्रहण एक वैधानिक प्रक्रिया के अंतर्गत किया जाना चाहिए, जिसके फलस्वरूप 'साक्ष्य' न्यायालय में स्वीकार्य हो।
- Electronic/Digital साक्ष्यों को अत्यन्त सावधानी पूर्वक संग्रह किया जाना चाहिए, अन्यथा उनके विकृत या लोप होने का खतरा बना रहता है। अतः अनुसंधानकर्ता से तकनीकि ज्ञान अपेक्षित है, वस्तुतः उन्हें ही न्यायालय के संग्रहित Electronic/Digital साक्ष्यों के कारण एवं प्रभाव को स्पष्ट करना है।
- 'मानक चलन प्रक्रिया' के अभाव में सवर्था अनुचित साक्ष्यों का संग्रहण होता है जिसके फलस्वरूप साक्ष्यों की श्रृंखला को खण्डित करते है।

साइबर क्राइम से संबंधित प्राथमिकी दर्ज करने में थाना का क्षेत्राधिकार

1. पीड़ित के जिस खाते से पैसों की अवैध निकासी होती है उस संबंधित थाने को दंड प्रक्रिया संहिता की धारा 156(1) सपठित धारा 177 के प्रावधानों के अंतर्गत प्राथमिकी दर्ज कर अनुसंधान करने का क्षेत्राधिकार होगा।

2. आर्थिक अपराधों के वैसे मामलों में जहाँ यह निश्चित न हो कि अपराध किस क्षेत्र में कारित किया गया है अथवा अपराध एक से अधिक क्षेत्रों के अंतर्गत कारित हुआ है अथवा लगातार प्रवृत्ति का है (कंटीन्यूअस ऑफेंस) वैसी स्थिति में धारा 178 सपठित धारा 156(1) दंड प्रक्रिया संहिता के प्रावधानों के अंतर्गत कांड किसी भी संबंधित थाने में दर्ज किया जा सकता है तथा उसका अनुसंधान किया जा सकता है।

   उदाहरण - किसी व्यक्ति के खाते से जो राँची में अवस्थित है, में से जामताड़ा में बैठे अपराधी द्वारा पैसे की निकासी की जाती है तथा उसे एक से अधिक खातों में स्थानांतरित कर दिया जाता है तो वैसी स्थिति में किसी भी थाने का जहाँ-जहाँ पैसे का अंतरण हुआ है क्षेत्राधिकार होगा।

3. वैसे मामलों में जहाँ अपराध किसी अन्य थाने के क्षेत्राधिकार से कारित किया गया है तथा उसका प्रभाव किसी अन्य थाने के क्षेत्राधिकार में हो दंड प्रक्रिया संहिता की धारा 189 सपठित धारा 156(1) के प्रावधानों के अंतर्गत दोनों में से किसी भी थाने का क्षेत्राधिकार होगा।

   उदाहरण - सोशल मीडिया से संबंधित अपराधों में यदि आपत्तिजनक पोस्ट एक थाने के क्षेत्राधिकार में बनाया गया है, तथा उसे इंटरनेट के माध्यम से सोशल मीडिया में अपलोड किया जाता है, तथा उसे अन्य थानों के क्षेत्राधिकार में देखा जाता है तो किसी भी थाने का क्षेत्राधिकार होगा।

4. ऐसे मामलों में जो किसी आपराधिक षडयंत्र का परिणाम होता है, वहाँ जहाँ अपराध कारित हुआ अथवा जहाँ आपराधिक षड्यंत्र किया गया दोनों जगहों पर धारा 180 सपठित धरा 156(1) दंड प्रक्रिया संहिता के प्रावधानों के अंतर्गत कांड दर्ज कर अनुसंधान किया जा सकता है।

   उदाहरण - ऐसे मामलों में जहाँ बैंक से धन की अवैध निकासी साइबर अपराध द्वारा एक से अधिक पीड़ितों के खाते से की गई हो, तथा वह राशि यदि किसी अन्य थाना क्षेत्र के बैंक के किस खाते में जमा की गई हो, और उस लाभुक खाताधारी कि यदि धारा **120 बी** आईपीसी के अंर्तगत संलिप्तता पाई जाती है तो इस संबंध में अपराध, लाभुक खाताधारी के क्षेत्राधिकार अथवा पीड़ित के क्षेत्राधिकार दोनों जगहों में से किसी एक जगह के थाने में कांड दर्ज कर अनुसंधान एवं विचारण किया जाता सकता है।

5. ऐसे मामलों में जहाँ आर्थिक अपराध अथवा सोशल मीडिया अपराध को दूरसंचार के माध्यम से जैसे इंटरनेट, मोबाइल आदि के द्वारा कारित किया जाता है, वैसी स्थिति में जहाँ से संवाद भेजा गया, अथवा जहाँ प्राप्त किया गया वहाँ के संबंधित थाना का क्षेत्राधिकार धारा **182** सपठित धारा **156(1)** दंड प्रक्रिया संहिता के अंतर्गत होगा।

उदाहरण - यदि किसी खाता धारी का ओटीपी किसी अन्य थाने के क्षेत्राधिकार में बैठे अपराधी मोबाइल अथवा दूरसंचार एवं इंटरनेट के माध्यम से प्राप्त कर लेते हैं तो दोनों थानों का क्षेत्राधिकार होगा।

साइबर अपराध से संबंधित मामलों के दर्ज होने के उपरांत अनुसंधानकर्ता द्वारा उठाए जाने वाले आवश्यक कदम

1. पीड़ित के संबंधित खाता से निकासी को रोकने के लिए बैंक को अविलंब सूचित करना :
   (1) फोन द्वारा,
   (2) इंटरनेट द्वारा, अथवा
   (3) व्यक्तिगत रूप से निकटतम शाखा में जाकर।
2. बैंक फ्रॉड मामलों में मूलतः जिन खातों से अवैध निकासी की गई है तथा जिन खातों में धन का अंतरण हुआ है उनके खाता विवरणी प्राप्त करना।
3. इसी प्रकार जिस मोबाइल अथवा आईपी ऐड्रेस का प्रयोग कर अपराध कारित किया गया है उसकी विवरणी यथा सीडीआर (CDR), सीएएफ (CAF) इत्यादि इंटरनेट सर्विस प्रोवाइडर से प्राप्त करना।
4. इस संबंध में I.O. द्वारा निम्नलिखित कार्रवाई करना अपेक्षित है -
   (a) संबंधित बैंक के शाखा से प्रबंधक से खाता कि अभिप्रमाणित प्रति धारा 4 बैंकर्स बुक एविडेंस एक्ट के तहत प्राप्त करना।
   (b) नहीं दिए जाने की स्थिति में संबंधित सक्षम न्यायालय के माध्यम से धारा 91 दंड प्रक्रिया संहिता के अंतर्गत उक्त विवरण की मांग की जाए।
   (c) ऐसी विशेष परिस्थिति में जब नियत समय में संबंधित उक्त विवरणी यदि अनुसंधानकर्ता को उपलब्ध नहीं कराई जाती तो संबंधित न्यायालय उक्त मामलों में अलग कांड दर्ज कर एवं संज्ञान लेकर शाखा प्रबंधक के विरूद्ध विधि सम्मत कार्रवाई धारा 175 आई0पी0सी0 के अंतर्गत कर सकती है।

   अथवा

   अनुसंधानकर्ता के द्वारा वैसे मामलों में अलग से संज्ञान लेने हेतु शिकायत वाद धारा 195(1) (a) दंड प्रक्रिया संहिता के प्रावधानों के अंतर्गत दाखिल कर भादवि की धारा 175 में संज्ञान लेने की प्रार्थना भी की जा सकती है।
   (d) यदि अनुसंधान के क्रम में खाता विवरण बिना सत्यापन के प्राप्त होती है, तो विहित सत्यापन प्रमाणपत्र विचारण के दौरान भी बैंकर्स बुक एविडेंस एक्ट की धारा 4 के प्रावधानों के अंतर्गत प्राप्त कर न्यायालय के समक्ष प्रस्तुत किया जा सकता है।
   (e) खाता विवरणी को किस पदाधिकारी से सत्यापित कर प्राप्त करें ?

   हर बैंक के शाखा प्रबंधक अथवा मुख्य लेखापाल खाता विवरणी की सत्यापित प्रति निर्गत करने हेतु बैंकर्स बुक एविडेंस एक्ट की धारा 2(8) के प्रावधानों के अनुसार सक्षम पदाधिकारी है।
   (f) धारा 4 बैंकर्स बुक एविडेंस एक्ट के प्रावधानों के आलोक में लेखा कि अभिप्रमाणित प्रति न्यायालय में साक्ष्य के रूप में ग्राह्य होगी और निर्गत करने वाले बैंक पदाधिकारी को न्यायालय में साक्षी के रूप में प्रस्तुत करने की आवश्यकता नहीं होगी। उक्त प्रमाणपत्र को अनुसंधानकर्ता द्वारा न्यायालय में प्राप्तकर्ता के रूप में पहचान करने मात्र से वह ग्राह्य होगा। वैसी परिस्थिति में जहाँ खाता विवरणी कंप्यूटर प्रिंट आउट द्वारा प्राप्त की जाती है, वहाँ अलग से धारा 65 बी (4) भारतीय साक्ष्य अधिनियम के अंतर्गत प्रमाण पत्र लेना भी अनिवार्य होगा।

(g) धारा 65 बी (4) साक्ष्य अधिनियम के अंतर्गत सर्विस प्रोवाइडर से ही प्रमाण पत्र प्राप्त कर न्यायालय में दाखिल करें तथा उक्त प्रमाणपत्र प्राप्त करने हेतु धारा 91 दंड प्रक्रिया संहिता की ऊपर विहित पद्धति का पालन करें।

(h) धारा 65 बी (4) साक्ष्य अधिनियम के अंतर्गत प्रमाण पत्र निर्गत करने वाले नोडल पदाधिकारी को साक्षी के रूप में प्रस्तुत करने की आवश्यकता नहीं होगा। उक्त प्रमाण पत्र को अनुसंधानकर्ता द्वारा न्यायालय में प्राप्तकर्ता के रूप में पहचान करने मात्र से ही ग्राह्य होगा।

(i) धारा 65 बी (4) साक्ष्य अधिनियम के अंतर्गत प्रमाण पत्र जहाँ तक हो सके उक्त सी0डी0आर0 अथवा इलेक्ट्रॉनिक रिकार्ड के साथ ही प्रस्तुत किया जाएगा। परंतु विहित प्रमाण पत्र प्राप्त ना होने की स्थिति में विचारण के दौरान भी न्यायालय द्वारा ग्राह्य होगा।

(j) सीसीटीवी फुटेज प्राप्त करने हेतु भी उक्त प्रक्रिया का पालन किया जाएगा। साथ ही सीसीटीवी फुटेज से अभियुक्त के फोटो की पहचान कराने हेतु उसका स्टिल फोटो प्राप्त कर एवं अभियुक्त का जेल से प्रमाणित फोटो प्राप्त कर पहचान हेतु एक्सपर्ट के पास भेजा जा सकता है।

(k) धारा 65 बी (4) साक्ष्य अधिनियम के अंतर्गत विहित प्रमाणपत्र धारा 4 I.T. Act के प्रावधानों के अंतर्गत डिजिटल हस्ताक्षर अथवा हस्ताक्षर एवं सील मुहर लगाकर भी निर्गत किया जा सकता है।

(l) जहाँ पीड़ित का पैसा किसी ऐसे खाते के माध्यम से निकाला गया है जिसका KYC बैंक के नियमों के अनुसार सत्यापित नहीं है तो संबंधित खाता खोलने वाले बैंककर्मी को भी धारा 120 बी आईपीसी के तहत आरोपित किया जा सकता है और जहाँ पर बैंककर्मी की संलिप्तता उक्त अपराध में पाई जाती है तो वैसी स्थिति में उक्त बैंककर्मी पर भी कार्यवाही हो सकती है।

(m) वैसे व्यक्ति जो अपना बैंक खाता तथा एटीएम साइबर अपराधकर्मी की उपयोग हेतु देते हैं वे अन्य धाराओं के साथ भा0द0वि0 की धारा 413 के अंतर्गत आरोपित किये जा सकते हैं।

(n) ऐसे मामलों में जहाँ पीड़ित अथवा साक्षी किसी अन्य थाना क्षेत्र में रहते हैं उनके बयान को दर्ज करने में अवांक्षित विलंब हो सकता है वैसे मामलों में अनुसंधानकता धारा 161 के Proviso 1 Cr.P.C. के तहत Audio Video Electronic साधन की मदद से साक्षी का बयान अभिलिखित कर सकते हैं। साथ ही अनुसंधानकर्ता उक्त बयान की काण्ड दैनिकी में भी अंकित करेंगे तथा Audio एवं Video को भी काण्ड दैनिकी से साथ संलग्न करेंगे।

अपराध दृश्य अनुसंधान

साइबर जनित अपराध के दृश्य परामपरागत अपराधों से सर्वथा भिन्न होते है। Electronic/Digital साक्ष्य अत्यंत भंगुर (fragile) होते है। इसे आसानी से चुराया जा सकता तथा इसके साथ छेड़-छाड़ की प्रबल संभावना रहती है। अतः इन साक्ष्यों के संग्रहण, संचालन एवं संरक्षण परिक्षण में अत्यंत सावधानी बरतने की आवश्यकता पड़ती है।

अपराध परिदृश्य के क्रमवार चरण है-

- अपराध परिदृश्य की सम्यक पहचान तथा संरक्षण
- 'जो जैसा है वैसा ही'-अपराध परिदृश्य की लिखित प्रमाण
- साक्ष्यों के संग्रहण की प्रक्रिया

जब 'system' switch off हो

जब system on हो

- विधि चिकित्सा शास्त्रीय अनुलिपिकरण (Forensic Duplication)
- साक्षात्कारों का संचालन
- साक्ष्यों का वर्गीकरण
- साक्ष्यों का परिचालन और Packaging

पंचनामा (Seizure Memo) एवं जब्ती कार्यवाही

धारा 165 अपराधिक प्रक्रिया संहिता 1973 और धारा 30 सू.प्रौ. सं. अं-2008 अनुसंधान अधिकारी को अधिकृत करता है परिक्षण एवं जब्ती के लिए।

पंचनामा तथा जब्ती कार्यवाही साइवर जनित अपराधों उतने ही महत्वपूर्ण है जितना की किसी अन्य अपराध में, अनुसंधान अधिकारी को Electronic/Digital साक्ष्यों के प्रकृति के अनुरूप अतिरिक्त सावधानी बरतने की अनिवार्यता होती है। Digital उपकरणों की मूलभूत जानकारी तथा अनुसंधान पूर्व आकलन में सक्षमता की महती प्रासंगिकता होती है साक्ष्यों के उचित परिक्षण एवं जब्ती के संदर्भ में।

पंचनामा के लिए आवश्यक दिशा-निर्देश निम्न है :-

यह सुनिशिचित किया जाए परिक्षण दल में दो स्वतंत्र गवाह के साथ एक तकनीक का जानकार हो जो उपकरणों को सही से पहचान कर सके तथा वह अनुसंधान पदाधिकारी को उचित परामर्श दे सकें।

'समय' Time zone/ System Time Plan की अत्यंत ही महत्वपूर्ण भूमिका है संपूर्ण अनुसंधान प्रक्रिया में। पंचनामा में इस बात की सुनिश्चता की जाए सही समय अंकित किया जाए। जब System switch on स्थिति में हो।

System यदि Switch off हो तो उसे Switch on न किया जाए।

यह सुनिशिचित किया जाए क्रम संख्या जो जिस उपकरण पर निर्धारित किया गया हो वही पंचनामा में भी दर्ज हो, जिससे अभिरक्षण की श्रृंखला खंडित न हो।

प्रत्येक उपकरण के छाया-चित्र लिए जाऐं अनुसंधान के आरंभ में ही, उनके मूल स्थान पर ही, यदि Hard disk को उपकरण से अलग किया जा रहा हो तो उसकी छाया चित्र अवश्य लिया जाना चाहिए।

- **अभिरक्षण की श्रृंखला (chain of custody)**

  अभिरक्षण की श्रृंखला इस बात का लिखित प्रमाण प्रस्तुत करती है कि साक्ष्य की सुपुर्दगी के संबंध में कि इसे कब और किसे सौंपा गया। ये वे लोग होते है जिन्होंने उपकरण को जब्त किया, और जिन्होंने अपराध परिदृश्य से साक्ष्यों का हस्तांनान्तर विधि चिकित्साशास्त्र लैब को किया, और वे लोग जिन्होंने इन साक्ष्यों का विश्लेषण किया। जैसा कि Electronic Evidence की प्रकृति ऐसी है कि इसे असानी से छेड़ा जा सकता है, या इसे क्षति पहुँचाई जा सकती है। अतः यह अत्यंत आवश्यक है- इन साक्ष्यों को वस्तुतः कौन, कब, क्यों कहाँ, कैसे किस व्यक्ति द्वारा हस्तांतरित किया गया हो इसकी विस्तृत जानकारी।

  साक्ष्यों की समग्रता यथावत करने लिए यह आवश्यक है कि अभिरक्षण की श्रृंखला नियंत्रित किया जाए।

  साक्ष्यों में समानता का अभाव और लिखित प्रमाणों की कमी 'अभिरक्षण की श्रृंखला' खण्डित ही नहीं वरण् अनुसंधान की सुचारू प्रक्रिया मे अवरोध उत्पन्न करेंगे। तदोपरान्त मुकदमे के विचारण के दौरान 'अनुसंधान अधिकारी' को धारा 72 सु० प्रा० सं० अ० 2008 के अर्न्तगत अपराधिक दायित्व का दोष अधिरोपित किया जाएगा।

'अभिरक्षण की श्रृंखला' के मुख्य बिन्दु'

- वास्तविक निरिक्षण भंडारण माध्यम Storage medium का- छाया चित्र लिया गया हो और अभिलेखों का व्यवस्थित अवलोकन
- 'चोरी' और अन्य अपदाओं से साक्ष्यों की समुचित अभिरक्षा
- Digital/ Electronic साक्ष्यों की अभिरक्षा बाहय विद्युत और चुम्बकीय क्षेत्र से। Digital साक्ष्यों विशेषतः 'कॉम्पाक्ट डिस्क' को खरोचों से सुरक्षित रखना
- उपकरणों के रख रखाव में शामिल लोगों की संख्या कम से कम हो।
- साक्ष्यों की पहचान सकारात्मक हो, स्पष्ट तथा स्थायी स्याही से लिखित हो

'सांख्यिक साक्ष्य संग्रहण प्रविष्टी' 'Digital Evidence Collection Form' DEC

'सांख्यिक साक्ष्य संग्रहण प्रविष्टी' एक अति महत्वपूर्ण कड़ी है विधि चिकित्सीय शास्त्र प्रक्रिया (forensic) कि, यह आवश्यक है कि साक्ष्य संग्रहण प्रक्रिया पूर्णतः सटिक हो तथा किसी भी परिस्थिति उदाहरण स्वरूप 'पुनरावृत्ति'

में भी परिणाम सटिक और समरूप आयें। अतः लिखित प्रमाण साक्ष्यों के संग्रहण के संबंध एक आवश्यक पहलु है जिसके द्वारा हमें यह जानकारी प्राप्त होती है कि कौन सा Digital Evidence सांख्यिक साक्ष्य या उपकरण के संग्रहण में वैज्ञानिक प्रक्रिया का पालन हुआ है अथवा नहीं।

इस प्रक्रिया के लिखित दस्तावेज/ प्रमाण को 'सांख्यिक साक्ष्य संग्रहण प्रविष्टि' का नाम दिया गया है।

'DEC' प्रविष्टि के अन्तर्गत निम्न विवरण अंकित होते है :-

- अपराध संख्या/जाँच संख्या
- विधि की 'धारा' जो काण्ड पर प्रयुक्त हो
- तिथि - जब सांख्यिक साक्ष्य या उपकरण जब्त किया गया हो या उसे विश्लेषण के लिए forensic lab भेजा गया हो।
- नाम - अनुसंधान पदाधिकारी का
- पता - स्थान जहाँ से सदस्यों का संग्रहण किया गया है।
- उपकरण संबंधी जानकारी
  - किस प्रकार के उपकरण का संग्रहण किया गया 'साक्ष्यों को एकत्रित' करने के लिए जैसे- Hard Disk, Laptop, etc.
  - निर्माता - उपकरण के निर्माता का लिखित ब्योरा
  - मॉडल न० उपकरण का
  - क्रम संख्या उपकरण की
  - परिग्रहण/ प्रतिरूप सांख्यिक साक्ष्यों का (acquisition/ imaging)

  अपराधिक परिदृश्य से किया गया हो 'समय' का उल्लेख आवश्यक है

  उपकरण की पहचान अथवा जब्त उपकरणों का आवश्यक रूप से विश्लेषण किया जाना चाहिए। यदि अनुसंधान अधिकारी तकनिकी विशेषज्ञ हो तो अपराध स्थल से उपकरण की पहचान कर स्थल से ही सांख्यिक साक्ष्यों का प्रतिरूप तैयार कर सकता है, अन्यथा वह सामान्य तौर पर उन उपकरणों को जब्त कर वैधानिक प्रक्रिया के द्वारा कर सकता है।

'साक्षात्कार' – संचालन

अनुसंधान में साक्ष्यों की महत्वपूर्ण भुमिका होती है, न्यायलय सदैव ही 'साक्ष्यों की समग्रता' पर ध्यान आकृष्ट करते है।

परन्तु परंपरागत भैतिक/वास्तविक या दस्तावेजी साक्ष्यों से इतर सांख्यिक साक्ष्यों की समग्रता सुनिश्चित करना वर्तमान परिस्थितियो में एक चुनौतीपूर्ण कार्य है। साक्ष्यों (सांख्यिक) की 'अभिरक्षण की श्रृंखला' एवं साक्ष्यों (सांख्यिक) की प्रमाणिकता स्थापित करना अभियोग पक्ष द्वारा न्यायलय में अत्यंत चुनौतिपूर्ण कार्य साबित हो रहा है। कतिपय स्थिति में यह पाया गया है कि सांख्यिक साक्ष्यों में अनजाने में समग्र जानकारी के आभाव में आमूल परिवर्तन पीड़ित द्वारा स्वयं ही कर दिया जाता है, जिसके फलस्वरूप अनुसंधान में अवांछित अवरोध उत्पन्न हो जाता है।

अतः 'साक्ष्यों के जब्ती' के दौरान/क्रम में निम्न प्रश्नों के उत्तर सुनिश्चित करने चाहिए पीड़ित और गवाहों से में अनुसंधान पदाधिकारी द्वारा-

- सर्वप्रथम घटना की जानकारी पीड़ीत /गवाह को कब हुई?
- यह कैसे स्थापित होता है कि जिस कार्य पर प्रश्न उठ रहे है, उसे करने वाला बाहरी है?
- किन क्षति का अनूमान है?
- मुख्य संदिग्ध व्यक्ति कौन हो सकता हैं?
- इस कार्य मुख्य प्रभाव व्यवसाय पर किस प्रकार पड़ेगा?

- कौन से मुख्य System है जिसके द्वारा व्यवसाय, का संचालन किया जाता है?
- संबन्धित उपकरण अथवा आँकड़ो की पहचान, एकत्रित, संरक्षण, और विश्लेषण के लिए क्या किया गया?
- क्या साक्ष्यों का संग्रहण किसी विशेषज्ञ द्वारा किया गया?

Packaging / वर्गीकरण/ परिचालन सदस्यों का :

यह अनुसंधान अधिकारी का दायित्व है कि वह सांख्यिक साक्ष्य तथा जब्त किए गऐ उपकरणों की packaging इस हद तक सुनिश्चित करें जिससे कि साक्ष्यों या आकड़ों को पुनः प्राप्त किया जा सकें।

विभिन्न साक्ष्यों के उनके प्रकृति के अनुरूप packaging कि व्यवस्था सुनिशिचित किया जाना चाहिए, अनुसंधान अधिकारी अपराध स्थल पर समस्त तैयारी से प्रस्थान करें उनके पास साक्ष्यों के packaging के लिए समुचित और पर्याप्त संख्या में साक्ष्य लिफाफे, बैग और पात्र उपलब्ध होने चाहिए। इसके अतिरिक्त प्रत्येक साक्ष्यों की packaging अलग से हुई हो, समुचित तौर पर वर्गीकृत, मुहर बंद, तथा औपचारिक दस्तावेज से परिपूर्ण हो। इन बातों का ध्यान रखने से साक्ष्यों की 'अभिरक्षण की श्रृंखला' न्यायालय में सरलता से स्थापित किया जाता है।

साक्ष्यों की रवानगी एवं परिचालन (dispatch और transportation) एक निर्णायक पहलु है जिसका ध्यान, अनुसंधान पदाधिकारी को विशेष रूप से रखना चाहिए। अनुचित या अव्यावसयिक ढ़ंग से साक्ष्यों की रवानगी एवं परिचालन संग्रहित साक्ष्यों को भौतिक क्षति कर सकते है, जिसके फलस्वरूप परिश्रम से 'संग्रहित साक्ष्य' व्यर्थ साबित हो जाऐंगे।

कुछ परिस्थितियों में यह देखा /पाया गया है कि संग्रहित साक्ष्यों को यदि अनुचित या अव्यवहारिक ढंग से संभाला जाए तो संग्रहित सांख्यिक साक्ष्यों कि विषय-वस्तु अपना वास्तविक रूप खो देती है, तथा उसमे परिवर्तन आ जाता है। साक्ष्यों का परिवर्तित स्वरूप न्यायलयों में बचाव पक्ष 'साक्ष्यों की समग्रता' पर प्रश्न, उठाने में सफल हो जाता है? तथा 'संग्रहित साक्ष्य' अपनी प्रमाणिकता खो देता है। अतः अनुसंधान अधिकारी यह सदैव सुनिशिचित करें कि, संदिग्ध कम्प्यूटर भंडारण माध्यम, forensic lab में व्यक्तिगत तौर पर संदेशवाहक के द्वारा भेजा जाए न कि रजिस्टर पोस्ट द्वारा। संदिग्ध hard-disk के साथ एक नई hard-disk समान क्षमता वाला forensic lab भेजा जाए साक्ष्यों के प्रतिरूप तैयार करने हेतु।

साक्ष्य जब्ती उपरान्त विधिक प्रक्रिया का अनुसरण

- अनुसंधान के दौरान क्रम में जब्त किए गए सांख्यिक साक्ष्य, तत्काल न्यायालय के अधिकार क्षेत्र में लाया जाता है, अनुसंधान अधिकारी द्वारा
- आदेश प्राप्त किए जाते है सक्षम न्यायलय के द्वारा कि जब्त वस्तु को अनुसंधान अधिकारी के अभिरक्षण में दिया जाय अनुसंधान के उद्देश्य हेतु।
- आदेश प्राप्त किए जाते है सक्षम न्यायलय के द्वारा कि संग्रहित सांख्यिक साक्ष्य को विश्लेषण के उद्देश्य हेतु Forensic Lab भेजा जा सके।
- कुछ परिस्थितियों में यदि 'आरोपी न्यायालय के समक्ष जब्त किए जाऐ वस्तु को मुक्त कराने हेतु पहल करता है, तो अनुसंधान अधिकारी विचारपूर्वक आपत्ति दर्ज न्यायलय के समक्ष कराऐ और यह सुनिश्चित करें कि कोई मूल/मौलिक साक्ष्य न वापस किए जाऐं जिसका प्रभाव अभियोजन पक्ष के काण्ड पर न पड़े।
- परिक्षक द्वारा विशेषज्ञ राय के संबंध में।

अनुसंधान अधिकारी जब संग्रहित सांख्यिक साक्ष्यों को Forensic विशलेषण के लिए अग्रेसित करता है, तब उसे निम्न दिशा-निर्देशों का पालन करना चाहिए।

- FSL को उनकी विशेषज्ञ राय के लिए अग्रेसित पत्र निम्न जानकारियाँ निहित हो:
- संक्षिप्त केस रिर्पोट
- जब्त किए गऐ प्रदर्श का ब्योरा तथा जब्ती का स्थान
- HardDisk का मॉडल, मेक और विवरण
- अपराध स्थान पर जाने कि तारीख और समय अपराध स्थल पर कम्प्यूटर की स्थिति
- छाया-चित्र अपराध स्थल का अगर हो तो

- कंप्यूटर का किसी System से जुड़ा होना अथवा किसी अन्य माध्यम से बाहय कंप्यूटर से जुड़ा होना
- सभी Electronic Evidence का विशेषज्ञ परिक्षण अनिवार्य है, [धारा 79A ITAA 2008]
- आरोप-पत्र तैयार करने के दिशा-निर्देश

  आरोप-पत्र तैयार करने में अपर्याप्त दक्षता या दक्षता का अभाव का कारण बनते है, आरोपी के बरी होने का साइबर अपराध करने के उपरान्त भी। न्यायालयों साइबर मुकदमों की असफलता का मुख्य कारण आरोप-पत्र में व्याप्त त्रुटि/दोष। ऐसे मुकदमों कि संख्या ज्यादा है जिसमें अनुसंधान अधिकारी ने अपेक्षित जानकारियों, दस्तावेजों के बैगर ही आरोप-पत्र कर दिया हो।

आरोप पत्र तैयार करने के दिशा–निर्देश निम्न हैः–

- शिकायतकर्ता द्वारा बताई गई सारी जानकारियाँ जो प्राथमिकी में उपलब्ध है, उसे आरोप-पत्र में सम्मिलित किया जाता
- इस बात कि सुनिश्चता तय कि जाए कि विधि की जिन धाराओं के अर्न्तगत आरोप तय किए जा रहे हों वह रद्द नहीं किए गए हो। (श्रेया सिंघल बनाम भारत सरकार AIR2015SC1523 इस बाद में माननीय सर्वोच्च न्यायलय ने सुचना प्रौद्यौगिक संशोधित अधिनियम की धारा 66A अवैध घोषित कर दिया)
- इस बात कि सुनिश्चित रहे की आरोप पत्र के साथ समस्त दस्तावेज संलग्न हो, जो जाँच और जब्ती प्रक्रिया के दौरान 'अभिरक्षण की श्रृंखला' (chain of custody) को न्यायालय में सफलता पूर्वक स्थापित करें सकें
- FSL रिर्पोट आरोप-पत्र के साथ संलग्न हो।
- अपराध -परिदृश्य कि विस्तृत जानकारी तथा अनुसंधान अधिकारी द्वारा अपनायी जानेवाली System के पहचान की पद्धति का विस्तृत ब्योरा आरोप-पत्र में निहित हो।
- तकनीक विशेषज्ञ जिन्होंने System की पहचान एवं प्रारंभिक विश्लेषण किया हो 'गवाह के तौर पर नाम आरोप-पत्र में उल्लेखित हो।
- अपराध को जाँच सापेक्ष न्यायलय में स्थापित करने के लिए यह आवश्यक है कि 'घटनाओं का उल्लेख काल अनुक्रम में किया जाए
- न्यायलय के समक्ष साक्ष्य

  अनुसंधान अधिकारी से अपेक्षित है कि वह साक्ष्यों के न्यायालय में Deposition में, निम्न क्रम का अनुसरण करें
  - प्राथमिकी दर्ज
  - जानकारियों का संग्रहण
  - अपराध स्थल का दौरा
  - साक्ष्यों की पहचान
  - साक्ष्यों का संग्रहण
  - साक्ष्यों का संरक्षण
  - साक्ष्यों का FSL मे परिचालन
  - साक्ष्यों के विश्लेषण का आग्रह
  - केस का पुर्नरचना/पुर्निमाण
  - आरोप-पत्र तैयार करना।

नोट : अनुसंधानकर्ता पीड़ित को I.T. Act की धारा 43A एवं आर०बी०आई० के पत्र संख्या RBI/2017-18/15 DBR No. Leg. BC. 78/09.07.005/2017-18 दिनांक 6/7/2017 के आलोक में यदि उपभोक्ता की गलती नहीं हो तो बैंक से अवैध निकासी की गई राशि बैंक वापस देगा, की जानकारी देंगे जिससे की वह क्षतिपूर्ति हेतु सक्षम पदाधिकारी (सचिव, सूचना एवं प्रौद्योगिकी विभाग, झारखण्ड सरकार) के समक्ष आवेदन दे सकें।

विवरणी–3

❖ झारखण्ड में मुख्यता निम्न साइबर अपराध अत्याधिक घटित होते है:

1. ATM से अवैध धन निकासी / ATM Clonning / Social Eng.
2. Social Network साइट पर अश्लील एवं अपत्तिजनक सामग्री को पोस्ट करना / बैंक पदाधिकारी बनकर ठगी करना / अनजान से दोस्ती कर ठगी करना / साइबर स्टॉकिंग
3. स्पूफिंग / स्किमिंग / स्पैकिंग / लैकिंग
4. VOIP कॉल के जरिये ठगी को अंजाम देना।
5. UPI के गुप्त कोड पूछकर या दूसरे नम्बर पर भिजवाकर ठगी करना।
6. OLX के जरिये लोगों को फंसाकर ठगी करना।

उपर्युक्त अपराधों के घटित होने पर अनुसंधान अधिकारी से निम्न दिशा-निर्देशों का अनुसरण अपेक्षित है-

1. प्राथमिकी दर्ज करने संबधी क्षेत्राधिकार पीड़ित घटना कि सुचना अपने निकटवर्ती थाने में तुरंत करें। माननीय सर्वोच्य न्यायलय के आदेश के आलोक में।
2. प्राथमिकी दर्ज होने के उपरान्त अनुसंधान अधिकारी धारा 91 अ०प्र०सं० 1973 संख्या के अंतर्गत बैंक अधिकारी से पीड़ित के खाते का ब्योरा तथा लाभुक के खाते का ब्योरा CAF, KYC की माँग कर सकता है बैंक अधिकारी से यह अपेक्षित है कि माँगी गई समस्त जानकारियों भारतीय साक्ष्य अधिनियम-1872 के अनुच्छेद 65 (B) के तहत दस्तावेजों को प्रामाण पत्र के साथ अनुसंधान अधिकारी बिना विलंब के 24 घंटे के अन्दर मुहैया कराऐं।

   यदि बैंक अधिकारी इन साक्ष्यों कों अकारण ही देने में विलंब अथवा मना करता है तो बैंक अधिकारी पर विधि सम्मत कार्यवाही किया जाऐगा।
3. अनुसंधान अधिकारी अनु० 102 आ०प्र०सं० 1973 के अर्न्तगत बैंक को आरोपी के बैंक खातों को freeze करने कि माँग करेगा, बैंक माननीय सर्वोच्च न्यायलय के आदेश [महाराष्ट्र सरकार बनाम तापस डी नियोगी (1999) 7SCC 685] के अनुपालन में उन खातों को तिमम्रम करने के लिए बाध्य है।
4. ATM क्लोनिंग के माध्यम से कि गई धोखाधड़ी में जिस ATM मशीन से पैसे की निकासी कि गई हो, उसकी CCTV footage, यदि वहाँ सुरक्षा प्रहरी (Guard). तैनात हो तो उसका बयान लिया जाना चाहिए। बैंक से प्राप्त CCTV footage धारा 65 (B) भारतीय साक्ष्य 1872 अधिनियम के अर्न्तगत बैंक द्वारा प्रमाणित किया गया हो। आरोपी की तस्वीर को तथा CCTV footage के आरोपी की मौजुदगी को SFL (राज्य अपराध चिकित्सा शास्त्र प्रयोगशाला) भेज कर आरोपी के पहचान की पुष्टि कि जानी चाहिए। ATM क्लोनिंग के माध्यम से कि गई धोखाधड़ी यदि बैंक कि ग्राहक सेवा केन्द्र से किया गया हो, वहाँ के संबंधित अधिकारी का बयान लिया जाना चाहिए बैंक से माँगी गई तमाम जानकारियों को भा० सा० अ० 65(B) तहत बैंक द्वारा प्रमाणित कर दिया जाएगा।
5. साइबर स्टॉकिंग और अश्लील समग्री का social network site पर पोस्ट करने पर भारतीय दण्ड विधा 1860 के अनु० 354 (D) 1(ii) के अर्न्तगत पीड़ित महिला अपराध संबंधित प्रथामिकी पीड़ित के द्वारा किसी भी थाने में दर्ज की जा सकती है। यदि थाना प्रभारी प्राथमिकी दर्ज से मनाही करता है, तो उस थाना प्रभारी पर विधि सम्मत कार्यवाही कि जाएगी। घटना की प्राथमिकी दर्ज करना थाना-प्रभारी के लिए बाध्यकारी है [ललिता कुमारी बनाम उत्तर प्रदेश सरकार (2014) 2 SCC 1]
6. प्राथमिकी दर्ज होने के उपरांत अनुसंधान कर्ता द्वारा विशेष न्यूनतम निर्देश वांछनीय है-
   - पीड़िता की आपत्तिजनक तस्वीर और दस्तावेज सेवा प्रदाता 65 (B) से भा० सा० अ० 65(B) तहत प्रमाणित किया गया हो तथा उसकी माँग अनुसंधान कर्ता द्वारा अनुच्छेद 91 अपराध प्रक्रिया संहिता 1872 के अर्न्तगत किया गया हो वैसी स्थिति में जहाँ सेवा प्रदाता का कार्यालय विदेश में स्थित हो तथा 65(B) प्रमाणित दस्तावेज साक्ष्य उपलब्ध न हो, तो secondary evidence के तौर पर पीड़िता द्वारा प्रस्तुत स्वाअभिप्रमाणित आपत्तिजनक दस्तावेज और तस्वीरे स्वीकार की जाएगी।

❑❑❑

न्यायिक अकादमी झारखण्ड
धुर्वा डैम के समीप, धुर्वा, राँची-834004,
फोन : 0651-2902833, 2902831,
फैक्स : 0651-2902834, 2902831
ईमेल : judicialacademyjharkhand@yahoo.co.in,
वेबसाइट : www.jajharkhand.in

झारखण्ड राज्य विधिक सेवा प्राधिकार
न्याय सदन, ए.जी. ऑफिस के समीप, डोरण्डा, रांची
फोन : 0651-2481520
फैक्स : 0651-2482397
ईमेल : jhalsaranchi@gmail.com
वेबसाइट : www.jhalsa.org