नेपालमा डिजिटल प्रमाणको नियन्त्रणको श्रृंखला (चेन अफ कस्टडी) र नियमनको वकालतका लागि नीतिगत पुस्तिका

ह्युमन राइट्स एण्ड जस्टिस सेन्टर २०२४

HUMAN RIGHTS
AND JUSTICE CENTRE

CYRILLA
Advancing Access to
Digital Rights Law

विषय

१. परिचय - - - १

  १.१ ऐतिहासिक परिप्रेक्ष्य - - - १

  १.२ नेपालमा प्रमाण सङ्कलन प्रक्रिया र अभ्यास - - - ३

  १.३ चेन अफ कस्टडी र डिजिटल प्रमाणको नियमनको महत्व - - - ४

२. डिजिटल प्रमाणहरूलाई संचालन गर्ने निर्देशिका: अन्तर्राष्ट्रिय परिप्रेक्ष्य - - - ५

  २.१ विद्युतीय उपकरणहरूको संचालन - - - ६

  २.२ विद्युतीय प्रमाणको पहिचान - - - ७

  २.३ विद्युतीय प्रमाण सङ्कलन - - - ७

  २.४ विद्युतीय प्रमाणको प्रतिलिपि - - - ८

  २.५ विद्युतीय प्रमाणको संरक्षण - - - ८

  २.६ विद्युतीय प्रमाणको विश्लेषण - - - ९

३.नेपालमा डिजिटल प्रमाणको स्वीकार्यता सम्बन्धी कानूनी रूपरेखा र न्यायिक निर्णयहरू - - - १०

  ३.१ प्रमुख राष्ट्रिय कानूनी प्रावधानहरू - - - १०

    क. मुलुकी फौजदारी कार्यविधि संहिता २०७४ (२०१७) - - - १०

    ख. विद्युतीय कारोबार ऐन, २०६३ - - - ११

    ग. वैयक्तिक गोपनीयता सम्बन्धी ऐन २०७५ (२०१८) - - - १२

    घ. प्रमाण ऐन २०३१ (१९७४) - - - १२

    ङ. राष्ट्रिय साइबर सुरक्षा नीति २०८० (२०२३) - - - १३

  ३.२ सिमानापारको डिजिटल प्रमाणमा राज्य पहुँचको सहजता: कानूनी रूपरेखा र संयन्त्र - - - १३

  ३.३ नेपालको न्यायिक कारवाहीमा डिजिटल प्रमाणको स्वीकार्यता - - - १४

    १. अख्तियार दुरूपयोग अनुसन्धान आयोग सम्पर्क कार्यालय विरूद्ध प्रेमबहादुर थापा - - - १४

    २. बाबुराम अर्यालसमेत विरूद्ध नेपाल सरकार, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, सिंहदरबार, काठमाडौंसमेत - - - १५

    ३.रुपा सुनार विरूद्ध कृष्ण गोपाल श्रेष्ठ, मन्त्री, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय समेत - - - १५

    ४.रामबहादुर थापा विरूद्ध अख्तियार दुरूपयोग अनुसन्धान आयोग - - - १५

५.सीतादेवी ठाकुर समेत विरुद्ध बुधनी ठाकुर - - - - - - - - - - - - - - - - - - - १६
६.नेपाल सरकार विरूद्ध उर्मिला बोट - १७
७. बमबहादुर बस्नेतसमेत विरूद्ध नेपाल सरकार - - - - - - - - - - - - - - - - १७
८. मखमली मिश्र समेत विरुद्ध लक्ष्मीकुमारी मिश्र (श्रेष्ठ) - - - - - - - - - - - - - - १७
९.अशोकराम महरा विरुद्ध छोटेलाल राम - - - - - - - - - - - - - - - - - - - १८
१०. रामबहादुर बस्नेत विरुद्ध नेपाल सरकार - - - - - - - - - - - - - - - - - - १८
४. डिजिटल प्रमाणको कानूनी मान्यता - १९
४.१ डिजिटल प्रमाणको मान्यताका लागि पूर्वावश्यक आधारहरु - - - - - - - - - - - - १९
क. डिजिटल डाटा प्रमाणका रूपमा प्रस्तुत गर्ने प्रक्रिया - - - - - - - - - - - - - - १९
ख. डिजिटल प्रमाणको मूल्याङ्कन - २०
ग. डिजिटल प्रमाणको परीक्षण - २०
घ. डिजिटल प्रमाणको निर्धारण - २१
४.२ डिजिटल प्रमाणको स्वीकार्यताका चुनौतीहरू - - - - - - - - - - - - - - - - - २१
क. प्रामाणीकता - २२
ख. सटिकता - २२
ग. पूर्णता - २३
घ. विश्वसनीयता- २३
५. डिजिटल प्रमाणको मान्यता र कार्यान्वयन सम्बन्धी अन्तर्राष्ट्रिय अभ्यासहरू- - - - - - - - - २३
६. नेपालमा डिजिटल प्रमाण सङ्कलन प्रक्रियाका केही सामान्य अवलोकनहरू - - - - - - - - - - २८
७. सुझावहरू - ३१
ग्रन्थसूची - ३५

१. परिचय

१.१ ऐतिहासिक परिप्रेक्ष्य

विभिन्न आपराधिक गतिविधिहरूको अनुसन्धान र अभियोजनमा डिजिटल प्रमाण महत्वपूर्ण घटकको रूपमा देखा परेको छ । पहिल्यै परम्परागत माध्यम, जस्तै भौतिक कागजातहरू वा मौखिक सञ्चारको माध्यमबाट गरिएका अपराधहरू अहिले डिजिटल उपकरणहरूको प्रयोगद्वारा गरिन्छ । उदाहरणका लागि, पहिले मौखिक रूपमा वा मुद्रित सामग्रीहरूको माध्यमबाट गरिने मानहानी अहिले प्रायः सामाजिक सञ्जाल प्लेटफर्महरू तथा विद्युतीय सञ्चार मार्फत हुने गरेको छ । त्यस्तै, पहिले भौतिक अभिलेखहरूको परिमार्जनद्वारा गरिने भ्रष्टाचार अहिले डिजिटल डाटाबेसभित्र डेटा परिमार्जनद्वारा गरिन्छ । अझै, बैंकिङ संस्थाहरूमा पहिले फाइल तथा अन्य भौतिक माध्यमहरुमा व्यक्ति आफैंले परिमार्जन गरेर हुने कोषको दुरुपयोग अहिले विद्युतीय माध्यमद्वारा गरिन्छ । अपराधका विधिहरूमा भएको यो परिवर्तन र आपराधिक गतिविधिहरूमा विद्युतीय उपकरणहरूको व्यापक प्रयोगका साथ, प्रमाणका ट्रेलहरू प्रायः डिजिटल स्वरूपमा मात्र पाइन्छन्, जसले डिजिटल प्रमाणको प्रभावकारी व्यवस्थापनको आवश्यकतालाई रेखांकित गरेको छ ।

विधिको परिवर्तन र आपराधिक गतिविधिहरूमा विद्युतीय उपकरणहरूको व्यापक प्रयोगको परिपाटीले गर्दा प्रमाण प्रायः डिजिटल स्वरूपमा मात्र पाइने हुनाले डिजिटल प्रमाणको प्रभावकारी नियमनको आवश्यकता देखाएको छ ।

आपराधिक अनुसन्धान प्रक्रियामा डिजिटल प्रमाणको निर्णायक भूमिकाको साथ, यसको स्वीकार्यता, विश्वसनीयता र प्रमाणिकतासँग सम्बन्धित चिन्ताहरू उत्पन्न भएका छन् । प्रमाण कानूनको आधारभूत माग भनेको अदालतमा उत्कृष्ट प्रमाण पेश गर्नु हो । यसमा स्वीकार्य मात्र नभएर विश्वसनीय र भरोसायोग्य प्रमाण प्रस्तुत गर्नुपर्ने कुरामा समावेश भएको हुन्छ, जसकारण आरोपी वा उनीहरूमाथि लगाइएका आरोपहरूबारे शंका उत्पन्न नगरोस् । प्राविधिको विकासले विभिन्न डिजिटल प्रविधिहरूको प्रयोग गरि अदालतमा प्रमाण प्रस्तुत गर्न सहज बनाएको छ । डिजिटल प्रमाण विभिन्न क्षेत्र (domains) मा प्रयोग गरिएको छ, जसमा लग विश्लेषण, डाटाबेस, लग परीक्षण, ध्वनीको गुणस्तर वृद्दि, फोटोग्राफ सुधार, फरेन्सिक भिडियो विश्लेषण र डिजिटल प्रविधिबाट औंठाछापहरूको गुणस्तर वृद्दि समेत पर्दछन् । डिजिटल प्रमाण विभिन्न क्षेत्रहरूमा उपयोग गरिंदै आएको छ जसमा लग एनालाइसिस, डाटाबेस, लग ट्रायल, अडियो सुधार, फोटो सुधार, फरेन्सिक भिडियो विश्लेषण, र अस्पष्ट फिंगरप्रिन्टहरूको डिजिटल प्रविधिबाट गुणस्तर वृद्दिपर्दछन् ।

अदालतमा डिजिटल प्रमाणको कानूनी महत्व उल्लेखनीय छ र दैनिक जीवनमा डिजिटल प्रविधिहरूमा बढ्दो निर्भरताका साथ यसको महत्व निरन्तर बढ्दै गएको छ । डिजिटल प्रमाण विभिन्न प्रकारका विद्युतीय डेटा, जस्तै इमेल, टेक्स्ट मेसेज, सामाजिक मिडिया पोस्ट, फोटो, भिडियो, कम्प्युटर फाइल, र विद्युतीय लेनदेन सहित विद्युतीय डाटाका विभिन्न रूपहरू पर्दछन् । अदालतमा डिजिटल प्रमाणको स्वीकार्यता र यसको महत्वका विभिन्न कारकहरू जस्तै, यसको सान्दर्भिकता, प्रमाणिकता, विश्वसनीयता, र कानूनी मापदण्ड र प्रक्रियाहरूको पालना माथि निर्भर गर्दछ । जब डिजिटल प्रमाणलाई सही तरिकामा सङ्कलन, संरक्षित, र प्रस्तुत गरिन्छ त्यसले विवादमा रहेका तथ्यहरू प्रमाणित वा अस्वीकार गर्नमा अत्यन्त प्रभावकारी र प्रेरक भूमिका खेल्न सक्छ ।

न्यायालयहरूले आधुनिक न्यायिक प्रक्रिया र अपराध सम्बन्धी कार्यवाहीहरूमा डिजिटल प्रमाणको महत्वलाई बढ्दो रुपमा स्वीकार्न थालेका छन ।, न्यायालयहरू प्राय: घटनाक्रमको समयरेखा स्थापन गर्न, साक्षीहरूको बयानलाई पुष्टि गर्न, मनसाय वा उद्देश्य देखाउन र व्यक्तिहरूलाई आपराधिक गतिविधिहरूसँग जोड्ने जस्ता कार्यको लागि यसमा निर्भर भएको पाइन्छ । यद्यपि, डाटाको गोपनीयता, प्रमाणको प्रामाणिकता र डिजिटल फरेन्सिक्समा विशेषीकृत विशेषज्ञताको आवश्यकताका जस्ता चुनौतीहरूले डिजिटल प्रमाणको स्वीकार्यताको र भरपर्दोपनमा प्रभाव पार्न सक्छ । त्यसैले, डिजिटल प्रमाण प्रस्तुत गर्ने पक्षहरूले कानूनी मापदण्ड र प्रक्रिया पालना गर्नु अत्यन्त महत्त्वपूर्ण छ, जस अन्तर्गत प्रमाणको प्रामाणिकता र अखण्डता प्रदर्शन गर्नु, अभिलेखहरूको नियन्त्रणको श्रृंखला (chain of custody) कायम राख्नु र आवश्यक परे विशेषज्ञको राय लिने कार्य पर्दछ । एक समयमा भौतिक कागजातहरूको जालसाजी/छेडछाड न्यायिक प्रक्रियामा भ्रम फैलाउने तरिकाको रुपमा प्रयोग हुन्थ्यो भने हालको प्राविधिक विकासको कारण जालसाजी/छेडछाडको परिभाषा विस्तार भएको र यसले न्याय सुनिश्चित गर्ने क्रममा भर पनुपर्ने प्रमाणको विश्वसनीयतालाई चुनौती पुऱ्याउँछ। समग्रमा, डिजिटल प्रमाणले अदालतको कार्यवाहीमा निकै नै कानूनी मूल्य राख्छ र प्रविधिको विकास हुँदै जाँदा न्याय प्रणालीमा बढ्दो रूपमा प्रमुख भूमिका खेल्ने अपेक्षा गरिएको छ ।

फोटो, भिडियो, र अडियो रेकर्डिङ सहित फौजदारी कारवाहीमा विद्युतीय प्रमाणको प्रयोग लामो समयदेखि चलिरहेको छ । न्युरेम्बर्ग ट्रायलदेखि यी सामग्रीहरूले विभिन्न प्रकारका अपराधहरूको अभिलेखीकरण र अभियोजनमा महत्वपूर्ण भूमिका खेलेको छ । पछिल्ला दशकहरूमा प्रविधिको वृद्धिसँगै आपराधिक गतिविधिहरूको प्रविधिको प्रयोग बढेको छ जुन कुरा घरेलु, क्षेत्रीय र अन्तर्राष्ट्रिय अदालतहरूमा आएका मुद्दाहरूमा देखा परेको छ । यस्तै, डिजिटल प्रविधिहरूले अपराधसँग सम्बन्धित प्रमाणहरू अभिलेख गर्न पनि उपकरणको रूपमा सेवा पुऱ्याइरहेका छन् । यी दुवै अवस्थामा मुद्दाको समाधानका लागि प्रमाणका रूपमा डिजिटल अभिलेखहरूको मान्यता समयको आवश्यकता बनेको छ ।

उदाहरणका लागि, सिरियाली द्वन्द्वसँग सम्बन्धित ४० लाखभन्दा बढी भिडियोहरू यूट्युबमा मात्र अपलोड गरिएका छन यि भिडियोको अवधिले द्वन्द्वको अवधिलाई पनि नाघेको छ । अन्तराष्ट्रिय फौजदारी अदालतका अनुसन्धानकर्ताहरू र अभियोजनकर्ताहरूले प्रयोगकर्ताद्वारा सिर्जित डिजिटल र ओपन-सोर्स प्रमाण सङ्कलन गरेर मुद्दाहरूमा प्रयोग गर्न थालेका छन् । अभियोजनकर्ताको कार्यालय (The Office of Prosecution) ले Bemba Case[1] मा २००८ मा डिजिटल प्रमाणहको सङ्कलनको सुरुवात गरेको थियो र Prosecutor v Thomas Lubanga Dyilo[2] को पहिलो पेशीमा अदालतमा भिडियो प्रमाण पेश गरिएको थियो । २०११ सम्ममा केन्या, आइभरी कोस्ट र लिबिया सम्बन्धी अनुसन्धानहरुमा यस प्रकारका प्रमाणहरू

---

[1] The Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 21, 2016), available at: https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/BembaEng.pdf

[2] Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 14, 2012), available at : https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/LubangaEng.pdf

सङ्कलन गरिएको थियो । अदालतको कार्यवाहीको प्रामाणिकता, शुद्धता, गोपनीयता र संरक्षण सुनिश्चित गर्न अदालतले 'ई-कोर्ट प्रोटोकल' (e-Court Protocol)[3] विकास गरेको छ ।

१.२ नेपालमा प्रमाण सङ्कलन प्रक्रिया र अभ्यास

डिजिटल प्रमाणको सङ्कलन यसको अखण्डता, प्रामाणिकता, र कानूनी कार्यवाहीहरूमा स्वीकार्यतामा कायम राख्नका लागि केही आधारभूत सिद्धान्तहरूमा निर्भर गर्दछ । सर्वप्रथम, अखण्डता अत्यन्त सर्वोपरि छ, जस अनुसार डिजिटल प्रमाण सङ्कलन र विश्लेषण प्रक्रिया भरी नै प्रमाण अपरिवर्तित रहनुपर्छ भनी माग गर्दछ । दोस्रो, चेन अफ कस्टडी स्थापना गर्नु अनिवार्य छ, जसले प्रमाण सङ्कलनदेखि अदालतमा प्रस्तुत हुने बेलासम्मको प्रक्रिया दस्तावेज गरि प्रमाण चलाउन तथा बिगार्नबाट जोगाउँछ ।

प्रमाणको उत्पत्तिको प्रमाणिकरण गर्नु आवश्यक छ, यसले प्रमाणमा केहि परिवर्तन गरिएको वा प्रमाण नक्कल गरिएको छ वा छैन भनी सुनिश्चित गर्दछ । यसले कुनै चीजको वास्तविकतालाई पनि जनाउँछ, त्यसको वास्तविक पहिचान र अखण्डता पुष्टि गर्दछ । विशेष गरी दस्तावेज सामग्रीको सन्दर्भमा, प्रामाणिकता भन्नाले त्यस सामग्रीको पहिचान र अखण्डता दुवै सुरक्षित राख्नु आवश्यक छ, जसले यसको सिर्जना देखि सूचना स्रोतको रूपमा प्रयोग वा प्रमाणको रूपमा पेश गर्न सम्म कुनै परिवर्तन वा छेड़छाड़ नगरी रहेको हुनुपर्छ ।[४]

यसबाहेक, डिजिटल प्रमाण मुद्दासँग सान्दर्भिक हुनुपर्छ र स्वीकार्यताको लागि विश्वसनीयता र प्रक्रियागत अनुपालन सहित, कानूनी मापदण्डहरू पूरा गरेको हुनु पर्छ । गोपनीयता र कानूनी अनुपालन पनि सर्वोपरि छन्, डेटा सङ्कलन र संचालनलाई नियन्त्रण गर्ने सान्दर्भिक कानून र नियमहरूको पालना गर्न आवश्यक छ । यी सिद्धान्तहरूलाई समर्थन गरेर, डिजिटल प्रमाण सङ्कलन गर्नाले कानूनी प्रक्रियाको अखण्डतालाई कायम राख्दै संलग्न सबै पक्षहरूको अधिकार र गोपनीयता सुरक्षित गर्दछ ।[५]

नेपालमा, फौजदारी मुद्दाहरूमा प्रमाण सlngsf लागि प्रक्रिया र प्रोटोकलहरू फौजदारी कार्यविधि संहिता, २०७४ (२०१७) ले निर्दिष्ट गर्दछ । यी कानूनी प्रावधानहरूले अनुसन्धान अधिकारीहरूåfरा प्रमाणहरूको सlng, संचालन, र प्रस्तुतीकरणको प्रक्रियालाई नियमन गर्दछ । प्रारम्भिक चरणमा, प्रमाण सङ्कलन अपराध स्थलमा शुरु हुन्छ, जहाँ औंठाछाप, डिएनए नमुना, र हतियार जस्ता भौतिक प्रमाणहरू सङ्कलन गरिन्छ। अपराधसँग सम्बन्धित सान्दर्भिक जानकारी सङ्कलन गर्न साक्षीको बयान पनि अभिलेख गरिन्छ । थप रूपमा, फोरेन्सिक विशेषज्ञहरूले थप जानकारीको

---

[3] Mark Kersten, Challenges and Opportunities: Audio-Visual Evidence in International Criminal Proceedings Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings

[4] Duranti, Luciana, and Allison Stanfield. "Authenticating Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 236–78. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.13. Accessed 27 Mar. 2024.

[5] Digital Evidence and the New Criminal Procedure Author(s): Orin S. Kerr Source: Columbia Law Review , Jan., 2005, Vol. 105, No. 1 (Jan., 2005), pp. 279-318 Published by: Columbia Law Review Association, Inc. Stable URL: https://www.jstor.org/stable/4099310

लागि भौतिक प्रमाणहरू विश्लेषण गर्न सक्छन् । प्रविधिको विकाससँगै कम्प्युटर र मोबाइल फोनबाट प्राप्त डाटाजस्ता विद्युतीय प्रमाणहरूको महत्व बढिरहेको छ र यो विशेष फोरेन्सिक परीक्षणको विषय पनि हो ।

डिजिटल प्रमाण अदालतमा ग्राह्य हुनका लागी, प्रभावकारी रूपमा सङ्कलन गरिनुपर्छ, अनुसन्धान निकायद्वारा मनासिव नियन्त्रणको श्रृंखला कायम राख्नुपर्छ, र अदालतमा सुरक्षित र स्थापित प्रक्रिया अनुसार हस्तान्तरण गर्नुपर्छ । यसले प्रक्रियाभर प्रमाणको सत्यनिष्ठता र विश्वसनीयता कायम राख्ने सुनिश्चितता प्रदान गर्छ ।

संकलित प्रमाणहरूको सत्यनिष्ठता र विश्वसनीयता सुनिश्चित गर्नका लागी यसको नियन्त्रणको श्रृंखला कायम राख्नु महत्वपुर्ण छ। सबै प्रमाण सङ्कलन प्रक्रियामा, अभियुक्तको अधिकारको रक्षा गर्न, कानूनी मापदण्ड र प्रोटोकलहरू पालना गर्नुपर्छ। अन्तरदेशीय अपराध सम्बन्धी मुद्दाहरूमा नेपालले कूटनीतिक माध्यम वा पारस्परिक कानूनी सहायता सन्धिहरू मार्फत अन्तर्राष्ट्रिय सहयोग लिन सक्छ। अन्य देशबाट प्राप्त प्रमाणहरूको स्वीकार्यता त्यसको वैधानिकता, अन्तर्राष्ट्रिय सम्झौताको परिपालना, र मुद्दासँगको सान्दर्भिकतामा निर्भर गर्दछ। समग्रमा, नेपालमा प्रमाण सङ्कलनका प्रक्रियाहरू, सम्बन्धित सम्पूर्ण पक्षहरुको अधिकारको सम्मान गर्दै, न्याय सुनिश्चित गर्न रुपांकित गरिएका छन् ।

१.३ नियन्त्रणको श्रृंखला र डिजिटल प्रमाणको नियमनको महत्व

विशेष गरी विद्युतीय प्रमाणको सम्बन्धमा, नियन्त्रणको निरन्तरता (continuity of custody)जसलाई प्रमाणको श्रृंखला पनि भनिन्छ, को अवधारणाको मनन गर्न वाञ्छनिय छ । विद्युतीय प्रमाणहरु फेरबदल हुन सक्ने जोखिम विध्यमान रहने हुँदा यसको अखण्डता प्रमाणित गर्न, यसको अधिग्रहण वा प्रतिलिपि गरेदेखि, यसलाई छेडछाड गरिएको छैन भन्ने कुरा समेत सुनिश्चित गर्न आवश्यक छ । विद्युतीय प्रमाणको नियन्त्रणलाई, विशेष गरी बहुभागी हार्डवेयर वस्तुहरू र कम्प्युटरहरू समावेश भएका अवस्थामा, हार्डवेयर र प्रतिलिपि गरिएका प्रमाणहरू बीचको अनुबन्धन स्पष्ट रुपमा स्थापित गर्न, सावधानीपूर्वक अभिलेख गर्न आवश्यक हुन्छ। यस अभिलेखमा कसले प्रमाण सङ्कलन गऱ्यो, कसरी र कहाँ सङ्कलन गरिएको हो, कसले परिग्रहण गऱ्यो, भण्डारण प्रक्रियाहरू, भण्डारणमा हुँदा गरिने संरक्षण, र प्रमाणमा पहुँच रहेकाहरुको अभिलेख र त्यसो गर्नुको कारणहरू, जस्ता विवरणहरू समावेश गर्नुपर्छ। अनलाइन भण्डारण र सेवाहरूको व्यापकतालाई ध्यानमा राख्दै, प्रमाण बन्नु अघि अभिलेखहरूको पहुँच र नियन्त्रणको व्यवस्थापन गर्नु पनि महत्त्वपूर्ण छ, विशेष गरी जब क्रिप्टोग्राफिक सुरक्षणहरू अव्यावहारिक रहेका हुन्छन् ।[6] नेपालको सन्दर्भमा, प्राविधिक स्रोतको अभाव र सम्बन्धित उपकरणहरूको जटिलताका कारण क्रिप्टोग्राफिक सुरक्षणहरू अव्यावहारिक हुन्छन्, प्रविधिहरू असंगत हुँदा र मानकीकरणको कमी हुँदा अक्षमताका समस्याहरू हुन्छन्, मानव त्रुटिहरूले पनि डाटाको हानि वा सो मा पहुँच नहुने जोखिमहरू प्रस्तुत गर्न सक्छ, त्यसैगरी, कार्यान्वयन खर्च बढ्दा कानूनी तथा कार्यविधिगत समस्या समेत त्यहाँ

---

[6] Wilson, Nigel, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 429–87. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.16. Accessed 27 Mar. 2024.

हुन्छन् । तसर्थ, व्यक्तिगत विवरणको गोपनीयताको रक्षा गर्न र प्रमाणहरूको विश्वसनीयता सुनिश्चित गर्न पर्याप्त सुरक्षाका साथै नियन्त्रणको उचित श्रृंखला कायम राख्न महत्त्वपूर्ण छ ।

२. डिजिटल प्रमाणहरूलाई संचालन गर्ने निर्देशिका: अन्तर्राष्ट्रिय परिप्रेक्ष्य

सूचना प्रविधिको विकाससँगै, डिजिटल प्रमाणहरूको पहिचान, सङ्कलन, अधिग्रहण, र संरक्षणको लागि अन्तर्राष्ट्रिय मञ्चमा विभिन्न मापदण्डहरू विकास भएका छन् । विशेष रूपमा, ISO/IEC २७०३७:२०१२[7] जसले डिजिटल प्रमाणहरूको संचालन गर्ने प्रक्रियामा सामान्य अवस्थामा व्यक्तिहरूलाई मार्गदर्शन प्रदान गर्दछ र संगठनहरूलाई तिनीहरूको अनुशासनात्मक प्रक्रियाहरूमा सहायता गर्दछ तथा विभिन्न न्यायक्षेत्रहरू बीच हुने सम्भावित डिजिटल प्रमाणहरूको आदानप्रदानलाई सहज बनाउँछ; ISO/IEC २७०४२[8] डिजिटल प्रमाणको विश्लेषणको लागि निर्देशनहरु; INTERPOL को डिजिटल फरेन्सिक अभ्यासहरू सम्बन्धी कार्यसञ्चालनका मार्ग निर्देशहरू; यूरोपोलको युरोपियन साइबरक्राइम सेन्टर(EC3) को डिजिटल प्रमाण संचालन गर्ने फ्रेमवर्क तथा उपकरणकिट; को साइबरक्राइम रिपोजिटरी जसमा आपराधिक अनुसन्धानमा विद्युतीय प्रमाण व्यवस्थापनको लागि स्रोतहरू र निर्देशहरू समावेश छन्, साइबर अपराध सम्बन्धित बुडापेस्ट महासन्धि (Budapest Convention on Cybercrime)[9] जसले विशेष गरी सीमापार अनुसन्धान र डिजिटल प्रमाणको संरक्षण र प्रामाणिकता सुनिश्चित गर्ने प्रावधानहरू प्रदान गर्दछ; अन्तर्राष्ट्रिय कम्प्युटर अनुसन्धान विशेषज्ञ संघ (IACIS) ले पनि डिजिटल फरेन्सिक विशेषज्ञहरूको लागि प्रमाणीकरण र उत्तम अभ्यासहरू अगाडि बढाएको छ । प्रमुख प्रहरी अधिकारीहरूको संघ (ACPO) को डिजिटल प्रमाणको लागि निर्देशहरूले पनि आपराधिक अनुसन्धानमा विद्युतीय डाटाको उचित व्यवस्थापन, संकलन, संरक्षण र विश्लेषणको लागि उत्तम अभ्यासहरू रेखांकित गरेको पाइन्छ । यसले डिजिटल प्रमाणको अखण्डता कायम राख्न जोड दिन्छ, र यसको प्राप्ति वा परीक्षणको क्रममा कुनै परिवर्तन नहोस् भन्ने सुनिश्चित गर्दछ । यी निर्देशनहरूले गरिएका सबै कार्यहरूको उचित अभिलेखीकरण, कानूनी प्रोटोकलहरूको पालना, र प्रमाणहरूमा छेडछाड हुन नदिन सुरक्षित भण्डारणको पक्षको वकालत गर्दछन् । यी उपकरणहरूको उद्देश्य डिजिटल प्रमाणलाई अदालतमा स्वीकार्य बनाउन र प्रभावकारी तथा न्यायपूर्ण अनुसन्धानलाई समर्थन गर्न सुनिश्चित गर्नु हो ।

---

[7] ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, ISO (2012), available at, https://webstore.ansi.org/preview-pages/INCITS/preview_INCITS+ISO+IEC+27037+2012+(R2019).pdf?srsltid=AfmBOoqREc1Pliql6CQCOGXgN4J0S3mPjdSRt9Ib_XYJjPLL1Yf8zWG_

[8] ISO/IEC 27042: ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*, ISO (Year varies)

[9] Council of Europe, *Convention on Cybercrime* (ETS No. 185), opened for signature Nov. 23, 2001

उपरोक्त अन्तर्राष्ट्रिय मापदण्डहरूलाई ध्यानमा राख्दै, हामीले विद्युतीय प्रमाणहरूको अनुसन्धान र परीक्षण अघि, फोरेन्सिक र कानून प्रवर्तन समूहरूमा “फरेन्सिक ट्राइएज” नामक विधिलाई ध्यान दिइरहेको देख्न सक्छौं । यसले डिजिटल फोरेन्सिक अनुसन्धानलाई अझ प्रभावकारी रूपमा प्राथमिकता मा राख्ने उद्देश्यले विभिन्न प्रक्रियाहरू, उपकरणहरू र विधिहरू समावेश गर्दछ । यद्यपि, फोरेन्सिक ट्राइएज हरेक मुद्धाका लागि उपयुक्त हुँदैन र प्रशिक्षित व्यक्तिहरूद्वारा उचित जोखिम मूल्याङ्कनसँगै प्रयोग गरिनुपर्छ भन्ने कुरामा ध्यानमा राख्नु महत्वपूर्ण छ ।

डिजिटल ट्राइएज प्रविधि प्रयोग मा ल्याउँदा, चासोको विषयवस्तु (material of interest) को द्रुत पहिचान तथा निर्दोशिता प्रमाणित गर्ने वा थप महत्वको सामग्रीहरु छुट्ने गरी थप विश्लेषणको क्रम रोकिन सक्ने जोखिमका बीच सन्तुलन राख्नु महत्वपूर्ण रहेको छ । उदाहरणका लागि, बाल यौन दुर्व्यवहार र अश्लिल तस्वीरहरू डाउनलोड गर्ने घटनामा, किवर्ड र ह्यास सेट विश्लेषणले अश्लिल तस्वीरहरू छिटो पत्ता लगाउन सक्छ । तर, केवल ट्राइएजको नतिजामा निर्भर रहँदा थप गम्भीर अपराधहरूको बेवास्ता हुने सम्भावना रहन्छ । त्यसैले, डिजिटल ट्राइएजलाई अनुसन्धानको प्राथमिक चरणको प्रविधि मान्नुपर्छ, जसले सुसूचित निर्णय गर्न सहयोग पुर्याउँछ, नकि एकमात्र अनुसन्धानको विधि ।

२.१ विद्युतीय उपकरणहरूको संचालन

डिजिटल प्रमाण व्यवसायीहरू फौजदारी वा देवानी जुनैसुकै मुद्दाहरूमा संलग्न भएता पनि, डिजिटल प्रमाणहरू सङ्कलन र संचालन गर्दा उच्च मापदण्डहरू कायम राख्न सल्लाह दिइन्छ । डिजिटल डाटाको अनुचित संचालनले डाटा नष्ट हुने र अपर्याप्त अभ्यासहरूको प्रयोग सम्बन्धी चुनौतीहरू निम्त्याउन सक्छ ।[10]

विद्युतीय प्रमाणको अस्थिर र सजिलै परिवर्तन हुन सक्ने प्रकृतिलाई ध्यानमा राख्दै, यसको उचित संचालन सुनिश्चित गर्न प्रमुख प्रहरी अधिकारी संघको मापदण्डहरू (Association of Chief Police Officers Guidelines)[11] को पालना गर्नु

---

[10] *Stanford International Bank Limited (in liquidation) v. Hamilton-Smith,* High Court (Antigua),See :https://ag.vlex.com/vid/alexander-m-fundora-applicant-805812073

[11] Williams, Janet. "Acpo good practice guide for digital evidence." *Metropolitan Police Service, Association of chief police officers, GB* (2012): 1556-6013., *Good Practice Guides for Digital Evidence (the latest of five revisions coming in 2012, the first being in 1998 [2]) are considered to provide core information for practitioners operating in the digital forensics field in England and Wales.* The,Principle 1, No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court. Principle 2, In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. Principle 3, An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result, Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

महत्वपूर्ण छ । यि सिद्यान्तहरूले डेटाको अखण्डताको संरक्षण, मूल डाटामा पहुँच गर्न योग्यता, लेखाको क्रम कायम राख्न, र डिजिटल प्रमाण संचालनमा कानूनी मापदण्ड र सिद्धान्तहरूको पालनाको लागि समग्र जिम्मेवारीको महत्वलाई जोड दिएको पाइन्छ । डिजिटल डाटाको प्रामाणिकता र अखण्डता कायम राख्नका लागि डिजिटल प्रमाण विशेषज्ञहरूले मापदण्डहरूको पालना गर्नुपर्ने विषयमा जोड दिइने भएता पनि अदालतहरूले कहिलेकाहीं यसको परिपालनाहरूलाई बेवास्ता गर्न सक्छन् । डाटा जफतमा डिजिटल फोरेन्सिकको महत्व बुझ्न असफल हुँदा कानूनी कार्यवाहीको अखण्डतालाई कमजोर बनाउन सक्छ । जफत गरिएका हार्डड्राइभहरूको फोरेन्सिक इमेजिङमा ह्यास भ्याल्यु (Hash Value) हरू उत्पन्न गर्ने जस्ता उत्कृष्ट अभ्यासहरू लागू गर्नाले डिजिटल प्रमाणहरूको अखण्डता सुनिश्चित गर्न मद्दत गर्न सक्छ, तर त्यस्ता अभ्यासहरूलाई अदालत वा सुरक्षा टोलीहरूले सधैं पूर्ण रूपमा प्रशंसा वा प्रयोग गर्न सक्दैनन् ।

२.२ विद्युतीय प्रमाणको पहिचान

डिजिटल स्वरुपमा रहेका प्रमाणको खोज प्रायः गलत कामको प्रारम्भिक संकेत हुन सक्छ जसले अनुसन्धानको आवश्यकतालाई दर्शाउँदछ । अनुसन्धान प्रारम्भ गर्दा अनजानमा विद्युतीय प्रमाणहरू परिवर्तन हुन सक्छन्, त्यसैले अनुसन्धान सुरु तथा सञ्चालन गर्न उपयुक्त प्रक्रियाहरू हुनु आवश्यक छ । दुवै दिवानी तथा फौजदारी मुद्दाहरूमा, सान्दर्भिक कागजातहरू खुलासा गर्ने दायित्व रहेको हुन्छ र अनुसन्धान अधिकारीहरूले मान्यता प्राप्त निर्देशहरूको पालना गर्ने अपेक्षा गरिन्छ । ACPO Good Practice Guide for Digital Evidence ले डिजिटल प्रमाण संचालन गर्नका लागि चार मुख्य चरणहरू रेखांकित गर्दछः सIng, परीक्षा, विश्लेषण, र रिपोर्टिङ, जसलाई फोरेन्सिक ट्राइज प्रविधिहरूको साथमा प्रारम्भिक मूल्याङ्कन चरणको साथ विस्तार गर्न सकिन्छ ।

२.३ विद्युतीय प्रमाण सङ्कलन

डिजिटल प्रमाण सङ्कलनको आवश्यकता निर्धारण भएपछि, घटनास्थलको व्यवस्थापन, प्रमाणको पहिचान र जफत गर्न आवश्यक परेमा डिजिटल प्रमाण पेशावरहरूsf मार्गदर्शन गर्न विशिष्ट प्रक्रियाहरूको पालना गर्नुपर्छ । अपराध स्थलको दस्तावेजीकरण फोटो वा भिडियो रेकर्डिङ मार्फत, हार्डवेयर लेआउट अधकृत लिने हाल मापदण्ड अनुसारको अभ्यास बनेको छ । अनुसन्धानकर्ताले स्थापित मापदण्डहरूको आधारमा कम्प्युटर वा भण्डारण गर्ने उपकरण जस्ता भौतिक प्रमाणहरू मध्ये कुन-कुन राख्नुपर्ने हो भन्ने निर्णय गर्नुपर्छ । हार्डवेयर वा नेटवर्कमा छेडछाड हुनबाट रोक्न र जफतका लागि तोकिएका कम्प्युटरहरू प्रशिक्षित कर्मचारीहरूले मात्र संचालन गर्ने कुरा सुनिश्चित गर्नु अत्यावश्यक छ ।

डिजिटल प्रमाणसँग जोडिएको एक प्रमुख चुनौती यसको परिवर्तनशीलता वा नष्ट हुने सम्भाव्यता हो । डिजिटल उपकरणहरू अस्थिर प्रकृतिका हुन्छन् र बन्द गर्दा महत्वपूर्ण डाटा गुमाउन सक्छन् । शारीरिक रूपमा कम्प्युटरमा उपस्थित संशयित व्यक्तिलाई पक्राउ गर्दा विशेष सावधानी आवश्यक पर्छ, किनभने उनीहरूले आपराधिक फाइलहरू मेटाउन वा बिगार्न प्रयास गर्न सक्छन् ।

२.४ विद्युतीय प्रमाणको प्रतिलिपि

विद्युतीय प्रमाणको प्रतिलिपि बनाउँदा ACPO मापदण्डमा उल्लेखित मुख्य सिद्धान्तहरूको पालना गर्नुपर्छ । यसमाः अदालतमा भरपर्दो प्रमाणका रूपमा प्रयोग हुने डाटालाई कुनै पनि प्रकारले परिवर्तन हुन नदिने, मूल डाटामा पहुँच गर्ने व्यक्ति दक्ष हुनपर्ने र आफ्नो कार्यहरूको व्याख्या गर्न सक्नुपर्ने, डिजिटल प्रमाणमा लागू गरिएका सबै प्रक्रियाहरूको अडिट ट्रेल तयार पार्ने र सुरक्षित गर्ने, अनुसन्धानको नेतृत्व गर्ने व्यक्तिले प्रमाण सम्बन्धी कानून र यी सिद्धान्तहरूको पालना सुनिश्चित गर्नुपर्ने, जस्ता सिद्धान्तहरू समावेश छन् । नेटवर्क प्रणालीहरूको हकमा, विभिन्न स्थानहरूमा रहेको डिजिटल प्रमाणहरुको स्रोत र यसको सांस्थिती बुझ्न जरुरी छ । विद्युतीय प्रमाणको प्रतिलिपि बनाउने प्रक्रियामा मूल डाटालाई परिवर्तन नगरी सटीक प्रतिलिपि उत्पादन गर्ने लक्ष्य राख्नुपर्छ । प्रतिलिपि फाइलहरूको प्रामाणिकता प्रमाणित गर्न ह्यासिङ प्रक्रियाको प्रयोग गरिन्छ ।

प्रतिलिपि गरिएका डिजिटल फाइलहरूको गुणस्तर कायम राख्नु महत्त्वपूर्ण छ, यस विषयलाई The Gates Rubber Company v. Bando Chemical Industries Limited[12] जस्ता मुद्दाहरूमा प्रकाश पारिएको पाइन्छ, यस मुद्दामा प्रमाणको गलत व्यवस्थापनको कारण अदालतमा सो प्रमाणले आफ्नो मूल्य गुमाएको थियो । डिजिटल प्रमाण व्यवसायीहरूले प्राय, विशेष गरी प्रत्यक्ष बैंकिङ प्रणालीहरू जस्ता असामान्य परिस्थितिहरुमा राम्रो अभ्यासको सिद्धान्तमा आधारित निर्णयहरू लिनुपर्ने हुन्छ । साम्प्रदायिक क्षेत्रमा रहेका सामाग्रीको परीक्षणले डिजिटल प्रमाणलाई पूरक बनाउन सक्ने गरी खुलासाहरू वा आपराधिक अनुसन्धानका लागि उपयोगी सामाग्री प्राप्त गर्न सकिन्छ । यो उदाहरणले देखाउँछ कि, प्रमाणको भरपर्दो अवस्था गुम्दा सम्बन्धित पक्षलाई गम्भीर चुनौतीहरू ;मना गर्नुपर्ने हुनसक्छ, जसलाई हरेक परिस्थितिमा पर्याप्त रूपमा सम्बोधन गर्न सधैं सम्भव हुँदैन ।

२.५ विद्युतीय प्रमाणको संरक्षण

विद्युतीय प्रमाणको प्रमाणिकता सुनिश्चित गर्न यसको परीक्षण आवश्यक छ । डिजिटल प्रमाण व्यवसायीहरूले प्रायः विभिन्न डिस्क वा स्टोरेज उपकरणहरूबाट डाटा प्रतिलिपि बनाउँछन्, जसकारण प्रतिलिपि गरिएका प्रमाणहरूको अखण्डता प्रमाणित गर्नका लागि उपायहरू अपनाउन आवश्यक पर्छ । विद्युतीय फिङ्गरप्रिन्टिङ एक क्रिप्टोग्राफिक प्रविधि हो, जसले प्रत्येक फाइल वा भण्डारणको उपकरणसँग अनौठो पहिचानकर्ता जोडी सङ्कलनको समयमा डाटाको अखण्डता जाँच गर्न सहायता गर्दछ ।

---

[12] United States Court of Appeals, Tenth Circuit, 9 F.3d 823 (10th Cir. 1993)

अखण्डता पूस्टी गर्न तथा छेडछाड हुन बाट रोक्नको लागि प्रमाण सङ्कलन, भण्डारण र व्यवस्थापनको हरेक प्रक्रियाको विस्तृत रुपमा अभिलेख राख्नु जरुरी छ, जुन विद्युतीय प्रमाण संरक्षित राख्नका लागी चाहिने नियन्त्रणको निरन्तरतामा आवश्यक छ । हार्डवेयर तथा डिजिटल प्रमाणहरू, ढुवानी तथा भण्डारण गर्दा तापक्रम, आर्द्रता, र चुम्बकीय प्रभाव जस्ता कारकहरूले डाटा क्षति तथा डाटा बिग्रिने(corrupt) सम्भावनालाई ध्यानमा राखेर सावधानी अपनाउनुपर्छ ।

क्लाउड कम्प्युटिङको उदयले डिजिटल फोरेन्सिकका लागि जटिल चुनौतीहरू प्रस्तुत गरेको छ, किनकि क्लाउडमा भण्डारण गरिएका प्रमाणहरू धेरै सर्भरहरूमा वितरित हुन्छन् र स्वचालित रूपमा व्यवस्थित हुन्छन् । त्यस्ता प्रमाणहरू प्राप्त गर्न सेवा प्रदायकहरूबाट सहयोग आवश्यक पर्न सक्छ, जसले गर्दा क्षेत्राधिकार सम्बन्धी समस्याहरू उठ्छन् । अनलाइन डेटाको समयमै मूल्याङ्कन र संरक्षणको लागि फोरेन्सिक ट्राइएज आवश्यक हुन्छ, विशेष गरी सुदूरबाट डाटा मेटिने जोखिम भएका अवस्थामा ।

२.६ विद्युतीय प्रमाणको विश्लेषण

डिजिटल प्रमाणका विभिन्न पक्षहरूको विश्लेषण गर्दा प्रमाण सङ्कलन तथा विश्लेषण दुवैमा डिजिटल प्रमाण विशेषज्ञहरूको महत्त्वपूर्ण भूमिकालाई स्वीकार्नुपर्छ। प्रमाण मात्र सङ्कलन गर्नु पर्याप्त हुँदैन; यसको शुद्धता र विश्वसनीयता सुनिश्चित गर्न यसको गहन विश्लेषण गर्नुपर्छ। डिजिटल प्रमाणको सही रूपमा मूल्याङ्कन नगर्दा गलत निष्कर्षमा पुग्न सकिन्छ ।

Liser v Smith[13] मा, अनुसन्धानकर्ताहरूले अनुसन्धानको लागि पर्याप्त समय भए तापनि बैंक प्रबन्धकको सरभेलेन्स टेपको समयसँग सम्बन्धित अपुष्ट बयानमा मात्र भर परी तिनीहरू टेपको टाइम स्ट्याम्पको शुद्धता प्रमाणित गर्न असफल भएको कारण गलत व्यक्ति पकाउमा परेको थियो यसले प्रमाणको सटीकता जाँच्न साथै प्रमाणिकरण गर्नु पर्ने महत्वलाई उजागर गर्छ । त्यसैगरी, *Mogford v Secretary of State for Education and Skills*[14], मा संदिग्धको गवाही र फाइल प्रणाली गतिविधिहरूको समयमा भएका विसंगतिहरू अपराध स्थापित गर्न महत्वपूर्ण थिए । संदिग्धको कथालाई पुष्टि गर्न असफल हुनु र कम्प्युटर गतिविधिको समयले न्यायाधिकरणको निर्णयमा महत्त्वपूर्ण भूमिका खेलेको थियो ।

---

[13] Jason Liser Plaintiff v. Jeffrey Smith et al, United States District Court, D. Columbia, No. CIV.A.00-2325 (ESH) (D.D.C. Mar. 26, 2003)

[14] England and Wales care Standards Tribunal, Mogford v Secretary of State for Education and Skills [2002] EWCST 11(PC) (26 June 2002), https://www.bailii.org/ew/cases/EWCST/2002/11(PC).html

समग्रमा, सो उद्धरणले कानूनी कार्यवाहीमा यसको शुद्धता र विश्वसनीयता सुनिश्चित गर्न विद्युतीय प्रमाणहरूको सावधानीपूर्वक विश्लेषण र प्रमाणीकरणको महत्वलाई जोड दिन्छ। उचित जाँचबिना, मात्र डिजिटल डाटामा भर पर्दा गलत निष्कर्ष र अनुचित नतिजा निम्त्याउन सक्छ।[१५]

३. नेपालमा डिजिटल प्रमाणको स्वीकार्यता सम्बन्धी कानूनी रूपरेखा र न्यायिक निर्णयहरू

३.१ प्रमुख राष्ट्रिय कानूनी प्रावधानहरू

क. मुलुकी फौजदारी कार्यविधि संहिता २०७४ (२०१७)

नेपालको देवानी तथा अपराध संहिता भित्रका देवानी तथा फौजदारी प्रमाणहरू सम्बन्धी प्रावधानहरू |डिजिटल प्रमाणका, गोपनीयता, डेटा सुरक्षा, साइबर अपराधहरू र विद्युतीय रेकर्डको स्वीकार्यता जस्ता विभिन्न समस्याहरू सम्बोधन गर्नका लागि प्रयोग गर्न सकिन्छ। मुलुकी फौजदारी कार्यविधि संहिता २०७४ र अपराध अनुसन्धा सम्बन्धी नियमावली २०७४ ले नेपालमा आपराधिक अनुसन्धान र परीक्षणको प्रक्रियाको व्यवस्थापन गर्दछन्। यि कानूनी प्रावधानहरुले विशेषरूपमा डिजिटल प्रमाणलाई सम्बोधन नगरे पनि, प्रमाण सङ्कलन, परीक्षण र प्रस्तुतीकरणका लागि उल्लेख गरिएका कानूनी प्रावधानहरू डिजिटल प्रमाणको हकमा समेत लागू हुन्छन्। प्रचलित कानूनी प्रावधानहरुले अदालतमा प्रमाणको स्वीकार्यताको मापदण्ड र प्रक्रिया निर्धारण गर्दछन्, जसले अप्रत्यक्ष रूपमा डिजिटल उपकरणहरूलाई समेत समावेश गरेता पनि ती उपकरणहरू भित्रका डिजिटल प्रमाणहरूको समावेशलाई भने निषेध गरेको पाइन्छ। कुनै पनि उपकरणको सामग्री गोपनीयता कानूनको दायरा भित्र पर्दछ र फौजदारी कार्यविधि संहिताका प्रावधानहरूमा गोपनीयता कानूनको उचित सन्दर्भ व्यवस्था गरिएको पाईंदैन।

नेपालमा, संहिताहरूले विद्युतीय रेकर्डहरूलाई न्यायिक प्रणाली भित्र ग्राह्य प्रमाणको रूपमा स्वीकार गरेको छ।[१६] डजिटल रेकर्ड र प्रमाणहरूलाई कागजात प्रमाणको रूपमा वर्गीकृत र व्यवस्थित गरिएको छ। डिजिटल रेकर्डहरूलाई अलग प्रमाणको प्रकारको रूपमा मान्यता नदिइएकाले डेटा सङ्कलनसँग सम्बन्धित कुनै विशेष प्रावधानहरू छैनन्। तिनीहरू कानूनी प्रकृया भित्र कागजीय प्रमाणको दायरामा पर्दछन्।[१७]

---

[15] Mason, Stephen, et al. “Proof: The Technical Collection and Examination of Electronic Evidence.” *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 285–338. *JSTOR*, http://www.jstor.org/stable/j.ctv512x65.16. Accessed 27 Mar. 2024.

[16] मुलुकी फौजदारी कार्यविधि संहिता २०७४, दफा ८९(१)

[17] मुलुकी फौजदारी कार्यविधि संहिता २०७४, दफा २७६(१)

मुलुकी फौजदारी कार्यविधि संहितामा प्रमाण संचालनको, प्रमाण सङ्कलनदेखि अदालतमा प्रस्तुति सम्मका प्रक्रिया समावेश छन् । मुलुकी फौजदारी कार्यविधि संहिताको दफा ६[१८] ले जानकारी प्राप्त भए पश्चात प्रहरीले तत्काल कारवाहीको सुरुवात गर्नु पर्ने विषय व्यवस्था गर्दछ, जसमा कसूरसँग सम्बन्धित कुनै प्रमाण लोप वा नास हुन नदिने र कसूर गर्ने व्यक्ति भाग्न उम्कन नपाउने आवश्यक र प्रभावकारी कार्य यथाशिघ्र गर्नु पर्नेछ भन्ने व्यवस्था समावेश गरिएको छ । प्रहरीले प्रमाण जफत गरी अपराधीलाई पक्राउ गर्नुपर्छ, र सोको अभिलेख राख्नुपर्छ, र यदि तुरुन्तै जफत गर्न सम्भव छैन भने बाह्य सहयोगको लागी अनुरोध समेत गर्न सक्नेछ । यसले प्रमाणको अखण्डता र अपराधीको पक्राउ सुनिश्चित गर्दछ । यसैगरी, दफा ८[१९] ले जाहेरी गरिएको अपराधको अनुसन्धानका लागि प्रक्रियाहरू निर्दिष्ट गरेको छ, जसमा प्रमाण सङ्कलनको प्रकृया समावेश छ । अभियोजनका लागि मुद्दा पेश गर्दा, अनुसन्धान अधिकृत निकायले प्रमाणको नियन्त्रण लिई, आरोपीलाई हिरासतमा राखी, सरकारी वकिलको निर्देशन बमोजिम, अदालतमा प्रस्तुत गर्नुपर्छ ।[२०]

ख. विद्युतीय कारोबार ऐन, २०६३

नेपालको कानूनले "विद्युतीय प्रमाण" को परिभाषा गरेको छैन । तर, विद्युतीय कारोबार ऐन, २०६३ ले विद्युतीय अभिलेख को परिभाषा दिएको छ, "विद्युतीय अभिलेख (रेकर्ड)" भन्नाले विद्युतीय स्वरुपको कुनै माध्यमबाट सृजना गरी सम्प्रेषण गरिएका, प्राप्त गरिएका वा जम्मा गरिएका तथ्याङ्क, अभिलेख, आकृति वा ध्वनि सम्झिनु पर्छ (दफा २ (ख)) साथै "विद्युतीय स्वरुप" भन्नाले कुनै चुम्बकीय, दृश्यगत, कम्प्युटर स्मरण वा अन्य त्यस्तै प्रकारको माध्यमबाट सृजना गरिएको, प्राप्त गरिएका वा जम्मा गरिएको सूचनाको स्वरुपलाई सम्झीनु पर्छ , भनी व्यवस्था गरिएको छ ।

विद्युतीय कारोबार ऐनको दफा ४ ले विद्युतिय अभिलेखको कानूनी मान्यता प्रदान गरेको छ, जसनुसार प्रचलित कानूनमा कुनै सूचना, लिखत, अभिलेख वा अन्य कुनै कुरा लिखित वा मुद्रित रुपमा राखिएको वा टाइप गरिएको हुनु पर्ने भनी उल्लेख गरिएको भए तापनि त्यस्ता सूचना, लिखत, अभिलेख वा कुरा यो ऐन वा यस अन्तर्गत बनाइएका नियममा उल्लेखित प्रकृिया पूरा गरी विद्युतीय अभिलेखको रूपमै राखिएको भए, त्यस्तो विद्युतीय अभिलेखले पनि कानूनी मान्यता प्राप्त गर्नेछ ।[२१]

---

[18] मुलुकी फौजदारी कार्यविधि संहिता २०७४, दफा ६

[19] मुलुकी फौजदारी कार्यविधि संहिता २०७४, दफा ८

[20] मुलुकी फौजदारी कार्यविधि संहिता २०७४, दफा ३८(१)

[21] विद्यतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ दफा १६

ग. वैयक्तिक गोपनीयता ऐन २०७५ (२०१८)

गोपनीयता सम्बन्धी ऐनको दफा १९ मा विद्युतीय सञ्चारको गोपनीयता सम्बन्धी नियमहरू उल्लेख गरेको पाइन्छ। यस अनुसार प्रत्येक व्यक्तिलाई विद्युतीय मध्यममा रहेको निजको कुनै पनि व्यक्तिगत सूचना, लिखत, पत्राचार, डेटा र चरित्र सम्बन्धी कुराको गोपनीयता कायम राख्ने अधिकार हुनेछ। गोपनीयतामा अनधिकृत पहुँच वा सो मा हुने उल्लङ्घनलाई निषेध गरिएको छ। व्यक्तिको सहमति वा कानूनी अधिकार बिना, कसैले पनि यान्त्रिक उपकरणहरू प्रयोग गरेर विद्युतीय सञ्चारहरू अवरोध गर्न वा ध्वनि अङ्कन वा रेकर्ड गर्न गराउनु हुदैन। यद्यपि, यो प्रावधान सार्वजनिक रूपमा गरिएका भाषण वा वक्तव्यहरूमा लागू हुँदैन। यी नियमहरूको अपवाद व्यक्तिको सहमतिमा वा अधिकार प्राप्त अधिकारीको आदेशमा गर्न सकिन्छ। विद्युतीय सूचना र तथ्याङ्क, गोपनीयता सम्बन्धी अन्य व्यवस्थाहरू कानूनद्वारा तोकिए बमोजिम प्रदान हुनेछ।

तर, डिजिटल प्रमाण सङ्कलन र निर्णय प्रक्रिया सम्बन्धी विस्तृत कानूनी प्रावधानहरूको अभाव छ। उदाहरणका लागिः कुनै पनि आपराधिक अनुसन्धानको क्रममा, अपराधसँग सम्बन्धित प्रमाणहरू स्थापित नियमहरू अनुसार राख्न सकिन्छ। यद्यपि, अन्य अप्रासंगिक सामग्रीलाई नियन्त्रणमा लिने कुरा स्वीकार्य छैन; यसै तर्कमा, ल्यापटप, मोबाइल फोन र अन्य भण्डारण उपकरणहरूमा रहेका व्यक्तिगत विवरण जुन अपराधसँग सम्बन्धित छैनन्, संवेदनशील र जोखिमपूर्ण रहन्छ। यसका लागि, राज्यले यस्ता व्यक्तिगत र गोपनीय जानकारीहरूको सुरक्षा गर्ने उचित प्रक्रिया लागू गर्न अत्यन्त आवश्यक छ। प्रमाणको स्वीकार्यता सम्बन्धी वर्तमान अभ्यासहरू अपर्याप्त छन्, जसले अदालतलाई अविश्वसनीय प्रमाणहरूमा आधारित हुन वा अवैध तरिकामा प्राप्त प्रमाणहरूमा निर्भर रहन सक्ने जोखिम सृजना गर्छ।

घ. प्रमाण ऐन २०३१ (१९७४)

नेपालको प्रमाण ऐनले कानूनी कारवाहीहरूमा प्रमाणको स्वीकार्यता सम्बन्धी सामान्य प्रावधानहरू व्यवस्था गर्दछ। प्रमाण ऐनको दफा ३५, परिच्छेद ६ ले लिखित प्रमाणको लागि आधारभूत मापदण्डहरू निर्धारण गरेको छ।

प्रमाण ऐनको दोस्रो संशोधन, २०२० ले डिजिटल र विद्युतीय प्रमाणलाई पहिचान गरेको छ। संशोधनपछि, प्रमाण ऐनको दफा २(ग) ले सार्वजनिक लिखतको डिजिटल वा विद्युतीय स्वरुपलाई समेत सार्वजनिक लिखतको परिभाषा भित्र समावेश गरेको छ। यसका साथै, दफा ६ ले डिजिटल वा विद्युतीय कारोवारबाट लिखत वा सम्झौता भएकोमा रितपूर्वक लिखत वा सम्झौता भएको हो भनी अदालतले अनुमान गर्नेछ भनी व्यवस्था गरिएको छ। दफा १३क (दोस्रो संशोधनद्वारा) ले श्रव्य दृश्य माध्यमबाट विद्युतीय रूपमा अभिलेख गरिएका सामग्रीलाई प्रमाणको रूपमा स्वीकार गर्ने व्यवस्था गरेको छ। यसप्रकार श्रव्य दृश्य माध्यम मार्फत अभिलेखित कुराहरु सोही रुपमा वा लिपिबद्ध गरी अदालतले अभिलेख राख्न सक्नेछ। ऐनको दफा १४ ले कुनै पनि काम, कारबाही वा व्यावसायको सिलसिलामा नियमित रुपमा

डिजिटल र विद्युतीय माध्यमबाट राखिएका विवरणलाई अदालतमा प्रमाणको रूपमा स्वीकार गर्ने व्यवस्था गरेको छ। प्रमाण ऐनको दफा ३५ मा, कुनै पनि लिखतमा उल्लेखित जानकारीलाई प्रमाणित गर्न सो लिखत नै पेश गर्नु पर्छ, भनी उल्लेख गरिएको छ। यसै दफामा लिखत भन्नाले डिजिटल र विद्युतीय अभिलेखमा रहेको कुनै विषय वा त्यसको छापिएको वा भण्डारण गरिएको अप्टिकल वा इलेक्ट्रो-म्याग्नेटिक स्वरूपमा रहेको वा प्रकाशित वा पुनः प्रकाशित भएको डिजिटल र विद्युतीय सामग्री वा त्यस्ता सामग्रीका प्रतिलिपिलाई समेत जनाउँछ, भनी स्पष्ट पारिएको छ। प्रमाण ऐनको दफा ५२ मा यदि अदालतलाई कुनै प्राविधिक पक्ष यकीन गर्न आवश्यक भए अनुसार विशेषज्ञ साक्षी सरह उपस्थित गराई बकाउन सक्छ, जसको पक्षहरूले कानून बमोजिम जिरह गर्ने मौका प्राप्त गर्नेछन्। यस ऐन अनुसार, विशेषज्ञ साक्षीहरूले डिजिटल प्रमाणका मुद्दाहरूमा महत्वपूर्ण भूमिका निभाउँछन्, जहाँ तिनीहरूले आफ्ना विशेषज्ञ राय र गवाही प्रस्तुत गर्दछन्। त्यसैले, विशेषज्ञ साक्षीहरूले डिजिटल फोरेन्सिक अनुसन्धान र आलेखका पछिल्ला विकासहरूसँग अद्यावधिक रहनु आवश्यक छ र अदालतमा आफ्नो विधि, नतिजा र निष्कर्षहरूको बचाउ गर्नका लागि तयारी अवस्थामा रहनु पर्छ।

ङ. राष्ट्रिय साइबर सुरक्षा नीति २०८० (२०२३)

कुनै निश्चित कानून नभए पनि नेपालमा राष्ट्रिय साइबर सुरक्षा नीति छ जसले साइबर अपराध र डिजिटल जानकारीको सुरक्षा लगायत साइबर सुरक्षा चुनौतीहरूलाई सम्बोधन गर्ने रणनीतिहरूको रूपरेखा प्रस्तुत गर्दछ। यो नीतिले साइबर अपराधसँग सम्बन्धित डिजिटल प्रमाणहरू संचालन गर्न मार्गदर्शन गर्न सक्छ।

३.२ सिमानापारको डिजिटल प्रमाणमा राज्य पहुँचको सुविधाः कानूनी रूपरेखा र संयन्त्र

सीमापार मुद्दाहरूमा विदेशबाट डिजिटल प्रमाणहरू अनुरोध गर्न र प्राप्त गर्नको लागि नेपालको कानूनी ढाँचा मुख्य रूपमा अन्तर्राष्ट्रिय सहयोग संयन्त्र र घरेलु कानूनमा निर्भर हुन्छ। नेपालमा यस उद्देश्यका लागि मात्र समर्पित विशेष द्विपक्षीय सन्धि वा कानून नभएकोले पारस्परिक कानूनी सहायता सन्धि (MLATS) र अन्तर्राष्ट्रिय महासन्धिहरू जस्ता संयन्त्रहरू मार्फत पारस्परिक कानूनी सहायता अन्तर्गत संलग्न रहेको छ। MLATS ले डिजिटल प्रमाणको आदानप्रदान लगायतका आपराधिक मामिलाहरूमा अनुरोध र सहयोग गर्ने प्रक्रियाहरू स्थापना गर्छन्, भने साइबर अपराध सम्बन्धी बुडापेस्ट महासन्धि जस्ता अन्तर्राष्ट्रिय सम्मेलनहरूले साइबर खतराहरू विरुद्ध लड्न सहयोगको लागि मापदण्ड प्रस्ताव गरेको पाइन्छ। यद्यपि, नेपालले न त पारस्परिक कानूनी सहयोगका लागि यस्ता द्विपक्षीय सन्धीहरू कार्यान्वयन गरेको छ न त प्रमाण साझेदारीमा सहयोगको लागि अन्तर्राष्ट्रिय वा क्षेत्रीय कानूनको पक्ष नै बनेको छ।

पारस्परिक कानूनी सहायता ऐन अनुसार,[२२] दफा १५ बमोजिम गरिएको अनरोध अनरुप विदेशी राज्यले सो राज्यको कानून बमोजिम प्रमाण बुझ्री केन्द्रीय अधिकारी मार्फत अदालतमा प्राप्त भएको प्रमाण कानून बमोजिम बुझिएको मानी प्रमाणको रुपमा लिन सकिनेछ ।यी शर्तहरू पुरा गरेपछि, कागजातहरूलाई कानून अनुसार प्रमाणको रूपमा स्वीकार गर्न सकिन्छ । अन्ततः यस ऐन बमोजिम पारस्परिक कानूनी सहायताका लागि अनुरोध गर्दा संलग्न गरी पठाइएको प्रमाण कागजहरु न्यायाधीश वा अधिकार प्राप्त सरकारी अधिकृतले प्रमाणित गरी कार्यालयको छाप लगाइएको हुनुपर्नेर्छ अन्यथा सो कागजाहरु लाई प्रमाणको रुपमा मान्यता दिइनेछैन ।[२३]

यद्यपि, नेपालले इन्टरपोल जस्ता संस्थाहरू;Fu ;हकार्य गर्दछ र कानूनी सहायता बढाउन र साइबर अपराधसँग लड्न क्षेत्रीय पहलहरूमा भाग लिन्छ । विदेशबाट डिजिटल प्रमाणका लागि विशेष प्रावधानहरूको अभाव हुन सक्छ, तर घरेलु रूपमा नेपालको कानूनी ढाँचा, फौजदारी कार्यविधि संहिता र प्रमाण ऐन सहितले, अदालतको कार्यवाहीमा डिजिटल प्रमाण स्वीकार गर्ने आधार प्रदान गर्दछन् । यी संयन्त्रहरूको बावजुद, कानूनी प्रणालीहरूमा भिन्नता र स्रोतसाधनको सीमितता जस्ता चुनौतीहरूले सीमापार मुद्दाहरूमा डिजिटल प्रमाण प्राप्त गर्न अन्तर्राष्ट्रिय सहयोगमा प्रभावकारी रूपमा संलग्न हुने नेपालको क्षमतालाई असर गर्न सक्छ ।[२४]

३.३ नेपालको न्यायिक कारवाहीमा डिजिटल प्रमाणको स्वीकार्यता

१. अख्तियार दुरूपयोग अनुसन्धान आयोग सम्पर्क कार्यालय विरूद्ध प्रेमबहादुर थापा[२५]

भ्रष्टाचारको कसुरमा गुप्तचरको प्रयोग गरी अनुसन्धान गर्दा, सङ्कित व्यक्ति उपर सूक्ष्म निगरानी गर्ने, कुनै सेवाग्राही र राष्ट्रसेवक बिच रिसवत लेनदेन भएको अवस्थामा सो रकम बरामद गरी प्रमाण पेस गर्ने, प्रविधिको माध्यमबाट श्रव्य दृश्य तयार पार्ने, आर्जित सम्पत्तिको स्रोत खोज्ने, प्रमाणको वैज्ञानिक सर्ing र परीक्षण गर्ने लगायतका आवश्यक र उपयुक्त तरिका अपनाउनु आवश्यक हुने । यो निर्णयले अनुसन्धान अधिकारीद्धारा प्रस्तुत गरिएको मुद्दालाई समर्थन गर्न डिजिटल रूपमा हुन सक्ने सहायक प्रमाणहरूको आवश्यकतालाई उजागर गर्दछ ।

---

[22] पारस्परिक कानूनी सहायता ऐन, दफा १६

[23] ऐजन दफा ३९

[24] Mark Kersten, Challenges and Opportunities: Audio-Visual Evidence in International Criminal Proceedings Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

[25] निर्णय नं.१०९५८ - भ्रष्टाचार (घुस÷ l/;jt_ भाग: ६४, साल: २०७९, महिना: माघ, अंक: १०, फैसला मिति: २०७८/०८/२१ , ०७५-CR-१४७२

२. बाबुराम अर्यालसमेत विरूद्ध नेपाल सरकार, प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय, सिंहदरबार, काठमाडौं समेत[२६]

स्थापित अन्तर्राष्ट्रिय मान्यता अनुरूप दूरसञ्चार सेवा प्रदायक कम्पनीहरूले कुनै पनि व्यक्तिलाई दूरसञ्चार सेवा उपलब्ध गराउँदा सो व्यक्तिको गोपनीयताको संरक्षण तथा त्यस व्यक्तिसँग सम्बन्धित तथ्याङ्कको संरक्षणको प्रत्याभूति गर्नुपर्ने हुन्छ । कुनै निश्चित कानूनी आदेश वा अग्रिम अधिकार सहितको औपचारिक लिखतको अभावमा अरूको दबाब प्रभाव वा प्रलोभनको भरमा अर्काको सूचना दिन नमिल्ने । निश्चित कानूनी आदेश वा पूर्व स्वीकृति बिना अन्य पक्षहरूलाई जानकारीमा पहुँच दिन असफल हुँदा अन्य व्यक्तिहरूमा अनावश्यक दबाब वा प्रभाव पर्न सक्ने सम्भावना रहन्छ ।

सूचना सेवा प्रदायक संस्थाहरूसँग संग्रहित डाटा बैंक मा व्यक्ति, संस्था र स्वयम् सरकारी निकायहरूको सूचना रहने हुनाले त्यस्तो सूचनाको संरक्षण व्यक्तिको हक हितको सुरक्षाको प्रश्न नभई राज्यकै हित र सुरक्षाको हकमा समेत लागू हुने कुरा हो । राज्यको अंग निकाय वा त्यहाँ कार्य गर्ने पदाधिकारी एवं कर्मचारीहरू सम्बन्धी सूचनालाई राज्यकै अन्य अंग वा निकायले समेत सम्मान र संरक्षण गर्नुपर्ने हुन्छ । त्यसको उल्लङ्घन गर्ने गलत वा आपराधिक चेष्टा गर्नु नहुने ।

३. रुपा सुनार विरूद्ध कृष्ण गोपाल श्रेष्ठ, मन्त्री, शिक्षा विज्ञान तथा प्रविधि मन्त्रालय समेत[२७]

यस मुद्दामा, अदालतले कुनै पनि अनलाइन वार्तालापलाई ईजलास समक्ष प्रस्तुत गर्नुपर्ने प्रक्रियाको बारेमा व्याख्या गरेको छ ।

अदालतले अनलाइन सञ्चार मार्फत गरिएको वार्तलापमा अनधिकृत पहुँच र अन्य डाटा तथा व्यक्तिगत जानकारीको संरक्षणको लागि सुपरिवेक्षण गर्नु पर्ने आदेश भएको देखिन्छ । साथै यस अनुसार सुपरिवेक्षण गर्नको लागि अदालतको सूचना तथा प्रविधि विभागका एक अधिकारी, एक आईटी विशेषज्ञ, र पहुँच प्रक्रियाको क्रममा आवेदक, उनीहरूको प्रतिनिधि, वा उनीहरूको कानूनी सल्लाहकारको उपस्थिति आवश्यक रहेको भनी आदेश भएको छ ।

४. रामबहादुर थापा विरूद्ध अख्तियार दुरूपयोग अनुसन्धान आयोग[२८]

प्रमाण ऐन, २०३१ को भाग ९ मा “पक्षले अदालत बाहेक अन्यत्र व्यक्त गरेको कुनै कुरा निजका विरूद्ध प्रमाणमा लिन हुन्छ“ भन्ने व्यवस्था रहेको छ । पक्षले बोली वचनद्वारा, लेखेर, ईशाराद्वारा वा आचरणद्वारा पनि कुनै कुरा व्यक्त

---

[26] निर्णय नं.९७४० -उत्प्रेषण / परमादेश भाग: ५९, साल: २०७४ महिना: बैशाख अंक: १ फैसला मिति :२०७२/१०/२१ ०६९-WO-०२६८

[27] ०७७ १२३६, उत्प्रेषण, सर्वोच्च अदालत. यो मुद्दामा भेदभाव र छुवाछुतको आरोप सम्बन्धी निवेदन समावेश छ र अदालतले अनुसन्धान अधिकारीलाई संलग्न पक्षहरू बीचको मोबाइल कुराकानीमा उनीहरूको पहुँचलाई कडाइका साथ प्रतिबन्ध लगाउन निर्देशन दिँदै अन्तरिम आदेश जारी गरेको थियो।

[28] निर्णय नं.९८८० - घुस रिसवत लिई भ्रष्टाचार गरेको भाग: ५९, साल: २०७४, महिना: पौस, अंक: ०९, फैसला मिति: २०७३।०९।०४ , ०७१-CR-१०८९

गरेको रहेछ भने सो समेत प्रमाणमा लिन मिल्छ । यसरी व्यक्त गरेको कुरा यदि प्रमाण ऐन, २०३१ को दफा ९(२)(ग) मा व्यवस्थित प्रावधानहरूको प्रतिकूल देखिँदैन भने त्यस्तो कुरालाई प्रमाणमा लिन मिल्ने नै देखिन्छ ।

विद्युतीय माध्यमबाट संकलन गरिएका कुराहरूलाई व्यवस्थित र नियमन गर्ने सम्बन्धमा कानूनले थप प्रष्ट मार्ग निर्देशन गर्नु आवश्यक छ । यस पक्षमा खासगरी प्रमाण लिने कुरामा केही अस्पष्टता रहेको कारणबाट द्विविधा उत्पन्न हुन सक्ने अवस्था पनि रहेको छ । तर यसको तात्पर्य सि.डी. लगायत विद्युतीय माध्यमबाट संकलित प्रमाणलाई मुद्दामा प्रमाणको रूपमा ग्रहण गर्न मिल्दैन भन्ने अवश्य होइन । विज्ञान र प्रविधिको क्षेत्रमा भएको अभूतपूर्व विकास र थपिएका अनेकौ नवीनतम् आयामहरूलाई न्याय निरूपणका सन्दर्भमा अदालतले अनदेखा गर्न नहुने ।

५. सीतादेवी ठाकुर समेत विरुद्ध बुधनी ठाकुर[२९]

यो मुद्दा Identifier Kit प्रयोग गरेर गरिएको डीएनए परीक्षण प्रतिवेदनसँग सम्बन्धित छ, जसमा परीक्षण प्रतिवेदन दिने विशेषज्ञ अदालतमा उपस्थित भई प्रक्रिया विस्तृत रूपमा व्याख्या गर्नुभएको थियो, र विशेषज्ञताको सम्बन्धमा कुनै प्रश्न उठाइएको थिएन । अदालतले स्पष्ट गरेको छ कि जब कुनै सुझाव वा प्रतिवेदन ठोस र वैज्ञानिक तर्कहरू तथा रासायनिक परीक्षणबाट प्राप्त भएको हुन्छ, र विशेषज्ञले प्रक्रिया तथा नतिजा प्रमाणित गरी प्रतिवेदनलाई स्पष्ट र अस्पष्टता बिना पुष्टि गरेका हुन्छन्, त्यस्तो प्रतिवेदनलाई प्रमाणको रूपमा मान्नुपर्छ । यो व्याख्या अन्य डिजिटल प्रमाणहरूको मामिलामा पनि व्यापक रूपमा लागू गर्न सकिन्छ ।

विशेषज्ञको राय वा प्रतिवेदन कुनै कुरा, तथ्य वा घटना प्रमाणित गर्न एक्लो निर्णायक प्रमाण (Single Detrimental Evidence) नभए पनि यो एउटा महत्वपूर्ण प्रमाण हो र अन्य प्रमाणसँग मिलेमा, साक्षी वकपत्र वा पक्षको भनाईसँग मिल्न भिड्न आएमा विशेषज्ञको प्रतिवेदनले ठोस र निर्णायक प्रमाणको रुप ग्रहण गर्ने ।

विशेषज्ञको विशेषज्ञता र दक्षता विवाद रहित हुनुका अतिरिक्त निजले ठीक, निश्चित, असन्दिग्ध वा द्विविधा विहीन ढंगले अदालतमा आई वकपत्र पनि गरेको हुनुपर्ने । विशेषज्ञको राय, प्रतिवेदन निश्चित, ठोस् र वैज्ञानिक तर्कहरू र रसायनिक परीक्षणबाट निकालिएको निष्कर्षहरूमा आधारित रहनुका अतिरिक्त विशेषज्ञले अदालतमा आई परीक्षण प्रक्रिया र निष्कर्ष एवं प्रतिवेदनलाई पुष्ट्याँई हुने गरी स्पष्ट एवं द्विविधा रहित ढंगले वकपत्र गरी दिएको अवस्था भएमा यस्तो प्रतिवेदनलाई प्रमाणको रुपमा ग्रहण गर्नुपर्ने ।

---

[29] ने.का.प.२०६७, अंकः ११, निर्णय नं. ८५०१

६. नेपाल सरकार विरूद्ध उर्मिला बोट[३०]

मृतकले आफू मर्ने बेलामा आफ्नो मृत्युको कारण सम्बन्धमा बोलेको कुरालाई प्रहरी कर्मचारीले नै आफ्नो मोबाइलमा रेकर्ड गरी, रेकर्ड भएको बेहोरा मैले रेकर्ड गरेको हो, मृतक सिरियस भई रोकिई रोकिई बोलेकी थिइन् भनी अदालतमा उपस्थित भई बकपत्र गरी प्रमाणित गरिदिएको अवस्थामा उक्त श्रव्य रेकर्डलाई मृत्युकालीन घोषणा (dying declaration) को परिभाषा भित्र नपर्ने भन्न नमिल्ने । यो एउटा उदाहरण हो, जहाँ अदालतले अडियो रेकर्डलाई प्रमाणको रूपमा अर्थात् 'मृत्युअघिको घोषणा' का रूपमा लिई, डिजिटल प्रमाणको स्रोत पुष्टि गर्न सकिएमा अदालतले त्यसलाई प्रमाणको रुपमा स्वीकार गर्न सक्दछ, भनी व्याख्या गरिएको छ ।

७. बमबहादुर बस्नेतसमेत विरूद्ध नेपाल सरकार[३१]

फोटो, भिडियो, अडियो, सीडी आदि डिजिटल सामग्री लिखत हुन् । यिनको प्रामाणिक मूल्यलाई अस्वीकार गर्नु न्यायसङ्गत हुँदैन । प्रमाणका प्रत्येक टुक्रा वैध हुन्छन् । मुद्दाका कुनै पक्षबाट फोटो, भिडियो, अडियो, सीडी आदि डिजिटल प्रति प्रमाणका रूपमा प्रस्तुत हुन्छन् र अर्को पक्षबाट तिनमा इन्कारी जनाइदैन भने लिखित प्रमाणका रूपमा यी ग्राह्य हुन्छन् । यस्ता प्रमाणका विषयमा विवाद उठेमा तिनको सत्यता परीक्षणको विषय बन्दछ । अन्यथा लिखत प्रमाणका आधुनिक स्वरूपलाई सतर्कता साथ ग्रहण गर्दै जानुपर्ने ।

८. मखमली मिश्र समेत विरुद्ध लक्ष्मीकुमारी मिश्र (श्रेष्ठ)[३२]

परीक्षण प्रतिवेदन प्राप्त भएको अवस्थामा तथा सो परीक्षण गर्ने विशेषज्ञले आफ्नो परीक्षण र प्रतिवेदनको आधिकारिकता एवं यथार्थता को सम्बन्धमा अदालतमा साक्षीसरह बकपत्र गरी दिएको अवस्थामा सो वकपत्र जिरहको माध्यमद्वारा अन्यथा देखिन नआए अदालतले त्यस्तो वैज्ञानिक परीक्षण प्रतिवेदनलाई अमान्य गर्ने कानूनी आधार नदेखिने । जिरह समेतबाट अन्यथा देखिन नआएको विशेषज्ञको रायलाई प्रमाण ऐन, २०३१ को दफा २३(७) बमोजिम अदालतले प्रमाणको रुपमा ग्रहण गर्नुपर्ने हुन्छ ।

यस मुद्दाले अदालतमा परीक्षण गर्ने विशेषज्ञले दिएको डीएनए परीक्षण रिपोर्टको रायलाई मान्य प्रमाणको रुपमा स्वीकार गर्नुपर्ने कुरालाई जोड दिएको पाइन्छ । अदालतले डीएनए परीक्षण रिपोर्टलाई जनाउन "वैज्ञानिक परीक्षण रिपोर्ट" शब्द प्रयोग गरेको छ, र यो वाक्यांशलाई व्यापक रूपमा, अन्य वैज्ञानिक तथ्यांकहरू ;मावेश गर्ने गरि व्याख्या गर्न सकिन्छ, जुन प्रमाणको रूपमा अदालत समक्ष पेश गर्न सकिन्छ ।

---

[30] ने.का.प.२०७८, अंक: ११, निर्णय नं. १०७७३

[31] ने.का.प.२०७०, अंक: ६, निर्णय नं. ९०२२

[32] ने.का.प.२०६७, अंक: १०, निर्णय नं. ८४८३

९. अशोकराम महरा विरुद्ध छोटेलाल राम[३३]

विशेषज्ञको राय न्यायकर्तालाई निष्कर्षमा पुग्न सहयोग गर्ने आधार अवश्य हो । तर, विशेषज्ञको रायलाई एक मात्र निश्चयात्मक प्रमाण मानी अन्य प्रमाणलाई उपेक्षा गर्नु न्यायसंगत हुँदैन । अन्य भरपर्दा प्रमाणको विपरीत विशेषज्ञको राय भएमा न्यायकर्तालाई विशेषज्ञको राय प्रतिकूल निष्कर्ष निकाल्न आपत्ति नहुने ।

१०. रामबहादुर बस्नेत विरुद्ध नेपाल सरकार [३४]

मिसिल संलग्न प्रमाण वा वस्तुस्थितसँग मेल नखाने विशेषज्ञको राय प्रमाणमा लिन नमिल्ने । मिसिल संलग्न प्रमाणलाई नजरअन्दाज गरी न्यायकर्ताले विशेषज्ञको रायलाई बाध्यात्मक रुपमा स्विकार गर्नै पर्दछ भनी न्यायकर्ताको विवेकलाई बन्धक बनाउन नमिल्ने । प्राविधिक कुरामा सम्वन्धित विषयका विशेषज्ञको विज्ञतालाई सहजै इन्कार गरिदैन । तर विशेषज्ञको राय मिसिल संलग्न वस्तुस्थिती एवं सबुद प्रमाणसँग मेल नखाने र वारदातवाट स्थापित तथ्यभन्दा ज्यादै नै पृथक भई शंकास्पद देखिन्छ भने त्यसलाई अस्विकार गर्न सकिने । भैरहेको कानूनी प्रावधानको उपेक्षा गरी वा गलत अर्थ लगाइ विशेषज्ञको रायलाई प्रमाणमा लिइनु पर्ने भन्ने जिकिर ग्रहणयोग्य नदेखिने ।

उल्लेख गरिएका मुद्दाहरूले न्यायिक कारबाही र कानूनी सिद्धान्तका धेरै महत्त्वपूर्ण पक्षहरूलाई हाइलाइट गर्दै नेपालको कानूनी परिदृश्यको विस्तृत दृष्टिकोण प्रस्तुत गर्दछ । सर्वप्रथम, यि मुद्दाहरुमा व्यक्तिगत अधिकार र गोपनीयताको संरक्षणमा बलियो जोड दिइएको पाइन्छ । यी मुद्दाहरुले कानूनको सीमाभित्र अनुसन्धान सञ्चालन गर्ने तथा अपराध रोकथाम र पत्ता लगाउने सन्दर्भमा पनि गोपनीयता अधिकारको सम्मान गर्ने महत्वलाई जोड दिन्छ । त्यसै गरी, अनुसन्धान प्रक्रियाको क्रममा पक्षहरूको गोपनीयता र डाटा सुरक्षाका मुद्दाहरूलाई सम्बोधन गर्न सर्वोच्च अदालतको सक्रिय दृष्टिकोणको महत्वलाई पनि उजागर गरेको छ । आफ्नो निर्देशनहरू मार्फत, अदालतले व्यक्तिको अधिकारको सम्मान गर्न र कानूनी प्रक्रियाको अखण्डता कायम राख्न अनिवार्य रूपमा पूर्ण अनुसन्धानको आवश्यकतालाई सन्तुलनमा राख्न खोजेको देखिन्छ ।

दोस्रो, विद्युतीय प्रमाणहरू, जस्तै सीडी र अडियो रेकर्डिङहरू, प्रमाणहरूको वैध रूपहरूको रूपमा मान्यताले न्यायपालिकाको प्राविधिक प्रगतिहरूको मान्यता र कानूनी कार्यवाहीमा तिनीहरूको सान्दर्भिकतालाई संकेत गर्दछ । यो मान्यताले विद्युतीय प्रमाणहरूको सIng, स्वीकार्यता र प्रामाणिकतामा स्पष्ट दिशानिर्देशहरूको आवश्यकतालाई प्रतिबिम्बित गर्दछ ।

---

[33] ने.का.प. २०६८,अंक: ३,निर्णय नं. ८५८२

[34] ने.का.प. २०६८ अंक: ७ निर्णय नं. ७९८५

यसबाहेक, अदालतको कार्यवाहीमा विशेषज्ञ रायको महत्व धेरै मुद्दाहरूमा प्रकाश पारिएको छ। ठोस प्रमाण र वैज्ञानिक विश्लेषणद्वारा समर्थित हुँदा विशेषज्ञ रायहरू मूल्यवान मानिन्छन्, तथा अदालतमा प्रस्तुत गरिएका अन्य प्रमाणहरूको पूरक हुने गरी अन्तर्दृष्टि समेत प्रदान गर्दछ।

अन्तमा, श्रव्यदृश्य प्रमाणहरूले सामूहिक अपराधहरूमा जवाफदेहितालाई अगाडि बढाउने अवसरहरू प्रस्तुत गरेतापनि, अदालतमा यसको प्रभावकारिता सुनिश्चित गर्न यसको उचित सङ्कलन, संरक्षण र प्रमाणीकरण आवश्यक छ। प्रविधीको विकास जारी रहँदा, अभ्यासकर्ताहरू डिजिटल र खुला स्रोत प्रमाणहरूद्वारा उत्पन्न अद्वितीय चुनौतीहरूलाई सम्बोधन गर्न सतर्क रहनुपर्छ।

समग्रमा, यी मुद्दाहरूले नेपालमा न्याय प्रशासनमा व्यक्तिगत अधिकार, प्राविधिक विकास र कानूनी सिद्धान्तहरू बीच सन्तुलन कायम गर्ने महत्वलाई जोड दिन्छन्। तिनीहरूले कानूनी अभ्यासहरूको विकासशील प्रकृति र निष्पक्षता, अखण्डता र कानूनी शासनलाई कायम राख्दै आधुनिक चुनौतीहरूसँग अनुकूलन गर्ने न्यायपालिकाको प्रयासलाई प्रतिबिम्बित गर्दछन्।

४. डिजिटल प्रमाणको कानूनी मान्यता

४.१ डिजिटल प्रमाणको मान्यताका लागि पूर्वावश्यक आधारहरु

क. डिजिटल डाटा प्रमाणका रूपमा प्रस्तुत गर्ने प्रक्रिया

डिजिटल प्रमाणलाई अदालतमा स्वीकार्य बनाउन, कानूनी र प्राविधिक रूपमा केही पूर्वावश्यकताहरू पूरा हुन आवश्यक छ।[35] कानूनी रुपमा, अदालतले डिजिटल जानकारीको खोजी र जफतको लागि दिइने अनुमति तथा डिजिटल प्रमाणको सान्दर्भिकता, प्रामाणिकता, अखण्डता र विश्वसनीयताको जाँच गर्दछ। प्राविधिक रुपमा, अदालतले डिजिटल फरेन्सिक प्रक्रिया, उपकरणहरू, प्रयोगशालाहरू, फरेन्सिक प्रतिवेदनहरू लगायत फरेन्सिक विश्लेषक र विशेषज्ञ (एक्सपर्ट विटनेस) हरूको योग्यताको मूल्याङ्कन गर्दछ। अनधिकृत खोजी र जफतद्वारा सङ्कलित डिजिटल प्रमाणलाई "विषालु रूखको फल" भनी चुनौती गर्न सकिन्छ र त्यस्ता प्रमाणहरु अदालतमा स्वीकार्य हुँदैनन्। त्यस्तो प्रमाणले गोपनीयता सुनिश्चित गर्ने र फौजदारी न्यायिक प्रक्रिया निष्पक्ष बनाउने कानूनी मापदण्डहरूको उल्लङ्घन गर्दछन्। अवैध रूपमा प्राप्त प्रमाण स्वीकार गर्नुले न्यायिक प्रक्रियामा जनताको विश्वास कम गर्दछ, अधिकारको दुरुपयोगलाई

---

[35] Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. https://doi.org/10.1007/978-3-319-67208-3_2

प्रोत्साहन दिन्छ र भविष्यमा गरिने अनुसन्धानका लागि नकारात्मक उदाहरण स्थापना गर्दछन् । त्यसैले कानूनको शासनलाई कायम राखी व्यक्तिगत अधिकारहरूको सुरक्षा गरिनु अत्यन्त जरुरी छ । न्याय प्रणालीको अखण्डता कायम राख्न र अनुचित खोजतलासी विरुद्धको व्यक्तिको संवैधानिक अधिकारको रक्षा गर्नका लागि नै यो अवधारणा आवश्यक पर्दछ ।

ख. डिजिटल प्रमाणको मूल्याङ्कन

यस चरणमा अदालतले, सूचना तथा सञ्चार प्रविधि (ICT) र सम्बन्धित डाटाको खोजी र जफतका लागि उचित कानूनी अधकिार प्राप्त भएको छ वा छैन भनी निर्धारण गर्दछ । यस्तो अनुमति प्रायः खानतलासी पुर्जी (सर्च वारेन्ट), अदालतको आदेश वा समाह्वानको रूपमा प्राप्त हुन्छ । कानून र मुद्दाको प्रकृतिका आधारमा यी आदेशहरूको आवश्यकता फरक-फरक हुन्छ । सूचना तथा सञ्चार प्रविधि (ICT) जफत गर्नका लागि प्रायः खानतलासी पुर्जी प्रयोग गरेको पाईन्छ, यद्पी कानूनी आदेशका आवश्यकताहरू भने अन्य न्यायिक क्षेत्रहरुमा फरक-फरक हुन सक्छन् र ती भिन्नताहरू मुद्दाको परिस्थिति, खोजतलासी संचालन गर्ने व्यक्तिहरूको योग्यता जस्ता आधारहरुमा निहित हुन्छन् ।

साथै, यस चरणमा डिजिटल प्रमाणको फरेन्सिक सान्दर्भिकताको समेत मूल्याङ्कन गरिन्छ जसमा प्रमाणले अपराधी र पीडित, घटनास्थल वा डिजिटल उपकरणबीचको सम्बन्ध स्थापित गर्छ वा गर्दैन भन्ने कुराको जाँच गरिन्छ । यसमा, प्रमाणले साक्षीहरूको बयानलाई समर्थन गर्ने वा खण्डन गर्ने, अपराधीको पहिचान गर्ने, अनुसन्धानको चरणलाई अधि बढाउन सहयोग गर्ने, अपराधको कार्यविधि (मोडस अपरेन्डाई) लाई प्रस्ट्याउने र अपराध घटेको तथ्यलाई पुष्टि गर्ने जस्ता कार्य गरेको छ वा छैन भन्ने कुराको पनि जाँच गरिन्छ ।[३६]

ग. डिजिटल प्रमाणको परीक्षण

यस चरणमा, डिजिटल प्रमाणको अखण्डता (इन्टेग्रीटी) परिक्षण गर्नका लागि सो प्रमाण प्राप्त गर्न प्रयोग गरिएका डिजिटल फोरेन्सिक प्रक्रिया र उपकरणहरूको जाँच गरिन्छ । साथै, प्रमाण प्राप्ति, संरक्षण र विश्लेषणमा संलग्न डिजिटल फोरेन्सिक विशेषज्ञहरूको योग्यता र क्षमताको समेत मूल्यांकन गरिन्छ। वैज्ञानिक सिद्धान्तहरूका आधारमा प्रमाणको संरक्षण, प्राप्ति र विश्लेषण भएको हो र प्रमाणको नियन्त्रण र परीक्षणमा समेत आवश्यक मापदण्डहरुको पालना गरिएको छ भनि सुनिश्चित गर्नु नै यस मूल्याङ्कनको उद्देश्य रहेको छ ।

डिजिटल फोरेन्सिक विशेषज्ञहरूले अदालतमा आफ्नो योग्यताको स्पस्टिकरण दिन, डिजिटल उपकरणहरू र ICT सम्बन्धित स्रोतहरूले काम गर्ने तरिका बताउन, डिजिटल फोरेन्सिक प्रक्रियाको रुपरेखा प्रस्तुत गर्न, विशेष खालको डिजिटल फरेन्सिक उपकरणको चयनको कारण देखाउन, डिजिटल प्रमाण कसरी सुरक्षित, प्राप्त र विश्लेषण गरियो

---

[36] US National Institute of Justice; 2004a; Maras, 2014

भन्ने विवरण दिन, छानविनको निष्कर्षको व्याख्या गर्न, ती व्याख्याहरूको सटीकताको मूल्यांकन गर्न र डाटामा भएका केही परिवर्तन तथा तिनको कारण उल्लेख गर्नका लागि बयान दिने गर्छन् ।

प्रमाण नियन्त्रण गर्ने र विश्लेषण गर्ने व्यक्तिहरूको क्षमताको विश्वसनीयता सुनिश्चित गर्नका लागि डिजिटल फोरेन्सिक विशेषज्ञहरूको योग्यता पनि परीक्षण गरिन्छ । त्यस्तो योग्यता भने कार्य उत्पादनको गुणस्तरलाई सुनिश्चित राख्न र उत्पादित नतिजालाई विश्वसनीय बनाउनका लागि आवश्यक छ । डिजिटल फोरेन्सिक विशेषज्ञहरूको योग्यताको विश्वव्यापी मापदण्ड तोकिएको छैन जसले गर्दा योग्यता मापदण्ड र प्रमाणपत्रको आवश्यकता देश पिच्छे फरक पर्न जान्छ । यस चरणमा विशेषज्ञहरूको ICT र ICT-सँग सम्बन्धित डाटा परीक्षण गर्न र विशेषज्ञको रूपमा कार्य गर्न आवश्यक योग्यता छ वा छैन र तिनको योग्यता प्रमाणित र परीक्षण गरिएको हो वा होईन भन्ने मूल्यांकन गर्दछ ।[३७]

घ. डिजिटल प्रमाणको निर्धारण

यस चरणमा, अघिल्लो चरणमा गरिएको मूल्यांकनको आधारमा डिजिटल प्रमाणको प्रामाणिकता, अखण्डता र विश्वसनीयताको मूल्यांकन गरिन्छ । यसमा, फरेन्सिक रुपमा उपयुक्त विधि र उपकरणहरूको प्रयोगको प्रमाणीकरण र प्रमाणको विश्वसनीयता पुष्टि गर्न विशेषज्ञको रायमा भर पर्ने कुराहरू समावेश हुन्छन् । स्वीकार्य डिजिटल प्रमाणले सान्दर्भिक तथ्यहरू:थापित गर्नुपर्छ, फरेन्सिक प्रक्रिया भरि अपरिवर्तित रहनुपर्छ र वैध तथा सहकर्मी-समीक्षा (पियर रिभ्यू) गरिएका परिणामहरूद्वारा समर्थित हुनुपर्छ । छानबिनको निष्कर्षको व्याख्या निष्पक्ष हुनु आवश्यक छ र साथसाथै त्यस निष्कर्षमा समावेश त्रुटि वा सो को सीमा समेत खुलासा गरिएको हुनुपर्छ । समग्रमा, यो तीन-चरण मोडेलले डिजिटल प्रमाण स्वीकार्यताको लागि कानूनी र प्राविधिक मापदण्डहरूलाई सामञ्जस्य गर्दै अन्तर्राष्ट्रिय साइबर अपराधको सामना गर्न मानंकीकृत डिजिटल फोरेन्सिक अभ्यासहरूको आवश्यकतालाई जोड दिन्छ ।

४.२ डिजिटल प्रमाणको स्वीकार्यतामा चुनौतीहरू

खानतलासी पुर्जी र जफत पूर्जीहरू (वारेन्ट) डिजिटल फरेन्सिक अनुसन्धानका महत्वपूर्ण आधारहरू हुन् जसले अदालतमा डिजिटल प्रमाण संकलन र स्वीकार्यतामा धेरै चुनौतीहरू;[जना गर्ने गर्छन् । डिजिटल प्रमाणको संकलन र अनुसन्धानमा पूर्जि वा न्यायिक जाँच संयन्त्र नभएमा अनुसन्धान स्वेच्छाचारी, अनुपातहीन र आवश्यकता भन्दा बाहिर जान सक्छ । अनुसन्धानकर्ताहरू साइबर घटनास्थलमा पुग्नु अघि अदालतले जारी गर्ने खानतलासी पुर्जीले कानून कार्यान्वयन तथा डिजिटल फरेन्सिक टोलीहरूलाई प्रमाण संकलन गर्न अधिकार दिन्छ भने जफत पूर्जीले अनुसन्धानकर्तालाई नियन्त्रणको श्रृंखला सुनिश्चित गर्न जफत पछि गरिएका सबै गतिविधिहरू दस्तावेजीकरण गर्न अधिकार दिन्छ । प्राविधिक

---

[37] Brezinski and Killalea, 2002; US National Institute of Justice, 2004a; European Network of Forensic Science Institute, 2015

चुनौतीहरूमा नेटवर्क सुरक्षा, पुराना उपकरणहरू र अनुसन्धानकर्ता माझ विशेषज्ञताको कमी जस्ता समस्याहरू समावेश छन् । प्रामाणिक, सटीक र विश्वसनीय प्रमाणको माग, साइबर अपराध कानूनको कार्यान्वयनमा रहेका कमी साथै प्रक्रियागत असंगतिहरू/सरोकारवालाहरूको हस्तक्षेपका कारण पूर्जी प्राप्त गर्न र कार्यान्वयन गर्नमा आउने कठिनाइहरू कानूनी चुनौतीमा पर्दछन् । पर्याप्त कानूनी प्रावधानहरूको अभावमा, डिजिटल प्रमाणहरूको अखण्डता र प्रामाणिकता प्रश्नयोग्य बन्न पुग्छ । सम्बन्धित व्यक्तिले गोपनीयताको अधिकारको उल्लंघनको सामना गर्नुपर्ने अवस्था आउन सक्छ । कानूनी परिणामहरूमा अनिश्चितता हुनेछ र अविश्वसनीय प्रमाणहरूको स्वीकृतिको प्रवृत्ति आउन सक्छ । प्राविधिक गलत व्याख्याहरूले गर्दा व्यक्तीको आफुविरुद्धको कुनै पनि प्रमाणलाई चुनौती दिने उचित अवसर गुम्न सक्छ । एक भन्दा बढी क्षेत्राधिकार समावेश भएका अपराधहरुमा फरक नियम वा नियमको अभावले डिजिटल प्रमाणहरूको प्रमाणिक मूल्यलाई कमजोर बनाउँछ जसले गर्दा अन्तर्राष्ट्रिय सहकारितामा कठिनाईहरु उत्पन्न हुन सक्छ ।

क. प्रामाणिकता

डिजिटल प्रमाण अदालतमा प्रयोग योग्य र स्वीकार्य हुनका लागि डिजिटल फेरेन्सिक अनुसन्धानमा डिजिटल प्रमाणलाई अपरिवर्तित राख्नु र प्रमाण संकलनका क्रममा उचित प्रक्रिया पालन गर्नु अत्यन्त आवश्यक छ । डिजिटल डेटा विभिन्न अवस्थामा रहन सक्छ, जस्तै स्थिर (at rest), सक्रिय (active), मेटिएको (deleted), लुकाइएको (hidden), एन्क्रिप्टेड (encrypted), वा ओभरराइट गरिएको (overwritten)। यी सबैले कानूनी कारबाहीका लागि र प्रमाणको विश्वसनीयता कायम गर्न महत्वपूर्ण भूमिका खेल्छन् । अनिश्चितताको अवस्थामा, आंशिक रूपमा ओभरराइट वा परिवर्तन भएको प्रमाणलाई पनि न्यायिक मापदण्डहरूको अनुसार सटीक र विश्वसनीय नतिजा सुनिश्चित गर्न उपयोग गर्न सकिन्छ ।

ख. सटिकता

सटिक डिजिटल फोरेन्सिक अनुसन्धानमा कानूनी रूपमा मान्य नियन्त्रणको श्रृंखलाको संलेखलाई कडाइका साथ पालना गर्न र, जफत पूर्व र पश्चात प्रमाणको विश्वसनीयता र एकरूपता सुनिश्चित गर्न आवश्यक छ । यसमा प्रमाण संकलन, संरक्षण र भण्डारण प्रक्रियाहरूको विस्तृत दस्तावेजीकरण र साथसाथै वैज्ञानिक सिद्धान्तहरूको आधारमा विश्लेषण पनि पर्दछ । प्राय, सटिक अनुसन्धान प्रक्रिया कायम राख्ने क्रममा चुनौतीहरु उत्पन्न हुन्छन् जसको कारण अदालतमा प्रमाणहरु स्वीकार्य हुदैंनन् । यसलाई कम गर्न नाम, मिति, समय, प्रश्न, निष्कर्ष र अनुमानहरू;मावेश गरी प्रत्येक गतिविधिको विस्तृत अभिलेख राख्न आवश्यक हुन्छ । प्रमाण संरक्षणका विधिहरू घटनास्थल र फरेन्सिक ल्याबमा फरक हुन्छन जसका निम्ति फरक प्रणालीको आवश्यकता पर्छ । डिजिटल प्रमाणलाई अचूक मानिए पनि, अनुसन्धानकर्ताले कानूनी विधि र उपकरणहरू प्रयोग गरेर प्रमाण पत्ता लगाउनुपर्छ । यद्यपी, लाइभ विश्लेषणको क्रममा प्रणाली बन्द हुनु वा डेड विश्लेषणको समयमा ट्रान्जिटको क्रममा प्रमाणको छेडछाड हुनु जस्ता केही अनिश्चितताहरूका कारण प्रमाणको प्रामाणिकता र शुद्धता खल्बलिन सक्छ ।

ग. पूर्णता

डिजिटल प्रमाण संकलन प्रक्रियामा प्रमाणको वास्तविकता र सटिकता सुनिश्चित गर्न नियन्त्रणको श्रृंखलाको आवश्यकता पर्छ । कानूनी आवश्यकताले अनुसन्धान प्रक्रिया सहित प्रयोग भएका उपकरणहरू र निर्माण गरिएका अनुमानहरू ;हित प्रत्येक प्रमाणको नम्बरको विस्तृत दस्तावेजीकरणको माग गर्छ । निर्विवाध रुपमा प्रमाणको वैधानिकता सुनिश्चित गर्न विज्ञद्वारा गरिएको समीक्षा अनिवार्य छ । अनुसन्धानकर्ताहरूले घटनास्थल र प्रयोगशालामा प्रमाणको पहिचान र संरक्षणका लागि अपनाइएका प्रक्रियाहरूको स्पष्ट व्याख्या गर्नुपर्छ ।

घ. विश्वसनीयता

न्यायाधीशहरूका लागि डिजिटल प्रमाण विश्वसनीय बनाउनका निम्ति ती प्रमाणहरुले शंकारहित तवरबाट स्वीकार्यताको उच्च मापदण्ड पूरा गरेको हुन पर्दछ । मेहनतका साथ गरिएको डिजिटल फोरेन्सिक अनुसन्धानले कानूनी मापदण्डहरू पूरा गर्दै प्रमाणको प्रामाणिकता, शुद्धता र पूर्णता सुनिश्चित गरेको हुन्छ । न्यायाधीश वा फैसला गर्ने व्यक्तीको पृष्ठभूमि विविध हुने भएकाले सो कुरालाई ध्यानमा राखी प्रमाणलाई प्राविधिक रूपमा जटिल नबनाई प्रस्तुत गर्नुपर्छ । डिजिटल प्रमाणले डिजिटल घटनाहरूलाई र वैज्ञानिक विधिहरू प्रयोग गरी परीक्षण गरिएका अन्य विकसित अनुमानहरू (हाइपोथेसिस) लाई प्रस्ट्याउँदछ ।

५. डिजिटल प्रमाणको मान्यता र कार्यान्वयन सम्बन्धी अन्तर्राष्ट्रिय अभ्यासहरू

अन्तर्राष्ट्रिय आपराधिक प्रहरी संगठन (इंटरपोल) द्वारा आयोजित र हडकª विश्वविद्यालयद्वारा सञ्चालित एक अनुसन्धान प्रतिवेदनले उजागर गरे अनुसार, डिजिटल प्रमाणले विभिन्न एशियाली देशहरूमा आपराधिक अनुसन्धान र अभियोजनमा महत्वपूर्ण भूमिका खेल्दछ ।[38]

क. बंगलादेश:

बंगलादेशमा, सम्बन्धीत् नजिरले भिडियो र अडियो रेकर्ड गरिएका प्रमाणलाई प्रमाण ऐन (१८७२) अन्तर्गतको “दस्तावेज” को परिभाषाभित्र पर्ने मान्यता दिन्छ । द्रुत सुनुवाई न्यायाधिकरण ऐन (Speedy Trial Tribunal Act) ले विद्युतीय रूपमा रेकर्ड गरिएका प्रमाणलाई स्पष्ट रूपमा स्वीकार गर्छ, तर अदालतले यस प्रमाणको आधारमा मात्र अभियुक्तलाई दोषी ठहऱ्याउन मिल्दैन । सूचना तथा सञ्चार प्रविधि ऐन (२००६) (ICTAB) र डिजिटल सुरक्षा ऐन

---

[38] Interpol, “एशियामा अभियोजनमा डिजिटल प्रमाणको प्रयोग, बंगलादेश, भूटान, ब्रुनेई, कम्बोडिया, माल्दिभ्स, मंगोलिया, नेपाल, श्रीलंका र भियतनाममा आपराधिक कार्यवाहीमा डिजिटल प्रमाणको स्वीकृति र प्रयोगलाई नियमन गर्ने कानून र नीतिहरूको तुलनात्मक अध्ययन“

(२०१८) (DSAB) बंगलादेशमा साइबर अपराध समाधान गर्न लागू गरिएका थिए। विद्युतीय स्वरूपमा डिजिटल रूपमा रेकर्ड गरिएको बयान प्रमाण ऐन अन्तर्गतको लिखित बयानको रूपमा योग्य हुन्छ भनी ICTAB ले स्पष्ट रूपमा प्रस्ट पारेको छ। DSAB ले डिजिटल प्रमाणको फरेन्सिक अनुसन्धानलाई नियमन गर्ने प्रक्रियाहरूको स्थापना गरेको हो। ICTAB अन्तर्गत स्थापना गरिएको साइबर न्यायाधिकरणले DSAB अन्तर्गत प्राप्त वा संकलित "फोरेन्सिक प्रमाण" लाई स्वीकार गर्न सक्ने छ।

ख. भुटान

भुटानको प्रमाण ऐन (२००५) मा "प्रमाण" को परिभाषामा विद्युतीय कागजात र अभिलेखहरू समावेश छन्। दस्तावेजलाई रेकर्ड वा संकलन गर्ने विद्युतीय दस्तावेज प्रणालीको सुरक्षा वा अखण्डता सम्बन्धी वास्तविक प्रश्न उठेमा अदालतले उक्त विद्युतीय दस्तावेजलाई अस्वीकार गर्न सक्छ। यद्यपि, कसैबाट सुनेको भरमा प्राप्त प्रमाण (हेअर्से) अस्वीकार्य भए पनि, अदालतसँग उक्त प्रमाण स्वीकार गर्ने व्यापक विशेषाधिकार रहेको छ। सूचना, सञ्चार र मिडिया ऐन, २०१८ (The Information, Communications and Media Act, २०१८) ले डाटा सन्देश (मेसेज) र विद्युतीय कागजातहरूलाई कानूनी मान्यता प्रदान गरेको छ।

ग. ब्रुनाई

ब्रुनाईको प्रमाण ऐन (२०१४ संस्करण) मा "दस्तावेज" को परिभाषामा कम्प्युटरद्वारा रेकर्ड गरिएको, भण्डारण गरिएको, प्रशोधन गरिएको, पुनःप्राप्त गरिएको, वा उत्पादन गरिएको कुनै पनि विषयवस्तुलाई समावेश गरेको पाइन्छ। यद्यपि, सुनेको भरमा प्राप्त प्रमाण (हेअर्से) अस्वीकार्य भए पनि, प्रमाण ऐन र कम्प्युटर दुरुपयोग ऐन (२००७ संस्करण) (Computer Misuse Act) दुवैले केही शर्तहरूको अधीनमा कम्प्युटरद्वारा उत्पादन गरिएका कथन (statement) हरूलाई सत्य प्रमाणित गर्नका लागि स्वीकार गर्ने अनुमति दिन्छ। कम्प्युटरद्वारा उत्पादन गरिएको दस्तावेज लाई दिइने महत्वको मूल्याङ्कन गर्दा, अदालतले सबै परिस्थितिहरू विचार गर्नुपर्छ। यसमा, सूचना कम्प्युटरमा उपलब्ध गराइएको समयमा तथ्यहरूको घटनासँग समकालीन समबन्ध थियो कि थिएन भन्ने कुरा र सूचना उपलब्ध गराउने व्यक्तिसँग तथ्यहरू लुकाउने वा गलत रूपमा प्रस्तुत गर्ने कुनै मनसाय थियो कि थिएन भन्ने कुरा समावेश हुन्छ।

घ. कम्बोडिया

कम्बोडियाको फौजदारी कार्यविधि संहिता (Cambodia's Code of Criminal Procedure) ले कानूनमा अन्यथा व्यवस्था गरिएको अवस्थामा बाहेक सबै प्रकारका प्रमाणलाई मान्य ठान्दछ। विद्युतीय वाणिज्य ऐन, २०१९ (The Law on Electronic Commerce, २०१९) ले कानूनी कारवाहीमा डिजिटल प्रमाणलाई केवल विद्युतीय अभिलेखको रूपमा भएको आधारमा अस्वीकृत गर्न नपाइने व्यवस्था गर्दछ। साइबर अपराध ऐनको मस्यौदा अझै पारित हुन बाँकी छ।

कम्बोडियाको असाधारण न्यायालय (Extraordinary Chambers in the Courts of Cambodia) को निर्णयले, प्रमाण पुनरावृत्त भएको र प्रमाणिकता पुष्टि गर्न लामो अनुसन्धान आवश्यक पर्ने भएको भनी एक कथित सोधपुछ केन्द्रको फिल्म फुटेजलाई प्रमाणका रूपमा अस्वीकार गरेको थियो ।

ङ. माल्दिभ्स

माल्दिभ्सको प्रमाण ऐन (१९७६) अझै सुधार हुन बाँकी छ, यद्यपी अदालतले यस ऐनका प्रासंगिक प्रावधान अन्तर्गत डिजिटल प्रमाणलाई स्वीकार गर्दछ। डिजिटल प्रमाणको स्वीकृतिको प्रावधान भएको नयाँ प्रमाण विधेयक हाल संसदमा विचाराधीन छ ।

च. मंगोलिया

मंगोलियाको फौजदारी कार्यविधि ऐन, २००२ (Criminal Procedure Law,२००२)ले अपराधको परिस्थितिसँग सम्बन्धित तथ्य र जानकारी यस ऐन अनुसार प्राप्त भएमा प्रमाणको रूपमा मान्यता दिन्छ । यस ऐनले अडियो र भिडियो रेकर्डिङ (यी रेकर्डिङबाट प्राप्त वा उत्पादन गरिएका फोटोहरू सहित) लाई "दस्तावेज" को रूपमा मान्यता दिन्छ र विद्युतीय रेकर्डिङहरु प्रमाणलाई सुदृढ गर्न प्रयोग गर्न सकिनेछ ।

छ. श्रीलंका

श्रीलंकाको प्रमाण (विशेष व्यवस्था) ऐन, १९९५ (Evidence (Special Provisions Act ,१९९५) ले अडियो-भिजुअल रेकर्डिङ र कम्प्युटरद्वारा उत्पादित बयानहरू जस्ता डिजिटल प्रमाणको स्वीकार्यताको व्यवस्था गरेको छ । विद्युतीय कारोबार ऐन, २००६ (Electronic Transactions Act,२००६) ले डाटा सन्देश (म्यासेज), विद्युतीय दस्तावेज, विद्युतीय अभिलेख वा अन्य सञ्चारमाध्यममा समावेश गरिएको जानकारीको स्वीकृतिका लागि थप प्रावधानको व्यवस्था गरेको छ । दुवै कानूनले, अन्यथा प्रमाणित नभएसम्म विद्युतीय दस्तावेज वा अभिलेखमा समावेश जानकारीलाई अदालतले सही वा सत्य ठान्न सक्ने व्यवस्था गरेको पाइन्छ। कम्प्युटर अपराध ऐन, २००७ (The Computer Crime Act, २००७) ले नयाँ साइबर अपराधहरू सिर्जना गरेको छ र कम्प्युटर डाटा प्राप्त गर्ने अधिकार पनि प्रदान गरेको छ।

ज. भियतनाम

भियतनामको फौजदारी कार्यविधि संहिता, २०१५ (Criminal Procedure Code, २०१५) ले "विद्युतीय डाटा" लाई प्रमाणको स्रोतको रूपमा मान्यता दिन्छ । सोही कानूनले विद्युतीय डाटा प्राप्त गर्ने, भण्डारण गर्ने, संरक्षित गर्ने, प्रतिलिपि बनाउने, पुनः प्राप्त गर्ने र प्रदर्शन गर्ने विशिष्ट नियमहरूको व्यवस्था गरेको छ । विशेषज्ञद्वारा गरिएको परीक्षणहरुको निष्कर्ष, डिजिटल प्रमाणलाई व्याख्या गर्न र प्रस्तुत गर्न प्रयोग गर्न सकिन्छ । विद्युतीय लेनदेन ऐन,

२००५ (Law on E–Transactions,२००५) ले डाटा सन्देश (म्यासेज) हरूको कानूनी वैधताको व्यवस्था गरेको छ ।

यी देशहरूले डिजिटल प्रमाणलाई आफ्नो कानूनी प्रणालीमा समावेश गर्न विभिन्न स्तरको तत्परता देखाएका छन् र आपराधिक मामिलाहरूमा डिजिटल प्रमाणको व्यवस्थापनका लागि कानून नविकरण गर्न र क्षमताहरू वृद्धि गर्न निरन्तर रुपमा प्रयासरत छन् ।

डिजिटल प्रमाणको खोज र जफतको वैधता सम्बन्धी निम्न उत्कृष्ट अभ्यासहरूको चर्चा गर्नु उपयुक्त देखिन्छ ।

क. भारत

भारतमा आपराधिक अनुसन्धानमा विद्युतीय उपकरणहरूको खोज र जफतलाई नियमन गर्ने कुनै विशिष्ट कानून छैन । 'वीरेन्द्र खन्ना विरुद्ध कर्नाटक राज्य' [३९] को मुद्दामा, कर्नाटक उच्च अदालतले सूचना प्रविधि ऐन, २००० को धारा ६९(१) अन्तर्गतको कानूनी प्रावधानलाई आधार बनाई डिजिटल उपकरणहरू र इमेल ठेगाना खोल्ने विस्तृत प्रक्रिया निर्धारण गरेको थियो । अदालतको निर्देशन अनुसार, पहिलो चरणमा अनुसन्धान अधिकृतले पासवर्ड, बायोमेट्रिक्स आदि उपलब्ध गराउन अनुरोध वा निर्देशन दिन सक्नेछ । वैकल्पिक रूपमा, अधिकृतले खोज र जफतको आदेशका लागि अदालतमा निवेदन दिन सक्नेछ । अन्तिम उपायको रूपमा, अदालतको आदेश प्राप्त गरेपछि ह्याकिङको विकल्प अपनाउन सकिन्छ । यी प्रक्रियाको पालना गर्न असमर्थ भएमा अभियुक्त विरुद्ध नकारात्मक अनुमान उत्पन्न हुनेछ भनी अदालतले उल्लेख पनि गरेको छ । नोभेम्बर ७, २०२३ मा, भारतको सर्वोच्च अदालतले 'फाउन्डेशन अफ मिडिया प्रोफेशनल्स' नामक पत्रकार समूहद्वारा दायर गरिएको आवेदनको परिणामस्वरूप डिजिटल उपकरणहरूको खोज र जफत सम्बन्धी निजी अधिकारको संरक्षणका लागि विस्तृत निर्देशिकाहरू जारी गरेको हो ।[४०] हालै, जनवरी ५, २०२४ मा, सर्वोच्च अदालतले अनलाइन पोर्टलद्वारा दायर गरिएको आवेदनको परिणाम स्वरुप, पत्रकारहरूको व्यक्तिगत डिजिटल उपकरणहरू छापामार्फत जफत गर्दा पारदर्शिता र औपचारिक प्रक्रियाको अभावलाई उजागर गर्दै अनुसन्धान निकाय (एजेन्सी) हरू र दिल्ली प्रहरीलाई पत्राचार जारी गरेको थियो । [४१]

---

[39] Virendra Khanna v. State of Karnataka, High Court of Karnataka, WP 11759/2020, Decided on March 12, 2021.

[40] https://www.scobserver.in/journal/guidelines-for-search-and-seizure-of-digital-devices-a-must-under-right-to-privacy-supreme-court-says/privacy-supreme-court-says/

[41] https://www.thehindu.com/news/national/sc-notice-on-newsclick-plea-for-guidelines-on-seizure-of-digital-devices/article67709600.ece

ख. संयुक्त राज्य अमेरिका

संयुक्त राज्य अमेरिकाको सर्वोच्च अदालतले, डिजिटल उपकरणहरूको खोज र जफत, र गोपनीयताको बारेमा 'राइली विरुद्ध क्यालिफोर्निया' (Riley vs. California) र 'युएस विरुद्ध वुरी' (US vs. Wurie)[४२] को मुद्दामा अप्रिल २९, २०१४ मा चर्चा गरेको थियो। प्रहरी अधिकारीहरूले साना अपराधहरूमा पक्राउ परेका व्यक्तिहरूको पक्राउ पछि सेलफोनलाई विशेष पूर्जी बिना खोजी गर्न मिल्छ वा मिल्दैन भन्ने विषयमा विवाद छ। केही अवस्थामा, यस्ता पूर्जीबिना गरिएको खोजीहरूले गम्भीर अभियोगको प्रमाण फेला पारेका छन्। सो प्रमाणलाई अस्वीकार गर्न माग गर्दै, यो अनुचित खोज र जफत विरुद्ध सुरक्षा प्रदान गर्ने अमेरिकी संविधानको चौथो संशोधनको उल्लङ्घन हो भन्ने दाबीका साथ निवेदन (अपिल) समेत गरिएको थियो । 'अनुचित' के हो भन्ने स्पष्ट निर्देशिकाहरूको अभावमा सो कुराको परिभाषा गर्नु चुनौतीको काम भएकाले अदालत प्रत्येक मुद्दा पिच्छे 'अनुचित' लाई व्याख्या गर्न बाध्य छ। चौथो संशोधनले वारेन्ट बिना गरिएको सरकारी हस्तक्षेप विरुद्धको सुरक्षा प्रदान गर्दछ । सामान्यतया, अपवाद लागू नभएसम्म वारेन्ट बिना गरिएको खोजीलाई अनुचित मानिन्छ। सुरक्षा भनेको व्यक्तिपरक हुन्छ, र सो कुरा खोजी गरिने भौतिक स्थान भन्दा व्यक्तिको गोपनीयता सम्बन्धि मनासिब अपेक्षामा आधारित रहेको हुन्छ।

संयुक्त राज्य अमेरिकामा, कानूनले विद्युतीय उपकरणहरू नियन्त्रणमा लिनु अघि, विशेष गरी त्यस्ता उपकरणहरू निजी स्थान जस्तै घर वा कार्यस्थलमा राखिएका अवस्थामा, खानतलासी पुर्जी (सर्च वारेन्ट) आवश्यक हुन्छ। सामान्यतया, घरको खानतलासीको लागि पूर्जी आवश्यक पर्छ किनभने घरमा स्वतः गोपनीयता अपेक्षीत हुन्छ । २०१४ मा, अमेरिकी सर्वोच्च अदालतले डिजिटल उपकरणहरूलाई पूर्जी वा सो उपकरणको धनीको सहमति बिना खोजी गर्न नसकिने निर्णय गरेको थियो । वालेट जस्तो वस्तुहरू भन्दा यी उपकरणहरूमा फरक र विशाल रुपमा व्यक्तिगत जानकारी समावेश भएको हुन्छ। यदि कुनै डिजिटल उपकरण सामान्य खोजीको क्रममा जफत गरिन्छ भने, त्यस्तो उपकरणको सामग्री खोजी गर्न उपयुक्त पूर्जि प्राप्त नभएसम्म कानूनले त्यस्तो उपकरणलाई सुरक्षित राख्नुपर्छ।[४३]

पूर्जि वैध हुनका लागि, यसले विशेष मापदण्डहरू पूरा गरेको हुनु पर्दछः अपराधसँग सम्बन्धित प्रमाणको सम्भावित कारण, पूर्जि माग गर्ने अधिकृतको शपथ, खोजी गरिने वस्तुहरूको विस्तृत विवरण र निष्पक्ष न्यायाधीशको स्वीकृति । पूर्जिले स्वतः भित्र फेला परेका विद्युतीय उपकरणहरूको खोजी गर्ने अधिकार प्रदान गर्दैन । घरभित्रको कुनै विद्युतीय उपकरणमा अपराधसँग सम्बन्धित प्रमाण रहेको शंका छ भने, सो कुरा प्रारम्भिक पूर्जि (इनिशियल वारेन्ट) मा वा छुट्टै पूर्जिमा उल्लेख गरेको हुनु पर्दछ।

---

[42] https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn1

[43] https://www.pumphreylawfirm.com/blog/search-and-seizure-of-computers-in-criminal-cases/

६. नेपालमा डिजिटल प्रमाण सङ्कलन प्रक्रियाका केही सामान्य अवलोकनहरू

विद्युतीय उपकरणहरूको सङ्कलन र जफत

व्यवहारमा भने, अधिकार प्राप्त अधिकारीहरूलाई गोप्य सूचना प्राप्त भएको वा शंकाको अवस्थामा प्रायः शंकास्पद व्यक्तिहरूबाट विद्युतीय उपकरणहरू तुरुन्तै जफत गरिन्छ। संदिग्धहरूलाई अदालतबाट जारी भएको पक्राउ पुर्जी वा कानून अनुसार आपतकालीन पक्राउ पुर्जी दिइन्छ। पक्राउपछि, अधिकार प्राप्त अधिकारीहरूले चलिरहेको अनुसन्धानसँग सम्बन्धित उपकरणहरूको खोजी र जफत गर्ने प्रक्रियाहरूको विधिवत रूपमा पालना गर्छन्। यी प्रक्रियामा सामान्य फौजदारी कार्यविधि कानूनहरू (General criminal procedural laws) र लागूऔषध कानून जस्ता विशेष कानूनहरू (specialized laws) मा उल्लिखित विशिष्ट प्रक्रियाहरूको पालना गरिन्छ। डिजिटल प्रमाण र उपकरणहरू सम्बन्धी स्पष्ट नियमको अभाव रहेको छ। अपराधसँग सम्बन्ध नै नभएका उपकरणहरू जफत भएतापनि व्यक्तिगत तथा गैर-वारन्टेड डिजिटल डाटामा आरोपीको पहुँच कटौती गरिन्छ।

डिजिटल सामग्रीको परीक्षण

जफत पश्चात, अधिकार प्राप्त अधिकारीहरूले विद्युतीय प्रमाणको जफतलाई दर्ता गर्छन् र उपकरणको भौतिक रूप मात्र नभई त्यसको विद्युतीय सामग्री (कन्टेन्ट) पनि परीक्षणका लागि लिने गर्छन्। जफत गरिएको उपकरणको विद्युतीय सामग्रीको विवरणमा प्रवेश गर्न अदालतको पूर्जि आवश्यक पर्दैन, जुन आश्चर्यजनक छ। नेपालको सर्वोच्च अदालतले गोपनीयताको अधिकारलाई जोड दिँदै कल विवरण र स्थान विवरण (location data) को लागि अदालतको पूर्जि आवश्यक पर्ने निर्णय गरे तापनि, डिजिटल प्रमाणको प्रयोग सम्बन्धी कुनै विशिष्ट निर्देशिका छैन। अनुसन्धानका लागि पठाइएका उपकरणहरूलाई नियमन गर्ने नियम अथवा विशिष्ट संलेखको अभाव छ। संलेखको यो अभावले डाटा विषय (सस्पेक्ट) लाई आफ्ना उपकरणहरूको अनुसन्धानको लागि सहमति दिने अवसरबाट वञ्चित गर्दछ, जसले आत्म-दोषारोपण (सेल्फ- इन्क्रिमिनेसन) को सम्भावना बढाउँदछ। यी अभ्यासहरू g]पालको संविधान åfरा प्रत्याभूत गरिएको आत्म-दोषारोपण विरुद्धको मौलिक अधिकारसँग बाझिएको पाइन्छ। साथै, डिजिटल प्रमाणको जफतको क्रममा, सस्पेक्टहरूलाई प्रायः आफ्ना डिजिटल उपकरणहरूको सुरक्षा प्रतिमान (security pattern) वा लक कोडहरू उपलब्ध गराउन बाध्य पारिन्छ, जसले आत्म-दोषारोपण को सिद्धान्तलाई थप उल्लङ्घन गर्दछ। डिजिटल प्रमाणहरूको परीक्षणको अभ्यास उचित नियमहरूको अभावमा विकसित भएको छ र परम्परागत परीक्षण प्रक्रियाहरूलाई नै उजागर गर्दै डिजिटल प्रमाणहरूको परीक्षण कार्यविधि समेटिएको छ। अनुसन्धान गर्ने निकायहरूले पटक-पटक डिजिटल प्रमाण सङ्कलनका लागि न्यायिक पूर्जिको माग गर्नाले मुद्दाको छिनोफानोमा ढिलाई हुन्छ भनी दाबी गरे तापनि, त्यसलाई

संवैधानिक अधिकारको इन्कारीको आधार मान्न मिल्दैन । त्यसैले, नेपालका फोरेन्सिक प्रयोगशालाहरूsf लागि विद्यमान निर्देशिकाहरूको दायरा विस्तार गर्ने र डिजिटल प्रमाणहरूको परीक्षणका लागि कानूनी निकायहरूले पालना गर्नुपर्ने प्रक्रियालाई स्पष्ट पार्ने प्रभावकारी कानूनी संयन्त्रहरू सिर्जना गर्न आवश्यक छ ।

आवश्यकता, आनुपातिकता र न्यायिक पूर्जि

अधीकार प्राप्त अधीकारीहरुले डिजिटल उपकरणहरूको अनुसन्धान गर्दाको बखत आवश्यकता, आनुपातिकता (proportionality) र न्यायिक पूर्जिको आवश्यकताको सीमा नाघेको अवस्थाहरू हुन सक्दछ । विशेष गरी, नेपालको कानूनले यस्ता अनुसन्धानहरूमा न्यायिक पूर्जिको स्पष्ट व्यवस्था गरेको छैन जसले गर्दा कानूनको कार्यान्वयन केही हदसम्म स्वेच्छाचारी बनेको छ । दूरसञ्चार सञ्चालकहरूबाट कल विवरण र प्रयोगकर्ताको स्थान (युजर लोकेसन) प्राप्त गर्दा न्यायिक पूर्जि अनिवार्य भएता पनि, सामाजिक सञ्जाल प्रदायकहरूबाट व्यक्तिगत जानकारी प्राप्त गर्न त्यस्तो कुनै आवश्यकता छैन । परिणाम स्वरूप, कानूनी निकायहरूले उचित प्रक्रियागत निर्देशनहरू बिना मेटा र एक्स जस्ता प्लेटफर्महरूबाट व्यक्तिगत विवरण बारम्बार झिक्ने गर्छन् र गोपनीयताको अधिकारको उल्लंघन हुन जान्छ । यस्तो जानकारीको लागि न्यायिक प्राधिकरण वा डाटा नियन्त्रकहरूको स्वीकृति लिने उचित प्रक्रियागत निर्देशनहरूको अभावका कारण, अनुसन्धान अधिकारीहरूको कार्य, आवश्यकता भन्दा बाहिर गएको, अनुपातहीन भएको र कानूनको पालना बिना गोपनीयताको उल्लंघन भएको अवस्थाहरू पनि छन् ।

प्रक्रियागत त्रुटिहरू र स्वेच्छाचारी अनुसन्धान

ठगीको एक विशिष्ट मुद्दामा, व्हाट्सएप कुराकानीको बारेमा दिइएको उजुरीको कारण एक शंकास्पद व्यक्ति पक्राउ परे । अनुसन्धानको क्रममा, संधिग्दको उपकरणमा क्रिप्टोकरेन्सी ट्रेडिङसँग सम्बन्धित एप भेटिएपछि, स्वभाविक रूपमा ध्यान सो एपमा सर्यो । परिणामस्वरूk, o} खोजको आधारमा संधिग्द विरुद्ध नयाँ मुद्दा दर्ता गरियो । कानून कार्यान्वयन गर्ने अधिकारीहरूले हितको लागि काम गरेतापनि उनीहरूबाट हुने प्रक्रियागत त्रुटिहरूले महत्वपूर्ण प्रश्नहरू उजागर गर्दछन् । माथि छलफल गरिए अनुसार, सर्वोच्च अदालतले स्वेच्छाचारी अनुसन्धानहरू रोक्न डिजिटल प्रमाणको प्राप्तिलाई नियमन गर्न आवश्यक रहेको कुरामा जोड दिएको भए पनि, यसलाई गम्भीरतापूर्वक लिइएको छैन र उचित समीक्षाको लागि छलफल गरिएको छैन । अधीकार प्राप्त अधिकारीहरूमा कुनै पनि गम्भीर अपराधको अनुसन्धान गर्दा, गोपनीयताको अवधारणाले सुरक्षाको अवधारणालाई उछिन्न सक्दैन भन्ने व्यापक धारणाले जरा गाडेको छ । डिजिटल प्रमाणको संकलन, प्रशोधन, प्रस्तुती र मूल्यांकनको लागि प्रक्रियागत निष्पक्षता कायम राख्न र विस्तृत निर्देशिकाहरू तयार गर्न सरकारको ध्यान नपुगेका कारण अधिकारीहरूले आफ्नै विचार र व्याख्याको आधारमा काम गर्ने परिदृश्य सिर्जना भएको छ । अदालतले प्रायः अनुसन्धान अधिकारीले अपनाएका स्वेच्छाचारी शैली, प्रक्रियागत कमीहरू र स्वयम्

अदालतमा रहेको उचित प्रक्रियागत र प्राविधिक स्रोतहरूको कमीप्रति आँखा चिम्लि बसेको पाइन्छ । यस्तो स्थितिले नेपालको समग्र फौजदारी न्याय प्रणालीका लागि खतरा उत्पन्न गर्ने हुनाले डिजिटल फरेन्सिक प्रमाणको संकलन, परीक्षण, प्रस्तुती र मूल्यांकनको प्रक्रियालाई सम्बोधन गर्ने एक कानूनी अवधारणा सिर्जना गर्न आवश्यक छ ।

फोरेन्सिक परीक्षण र प्रामाणिकता

नेपालमा डिजिटल उपकरणहरूको फोरेन्सिक परीक्षण मुख्यतया नेपाल प्रहरीको फरेन्सिक विभागद्वारा गरिन्छ । अभियुक्त वा प्रतिवादीहरूसँग प्रहरीले जफत गरेका उपकरणहरूको स्वतन्त्र डिजिटल फोरेन्सिक परीक्षण गर्ने वा सो को अनुरोध गर्ने कुनै कानूनी आधार छैन । प्रहरीको फोरेन्सिक परीक्षण माथिको यो एकलौटी नियन्त्रणले सन्तुलित र न्यायपूर्ण फौजदारी न्याय प्रणालीको लागि अत्यावश्यक 'इक्वालिटि अफ आर्मस'को सिद्धान्तलाई कमजोर बनाउँदछ । थप रूपमा, डिजिटल प्रमाण संकलन र परीक्षणको लागि मानंकीकृत प्रोटोकलहरूको अभावमा प्रमाणको छेडछाड र वास्तविकता बारे प्रश्न उठ्न सक्छ ।

डिजिटल प्रमाणको सुरक्षा र संरक्षण

डिजिटल प्रमाणको महत्वको बाबजुद, नेपालमा यसको संरक्षणको लागि कानूनी प्रावधान र प्रक्रियाहरूको अभाव छ । लग (log) र ट्रेलहरू (trails) सहितका डिजिटल प्रमाणहरू प्रायः उचित ब्याकअप प्रक्रिया वा सुरक्षा उपायहरू बिना सीमित अवधिको लागि भण्डारण गरिन्छ । यसो गर्नाले अदालतको सुनुवाईका क्रममा ती प्रमाणको अखण्डता माथि प्रश्न उठ्न सक्छ ।

डिजिटल फोरेन्सिकमा योग्यता र विशेषज्ञता

नेपालमा डिजिटल फोरेन्सिक परीक्षणहरू प्रहरी संगठन भित्रका प्राविधिकहरू द्वारा गरिन्छ, जसको योग्यता र विशेषज्ञता सम्बन्धी स्पष्ट वैधानिक वा कानूनी आवश्यकताहरू तोकिएको छैन । विशिष्ट योग्यता मापदण्डको यो अभावले अदालतमा फरेन्सिक प्रतिवेदनहरूको विश्वसनीयता र स्वीकार्यता सम्बन्धी चुनौतीहरू निम्त्याउन सक्छ ।

सुरक्षा मामलाहरु र सामग्री संरक्षण

अदालतहरूमा पेश गरिएका डिजिटल प्रमाणहरू प्रायः उचित रुपमा खाली (वाईपिंग) नगरी उही डिजिटल उपकरणहरूमा भण्डारण गरिन्छ, त्यसैले असुरक्षित रहन्छन् । सुरक्षाको यो अभावले संवेदनशील डाटामा अनधिकृत पहुँचको जोखिम निम्त्याउँछ, जसले सम्भवतः प्रमाणको अखण्डता र पीडितहरूको गोपनीयतालाई खलबलाउन सक्छ । प्रमाणको हकमा, अनुसन्धानकर्ताहरूले संकलन गरेका डिजिटल उपकरणलाई पूर्ण रूपमा नमेटाई सोही उपकरण अदालतमा पेश गरिन्छ। मुद्दाहरू धेरै वर्षसम्म अदालतमा विचाराधीन रहन्छन्। अदालती कारबाहीको क्रममा ती डिजिटल उपकरणहरूको

सुरक्षा कायम गरिएको हुँदैन । कुनै पनि अदालतका कर्मचारीहरूको ती उपकरणहरू र त्यसमा रहेको सामग्रीमा सजिलै पहुँच हुन्छ । मुद्दा समाप्त भएपछि, प्रतिवादीले सफाइ पाएको हकमा उपकरण फिर्ता दिइन्छ तर प्रतिवादीलाई अदालतले दोषी ठहर्याएको हकमा भने ती उपकरणहरू जफत गर्न आदेश दिएमा, त्यसमा रहेको सामग्रीको हेका नगरी उपकरणहरू खुला बजारमा बिक्री गरिन्छ । पूर्ण रूपमा खाली नगरी खुला बजारमा बिक्री गर्दा, ती उपकरणहरूको सामग्री सजिलै अन्य सामान्य मानिसहरूको पहुँचमा पुग्छ र पीडित पुनः पीडित हुने अवस्था सिर्जना हुन्छ ।

त्यसैले, आधुनिक आपराधिक अनुसन्धानमा डिजिटल प्रमाण महत्वपूर्ण भए पनि, नेपालले यसको संकलन, व्यवस्थापन र प्रस्तुतिमा धेरै चुनौतीहरूको सामना गरिरहेको छ । न्याय, निष्पक्षता र व्यक्तिहरूको अधिकारको संरक्षण सुनिश्चित गर्न, नेपालले स्पष्ट निर्देशिका, विशिष्ट प्रोटोकलहरू स्थापना गरेर र डिजिटल फरेन्सिक परीक्षणमा संलग्न व्यक्तिहरूको योग्यता र विशेषज्ञता सुनिश्चित गरेर यी चुनौतीलाई तत्काल सम्बोधन गर्न आवश्यक छ । यी चुनौतीहरूलाई सम्बोधन गरेर मात्र नेपालले आफ्नो कानूनी प्रणालीमा डिजिटल प्रमाणको विश्वसनीयता, स्वीकार्यता र दृढता बढाउन सक्छ ।

७. सुझावहरू

नेपालले आफ्नो कानूनी प्रणाली र अभ्यासहरूमा डिजिटल प्रमाणलाई मान्यता दिने र समावेश गर्ने दिशामा प्रगति गरेको भए पनि, सम्बोधन गर्नुपर्ने केही महत्वपूर्ण चुनौतीहरू छन् । यी सुझावहरूको पालना गरी, प्राविधिक प्रगति र उत्कृष्ट विश्वव्यापी अभ्यासहरू अपनाई, नेपालले आफ्नो कानूनी संरचनालाई सुदृढ बनाउन, डिजिटल प्रमाणको विश्वसनीयता र स्वीकार्यता बढाउन र कानूनी प्रणालीमा न्याय, निष्पक्षता, कानूनको शासन र व्यक्तिगत अधिकार प्रतिको सम्मान सुनिश्चित गर्न सक्दछ । अनुसन्धानको क्रममा रहेका व्यक्तिहरूले सामना गर्नुपर्ने प्रमुख समस्याहरू भनेको उनीहरूको व्यक्तिगत गोपनीयताको उल्लंघन र व्यक्तिगत उपकरणहरू मात्र नभई उनीहरूको व्यक्तिगत डाटाको अनुचित जफत रहेको छ । अनुसन्धान समाप्त भएपछि आफ्ना व्यक्तिगत उपकरणहरू फिर्ता पाउनमा पनि कठिनाई रहेको छ ।

स्पष्ट निर्देशन र प्रोटोकलहरू स्थापना गर्ने

डिजिटल प्रमाणको संकलन, व्यवस्थापन र परीक्षणको लागि विशेष रूपमा तयार पारिएका विस्तृत र स्पष्ट वैधानिक निर्देशिकाहरू विकास गर्न अत्यन्त आवश्यक छ । डिजिटल उपकरण र डाटाको जफत, परीक्षण र भण्डारणको क्रममा अधिकार प्राप्त अधिकारीहरू द्वारा एकरूपता र कानूनी प्रक्रियाहरू पालना गरिएको सुनिश्चित गर्न विशिष्टिकृत प्रोटोकलहरूको कार्यान्वयनको पनि आवश्यकता छ । समाजिक परिस्थिति र विद्यमान चुनौतीहरूलाई ध्यानमा राख्दै डिजिटल प्रमाणको संकलन, परीक्षण, स्वीकृति र मूल्यांकनको कानूनी र न्यायोचित प्रक्रिया सुनिश्चित गर्न र प्रत्येक

व्यक्तिलाई न्यायिक प्रणालीको हातमा सुरक्षित महसुस गराउन, अनुसन्धान र न्यायिक प्रक्रियाहरुमा चेन अफ कमान्ड सुनिश्चित गर्दै बलियो संयन्त्र विकास गरिनु पर्दछ ।

चेन अफ कस्टडी कायम राख्ने

संकलनदेखि अदालतमा प्रस्तुतिसम्म डिजिटल प्रमाणको चेन अफ कस्टडी कायम राख्न कडा प्रोटोकलहरू कार्यान्वयन गर्न आवश्यक छ । चेन अफ कस्टडी भनेको, प्रमाणको छेडछाड रोक्न र अखण्डता सुनिश्चित गर्न प्रमाण व्यवस्थापन, भण्डारण र पहुँचको प्रत्येक चरणको दस्तावेजीकरण गर्नु हो। डिजिटल प्रमाण प्राप्त गर्ने व्यक्तिले विशिष्ट योग्यता र पद धारण गरेको हुनुपर्दछ र नियन्त्रणको श्रृंखला कायम राख्न सक्षम हुनु पर्दछ । फोरेन्सिक प्रयोगशाला र कानून कार्यान्वयनमा लागू हुने विद्यमान निर्देशिकाहरूले प्रमाणको परीक्षण प्रक्रियाको क्रममा मात्र नियन्त्रणको श्रृंखलाको सिद्धान्तलाई जोड दिएको पाइन्छ तर सो सिद्धान्त व्यक्तिगत डाटाको अखण्डता र गोपनीयताको संरक्षण गर्न न्यायिक प्रक्रिया र अदालतहरू भित्र पनि कायम रहनु पर्दछ ।

अनिवार्य न्यायिक निरीक्षण

विशिष्ट विश्वव्यापी अभ्यासहरू र नेपालको सर्वोच्च अदालतको संवैधानिक प्रावधान र नजिरलाई ध्यानमा राख्दै डिजिटल सामग्रीको खोजी र परीक्षणको लागि न्यायिक पूर्जि आवश्यक पर्ने कानून ल्याउन तत्काल आवश्यक छ । त्यस्तो कानूनले, अनुसन्धान कानूनी सीमाभित्र रहेको, व्यक्तिको गोपनीयताको अधिकारको सम्मान गरिएको तथा न्यायिक रूपमा सो कुराको जाँच गरिएको अभ्यासलाई सुनिश्चित गर्दछ । साथै, कल विवरण र प्रयोगकर्ता स्थानको सन्दर्भमा अभ्यासमा रहेको न्यायिक सहमति संयन्त्र, नेपालको भित्र वा बाहिर रहेका कुनै पनि कम्पनीबाट जुनै पनि व्यक्तिको व्यक्तिगत जानकारी प्राप्त गर्दा समेत पालना गरिनु पर्दछ । आवश्यकता, आनुपातिकता र मानव अधिकारको सम्मानको सिद्धान्तहरूमा जोड दिँदै, राष्ट्रिय हित र आपतकालीन अवस्थालाई ध्यानमा राखी प्रक्रियागत रुपान्तरण र छुट सहित त्यस्ता वारेन्टहरू कहिले र कसरी प्राप्त गर्न सकिन्छ भन्ने स्पष्ट मापदण्डहरूको स्थापना गर्नुपर्दछ ।

डाटा विषयको सहमति र अधिकारहरू सुदृढ गर्ने

डाटा विषयहरू (सस्पेक्ट) लाई, उनीहरू आफ्ना अधिकार र सम्भावित प्रभावको बारेमा जानकार छन् भन्ने सुनिश्चित गर्दै, उनीहरूको डिजिटल उपकरणको अनुसन्धान गर्नु अघि उनिहरुबाट सूचित सहमति वा मञ्जुरी लिने गरी कानून बनाई उनिहरुलाई सशक्त बनाउन सकिन्छ । कानूनी प्रावधानहरूमा सुधार गरी व्यक्तिहरूलाई आत्म-दोषारोपण (सेल्फ-इन्क्रिमिनेसन) बाट जोगाउन र अधिकार प्राप्त अधीकारीहरुलाई अभियुक्तलाई डिजिटल उपकरणहरूको सुरक्षा पैटर्न वा लक कोडहरू उपलब्ध गराउन बाध्य पार्नबाट रोक्न सकिन्छ ।

डिजिटल फरेन्सिक अभ्यासहरू सुधार गर्ने

अदालतमा फोरेन्सिक प्रतिवेदनहरूको विश्वसनीयता र स्वीकार्यता सुनिश्चित गर्न डिजिटल फोरेन्सिक परीक्षकहरूको योग्यता र विशेषज्ञता सुनिश्चित गर्नुपर्ने कानूनी प्रावधानको कार्यान्वयन हुन आवश्यक देखिन्छ । डिजिटल फरेन्सिक विशेषज्ञहरू माफ्र्ंत आवश्यक सीप र ज्ञान सुनिश्चित गर्नको लागि तालिम कार्यक्रम र प्रमाणीकरणमा (सर्टिफिकेसन) लगानी गर्नका लागि सुझाव गरिन्छ। योग्यताको विशिष्ट मानकीकरण गर्नाले फोरेन्सिक परीक्षणहरूको विश्वसनीयतामा सुधार ल्याउन सकिन्छ । यसबाहेक, पक्षहरूको निष्पक्षता सुनिश्चित र सन्तुलन गर्न र स्वार्थको åGbलाई निर्मूल पार्न सरकारी कानूनी निकायहरू भन्दा बेग्लै डिजिटल फोरेन्सिक परीक्षण गर्ने जिम्मेवार स्वतन्त्र निकाय वा एजेन्सीको स्थापना गर्न पनि सुझाव दिइन्छ ।

डिजिटल सुरक्षा र संरक्षण बढाउने

डिजिटल प्रमाणहरू, लगहरू, ट्रेलहरू र अन्य सम्बन्धित डाटाको अनिवार्य रुपमा सुरक्षित भण्डारण, ब्याकअप र संरक्षणको लागि कानूनी प्रावधानहरू बनाउन सुझाव गरिन्छ । साथै, अदालती सुनुवाईको क्रममा प्रमाणको अखण्डता सुनिश्चित गरी अनधिकृत पहुँच वा छेडछाडलाई प्रतिबन्ध लगाई प्रमाणको सुरक्षा गर्ने संयन्त्रहरू विकास गर्न आवश्यक रहेको छ । यसका अतिरिक्त डिजिटल प्रमाणको विश्वसनीयता बढाउन इन्क्रिप्शन, डिजिटल हस्ताक्षर र अन्य प्रमाणीकरण प्रविधिहरूको प्रयोग गर्ने सुझाव रहेको छ ।

आवश्यकता, उद्देश्यपरकता र आनुपातिकतालाई प्राथमिकता दिने

डिजिटल अनुसन्धानको आवश्यकता, उद्देश्यपरकता र आनुपातिकताको महत्वलाई जोड दिनु पर्ने देखिन्छ । यसका साथै, डिजिटल प्रमाण नियमन प्रणालीले अनुसन्धानात्मक कार्यहरू न्यायोचित, लक्षित र उद्देश्यहरूको अनुपातमा रहेको कुरालाई सुनिश्चित गर्नुपर्दछ। यसरी अनावश्यक हस्तक्षेपलाई न्यूनीकरण गर्दै व्यक्तिहरूको अधिकारको सम्मान गर्न सकिन्छ ।

प्रमाणको स्वीकार्यता र विश्वसनीयता सुनिश्चित गर्ने

फोटो, भिडियो, अडियो रेकर्डिङ, सिडी र विशेषज्ञको राय लगायत अन्य डिजिटल प्रमाणको स्वीकार्यता र विश्वसनीयता बारे स्पष्ट निर्देशिका निर्माण गर्न सुझाव दिइन्छ । स्थापित कानूनी मापदण्ड र प्रमाणीकरण प्रक्रियाहरूको पालना गर्नाले पनि अदालती सुनुवाईमा प्रस्तुत गरिएका प्रमाणहरूको विश्वसनीयता बढाउनेछ ।

सार्वजनिक सचेतना र तालिम सुधार गर्ने

कानून कार्यान्वयन गर्ने अधिकारीहरू, कानूनी वयवसायीहरु र आम जनताको लागि डिजिटल प्रमाणको महत्व, कानूनी संरचना र विशिष्ट अभ्यासहरू सम्बन्धी सार्वजनिक सचेतना अभियान र तालिम कार्यक्रमहरू संचालन गर्न सुझाव दिइन्छ । साथै, डिजिटल प्रमाणको सन्दर्भमा दिनानुदिन उजागर हुने चुनौतीहरूको विषयमा ज्ञान आदान-प्रदान गर्न, अनुभव सुनाउन र नवीन समाधानहरू विकास गर्न सरकारी निकायहरू, कानूनी विशेषज्ञहरू, प्रविधिविद्हरू र नागरिक समाज संस्थाहरू लगायत सम्बन्धित सरोकारवालाहरूबीच सहकार्य गर्न पनि सुझाव दिइन्छ ।

विद्यमान कानूनको समीक्षा र सुधार गर्ने

उदीयमान प्रविधिक प्रगति, विशिष्ट विश्वव्यापी अभ्यास र विकासशील मानव अधिकार मापदण्डहरूलाई सम्बोधन गर्न डिजिटल प्रमाणसँग सम्बन्धित विद्यमान कानून र नियमहरूको नियमित समीक्षा र सुधार गर्नु पर्ने देखिन्छ । साथै निर्माण हुने नयाँ कानून गोपनीयताको अधिकार, आत्म-दोषारोपण विरुद्धको अधिकार, समानताको अधिकार लगायत अन्तर्राष्ट्रिय मापदण्ड, मानव अधिकारका सिद्धान्त र नेपालको संवैधानिक प्रत्याभूति सँग सुसंगत रहेको सुनिश्चित गर्न पनि जरुरी हुन्छ ।

जवाफदेहिता संयन्त्रको स्थापना

डिजिटल प्रमाण सम्बन्धी कानून र अभ्यासहरूको कार्यान्वयनलाई अनुगमन र मूल्याङ्कन गर्न बलियो जवाफदेहि संयन्त्रहरू लागू गर्न आवश्यक छ । यसले कानूनी आवश्यकताहरू, नैतिक मापदण्डहरू र मानव अधिकारका सिद्धान्तहरूको पालना सुनिश्चित गर्दछ । साथै, डिजिटल प्रमाणको सङ्कलन, व्यवस्थापन र प्रयोगसँग सम्बन्धित उजुरी, दुराचार वा दुरुपयोगको अनुसन्धान गर्न र कानून उल्लङ्घन वा उल्लङ्घनका लागि जिम्मेवार व्यक्तिहरूलाई जवाफदेही बनाउँन स्वतन्त्र अनुगमन निकायहरू वा संयन्त्रहरूको स्थापना गर्न आवश्यक छ ।

अन्तर्राष्ट्रिय सहयोग र सहकार्यलाई सुदृढ बनाउने

द्विपक्षीय वा बहुपक्षीय सन्धि व्यवस्थाहरू लागू गरी अन्तरदेशीय मुद्दाहरुमा डिजिटल प्रमाणको संकलन र स्वीकार्यतालाई सहज बनाउन पारस्परिक कानूनी सहायता सन्धि र इन्टरपोल जस्ता संस्थाहरूँगको सहकार्यलाई सुदृढ बनाउन आवश्यक भएकाले सम्बन्धित संयन्त्रको विकास गर्न सुझाव दिइन्छ ।

ग्रन्थसूची

Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. https://doi.org/10.1007/978-3-319-67208-3_2

Brezinski and Killalea, 2002; US National Institute of Justice, 2004; European Network of Forensic Science Institute, 2015

Council of Europe, *Convention on Cybercrime* (ETS No. 185), opened for signature Nov. 23, 2001

मुलुकी अपराध संहिता, २०७४

मुलुकी फौजदारी कार्यविधी संहिता, २०७४

निर्णय नं. १०९५८ - भागः ६४, सालः २०७९, महिनाः माघ, खण्डः १०, निर्णय मितिः २०७८/०८/२८, ०७५-CR-१४७२, मुद्दाः भ्रष्टाचार

निर्णय नं. ९७४० - भागः ५९, वर्षः २०७४, महिनाः बैशाख, खण्डः १, निर्णय मितिः २०७२/१०/२१, ०६९-WO-०२६८, मुद्दाः उत्प्रेषण /परमादेश

निर्णय नं. ९८८० - भागः ५९, सालः २०७४, महिनाः पौष, खण्डः ९, निर्णय मितिः २०७३/०९/०४, सर्वोच्च अदालत संयुक्त इजलास, ०७१-CR-१०८९, मुद्दाः भ्रष्टाचार

Digital Evidence and the New Criminal Procedure Author(s): Orin S. Kerr Source: Columbia Law Review , Jan., 2005, Vol. 105, No. 1 (Jan., 2005), pp. 279-318 Published by: Columbia Law Review Association, Inc. Stable URL: https://www.jstor.org/stable/4099310

Duranti, Luciana, and Allison Stanfield. "Authenticating Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 236–78. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.13. Accessed 27 Mar. 2024

विद्युतीय कारोबार ऐन, २०६३

England and Wales care Standards Tribunal, Mogford v Secretary of State for Education and Skills [2002] EWCST 11(PC) (26 June 2002) https://www.bailii.org/ew/cases/EWCST/2002/11(PC).html

https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn1

https://www.pumphreylawfirm.com/blog/search-and-seizure-of-computers-in-criminal-cases/

https://www.scobserver.in/journal/guidelines-for-search-and-seizure-of-digital-devices-a-must-under-right-to-privacy-supreme-court-says/

https://www.thehindu.com/news/national/sc-notice-on-newsclick-plea-for-guidelines-on-seizure-of-digital-devices/article67709600.ece

Interpol, "एशियामा अभियोजनमा डिजिटल प्रमाणको प्रयोग, बंगलादेश, भूटान, ब्रुनेई, कम्बोडिया, माल्दिभ्स, मंगोलिया, नेपाल, श्रीलंका र भियतनाममा आपराधिक कार्यवाहीमा डिजिटल प्रमाणको स्वीकृति र प्रयोगलाई नियमन गर्ने कानून र नीतिहरूको तुलनात्मक अध्ययन"

ISO/IEC 27042: ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*, ISO (Year varies)

ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, ISO (2012), available at, https://webstore.ansi.org/preview-pages/INCITS/preview_INCITS+ISO+IEC+27037+2012+(R2019).pdf?srsltid=AfmBOoqREc1Pliql6CQCOGXgN4J0S3mPjdSRt9Ib_XYJjPLL1Yf8zWG_

Jason Liser Plaintiff v. Jeffrey Smith et al, United States District Court, D. Columbia, No. CIV.A.00-2325 (ESH) (D.D.C. Mar. 26, 2003)

Kersten Mark , Challenges and Opportunities: Audio-Visual Evidence in International Criminal Prooceedings

Mason, Stephen, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 285–338. *JSTOR*, http://www.jstor.org/stable/j.ctv512x65.16. Accessed 27 Mar. 2024

पारस्परिक कानूनी सहायता ऐन, २०७० (२०१४)

ने.का.प. २०६५, खण्ड ७, निर्णय नम्बर ७९८५

ने.का.प. २०६७, खण्ड १०, निर्णय नम्बर ८४८३

ने.का.प. २०६७, खण्ड ११, निर्णय नम्बर ८५०१

ने.का.प. २०६८, खण्ड ३, निर्णय नम्बर ८५८२

ने.का.प. २०७०, खण्ड ६, निर्णय नम्बर ९०२२

ने.का.प. २०७८, खण्ड ११, निर्णय नम्बर १०७७३

Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 14, 2012), available at : https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/LubangaEng.pdf

Stanford International Bank Limited (in liquidation) v. Hamilton-Smith, High Court (Antigua), See : https://ag.vlex.com/vid/alexander-m-fundora-applicant-805812073

The Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 21, 2016), available at: https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/BembaEng.pdf

United States Court of Appeals, Tenth Circuit, 9 F.3d 823 (10th Cir. 1993)

US National Institute of Justice; 2004a; Maras, 2014

Virendra Khanna v. State of Karnataka, High Court of Karnataka, WP 11759/2020, Decided on March 12, 2021

Williams, Janet. "Acpo good practice guide for digital evidence." *Metropolitan Police Service, Association of chief police officers, GB* (2012): 1556-6013., *Good Practice Guides for Digital Evidence*

Wilson, Nigel, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.16. Accessed 27 Mar. 2024

SUPPORT OUR WORK! DONATE!

Human Rights and Justice Center
Sunrise Bank Ltd 0020388247701001

VISIT US

Jwagal-10, Kupondole,
Lalitpur, Nepal

☎ +977 9819033495

contact@hrjc.org.np

https://www.hrjc.org.np

https://tinyurl.com/2ym9byf2

https://www.facebook.com/HRJCNepal/

FIND US ON GOOGLE MAPS