ट्रेसेबिलिटी और साइबरसुरक्षा

भारत में एनक्रिप्शन पर विशेषज्ञों की वर्कशॉप श्रृंखला

नवंबर 2020

ट्रेसेबिलिटी (Traceability), या किसी विशिष्ट सामग्री या संदेश के प्रणेता का पता लगाने की क्षमता, भारत के ऑनलाइन मंचों और संचार प्रदाताओं के लिए नियमों से संबंधित बहस का मुख्य विषय है। 2018 के अंत में, भारतीय इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeiTy) ने, सूचना प्रौद्योगिकी अधिनियम के तहत सूचना प्रौद्योगिकी (मध्यस्थों के लिए दिशानिर्देश) नियमों में संशोधन प्रस्तावित किए।[1] प्रस्तावित परिवर्तनों में ट्रेसेबिलिटी की माँग रखी गई है, जिसका वर्णन "मंच पर जानकारी के प्रणेता का[2] पता लगाने में सक्षम होने" के रूप में किया गया है। यह संशोधन, यदि ट्रेसेबिलिटी प्रदान नहीं की जाती है, तो ऑनलाइन मंच या प्रदाता को उसके उपयोगकर्ताओं द्वारा पोस्ट की गई सामग्री के लिए ज़िम्मेदार ठहराएगा। MeiTY ने 2019 के शुरू में संशोधन के मसौदे पर सार्वजनिक टिप्पणियाँ आमंत्रित की थीं[3] और, 2020 के आरंभ में लगभग 30 साइबरसुरक्षा और क्रिप्टोग्राफिक विशेषज्ञों ने MeiTy को प्रस्तावित संशोधनों के संबंध में चिंताएं व्यक्त करते हुए एक खुला पत्र भेजा था।[4] इसी तरह से मद्रास हाईकोर्ट में कई बड़े ऑनलाइन मंचों और सरकार के बीच उपयोगकर्ताओं के द्वारा उत्पन्न सामग्री में कानून प्रवर्तन अधिकारियों को एक्सेस प्रदान करने को लेकर चल रहे एक मुकदमे में ट्रेसेबिलिटी एक मुद्दा बनी हुई है।[5]

वर्तमान में चल रही बहस के केंद्र में निम्नलिखित से संबंधित प्रश्न हैं:

- संचारों के आरंभ से लेकर अंत तक ट्रेसेबिलिटी की प्राप्यता[6]
- ट्रेसेबिलिटी सक्षम करने के लिए कौन सी विधियाँ उपलब्ध हैं, और
- प्रत्येक से संबंधित जटिलताएं क्या हैं?

संदेश भेजने वाले ऐप्स (उदा., व्हाट्सैप) जैसे आरंभ से अंत तक के संचारों में ट्रेसेबिलिटी हासिल करने की विधियों के रूप में दो तकनीकों, **डिजिटल हस्ताक्षरों के उपयोग** और **मेटाडेटा के उपयोग**, का प्रस्ताव किया गया है। फिर भी, ट्रेसेबिलिटी की आवश्ययकताओं का पालन करने के लिए, मंच अपने उपयोगकर्ताओं के संचारों की सामग्री में एक्सेस सक्षम करने के लिए मजबूर हो सकते हैं, **जिससे आरंभ से अंत तक का एनक्रिप्शन टूट सकता है** और ट्रेसेबिलिटी संभव करने के दौरान, उनके उत्पाद की सुरक्षा और निजता काफी कमज़ोर हो सकती हैं।

इंटरनेट सोसायटी द्वारा मीडियानामा नामक साइबरसुरक्षा सुरक्षा विशेषज्ञों और नीति विशेषज्ञों के एक अंतरराष्ट्रीय समूह के साथ साझेदारी में आयोजित Chatham House Rule की चर्चाओं की एक श्रृंखला में, भारतीय संदर्भ में संदेशों की ट्रेसेबिलिटी के मुद्दे की जाँच की गई। विशेषज्ञों ने दो तकनीकी विधियों को लेकर उल्लेखनीय चिंताएं व्यक्त कीं जिन्हें ट्रेसेबिलिटी सक्षम करने के लिए अक्सर प्रस्तावित किया जाता है: डिजिटल हस्ताक्षरों का उपयोग और मेटाडेटा का उपयोग। इनका उदाहरण केवल उपयोगकर्ताओं की निजता और सुरक्षा के प्रति

1 सूचना प्रौद्योगिकी [मध्यस्थों के लिए दिशानिर्देश (संशोधन)] नियम।

2 भारतीय सूचना प्रौद्योगिकी अधिनियम के तहत, प्रणेता को एक ऐसे व्यक्ति के रूप में परिभाषित किया जाता है जो कोई भी इलेक्ट्रॉनिक संदेश भेजता है, उत्पन्न करता है, भंडारित करता है या संचारित करता है या किसी अन्य व्यक्ति को कोई इलेक्ट्रॉनिक संदेश भेजने, उत्पन्न करने, भंडारित करने या संचारित करने की व्यवस्था करता है लेकिन किसी भी मध्यस्थ को शामिल नहीं करता है"

3 https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf

4 https://www.internetsociety.org/open-letters/india-intermediary-guidelines/

5 https://www.medianama.com/2019/09/223-sc-adjourns-hearing-on-facebook-transfer-petition-till-september-24/

6 आरंभ से अंत तक (E2E) एनक्रिप्शन - जहाँ किसी एनक्रिप्ट किए गए संचार को खोलने के लिए जरूरी कुंजियाँ केवल संचार करने वाली डिवाइसों पर ही मौजूद होती हैं - सुरक्षा और भरोसे का सबसे मजबूत स्तर प्रदान करता है, क्योंकि उनकी रचना इस तरह से की जाती है कि, केवल अभिप्रेत प्राप्तकर्ता के पास ही संदेश को खोलने की कुंजी होती है।

खतरे के रूप में ही नहीं दिया जाता है; इनका उपयोग किसी संदेश का श्रेय उसके प्रणेता को दे सकने की विश्वसनीयता भी संदेहास्पद है। ट्रेसेबिलिटी सक्षम करने के लिए उपयोगकर्ताओं के संचारों की सामग्री में तृतीय पक्षों को एक्सेस प्रदान करना सुरक्षा और निजता के लिए और भी अधिक चिंताएं प्रस्तुत करता है।

डिजिटल हस्ताक्षर

कुछ लोगों ने अनुशंसा की है कि प्रेषक के डिजिटल हस्ताक्षर को[7] संदेशों में जोड़ा जाना चाहिए, ताकि संदेश के प्रणेता को पहचाना जा सके। उदाहरण के लिए, मद्रास हाईकोर्ट में चल रहे मुकदमे में, डॉ. कामाकोटी ने व्हाट्सैप के भीतर अग्रेषित संदेश के प्रणेता का पता लगाने के लिए डिजिटल हस्ताक्षरों का उपयोग करने का प्रस्ताव रखा।[8] कामाकोटी के प्रस्ताव में, प्रणेता का हस्ताक्षर या तो संदेश की श्रृंखला में सभी को दिख सकता है या उसे व्हाट्सैप द्वारा प्रदान की गई एक सार्वजनिक कुंजी का उपयोग करके एनक्रिप्ट किया जा सकता है। व्हाट्सैप, संबंधित निजी कुंजी का उपयोग करके, अदालत के द्वारा आज्ञा दिए जाने पर प्रणेता की जानकारी को डीक्रिप्ट करने में सक्षम होगा।

हालांकि, इंटरनेट सोसायटी की चर्चाओं में भाग लेने वाले विशेषज्ञों सहित, कई लोगों ने, ट्रेसेबिलिटी सक्षम करने के लिए डिजिटल हस्ताक्षरों के उपयोग को लेकर चिंताएं जताई हैं।

- **डिजिटल आरोपण अभेद्य नहीं है और जालसाज़ी के खतरे से अरक्षित है:** आपराधिक उत्तरदायित्व स्थापित करने के लिए, अपराध को उचित शंका से परे सिद्ध करने की जरूरत होती है–जो एक ऐसी सीमा है जिसे लाँघना कठिन है, खास तौर पर जब ऑनलाइन जालसाज़ी इतनी आसान और व्यापक है। कानून प्रवर्तन अधिकारियों के पास प्रेषक का आईडी होने के बावजूद यह सिद्ध करना बहुत कठिन है कि, मोबाइल/कम्प्यूटर ए के उपयोगकर्ता, व्यक्ति ए ने, झूठी खबर फैलाने वाले संदेश वास्तव में भेजे थे। यह स्थापित करने के लिए कि क्या किसी व्यक्ति की डिवाइस का *उपयोग व्यक्ति के द्वारा* डिवाइस के उपयोग का सबूत है, अतिरिक्त जानकारी की जरूरत पड़ती है।[9] इससे भी अधिक चिंता का विषय यह है कि निर्दोष उपयोगकर्ताओं को उनके प्रेषक आईडी की जालसाज़ी करने वाले साइबर अपराधियों के द्वारा गैरकानूनी आचार में फंसाया जा सकता है। यही चिंता कामाकोटी के प्रस्ताव के प्रति व्हाट्सैप की अपनी प्रतिक्रिया में प्रतिबिंबित हुई, जिसमें उन्होंने कहा कि "बुरे तत्व संदेश को किसी अलग फोन नंबर से जोड़ने के लिए व्हाट्सैप के संशोधित संस्करणों का उपयोग कर सकते हैं।"[10]

- **डिजिटल हस्ताक्षर और अरक्षितताएं।** डिजिटल हस्ताक्षरों की निजी कुंजियाँ, खास तौर पर जब वे संचार सेवा प्रदाता जैसे संचार के तृतीय पक्ष के हाथों में होती हैं, बुरे तत्वों के लिए मूल्यवान लक्ष्य बन सकती हैं। मिसाल के तौर पर, कामाकोटी के प्रस्ताव में, जोखिम-ग्रस्त तृतीय पक्ष - प्रणेता की जानकारी को प्राप्त और डीक्रिप्ट करने के द्वारा - यह देखने में सक्षम हो सकता है कि कोई विशिष्ट उपयोगकर्ता कब संदेश भेज रहा है। गलत उपयोग करने पर, 'डिजिटल हस्ताक्षर' का तरीका नागरिकों की बोलने की आजादी को गंभीर रूप से खतरे में डालता है, और लोगों को (सबसे अरक्षित और कमज़ोर तबके के लोगों सहित) जालसाज़ी, उत्पीड़न और अत्याचार का सामना करना पड़ सकता है।

- **विभिन्न मंचों के बीच प्रकार्यात्मकता अव्यावहारिक होगी।** चूंकि विभिन्न सेवाएं और मंच विभिन्न प्रोटोकॉलों द्वारा प्रशासित हैं, सभी मंचों पर एक साथ काम करने वाली विधियाँ असाध्य होंगी। मंचों के बीच परस्पर ट्रेसेबिलिटी ईमेल या इंटरनेट रिले चैट (IRC) जैसी संघबद्ध प्रणालियों में भी कठिन होती है। अनेकों मंचों पर एक साथ ट्रेसेबिलिटी प्रदान करने की विधियों, जैसे वैश्विक रूप से प्रत्येक मंच के प्रत्येक संदेश के टेक्स्ट के भीतर एक ही अनिवार्य डिजिटल हस्ताक्षर का उपयोग करना, को अमल में लाना कठिन होगा। डिजिटल हस्ताक्षरों को प्रमाणित करने के लिए सारे विश्व की *प्रत्येक* डिवाइस और *प्रत्येक* ऐप क्लाइंट की एक केंद्रीय रजिस्ट्री की जरूरत पड़ सकती है। इससे नवाचार गंभीर रूप से बाधित हो सकता है - जिसके कारण हर जगह के डेवलपरों को केंद्रीय डेटाबेस के ऑपरेटरों के साथ अपने विकास का समन्वयन करना पड़ सकता है। इसके अलावा, डिजिटल हस्ताक्षर के अनिवार्य होने से उपयोगकर्ताओं की निजता और सुरक्षा विफलता के मात्र एक बिंदु पर खतरे में पड़ सकती है - या बुरे तत्वों को किसी उपयोगकर्ता की गतिविधियों को खतरे में डालने या ट्रैक करने के लिए मात्र एक बिंदु को लक्षित करने का अवसर मिल सकता है।[11] इन डिजिटल हस्ताक्षरों को खतरे में पड़ने की स्थिति में आसानी से रद्द करने और दोबारा जारी करने की क्षमता से भी युक्त होना पड़ेगा, जिससे उनसे संबद्ध गुप्त कुंजियों की सुरक्षा पर भी प्रश्नचिह्न लग सकता है। यदि यह उपयोगकर्ताओं के बायोमेट्रिक्स पर निर्भर है, तो तकनीकी और परिचालन संबंधी जटिलता की एक और परत जोड़ने की जरूरत होगी।

---

7 डिजिटल हस्ताक्षर यह सुनिश्चित करने की एक प्रक्रिया है कि भेजा जाने वाला संदेश, या जानकारी, प्रामाणिक है। वह संदेश के प्रेषक को एक हस्ताक्षर के रूप में काम करने वाला एक कोड संलग्न करने में सक्षम करता है। किसी व्यक्ति के हाथ से किए गए हस्ताक्षर की तरह ही, यह प्रत्येक हस्ताक्षरकर्ता के लिए अद्वितीय होता है, और इसकी तुलना एक टैंपर प्रूफ सील से की जा सकती है जो गारंटी देती है कि जानकारी के भेजे जाने के बाद से उसमें किसी भी तरह का बदलाव नहीं किया गया है।

8 https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/

9 मिसाल के तौर पर, उनकी डिवाइस का उपयोग कोई अन्य व्यक्ति कर रहा हो सकता है।

10 https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/

11 https://www.internetsociety.org/policybriefs/identity

मेटाडेटा

एनक्रिप्शन पर बहस में कई संस्थाओं ने ट्रेसेबिलिटी सक्षम करने के लिए मेटाडेटा के उपयोग का मुद्दा भी उठाया है। मेटाडेटा, जिसमें संचार के बारे में जानकारी मौजूद होती है, किंतु स्वयं संचार की सामग्री नहीं होती है, उसका उपयोग संचार के स्रोत, समय, तारीख, और गंतव्य जैसी चीजों, प्रेषक के स्थान का संभावित रुप से निर्धारण करने, और यहाँ तक कि स्वयं संचार की सामग्री की कुछ विशेषताओं का अनुमान लगाने के लिए भी किया जा सकता है।

कुछ लोगों ने जोर देकर कहा है कि संदेश, विशेष रूप से मीडिया संदेश, के आकार से संबंधित मेटाडेटा का उपयोग विशिष्ट संदेशों के अनियंत्रित वितरण पर रोक लगाने के लिए किया जा सकता है। मिसाल के तौर पर, व्हाट्सैप भेजे जाने वाले मीडिया संदेशों का एक एनक्रिप्ट किया हुआ लॉग कायम रखता है। उसे मीडिया फाइल की सामग्री में एक्सेस उपलब्ध नहीं होता है, लेकिन वह एक विशिष्ट आकार के डेटा के समूह के रुप में दिखाई देता है। जब भी इस मीडिया संदेश को अग्रेषित किया जाता है, सर्वर के पास इस बात का एक अनुमान होता है कि डेटा के उस समूह को कितनी बार अग्रेषित किया गया था - जिसका उपयोग वह अपने मंच पर स्पैम से रहित बनाने के लिए करता है। मीडिया फाइल की एनक्रिप्ट न की गई फाइल को एक्सेस करके संदेश के इतिहास का अनुमान लगाया जा सकता है, जिससे संचार की गोपनीयता प्रभावी रुप से नष्ट हो सकती है।

अन्य लोगों का कहना है कि मेटाडेटा का विश्लेषण करके विभिन्न ढांचा की पहचान की जा सकती है जैसे कि कौन किससे, कितनी बार और कब बात करता है। मंचों द्वारा बातचीतों की नेटवर्क बनाने के लिए मूलभूत सामाजिक ग्राफों की रचना की जा सकती है। किसी भी संचार मंच के लिए महत्वपूर्ण, निदेशिका संरचनाओं का, लाभ उठाकर स्वयं सामग्री को एक्सेस किए बिना जाँच-पड़ताल की जा सकती है। ये निदेशिकाएं स्वयं सामग्री का अवरोधन किए बिना रिकार्ड करती हैं कि किसने किसके साथ इंटरैक्ट किया था।

हालांकि, इंटरनेट सोसायटी की चर्चाओं में भाग लेने वाले विशेषज्ञों सहित, कई विशेषज्ञ, ट्रेसेबिलिटी को सक्षम करने के लिए मेटाडेटा के उपयोग पर चिंता प्रकट कर रहे हैं।

- **डिजिटल आरोपण, खास तौर पर मेटाडेटा के माध्यम से किया जाने वाला, अभेद्य नहीं है।** मेटाडेटा के आधार पर आपराधिक उत्तरदायित्व स्थापित करना और भी अधिक कठिन है। संदेश की सामग्री में छोटे से परिवर्तनों से संदेश का मेटाडेटा में बदलाव हो सकता है, जिससे एक प्रणेता से आने वाले एक जैसे मेटाडेटा की श्रृंखला का अनुसरण करने की क्षमता प्रतिबंधित हो सकती है। डिजिटल हस्ताक्षरों की तरह ही, किसी उपयोगकर्ता को किसी संदेश से जोड़ना कठिन है क्योंकि ऑनलाइन जालसाज़ी इतनी आसान और व्यापक है। केवल नकली मेटाडेटा के आधार पर किसी निर्दोष उपयोगकर्ता को आपराधिक आचार में फंसाए जाने की क्षमता और भी अधिक चिंता का विषय है।

- **डेटा के न्यूनीकरण, इरादतन निजता के सिद्धांतों का अवमूल्यन करना।** डेटा के न्यूनीकरण और इरादतन निजता, जिसे आजकल की कई डेटा संरक्षण नीतियाँ आवश्यक करती हैं, उसकी ओर कदम बढ़ाने के मंचों के द्वारा प्रयास को मेटाडेटा पर निर्भरता से नुकसान पहुँच सकता है। इससे हर किसी के लिए सुरक्षा मानकों की गिरावट के साथ लोगों की निजता और सुरक्षा को काफी व्यापक जोखिम पैदा हो सकते हैं। ट्रेसेबिलिटी को सक्षम करने में मदद करने के लिए रखा गया मेटाडेटा बुरे तत्वों के लिए उपयोगी लक्ष्य बन सकता है। अपराधी और विदेशी शत्रु भंडारित मेटाडेटा का उपयोग उपयोगकर्ताओं के सामाजिक ग्राफ विकसित करने या ऐसी जानकारी एकत्र करने के लिए कर सकते हैं जो जबरन वसूली, सोशल इंजीनियरिंग, या ब्लैकमेल जैसे हमलों को सक्षम कर सकती है।

- **सामाजिक प्रोफाइलिंग के जोखिम।** जहाँ ट्रेसेबिलिटी को सक्षम करने में मदद करने के लिए सामाजिक ग्राफों का विकास करने के लिए मेटाडेटा का उपयोग किया जाता है, वहाँ इन सामाजिक ग्राफों के अपराधियों या विदेशी शत्रुओं के हाथ पड़ जाने का जोखिम होता है। इस बात का भी जोखिम है कि स्वयं मंच भी इन सामाजिक ग्राफों का उपयोग पैसा कमाने के लिए कर सकते हैं - जिससे सरकारी अधिकारियों, निर्वाचित अधिकारियों, पत्रकारों, कार्यकर्ताओं, वकीलों, असहमत व्यक्तियों के संवेदनशील विवरण डेटा के दलालों और उनके ग्राहकों के हाथ लग सकते हैं।

- **डेटा का अधिक समय तक अवधारण करने से सुरक्षा जोखिम में पड़ सकती है:** मेटाडेटा अवधारण नियम अक्सर मेटाडेटा को किसी निश्चित समयावधि के लिए रखने की आवश्यकताओं को शामिल करते हैं। यदि सरकारें मेटाडेटा के अवधारण की अवधि को अधिक लंबा करती हैं, तो डेटा के उल्लंघन की स्थिति में अधिक मेटाडेटा के अरक्षित होने की संभावना के कारण निजता और सुरक्षा का जोखिम बढ़ जाता है। अधिक डेटा का अवधारण करने का मतलब है अपराधियों और विदेशी शत्रुओं के लिए अधिक उपयोगी, और अधिक आकर्षक एक लक्ष्य बनना।

- **सभी मंच मेटाडेटा की समान मात्रा एकत्र नहीं करते हैं:** उदाहरण के लिए, सिग्नल संचार को सुगम करने के लिए आवश्यक न्यूनतम मेटाडेटा एकत्र करता है और कोई भी अतिरिक्त डेटा एकत्र नहीं करता है।[12] मेटाडेटा की अधिक मात्रा का अवधारण करने

12 https://signal.org/blog/sealed-sender/

की आवश्यकताएं मंचों को अपनी प्रणालियों को उल्लेखनीय से रीकन्फिगर करने पर मजबूर कर सकती हैं, जिसमें अतिरिक्त लागत लगती है और सुरक्षा के लिए नई अरक्षितताओं के उत्पन्न होने का जोखिम बढ़ सकता है।

आरंभ से अंत तक एनक्रिप्शन को तोड़ना

चूंकि ट्रेसेबिलिटी सक्षम करने में डिजिटल हस्ताक्षरों और मेटाडेटा की उपयोगिता स्पष्ट नहीं है, ट्रेसेबिलिटी की आवश्यकताओं के साथ अनुपालन करने के लिए मंचों को संचारों की सामग्रियों को एक्सेस करने के लिए तृतीय पक्षों को अनुमति देने के लिए विधियों का उपयोग करने के लिए मजबूर होना पड़ सकता है, जिन्हें कभी-कभी असाधारण एक्सेस का नाम दिया जाता है। उपयोगकर्ताओं के संदेशों की सामग्रियों के लिए एक्सेस का निर्माण करके, मंच या सरकारी संस्था उपयोगकर्ताओं के द्वारा भेजे गए संदेशों की समीक्षा कर सकती है - जिससे वे आपत्तिजनक सामग्री का पता लगाने और वह संदेश भेजने वाले खाते की पहचान करने में सक्षम हो सकती है।

तृतीय पक्षों को एनक्रिप्ट किए गए संचारों में एक्सेस प्रदान करने के लिए कई तकनीकें प्रस्तावित की गई हैं।
इसमें शामिल है:

- *कुंजी एस्क्रौ,* जहाँ संदेशों को डीक्रिप्ट करने के लिए प्रयुक्त कुंजियों को (या तो आंशिक या पूर्ण रूप से) धारित किया जाता है किसी तृतीय पक्ष (जैसे मंच प्रदाता) द्वारा, एनक्रिप्ट किए गए संचारों की सामग्रियों तक एक्सेस सक्षम करने के लिए।
- *दोषज प्रस्ताव,* जहाँ किसी तृतीय पक्ष को संचार में एक सहभागी के रूप में चुपके से जोड़ा जाता है।
- *क्लाइंट-साइड स्कैनिंग,* जहाँ संचारों, या हैशों की[13]जो संचारों द्वारा निर्मित सामग्री के एक डेटाबेस के समक्ष मिलानों के लिए समीक्षा की जाती है, इससे पहले कि संदेश को अभिप्रेत प्राप्तकर्ता के पास भेजा जाए।

हालांकि, इंटरनेट सोसायटी की चर्चाओं में शामिल होने वाले विशेषज्ञों के सहित, विशेषज्ञों की बीच यह मतैक्य है कि तृतीय पक्ष की एक्सेस की विधियाँ तृतीय पक्षों को सामग्री में एक्सेस सक्षम करने के द्वारा आरंभ से अंत तक के एनक्रिप्शन को तोड़ देंगी, और उपयोगकर्ताओं के लिए सुरक्षा और निजता संरक्षणों को कमज़ोर करेंगी।

- **एक के लिए एक्सेस सबके लिए एक्सेस है।** किसी तृतीय पक्ष को उपयोगकर्ताओं के एनक्रिप्ट किए गए संचारों को एक्सेस करने के तरीके का निर्माण करके, प्रणाली में नई अरक्षितताओं का प्रभावी रूप से निर्माण किया जाता है। बुरे तत्वों के हाथ लग जाने के बाद, कानून प्रवर्तन या मंचों के लिए एक्सेस प्रदान करने के लिए प्रयुक्त इन्हीं विधियों का उपयोग घृणित गतिविधियों के लिए किया जा सकता है। उदाहरण के लिए, यदि किसी बुरे तत्व को एस्क्रौ की गई डीक्रिप्शन कुंजियों में एक्सेस प्राप्त हो जाती है, तो वे किसी संचार प्रणाली पर भेजे गए सभी संचारों को डीक्रिप्ट करने में सक्षम हो जाएंगे। यह सुनिश्चित करने का कोई तरीका नहीं है कि किसी असाधारण एक्सेस विधि द्वारा निर्मित अरक्षितताएं गलत हाथों में नहीं पड़ेंगी।[14]

- **असाधारण एक्सेस को लक्षित नहीं किया जा सकता है और वह सभी उपयोगकर्ताओं के लिए सुरक्षा को कमज़ोर करती है।** जब किसी प्रणाली को असाधारण एक्सेस सक्षम करने के लिए संशोधित किया जाता है, तब सभी उपयोगकर्ताओं के लिए जोखिम बढ़ जाता है। सभी उपयोगकर्ताओं के लिए अरक्षितता का निर्माण किए बिना एक उपयोगकर्ता को असाधारण एक्सेस प्रदान करने का कोई तरीका नहीं है। उदाहरण के लिए, दोषज प्रस्ताव को कार्यान्वयित करने के लिए, कुंजी वितरण प्रक्रिया को ग्रुप चैट में अनुपस्थित लोगों को गुप्त रूप से कुंजियाँ वितरित करने के लिए बदलना पड़ता है, और प्रदाताओं को उपयोगकर्ताओं को इस बात की अधिसूचनाओं का दमन करना पड़ता है कि अनधिकृत तृतीय पक्षों को उनके संचारों में एक्सेस प्राप्त है। संचार सेवा में कुंजी के वितरण और अधिसूचना को बदलकर, मंच ऐसी नई अरक्षितताएं प्रदान करता है जिनका उपयोग सभी उपयोगकर्ताओं पर किया जा सकता है।[15]

- **क्लाइंट-साइड स्कैनिंग अरक्षितताएं प्रदान करती है।** कुछ लोग तर्क देते हैं कि क्लाइंट-साइड स्कैनिंग सुरक्षित है, खास तौर पर जब संचारों को आपत्तिजनक सामग्री के डेटाबेस के साथ तुलना करने से पहले हैश किया जाता है। हालांकि, क्लाइंट-साइड स्कैनिंग अब भी ऐसी अरक्षितताएं प्रदान करती हैं जो उपयोगकर्ताओं की सुरक्षा और निजता को जोखिम में डालती हैं। बुरे तत्व, जिन्हें सामग्री के डेटाबेस में एक्सेस प्राप्त हो जाती है, मिथ्या पॉजिटिवों का निर्माण करने के लिए नई सामग्री जोड़ सकते हैं या पता लगा सकते हैं कि, किसी सामग्री को किसे, कब, और कहाँ सूचित किया गया था।[16] क्लाइंट-साइड स्कैनिंग प्रणालियाँ, जहाँ संदेश की सामग्री को डेटाबेस के साथ मिलान करने के बाद मैनुअल समीक्षा के लिए किसी तृतीय पक्ष को भेजा जाता है, विशेष

13 हैश उपयोगकर्ता सामग्री का प्रकार्यात्मक रूप से अद्वितीय डिजिटल "फिंगरप्रिंट" होता है
14 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf
15 https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/
16 https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

रूप से खतरनाक हैं क्योंकि वे बुरे तत्वों द्वारा उपयोग के लिए एनक्रिप्ट नहीं किए गए संचारों तक एक्सेस प्राप्त करने के एक नए तरीके की रचना करती हैं।

- **राष्ट्रीय सुरक्षा की चिंताएं।** यदि एक सरकारी या कानून प्रवर्तन करनेवाली संस्था किसी उपयोगकर्ता के संचारों को एक्सेस करने में सक्षम होती है, तो शत्रु देशों सहित, दुनिया के किसी भी अन्य देश के लिए भी वही क्षमता उपलब्ध हो जाएगी। सरकारी अधिकारियों और LEAs को सुरक्षित संचार चैनलों में एक्सेस नहीं मिलेगी और शत्रुओं द्वारा आवेक्षण के लक्ष्य बनने का जोखिम पैदा हो सकता है। कई सरकारी संस्थाओं ने, जिनमें यूरोपियन कमीशन[17] और अमेरिका की फौज[18] शामिल है, ने अपने कर्मचारियों को अपने संचारों को संरक्षित करने के लिए बाज़ार में उपलब्ध आरंभ से अंत तक एनक्रिप्टेड संचार सेवाओं का उपयोग करने का निर्देश दिया है।

निष्कर्ष

ट्रेसेबिलिटी के भारत में डिजिटल मंचों और संचार सेवा प्रदाताओं के लिए नियमों को लेकर बहस का एक प्रमुख मुद्दा बने रहने की संभावना है। हालांकि, ट्रेसेबिलिटी को सक्षम करने के लिए सबसे बहुधा प्रस्तावित दो विधियों की सुरक्षा, निजता और प्रभावकारिता को लेकर विश्वसनीय चिंताएं हैं, नामतः, **डिजिटल हस्ताक्षरों का उपयोग** और **मेटाडेटा का उपयोग।** ट्रेसेबिलिटी की आवश्यकताओं का अनुपालन करने के लिए, संचार सेवा प्रदाताओं को उपयोगकर्ताओं के संचारों की सामग्रियों को एक्सेस करने के लिए मजबूर होना पड़ेगा, जिससे सभी उपयोगकर्ताओं के लिए प्रणाली की सुरक्षा और निजता बहुत अधिक घट जाएगी और राष्ट्रीय सुरक्षा अधिक खतरे में पड़ जाएगी।

जब नीतिनिर्माता, विधायक, और कानूनी अधिकारी ऐसी कार्यवाहियों पर विचार करते हैं जो ट्रेसेबिलिटी आवश्यकताओं का निर्माण करेंगी, उन्हें सामग्री और सेवा प्रदाताओं से इन नियमों का अनुपालन करवाने के गंभीर निहितार्थों पर विचार करना चाहिए।

अभिस्वीकृति
हम जून से अगस्त 2020 की अवधि में वैश्विक तकनीकी विशेषज्ञों की बैठक की श्रृंखला में एशिया-पैसिफिक, अफ्रीका, यूरोप, लैटिन अमेरिका, और उत्तर अमेरिका के 50 से अधिक तकनीकी और नीति विशेषज्ञों की सहभागिता के लिए कृतज्ञ हैं।

17 https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/
18 https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/