The Dialogue™
INFORM ENGAGE IDEATE

पत्रकार अपने निजता के अधिकार का प्रयोग कैसे कर सकते हैं?

कामेश शेखर | मनरीत खेरा

संक्षिप्त

24 अगस्त, 2017 को, भारत के सर्वोच्च न्यायालय की नौ-न्यायाधीशों की संवैधानिक पीठ ने न्यायमूर्ति के.एस. पुट्टस्वामी और अन्य बनाम भारत संघ पर अपना निर्णय दिया, जिसमें संविधान के अनुच्छेद 21 के तहत गोपनीयता को मौलिक अधिकार घोषित किया गया था। एक संवैधानिक मूल्य के रूप में गोपनीयता विभिन्न मौलिक अधिकारों का विस्तार करती है। यह विशेष रूप से अभिव्यक्ति की स्वतंत्रता के अधिकार को सुरक्षित और मजबूत करता है, जो अच्छी तरह से काम करने वाली पत्रकारिता का आधार है।

लोकतंत्र के चौथे स्तंभ के सदस्यों के रूप में, नागरिकों को सूचित करने और सरकार को जवाबदेह बनाने में पत्रकारों की महत्वपूर्ण भूमिका होती है। पत्रकार अक्सर सरकार से खतरे में रहते हैं, जो उनके खिलाफ निगरानी कर सकती हैं, या अन्य प्रकार के दुर्व्यवहार कर सकती हैं। इसलिए, निजता का मौलिक अधिकार पत्रकारिता और सूचना की अखंडता को सुरक्षित करने का अभिन्न अंग है।

कोविड-19 के बाद के परिदृश्य में, पत्रकार अब न केवल अपने स्रोतों से बातचीत करने के लिए, बल्कि अपने काम का प्रसार करने के लिए भी डिजिटल माध्यमों पर निर्भर हैं। इंटरनेट या इंटरनेट-सक्षम तकनीकों का व्यापक रूप से उपयोग करते हुए पत्रकार सूचना को सुरक्षित रखने और इसकी अखंडता बनाए रखने के लिए अपने निजता के अधिकार का कहां तक प्रयोग कर सकते हैं?

यह पुस्तिका उन वैधानिक और कानूनी संरक्षणों के बारे में जानकारी प्रदान करने का प्रयास करती है जो पत्रकारों के पास उनके निजता के अधिकार को सुरक्षित करने के लिए है। इसके अलावा, इस पुस्तिका में सूचना के स्रोत और प्रसार का एक सुरक्षित शुरुआत-से-अंत तक का मॉडल विकसित करने के लिए विभिन्न उपकरणों और प्रथाओं को भी सूचीबद्ध किया गया है।

विषय सूची

1. अदालतों के क्या प्रस्ताव रहे है?

1954 से, सुप्रीम कोर्ट ने परीक्षण किया है कि क्या विभिन्न मामलों के तहत निजता का अधिकार मौलिक अधिकार होना चाहिए। लेकिन पुट्टस्वामी के फैसले ने सामूहिक रूप से गोपनीयता के मामलों की चिंताओं को संबोधित किया जो इससे पहले थे, यानी, ऐसे मामले जो राज्य की ज्यादतियों के खिलाफ गोपनीयता के लिए लड़े, अनुचित खोज और निगरानी, फोन टैपिंग के खिलाफ, शारीरिक गोपनीयता के आक्रमण, भाषण की स्वतंत्रता पर प्रतिबंध, और यहां तक कि पूछताछ के तरीकों के खिलाफ भी जो विचार की गोपनीयता पर आक्रमण करती है।

जबकि पुट्टस्वामी का फैसला 2017 में हुआ था, समय के साथ सुप्रीम कोर्ट के अलग-अलग फैसलों ने निजता के अधिकार को मौलिक अधिकार के रूप में मान्यता देने के लिए रूपरेखा तैयार की है। इन फैसलों ने निगरानी और मौलिक अधिकारों के बीच एक अनुकरणीय संबंध भी पाया, मौलिक अधिकार को सुरक्षित करने के लिए निगरानी के उपायों को पीछे धकेला गया ।

यह खंड पत्रकारों पर लक्षित कुछ निगरानी उपायों पर चर्चा करेगा और अदालत के फैसलों की चर्चा करेगा जो उनके निजता के अधिकार को सुरक्षित रखने में सहायता करते हैं।

1.1. खोज और जब्ती

भारत में कानूनी प्रवर्तन एजेंसियों (एलईए) को संबंधित कानून के उल्लंघन के सबूत एकत्र करने के लिए विभिन्न कानूनों के तहत तलाशी और जब्ती करने का अधिकार है। मीडिया घरानों पर एलईए की छापेमारी तेजी से पत्रकारों के लिए एक महत्वपूर्ण चिंता का विषय बन गई है क्योंकि इस बारे में कोई स्पष्टता नहीं है कि उन्हें क्या करना चाहिए और क्या करने के लिए वे उत्तरदायी नहीं हैं। उदाहरण के लिए, यह स्पष्ट नहीं है कि क्या कोई एलईए पत्रकारों के फोन जब्त कर सकता है क्योंकि वे सिर्फ कर्मचारी हैं और उनके फोन उनकी निजी संपत्ति हैं। एक बयान में, एडिटर्स गिल्ड ऑफ इंडिया ने सरकारी छापों की निंदा की और कहा कि उन्हें प्रेस की स्वतंत्रता को कुचलने के लिए जबरदस्ती के तरीकों का इस्तेमाल नहीं करना चाहिए।

पत्रकार अपनी सुरक्षा कैसे कर सकते हैं?

1978 के मेनका गांधी मामले ने अनुच्छेद 21 के व्यापक अंतर्संचालन की अनुमति दी, जिसने गोपनीयता को अनुच्छेद 21 के दायरे में जगह खोजने की अनुमति दी। फैसले ने यह भी प्रदान किया कि अनुच्छेद 14, 19 और 21 पर किसी भी प्रतिबंध को "उचित प्रक्रिया" से गुजरना होगा, कानूनन 'तीन परीक्षण' के अधीन। 2017 के पुट्टस्वामी फैसले द्वारा इस पर फिर से जोर दिया गया, जहां निजता के अधिकार पर किसी भी हस्तक्षेप को (i) वैधता, (ii) आवश्यकता, और (iii) आनुपातिकता की ज़रूरतों को पूरा करना चाहिए।

चूंकि खोज और जब्ती के रूप में राज्य का हस्तक्षेप पत्रकारों की निजता का उल्लंघन होगा, इसलिए इसे तीन परीक्षणों से गुजरना होगा। इसलिए, पत्रकार को यह सुनिश्चित करना चाहिए कि संबंधित एलईए के पास "कानून की उचित प्रक्रिया" के माध्यम से एक छापेमारी नोटिस है। पहले कदम के रूप में पत्रकार को छापे की वैधता सुनिश्चित करनी चाहिए, (ए) यदि अधीनस्थ प्राधिकारी के पास निदेशक या निदेशक द्वारा अधिकृत उप निदेशक का अनुमोदन है और (बी) सीआरपीसी की धारा 157 के तहत मजिस्ट्रेट को रिपोर्ट अग्रेषित की गई है । दूसरा, पत्रकारों को आवश्यकता की तलाश करनी चाहिए यानी, यह जांचने के लिए कि क्या आदेश में अनुसूचित अपराध का उल्लेख है और इसके लिए उपयुक्त सबूत हैं। तीसरा, जांच करें कि प्रस्तुत साक्ष्य तलाशी और जब्ती अभियान चलाने के लिए आनुपातिक है या नहीं।

लेकिन यह सुरक्षा संप्रभुता, राष्ट्रीय सुरक्षा और सार्वजनिक व्यवस्था जैसे उचित प्रतिबंधों के अधीन हैं।

1.2. फोन टैपिंग

भारत की संप्रभुता और अखंडता, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंध या सार्वजनिक व्यवस्था, जैसे हितों को सुरक्षित करने के लिए, सरकार कानूनी अवरोधन और संचार की निगरानी जैसे विभिन्न उपायों की स्थापना करती है।

भारतीय टेलीग्राफ अधिनियम 1885 की धारा 5 में कहा गया है कि केवल सार्वजनिक सुरक्षा और सार्वजनिक आपातकालीन मामलों में ही फोन टैपिंग की अनुमति है।

संशोधित भारतीय टेलीग्राफ अधिनियम में, धारा 5 (2) केंद्र सरकार, राज्य सरकार और केंद्र सरकार या राज्य सरकार द्वारा विशेष रूप से अधिकृत किसी भी अधिकारी को, सार्वजनिक आपात स्थिति या सार्वजनिक सुरक्षा के हित में, अवरोधन करने की अनुमति देती है। भारतीय टेलीग्राफ (संशोधन) नियम 2017 का नियम 419A भारतीय टेलीग्राफ अधिनियम की धारा 5 (2) के तहत अवरोधन के लिए दिशा प्रदान करता है। नियम बताते हैं कि अवरोधन की आवश्यकता को एलईए के प्रमुख या दूसरे सबसे प्रमुख अधिकारी द्वारा अनुमोदित किया जाना है, तीन कार्य दिवसों के भीतर। अनुमोदन के पश्चात; केंद्रीय एजेंसियों के मामले में केंद्रीय गृह सचिव और राज्य एजेंसियों के लिए राज्य के गृह सचिव से अंतिम पुष्टि की आवश्यकता है। इसके अलावा, नियम में एक समीक्षा समिति की स्थापना का प्रावधान है - कैबिनेट सचिव की अध्यक्षता में वैध अवरोधन के लिए एक निगरानी निकाय।

2013 की एक रिपोर्ट के अनुसार, केंद्र सरकार के विभिन्न एलईए द्वारा हर महीने औसतन 9000 टेलीफोन अवरोधन के आदेश जारी किए जा रहे थे। इसका मतलब है कि जब हम राज्य सरकार की एजेंसियों के आदेशों की गिनती करते हैं तो संख्या काफी अधिक होती है। एक फोन को ज्यादा से ज्यादा 180 दिन तक ही टैप किया जा सकता है। 60वें दिन के बाद, सक्षम प्राधिकारी यानी केंद्रीय एजेंसियों के मामले में केंद्रीय गृह सचिव और राज्य एजेंसियों के लिए राज्य के गृह सचिव से अवरोधन अनुरोध को एलईए द्वारा नवीनीकृत किया जाना चाहिए। हालांकि, एक आपात स्थिति में, "अधिकृत एजेंसियां" बिना अनुमति के फोन टैप कर सकती हैं, लेकिन अगर अनुमति से इनकार किया जाता है, तो टेप की गई बातचीत के सभी रिकॉर्ड को 48 घंटों में नष्ट करने की आवश्यकता होती है। एक पत्रकार के संचार को बाधित करना निजता के अधिकार का उल्लंघन कर सकता है और अभिव्यक्ति की स्वतंत्रता के अधिकार पर एक गहरा प्रभाव डाल सकता है। इसके अलावा, यह सूचना की अखंडता को भी बाधित करेगा क्योंकि स्रोतों की गुमनामी (यदि हो तो) उजागर हो जाएगी।

पत्रकार अपनी सुरक्षा कैसे कर सकते हैं?

पीपुल्स यूनियन फॉर सिविल लिबर्टीज मामले (जिसे अक्सर फोन टैपिंग मामले के रूप में जाना जाता है) में, अदालत ने फैसला सुनाया कि क्या किसी व्यक्ति के निजता के अधिकार का उल्लंघन किया गया है, यह मामले के तथ्यों और परिस्थितियों पर निर्भर करता है। लेकिन, निजता का अधिकार भी अनुच्छेद 19 से लिया गया है क्योंकि "जब कोई व्यक्ति फोन पर चैट कर रहा होता है, तो वह अपने भाषण और अभिव्यक्ति की स्वतंत्रता के अधिकार का प्रयोग कर रहा होता है"। इस मामले ने संचार को गोपनीयता के अधिकार के तहत लाया और फोन को कैसे और क्यों टैप किया जा सकता है, इस पर नियमों को निर्धारित करके संचार कानूनों को महत्वपूर्ण रूप से प्रभावित किया।इस मामले की वजह से, अब, फोन केवल अदालत या संबंधित विभाग की अनुमति से ही टैप किया जा सकता है। इसलिए, एक पीड़ित पत्रकार (एक नागरिक के रूप में) एक प्राथमिकी दर्ज कर सकता है और मानवाधिकार आयोग में जा सकता है क्योंकि अनधिकृत टैपिंग निजता के अधिकार का उल्लंघन करती है।

इसके अलावा, पुट्टस्वामी के फैसले के बाद, विनीत कुमार मामले में बॉम्बे हाई कोर्ट ने फोन टैपिंग और निगरानी से संबंधित कानून पर फैसला सुनाया, निजता के अधिकार के सिद्धांतों को भारतीय टेलीग्राफ अधिनियम की धारा 5 (2) के के संबंध में लागू किया। उच्च न्यायालय ने दृढ़ता से स्पष्ट किया कि भारतीय टेलीग्राफ अधिनियम की धारा 5 (2) के तहत अवरोधन अनुरोध 'सार्वजनिक आपातकाल' या 'सार्वजनिक सुरक्षा' स्थितियों में होना चाहिए। सिद्ध उल्लंघनों के मामले में, एजेंसी को डेटा को नष्ट करना होगा, और उसी डेटा को अदालत में सबूत नहीं माना जाएगा। इसलिए, उल्लंघन साबित होने की स्थिति में एक पीड़ित पत्रकार एजेंसी से डेटा को नष्ट करने की मांग कर सकता है।

1.3. स्रोत और डेटा को उजागर करना

पेशेवर पत्रकारों का अपने स्रोतों की रक्षा करने का एक मजबूत दायित्व है क्योंकि वे अक्सर सबसे अधिक जोखिम वाले व्यक्ति होते हैं। सूचना का स्रोत आमतौर पर पत्रकार से यह समझने की अपेक्षा करता है कि वे जो जानकारी प्रदान करते हैं उसे कैसे सुरक्षित रखा जाए, जो विश्वास बनाने के लिए महत्वपूर्ण है। लेकिन ऐसे उदाहरण हैं, जहां राज्य और गैर-राज्य नायक पत्रकार को अपने स्रोत का खुलासा करने के लिए मजबूर करते हैं और इनकार करने पर उन्हें सलाखों के पीछे डाल देते हैं।

पत्रकार अपनी सुरक्षा कैसे कर सकते हैं?

इस समस्या का कोई ठोस समाधान नहीं है क्योंकि व्यापक जनहित को सुरक्षित रखते हुए स्रोत की गोपनीयता बनाए रखने की कानूनी कमी को अभी पूरा किया जाना है। लेकिन, गोपनीयता के दृष्टिकोण से, 2014 के आधार मामले (यूआईडीएआई बनाम सीबीआई) में, अदालत ने "सहमति" को सूचनात्मक गोपनीयता के एक आवश्यक पहलू के रूप में बरकरार रखा। इसने यूआईडीएआई को मालिक की सहमति के बिना अपने डेटाबेस से किसी भी जीवमितीय जानकारी को साझा करने से रोक दिया।

इस फैसले ने गुमनामी की रक्षा के लिए एक बड़ी छलांग लगाई, जहां अदालत ने कहा कि लोग अपने बारे में डेटा और जानकारी के मालिक हैं। सूत्रों के जबरन प्रकटीकरण के मामले में इसकी व्याख्या करते हुए, तकनीकी रूप से किसी कहानी के स्रोत की कोई भी जानकारी स्रोत के स्वामित्व में होती है, न कि पत्रकार के पास। इसलिए, 2014 के आधार मामले का फैसला संभावित रूप से पत्रकारों को अपने स्रोतों की रक्षा करने में मदद कर सकता है।

2. क़ानून/मसौदा क़ानून क्या प्रदान करते हैं?

2017 के पुट्टस्वामी फैसले ने सूचनात्मक गोपनीयता की रक्षा के लिए सरकार पर एक सकारात्मक दायित्व निहित किया, जहां मेइटी ने न्यायमूर्ति श्रीकृष्ण की अध्यक्षता में डेटा संरक्षण ढांचे पर एक समिति का गठन किया। समिति ने 27 जुलाई, 2018 को अपनी रिपोर्ट और मसौदा डेटा संरक्षण विधेयक प्रस्तुत किया। व्यक्तिगत डेटा संरक्षण विधेयक, 2019 (2018 संस्करण में कुछ महत्वपूर्ण बदलाव करने के बाद) संसद के 2019 शीतकालीन सत्र में पेश किया गया और संयुक्त संसदीय को संदर्भित किया गया। आगे के विचार-विमर्श के लिए समिति (जेपीसी) ने पर्सनल डेटा संरक्षण विधेयक पर दो साल के विचार-विमर्श के बाद अपनी रिपोर्ट और ड्राफ्ट डेटा संरक्षण विधेयक, 2021 को संसद के 2021 के शीतकालीन सत्र में पेश किया।

पीडीपी विधेयक 2019 (अब डेटा संरक्षण विधेयक, 2021) पत्रकारों को उनके मौलिक अधिकारों जैसे निजता के अधिकार और अभिव्यक्ति की स्वतंत्रता के अधिकार को हासिल करने में मदद करेगा। जबकि जेपीसी रिपोर्ट के हिस्से के रूप में मसौदा विधेयक कानून बनने की दिशा में एक कदम करीब है, लेकिन इसे अभी तक अधिनियमित नहीं किया गया है। इस बीच, सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008, धारा 43, 43ए, 72ए, और 66ई के तहत सूचनात्मक गोपनीयता के कुछ पहलुओं को कानून बनाकर इस कमी को पूरा करता है।

यह खंड इन विधियों के माध्यम से पत्रकारों को प्रदान किए गए कुछ विधायी सुरक्षा उपायों पर चर्चा करेगा।

2.1. डेटा सुरक्षा

अभिव्यक्ति की स्वतंत्रता और सूचनात्मक गोपनीयता के अधिकार के बीच संतुलन बनाने के लिए, न्यायमूर्ति श्रीकृष्ण समिति ने सुझाव दिया कि प्रस्तावित कानून को "पत्रकारिता उद्देश्यों" पर विचार करना चाहिए और क्या विशिष्ट डेटा के प्रकटीकरण ने "सार्वजनिक हित" की सेवा की है। मसौदा विधेयक जनहित पर जोर देता है, और यह डेटा संरक्षण के संदर्भ में "पत्रकारिता" और "पत्रकार" की व्यापक परिभाषाओं के लिए भी तर्क देता है।

समिति की रिपोर्ट के अनुसार, कानून से पत्रकारिता छूट का आह्वान करने वाले मीडिया व्यक्तियों को डेटा प्रधानों के अधिकारों को लागू करने के अनुरोधों को अस्वीकार करने में सक्षम होना चाहिए, जैसे कि "पहुंच, पुष्टि और सही करना", जो एक रिपोर्ट के प्रकाशन या सूचना का संग्रह में बाधा उत्पन्न कर सकता है, या डेटा प्रधानों के उत्पीड़न का कारण बन सकता है। इसने एक छूट का प्रस्ताव दिया है जो पत्रकारों को भविष्य के काम के लिए डेटा को संरक्षित करने की अनुमति देगा, जब तक कि उनके पास एक स्पष्ट तर्क हो, जो किसी विशिष्ट समाचार की प्रासंगिकता, हस्तक्षेप के स्तर की आवश्यकता, डेटा प्रधान और तीसरे पक्ष पर प्रभाव, से निर्देशित होगा। मसौदा विधेयक पत्रकारों के व्यक्तिगत डेटा के लिए सुरक्षा उपायों की स्थापना की भी वकालत करता है। समिति ने जोर देकर कहा, "उन्हें डेटा हानि, चोरी या दुरुपयोग को रोकने के लिए उचित प्रयास करने चाहिए," यह कहते हुए कि छूट का लाभ उठाने वाले व्यक्तियों को यह गारंटी देनी चाहिए कि उनका प्रकाशित कार्य भ्रामक नहीं है और तथ्यों को राय से अलग करता है।

इसके अलावा, सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की धारा 72 ए को गोपनीयता और स्रोतों की गुमनामी को सुरक्षित करने के लिए बढ़ाया जा सकता है, क्योंकि सेवा प्रदाता (पत्रकार) सहमति के बिना किसी व्यक्ति की जानकारी का खुलासा नहीं करने के लिए (अनुबंध के माध्यम से) बाध्य हैं।

2.2. साइबर स्टॉकिंग (छेड़खानी) और साइबर बुलिंग (जबरदस्ती) से सुरक्षा

पत्रकारों को साइबर धमकी देना और साइबर स्टॉकिंग करना डराने -धमकाने का आम तरीका हो गया है। अगर लोग किसी खास पत्रकार को पसंद नहीं करते हैं, तो वे सब कुछ व्यक्तिगत पता लगा कर डाल देंगे या उन्हें डिजिटल स्पेस में धमकाएंगे। जबकि भारत में साइबर धमकी और साइबर स्टॉकिंग से निपटने के लिए एक अलग क़ानून का अभाव है, भारतीय दंड संहिता (आईपीसी) और सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के कुछ प्रावधानों की व्याख्या उसी के खिलाफ सुरक्षा उपायों का विस्तार करने के लिए की जा सकती है। भारतीय दंड संहिता की धारा 353-357 'पीछा करने' के मामले में सुरक्षा उपाय प्रदान करती है, विशेष रूप से आपराधिक कानून (संशोधन) अधिनियम, 2013 में धारा 354डी के तहत अपराध के रूप में "पीछा करना" शामिल है। इसलिए पत्रकार भारतीय दंड संहिता की इन उपयुक्त धाराओं के तहत शिकायत दर्ज करके साइबर स्टॉकिंग से अपनी रक्षा कर सकते हैं।

इसके अलावा, भारतीय दंड संहिता की धारा 499-507 मानहानि के लिए आपराधिक प्रावधान प्रदान करती है। पत्रकार अपनी साइबरबुलिंग शिकायतों को दर्ज करने के लिए विशेष रूप से धारा 500 (जो बदनामी को प्रकाशित करने योग्य बनाता है) और धारा 503 (जो आपराधिक धमकी में ईमेल के माध्यम से धमकी देता है) का उपयोग कर सकते हैं।

इसके अलावा, साइबर स्टॉकिंग और साइबरबुलिंग को रोकने के लिए आसानी से हैक किए जा सकने वाले डेटा की सुरक्षा करना महत्वपूर्ण है। व्यक्तिगत डेटा संरक्षण विधेयक, 2019 के अधिनियमित होने तक, संशोधित सूचना प्रौद्योगिकी अधिनियम की धारा 43A किसी फर्म या कंपनी के मामले में मुआवजे की अनुमति देती है जो किसी भी संवेदनशील जानकारी को प्रसारित करके किसी भी व्यक्ति को गलत तरीके से नुकसान या लाभ पहुंचाती है। अश्लील या आपत्तिजनक सामग्री के बजाय 'संवेदनशील जानकारी' शब्दों का उपयोग करने से यह खंड पत्रकारों के लिए कुछ हद तक प्रासंगिक हो जाता है क्योंकि कोई भी संस्था जो स्रोतों या संवेदनशील डेटा का खुलासा करती है,

सबसे आसान तरीका यह है कि आप अपने पेशेवर और व्यक्तिगत जीवन दोनों के लिए एक व्यक्ति के रूप में डिजिटल रूप से सबसे बुरे सपने का सामना कर सकते हैं। इसके अलावा, यह क्रमशः आपके संगठन और प्रियजनों को कैसे प्रभावित कर सकता है। अपना 'खतरा-मॉडल' स्थापित करने के बाद आप अपनी प्रथाओं और उपकरणों को ज़रूरतों के अनुसार तैयार कर सकते हैं:

- **जागरूकता और शिक्षा:** रॉयटर्स द्वारा जारी डिजिटल ट्रेनिंग मॉड्यूल ऑन हाउ टू प्रोटेक्ट प्राइवेसी ऑफ सोर्स एंड सेल्फ के माध्यम से पत्रकार खुद को शिक्षित कर सकते हैं और अपने अधिकारों और उपकरणों के बारे में अधिक जागरूक हो सकते हैं। वैकल्पिक रूप से, संदर्भ-विशिष्ट प्रश्नों के लिए बेझिझक हमें editor@thedialogue.co पर संपर्क करें |

- **सूत्रों से बात करना:** पत्रकारों को पहले यह निर्धारित करना चाहिए कि क्या एन्क्रिप्टेड संचार कानूनी, तकनीकी और व्यावहारिक रूप से व्यवहार्य है (अनावश्यक ध्यान आकर्षित किए बिना)। संपर्क या स्रोतों वाले डेटाबेस पासवर्ड से सुरक्षित होने चाहिए, और साक्षात्कार नोट्स और रिकॉर्डिंग को खंड 4.3 में चर्चा किए गए तकनीकी उपकरणों का उपयोग करके सुरक्षित रूप से संग्रहीत किया जाना चाहिए।

- **जांचते रहें:** पत्रकारों को मैलवेयर और खाता उल्लंघनों के लिए अपने फोन की जांच करनी चाहिए। इसके अलावा, पत्रकार Have I Been Pwned? जैसे टूल और प्लेटफॉर्म का भी उपयोग कर सकते हैं, यह जांचने के लिए कि क्या डेटा उल्लंघनों के माध्यम से उनकी व्यक्तिगत जानकारी से समझौता किया गया है।

- **मदद लें:** अगर कोई पत्रकार फंस गया है और तकनीक का जानकार नहीं है, तो उसे मदद के लिए पहुंचना चाहिए। उदाहरण के लिए, टैक्टिकल टेक की डेटा डिटॉक्स किट डिजिटल जीवन के सभी हिस्सों को नियंत्रण में रखने, बेहतर और समझदार विकल्प बनाने और ऑनलाइन आदतों को बदलने के लिए एक पत्रकार के जीवन के लिए सबसे उपयुक्त योजना बनाती है।

उसे जवाबदेह ठहराया जा सकता है। इसके अलावा, सूचना प्रौद्योगिकी अधिनियम में धारा 66सी, 66ई और 67 जैसे विभिन्न प्रावधान हैं जो पत्रकारों को साइबर धमकी से बचाते हैं।

2.3. गिरफ्तारी से उन्मुक्ति

जब पत्रकार सत्ता से सच का सामना कराते है तो उन्हें कारावास के माध्यम से निशाना बनाया जा सकता है। लेकिन पत्रकार मानहानि कानूनों के खिलाफ आंशिक रूप से अपनी रक्षा कर सकते हैं यदि वे जो सुनिश्चित हैं उसे प्रकाशित करने के लिए सावधानी बरतते हैं और सबूत के साथ इसका समर्थन कर सकते हैं। मानहानि के खिलाफ सबसे अच्छा बचाव सत्य है, इसलिए इसे मानहानिकारक नहीं कहा जा सकता। फिर भी, गैरकानूनी गतिविधि (रोकथाम) अधिनियम, 1967 और भारतीय दंड संहिता (IPC) की धारा 124A (देशद्रोह) का इस्तेमाल कई पत्रकारों को गिरफ्तार करने के लिए किया गया है, जिन्होंने " अत्यावश्यक " राज्य हित के अपवाद का उपयोग करके सरकार के खिलाफ बात की है।

हालांकि कोई अलग क़ानून नहीं है जो पत्रकारों को गैरकानूनी गिरफ्तारी से प्रतिरक्षा प्रदान करता है, फिर भी वे स्वतंत्र भाषण, स्वतंत्र प्रेस के संवैधानिक अधिकार को लागू करने के लिए अदालतों तक पहुंच सकते हैं और सत्यापित कर सकते हैं कि क्या राज्य के हित में अनिवार्य है।

3. एक पत्रकार निजता की स्वच्छता की जांच कैसे कर सकता है?

जबकि कानूनी ढांचे और क़ानून उपचार के रूप में कार्य करते हैं, पत्रकारों को नीचे दिए गए साधन और जांच सूची का उपयोग करके अपनी गोपनीयता स्वच्छता का सक्रिय रूप से परीक्षण करना चाहिए ताकि यह सुनिश्चित हो सके कि उनके कार्य सुरक्षित हैं। यह समझना महत्वपूर्ण है कि 'खतरे' की अलग-अलग धारणाएं हैं। उदाहरण के लिए, एक पत्रकार को धमकी एक वकील को दी जाने वाली धमकियों से अलग होगी। इसी तरह, एक बिजनेस-बीट पत्रकार और एक फोटो जर्नलिस्ट के लिए यह अलग होगा। अपने 'खतरे-मॉडल' को प्रभावी ढंग से निपटने में सक्षम होने के लिए निर्धारित करने का

4. प्रौद्योगिकी क्या प्रदान करती है?

पत्रकारों को गोपनीयता के प्रति जागरूक बनाने के लिए एक चेकलिस्ट होने के बावजूद, यह नोट किया गया है कि गोपनीयता जागरूकता गोपनीयता-सुरक्षित व्यवहार में तब्दील नहीं होती है, सीमित तर्कसंगतता और जानकारी के आभाव के कारण । इसलिए, यह खंड बिना किसी प्रयास के उनकी सूचनात्मक गोपनीयता को सुरक्षित करने के लिए तकनीकी उपकरणों (जैसा कि नीचे दिखाया गया है) को सक्षम करने वाले पत्रकार के विभिन्न कार्यों को लेकर गोपनीयता का मानचित्र बनाता है।

चित्र 1: तकनीकी उपकरणों का मानचित्रण

एन्क्रिप्टेड मैसेजिंग प्लेटफॉर्म एन्क्रिप्टेड मेल सर्वर वीपीएन और ट्रैकर ब्लॉकर्स	गोपनीयता के अनुकूल ब्राउज़र	पासवर्ड प्रबंधक यूबीकी ऑपरेटिंग सिस्टम एन्क्रिप्शन कलम और कागज़	अनाम फ़ाइल-साझाकरण उपकरण
स्रोतों के साथ संचार सुरक्षित करना	डेटा संग्रह सुरक्षित करना	डेटा संग्रहण सुरक्षित करना	डेटा साझाकरण सुरक्षित करना

4.1. स्रोतों के साथ संचार सुरक्षित करना

एन्क्रिप्टेड मैसेजिंग प्लेटफॉर्म: पत्रकार समुदाय द्वारा सिग्नल और टेलीग्राम का व्यापक रूप से उपयोग किया जाता है। ये एन्क्रिप्टेड मैसेजिंग ऐप हैं जो आपकी बातचीत का कोई डेटा (या मेटाडेटा भी) नहीं रखते या साझा नहीं करते हैं। इसके अलावा, ये मैसेजिंग प्लेटफॉर्म गायब होने वाले संदेशों जैसी ऑप्ट-इन सुविधाएं भी प्रदान करते हैं, जहां पत्रकार और स्रोत के बीच कोई भी बातचीत निर्धारित समय के बाद स्वचालित रूप से हटा दी जाती है ।

सिग्नल पर कॉल भी की जा सकती हैं और रिकॉर्ड की जा सकती हैं। प्रतिलेखन और बाद के संदर्भ उद्देश्यों के लिए रिकॉर्डिंग कॉल अपेक्षित हैं, लेकिन इन रिकॉर्डिंग को सुरक्षित रूप से संग्रहीत किया जाना चाहिए। कुछ लोग उन्हें पेन ड्राइव में स्टोर करते हैं, लेकिन शायद ही कोई क्लाउड सेवाओं पर भरोसा करता है।

एन्क्रिप्टेड मेल सर्वर: प्रोटॉनमेल और टूटनोटा उन पत्रकारों के लिए अतिरिक्त एन्क्रिप्शन और सुरक्षा प्रदान करते हैं, जिन्हें एक एन्क्रिप्टेड और सुरक्षित ईमेल प्रदाता की आवश्यकता होती है, जिससे वे लॉग को बंद करने में सक्षम हो जाते हैं, खासकर जब अधिक संवेदनशील जानकारी से निपटते हैं। इन मेल सर्वरों का उपयोग अभी प्रचलित होना बाकि है, पत्रकार इन संसाधनों का बुद्धिमानी से पता लगा सकते हैं और उनका उपयोग कर सकते हैं।

वीपीएन और ट्रैकर ब्लॉकर्स: वीपीएन का इस्तेमाल सुरक्षा के लिए किया जाता था, खासकर स्रोतों के साथ बातचीत के लिए। उदाहरण के लिए, पत्रकार अपनी वास्तविक पहचान के बजाय एक अवतार का उपयोग कर सकते हैं, अपने कनेक्शन को एन्क्रिप्ट करने और आईपी पते को सुरक्षित करने के लिए वीपीएन का उपयोग कर सकते हैं, डिवाइस को छिपाने के लिए पीसी का पता बदल सकते हैं, और इसी तरह। पत्रकार निगरानी आत्मरक्षा की सहायता का भी उपयोग कर सकते हैं, जिसे इलेक्ट्रॉनिक फ्रंटियर फाउंडेशन ने विकसित किया है। इन उपायों को लागू करके, पत्रकार कुछ हद तक गुमनामी हासिल कर सकते हैं और खुद को ऑनलाइन ट्रैक करना या पहचानना थोड़ा कठिन बना सकते हैं। हालाँकि, यह ध्यान रखना आवश्यक है कि वीपीएन अजेय नहीं हैं और फिर भी इनका उल्लंघन किया जा सकता है। इसके अलावा, जीरो-ट्रस्ट सिक्योरिटी नेटवर्क एक्सेस, सिक्योर एक्सेस सर्विसेज (क्लाउड-आधारित) आदि जैसे कम उपयोग किए जाने वाले विकल्प भी हैं।

इसके अलावा, ट्रैक ब्लॉकिंग ब्राउज़र एक्सटेंशन पत्रकारों को तीसरे पक्ष द्वारा गुप्त ट्रैकिंग को अवरुद्ध करने में मदद करते हैं, जो की यह पता लगते है की वो क्या खोजते हैं, और वे किन पृष्ठों पर जाते हैं। उदाहरण के लिए, इलेक्ट्रॉनिक फ्रंटियर फ़ाउंडेशन का प्राइवेसी बैजर एक मुफ़्त ब्राउज़र एक्सटेंशन है, जो पत्रकारों को तीसरे पक्ष को गुप्त रूप से ट्रैक करने और विज्ञापन पोस्ट करने से रोकने में मदद करता है, जिस भी पेज पर वे होते हैं।

4.2. डेटा संग्रह सुरक्षित करना

गोपनीयता के अनुकूल ब्राउज़र: पत्रकार जो संवेदनशील डेटा ब्राउज़ करते हैं और उन्हें गुमनामी की आवश्यकता होती है, वे टोर जैसे गोपनीयता-अनुकूल ब्राउज़रों का उपयोग करके अपनी पहचान को ऑनलाइन छिपा सकते हैं, जो आपके कंप्यूटर से आपके द्वारा इस्तेमाल किये जाने वाली वेबसाइटों से किसी भी पहचान की जानकारी को अलग कर देता है। इसे कई ऑपरेटिंग सिस्टम में स्थापित और उपयोग किया जा सकता है। टोर के अलावा, आप एक सुरक्षित, गोपनीयता-सचेत ब्राउज़र जैसे फ़ायरफ़ॉक्स, क्रोमियम या ब्रेव, और एक्सटेंशन HTTPS एवरीवेयर का उपयोग वेबसाइटों से अधिक सुरक्षित कनेक्शन का उपयोग कराने के लिए कर सकते हैं, और यूब्लॉक ओरिजिन, सामग्री को फ़िल्टर करने के लिए एक एक्सटेंशन का उपयोग कर सकते हैं।

4.3. डेटा संग्रहण सुरक्षित करना

पासवर्ड प्रबंधक: पासवर्ड मजबूत और जटिल होने चाहिए। बहु-कारक प्रमाणीकरण सुरक्षा की एक अतिरिक्त परत जोड़ता है। यह न केवल क्लाउड स्टोरेज के लिए बल्कि इंटरनेट खातों और गैजेट्स की सुरक्षा के लिए भी महत्वपूर्ण है। अगर कोई हैकर किसी पत्रकार का पासवर्ड हैक भी कर लेता है, तब भी उन्हें फ़ाइल तक पहुंचने के लिए एक कोड की आवश्यकता होगी। इसलिए, पासवर्ड सुरक्षित करने के लिए, पत्रकार एक पासवर्ड मैनेजर का उपयोग कर सकते हैं जो मजबूत, अलग पासवर्ड बनाता है और उन्हें प्रबंधित करता है। (जैसे, कीपास या बिटवार्डेन)

पासवर्ड प्रबंधकों के माध्यम से लिंक किए गए खातों और ऐप्स को प्रतिबंधित करने से पत्रकारों को अपने क्लाउड डेटा की सुरक्षा करने में मदद मिलेगी। हालांकि, क्लाउड डेटा का अस्तित्व जोखिम भरा है। अधिकारी और हैकर पारंपरिक प्लेटफार्मों पर क्लाउड डेटा

तक पहुंचने का प्रयास कर सकते हैं। यदि कोई पत्रकार तकनीक-प्रेमी है और उसके पास पर्याप्त संसाधन हैं, तो उन्हें अपना स्वयं का या व्यक्तिगत क्लाउड सर्वर बनाने का विकल्प चुनना चाहिए; अन्यथा, एक पॉड प्राप्त करें।

यूबीकी: एक हार्ड डिस्क की तुलना में एक पेन ड्राइव आसान है, और हालांकि ऐसा लग सकता है कि मोबाइल स्टोरेज और क्लाउड स्टोरेज इन्हें अप्रचलित बना रहे हैं, फिर भी वे पत्रकारों के लिए प्रासंगिक और फायदेमंद हैं। इसके अलावा, पत्रकार पेन ड्राइव को पासवर्ड से सुरक्षित कर सकते हैं। उदाहरण के लिए, पत्रकार यूबीकी जैसे बहु-प्रोटोकॉल टूल का उपयोग भौतिक पासवर्ड के रूप में या शाब्दिक रूप से एक कुंजी के रूप में कर सकते हैं जो कंप्यूटर, नेटवर्क और ऑनलाइन सेवाओं तक पहुंच की सुरक्षा करता है। उन्हें अधिकांश ऑपरेटिंग सिस्टम के साथ प्लग इन भी किया जा सकता है। हालांकि, यदि पत्रकारों की तलाशी ली जाती है तो यह संभवतः मिल जाएगा और जब्त कर लिया जाएगा, इसलिए उन्हें अच्छी तरह से छिपाना और उन्हें एन्क्रिप्ट करना आदर्श होगा।

ऑपरेटिंग सिस्टम एन्क्रिप्शन: पत्रकार दो सबसे प्रमुख ऑपरेटिंग सिस्टम, यानी विंडोज ओएस और ऐप्पल के आईओएस द्वारा प्रदान की जाने वाली फाइल एन्क्रिप्शन सुविधाओं का उपयोग करके अपने डेटा को पीसी पर सुरक्षित रूप से स्टोर कर सकते हैं। विंडोज ओएस में, एक ऑप्ट-इन फीचर है जिसे एनक्रिप्टिंग फाइल सिस्टम (ईएफएस) कहा जाता है, जो उपयोगकर्ता को हार्ड डिस्क में संग्रहीत जानकारी को एन्क्रिप्ट करने में सहायता करता है। ऐप्पल के मामले में, आईओएस के अधिकांश संस्करणों में डिफ़ॉल्ट सेटिंग के रूप में फ़ाइलों का एन्क्रिप्शन होता है। लेकिन सुरक्षा को बढ़ाने के लिए, आईओएस फाइलवॉल्ट नामक एक ऑप्ट-इन सुविधा भी प्रदान करता है, जो एन्क्रिप्टेड फाइलों (पासवर्ड-आधारित) की सुरक्षा करता है।

कलम और कागज़: संवेदनशील डेटा के लिए यह सबसे पुरानी लेकिन सबसे अच्छी नोट लेने और प्रतिलेखन की विधि है। फिर भी, इसके गलत हाथों में आने की भी सबसे अधिक संभावना है, इसलिए पत्रकारों को कार्य खत्म करते ही संवेदनशील जानकारी वाले किसी भी पेपर को नष्ट कर देना चाहिए (आग से - पेपर श्रेडर फुलप्रूफ नहीं हैं)।

4.4. डेटा साझाकरण सुरक्षित करना

अनाम फ़ाइल-साझाकरण उपकरण: संवेदनशील डेटा साझा करने के लिए, प्रत्येक पत्रकार को एक सुरक्षित और अनाम फ़ाइल-साझाकरण उपकरण की आवश्यकता होती है जैसे कि अनियनशेयर या सिक्योर ड्राप ।

5. आपका संगठन क्या पेशकश कर सकता है?

यदि आप एक फ्रीलांसर हैं, तो दोस्तों अभी के लिए बस इतना ही। हालाँकि, यदि आप किसी संगठन के लिए काम करते हैं, तो सुनिश्चित करें कि आप उनसे पूछें कि वे आपको कौन सी गोपनीयता सुरक्षा प्रदान करते हैं: संरक्षित सर्वर, बेखौफ भाषण की स्वतंत्रता, एन्क्रिप्टेड डिवाइस, सॉफ़्टवेयर, और यहां तक कि गुमनामी, और एक वकील की भी ।

व्यक्तिगत जानकारी की सुरक्षा के लिए, आपके संगठन को विशिष्ट उपकरणों और प्रक्रियाओं में निवेश करना चाहिए। क्या आपको फ़ाइलों को स्थानांतरित करने के लिए एक सुरक्षित ड्रॉपबॉक्स फ़ोल्डर की आवश्यकता है? अपने व्यक्तिगत नाम के बजाय, प्रत्येक उपयोगकर्ता के लिए अपनी कंपनी का नाम और एक सम्बन्ध-विहीन विशिष्ट संख्या का उपयोग करें। यदि आपका संगठन इन चीजों में निवेश नहीं कर रहा है या आपके पास कोई सुरक्षा प्रबंधक नहीं है जो आपकी सहायता कर सकता है, तो अपने अधिकारियो को एक भरोसेमंद डिजिटल सुरक्षा विशेषज्ञ के साथ काम पर रखने और/या कार्यशाला आयोजित करने के लिए कहें जो आपको इसे सफलतापूर्वक करना सिखाएं।

हमें लिखें और बताएं कि आपके संगठन द्वारा आपको क्या गोपनीयता सुरक्षा प्रदान की गई हैं

6. अगला: गोपनीयता जो पत्रकार देते हैं

अगले अंक के लिए प्रश्नोत्तरी:

1) कहानी के लिए तस्वीर लेने से पहले क्या आप अनुमति लेते हैं

क) जब आप किसी सार्वजनिक स्थान पर हों (हा/ना)

ख) जब विषय बच्चा हो (हा/ना)

ग) जब फोटो का विषय कहानी का विषय हो (हा/ना)

घ) जब फोटो में कोई इंसान नहीं है, लेकिन यह एक निजी स्थान है (हा/ना)

ज) जब विषय एक सेलिब्रिटी है (हा/ना)

च) जब विषय पीड़ित हो (हा/ना)

2) क्या जानकारी का खुलासा करने के बाद अगर कोई व्यक्ति ऑफ द रिकॉर्ड कहता है तो क्या जानकारी ऑफ द रिकॉर्ड है? (हा/ना)

क) क्या आप अब भी इसे गुमनाम रूप से प्रकाशित कर सकते हैं? (हा/ना)

ख) क्या आप इसे अभी भी संगृहीत कर सकते हैं? (हा/ना)

ग) क्या आप सुनी सुनाई बात या एक गुपचुप की बातचीत रिपोर्ट कर सकते हैं? (हा/ना)

3) आप गुमनाम स्रोतों की सुरक्षा कैसे करते हैं? (संक्षिप्त जवाब)

4) क्या ऐसी कोई परिस्थिति है जिसके तहत आप गुमनामी तोड़ सकते हैं? (वे क्या हैं?)

पेंसिल्वेनिया विश्वविद्यालय द्वारा देखे जाने वाले शीर्ष 10 थिंक टैंकों में से एक के रूप में मान्यता प्राप्त है।

21वीं सदी में तेजी से तकनीकी प्रगति के परिणामस्वरूप उत्पन्न होने वाली अनूठी समस्याओं को हल करने के लिए 'डायलॉग' भारत में सुसंगत सार्वजनिक नीति प्रवचन बनाता है। 'डायलॉग' का मिशन लोगों के लिए नीति लाना है और बाद में उन्हें उन मुद्दों से जोड़ना है जो आज की दुनिया में वास्तव में महत्वपूर्ण हैं, जिसमें सूचित जनमत और नागरिक भागीदारी के माध्यम से सुधारों को चलाने का दीर्घकालिक उद्देश्य है।

अधिक जानने के लिए
www.thedialogue.co पर जाएं,
या मेल करें info@thedialogue.co

The Dialogue™
INFORM ENGAGE IDEATE