मल्टीमीडिया प्रशिक्षण किट

इंटरनेट अधिकार मानव अधिकार हैं: गोपनीयता थिसिस हैंडआउट्स

कार्ली नीस्त द्वारा विकसित

मल्टीमीडिया प्रशिक्षण किट.....1

इंटरनेट अधिकार मानव अधिकारों हैं: गोपनीयता वितरण प्रपत्र हैंडआउट्स.....1

इस दस्तावेज़ के बारे में.....2

कॉपीराइट जानकारी..... 3

मॉड्यूल रूपरेखा..... 3

गोपनीयता का परिचय.....4

गोपनीयता की परिभाषा.....4

अंतरराष्ट्रीय मानवाधिकार उपकरणों में निजता के अधिकार 5

राष्ट्रीय कानूनों में गोपनीयता के अधिकार का कार्यान्वयन.....11

संस्कृतियों और संदर्भों में गोपनीयता.....14

गोपनीयता के लिए चुनौतियां.....16

डेटा संरक्षण.....17

पहचान के मुद्दे 19

निगरानी..... 20

असुरक्षित समूह.....22

गोपनीयता पर इंटरनेट और आईसीटी का प्रभाव.....23

गोपनीयता के अधिकार के कार्यान्वयन, प्रवर्तन, आनंद और उल्लंघन.....28

सरकार द्वारा व्यक्तिगत सूचना तक पहुंच और उसका प्रयोग.....30

कॉर्पोरेट जगत द्वारा व्यक्तिगत सूचना तक पहुंच और उसका प्रयोग 32

व्यक्तियों और तृतीय पक्षों से व्यक्तिगत जानकारी तक पहुंच और उसका प्रयोग...35

सारांश.....37

इस दस्तावेज के बारे में

यह सामग्रियाँ मल्टीमीडिया प्रशिक्षण किट (MMTK) का हिस्सा हैं. MMTK समुदायों और समर्थन के विकास कार्य को सशक्त करने के लिए सूचना और संचार प्रौद्योगिकी (आईसीटी) का उपयोग कर मल्टीमीडिया प्रशिक्षण सामग्री और समुदाय मीडिया, समुदाय मल्टीमीडिया केंद्र, टेलेसेन्ट्रेस समर्थन करने के लिए संसाधनों, और अन्य पहलों से एक एकीकृत सेट प्रदान करता है.

इस मॉड्यूल को प्रगतिशील संचार के लिए एसोसिएशन (एपीसी) द्वारा कमीशन और स्वीडिश अंतर्राष्ट्रीय विकास सहयोग एजेंसी (सीडा) से समर्थन के साथ आयोजित किया गया है.

कॉपीराइट संबंधी जानकारी

इस इकाई को (Attribution-Noncommercial-ShareAlike) नेकां-एसए द्वारा क्रिएटिव कॉमन्स लाइसेंस के अंतर्गत उपलब्ध कराया गया है। इन सामग्रियों का आप कैसे उपयोग कर सकते हैं यह पता लगाने के लिए इस यूनिट के साथ शामिल कॉपीराइट बयान पढें या कृपया देखें creativecommons.org/licenses/by-nc-sa/3.0/legalcode

मॉड्यूल रूपरेखा

यह मॉड्यूल निजता के अधिकार को इंटरनेट और आईसीटी के संदर्भ में देखने का प्रयास करता है. यह अंतरराष्ट्रीय और राष्ट्रीय कानूनी चौखटे में निजता के अधिकार का विश्लेषण करके शुरू होता है, और विभिन्न संस्कृतियों और संदर्भों में गोपनीयता के संरक्षण और संवर्धन के लिए प्राथमिक चुनौतियों में से कुछ का सारांश प्रस्तुत करने का प्रयास करता है.

तत्पश्चात यह गोपनीयता पर इंटरनेट और आईसीटी के प्रभाव को विश्लेषित करता है, और कार्यान्वयन और प्रवर्तन के सवालों के जवाब को व्यक्तिगत जानकारी के उपयोग के आलोक में, सरकारों, कॉर्पोरेट संस्थाओं और तीसरे पक्ष द्वारा व्यक्तिगत जानकारी के उपयोग के आलोक में गहराई से विचार करता है. यह निजता के अधिकार और निजता को बढ़ावा देने और अन्य मानव अधिकारों के बदलते स्वरूप पर केंद्रित है और इनके बीच कठिन संतुलन को किस तरह बनाये रखा जाए, उसको विश्लेषित करता है.

इस मॉड्यूल के दौरान, निम्नलिखित प्रश्न पूछे जाएंगे:

1. कैसे हम विभिन्न संस्कृतियों और राजनीतिक संदर्भों के संदर्भ में निजता के अधिकार समझते हैं?

2. निजता के अधिकार के बारे में हमारी संकल्पना को किन मुद्दों या स्थितियों से चुनौती मिलती है, और गोपनीयता की बढ़ावा देने के प्रयासों को चुनौती मिलती है?

3. इंटरनेट और आईसीटी कैसे बदल गया है और निजता के अधिकार को इसने किस तरह चुनौती दी है?

4. कैसे सरकार द्वारा व्यक्तिगत जानकारी के उपयोग और उस तक पहुँच से निजता के अधिकार को किस तरह खतरा उत्पन्न होता है?

5. कैसे कंपनियों द्वारा व्यक्तिगत जानकारी के उपयोग और उस तक पहुँच से निजता के अधिकार को किस तरह खतरा उत्पन्न होता है?

6. कैसे तीसरे पक्ष द्वारा निजता के अधिकार के उपयोग और उस तक पहुँच से निजता के अधिकार को किस तरह खतरा उत्पन्न होता है?

गोपनीयता का परिचय

गोपनीयता की परिभाषा

सरल शब्दों में, गोपनीयता के अधिकार का सही मतलब होता है अकेला छोड़ दिया जाना. गोपनीयता में निहित है अवधारणा कि व्यक्तियों को इस बात का अधिकार है कि वो तय करें कि उनके बारे में सूचना किसके पास होनी चाहिए और उस पर नियंत्रण भी रखें कि कब, कहा और कैसे इस सूचना का प्रसारण किया जायेगा? गोपनीयता का अधिकार एक मौलिक मानव अधिकार है. यह व्यक्तिगत स्वायत्तता और मानव गरिमा का एक महत्वपूर्ण रक्षा कवच है क्योंकि यह व्यक्तियों को अपने जीवन जीने के तरीके के बारे में विभिन्न विकल्प तलाश

करने की स्वेच्छता प्रदान करता है. यह आवश्यक है अन्य बुनियादी मानव अधिकार के क्रियान्वयन और आनंद के लिए, विशेष रूप से अभिव्यक्ति और आस्था की स्वतंत्रता से संबंधित मुद्दों के बारे में.

अंतरराष्ट्रीय मानवाधिकार उपकरणों में निजता के अधिकार

गोपनीयता के अधिकार को प्रमुख अंतरराष्ट्रीय और क्षेत्रीय मानव अधिकार उपकरणों में मुखरता से व्यक्त किया गया है:

• **मानव अधिकार पर (यूडीएचआर) 1948, का संयुक्त राष्ट्र घोषणा पत्र, अनुच्छेद 12:**

किसी की भी गोपनीयता के साथ मनमाना हस्तक्षेप नहीं किया जाएगा, और न ही उसकी सम्मान और ख्याति, गोपनीयता, परिवार, घर या पत्रव्यवहार के प्रति कोई मनमाना हस्तक्षेप किया जाएगा। ऐसे हस्तक्षेप या हमलों के खिलाफ हर एक को कानून का संरक्षण प्राप्त करने का करने का अधिकार है.

· **नागरिक और राजनीतिक अधिकारों (ICCPR) पर 1966 का अंतर्राष्ट्रीय वाचा, अनुच्छेद 17**:

1. किसी की भी गोपनीयता, परिवार, घर या पत्राचार के साथ मनमाना या गैर कानूनी हस्तक्षेप नहीं किया जाएगा, और न ही उनके सम्मान या प्रतिष्ठा पर अवैध हमले करने की अनुमति दी जाएगी.

2. ऐसे हस्तक्षेप या हमलों के खिलाफ कानून का संरक्षण प्राप्त करने का अधिकार है.

मानव अधिकार पर यूरोपीय कन्वेंशन (ECHR) 1950, अनुच्छेद 8 - निजी और पारिवारिक जीवन सम्मान से जीने का अधिकार

1. प्रत्येक व्यक्ति को अपने निजी और पारिवारिक जीवन, अपने घर और अपने पत्राचार के लिए सम्मान से जीने का अधिकार अधिकार है.

2. एक लोक प्राधिकरण द्वारा कोई हस्तक्षेप नहीं किया जाएगा, इस क़ानून के क्रियान्वयन में, सिर्फ उनको छोड़कर जो विधि द्वारा निर्धारित है और तर्कसंगत हैं, एक लोकतांत्रिक समाज में आवश्यक है, राष्ट्रीय सुरक्षा, सार्वजनिक सुरक्षा या देश की आर्थिक भलाई के हित में है, स्वास्थ्य या नैतिकता की रक्षा के लिए, या दूसरों के अधिकारों और स्वतंत्रता की रक्षा के लिए विकार या अपराध की रोकथाम के लिए.

गोपनीयता के अधिकार को 1990 के बाल अधिकारों पर कन्वेंशन (अनुच्छेद 16), यूरोपीय संघ के मौलिक अधिकारों के चार्टर, 2000 (अनुच्छेद 7), और मानव अधिकार पर 1969 अमेरिकी कन्वेंशन(अनुच्छेद 11) में भी परिभाषित किया गया है. 2012 नवंबर में अपनाया आसियान मानवाधिकार घोषणा पत्र, भी निजता के अधिकार (अनुच्छेद 21) को प्रतिपादित करता है.

गोपनीयता के अधिकार का विशेष रूप से इंटरनेट के संबंध में एक महत्वपूर्ण तत्व है, व्यक्तिगत डेटा का संरक्षण. हालाँकि डेटा संरक्षण का अधिकार गोपनीयता के अधिकार पारिभाषित हो सकता है, कुछ अंतरराष्ट्रीय प्रबंधन भी व्यक्तिगत डेटा के संरक्षण के लिए एक अधिक विशिष्ट अधिकार को प्रोत्साहित करते हैं:

- आर्थिक सहयोग और विकास (ओईसीडी) के पर्सनल डाटा के फ्लो और सीमाओं के आर पार दिशा गोपनीयता का संरक्षण पर निर्देशों के लिए संगठन 1981

- व्यक्तियों के संरक्षण के लिए यूरोप कन्वेंशन की परिषद 1985 के अनुसार पर्सनल डाटा का स्वत: प्रसंस्करण

- यूरोपीय संघ के 2000 के मौलिक अधिकार के चार्टर, अनुच्छेद 8

गोपनीयता का अधिकार एक पूर्ण अधिकार नहीं है. ऐसे भी उदाहरण हैं जहाँ गोपनीयता के अधिकार को वैध तरीके से राज्य द्वारा सीमित किया जा सकता है, सुनिश्चित करने के लिए ताकि अन्य बुनियादी मानव अधिकारों के संरक्षण या भोग में कोई व्यवधान न उत्पन्न हो. हालांकि, गोपनीयता के अधिकार का आनंद के साथ हस्तक्षेप केवल निर्धारित परिस्थितियों में होने चाहिए. अधिकार के साथ हस्तक्षेप मानव अधिकार कानून के तहत अनुमत होने के लिए, निम्न आवश्यकताओं को पूरा करना होगा:

1. **यह विधि के अनुसार होना चाहिए**: इसका मतलब है कि इस सीमा को तय करने के लिए एक कानूनी आधार होना चाहिए, कि सम्बंधित प्रश्न में कानून सटीक है, और कानून के मनमानी आवेदन के खिलाफ रक्षा करने के लिए सुरक्षा उपायों की व्यवस्था है .

2. **इसे एक वैध उद्देश्य को आगे बढ़ाना चाहिए** : इस तरह के वैध उद्देश्य यूरोपीय कन्वेंशन के मानव अधिकार अनुच्छेद 8 (2) में संदर्भित उद्देश्य के समान हैं, जैसे कि राष्ट्रीय सुरक्षा के हितों या विकार और अपराध की रोकथाम के रूप में.

3. **एक लोकतांत्रिक समाज में यह आवश्यक होना चाहिए**: इसका मतलब है कि यह सीमा एक अहम सामाजिक आवश्यकता का जवाब होना चाहिए और यह अपनाए वैध उद्देश्य के अनुपात में होना चाहिए.

हालाँकि इन आवश्यकताओं को स्पष्ट रूप से यूडीएचआर और ICCPR में व्यक्त नहीं किया जा रहा है, इनको ECHR की परिभाषा में पाया जा सकता है और लगातार मानव अधिकार के यूरोपीय न्यायालय द्वारा लागू किया गया है(उदाहरण के लिए, देखते हैं, ओलसन बनाम स्वीडन (संख्या 1), ECHR, आवेदन संख्या 10465/83, 24 मार्च, 1988 का निर्णय). आतंकवाद का मुकाबला करते हुए निजता के अधिकार की रक्षा करने पर उनकी 2009 की रिपोर्ट में, पदोन्नति और मानव अधिकारों के संरक्षण और आतंकवाद, का मुकाबला करते हुए मौलिक स्वतंत्रता पर संयुक्त राष्ट्र के विशेष दूत, मार्टिन शेनिन ने इस बात की पुष्टि की कि यूडीएचआर और ICCPR के तहत अनुमेय सीमाओं के परीक्षण पर निजता के अधिकार की व्याख्या लागू होती है(A/HRC/13/37).

राष्ट्रीय कानूनों में गोपनीयता के अधिकार का कार्यान्वयन

राष्ट्रीय स्तर पर गोपनीयता के अधिकार को कई विधायी और विनियामक उपकरणों में प्रासंगिकता प्राप्त है. विधान की आवश्यकता होती है जो यह सुनिश्चित करता है कि गोपनीयता व्यापक घरेलू कानूनी शासनों में सुरक्षित है, जिनमे शामिल हैं गोपनीयता के विभिन्न प्रकार - संचार, सूचना और व्यक्तिगत डेटा, सहित शारीरिक गोपनीयता से संबंधित- विभिन्न क्षेत्रों की सीमा के पार , जैसे सूचना प्रौद्योगिकी और संचार, बैंकिंग और वित्त, स्वास्थ्य, आपराधिक न्याय और कानून प्रवर्तन, आव्रजन के रूप में.

हालाँकि गोपनीयता के लिए इस्तेमाल किये जाने वाले विधायी और विनियामक उपकरणों के प्रकार देशों और क्षेत्रों के बीच काफी अलग है, किसी भी देश के गोपनीयता ढांचे के तत्वों के गठन के उदाहरणो में शामिल हो सकता है:

- एक **संवैधानिक प्रावधान** गोपनीयता का सुस्पष्ट अधिकार स्थापित करने, या संवैधानिक न्यायशास्त्र द्वारा गोपनीयता के लिए एक अनुमानित अधिकार की स्थापना करे

- **अधिकार** या **राष्ट्रीय मानवाधिकार के बिल** में गोपनीयता के लिए एक खंड की आधिकारिक स्थापना अधिनियम, या राष्ट्रीय न्यायशास्त्र द्वारा गोपनीयता के लिए एक अनुमानित आधिकारिक स्थापना करे.

- **डेटा संरक्षण कानून** जो तय करे कि एक व्यक्ति के निजी डेटा का उपयोग किस तरह किया जाये और संग्रहीत और स्थानांतरित किस तरह किया जाये, और इसके लिए एक आयुक्त के रूप में, एक नियामक प्राधिकरण की स्थापना करे.

- **सूचना की स्वतंत्रता का कानून** जो रेखांकित करे कि कैसे जानकारी को नियंत्रित और सार्वजनिक किया जा सकता है, और इसके लिए एक आयुक्त के रूप में, एक नियामक प्राधिकरण की स्थापना करे.

- **कानून प्रवर्तन और राष्ट्रीय सुरक्षा कानून** जो अन्य विधायी उपकरणों सहित आपराधिक प्रक्रिया कोड या कानून, आतंकवाद विरोधी कानून, साइबर अपराध कानून, और खोजों और अवरोधन के आचरण और संचार की निगरानी के लिए कानून प्रवर्तन अधिकारियों की क्षमता को विनियमित करे.

- विधान, **खुफिया सेवाओं** को विनियमित करने, खोजों, अवरोधन और निगरानी के लिए संचार का संचालन करने के लिए खुफिया सेवाओं के अधिकार की स्थापना.

- **सूचना और संचार कानून**, नियमन स्थापित करना ताकि संचार जानकारी के संग्रह की परिस्थितियों तय की जा सकें, आवागमन डाटा और सामग्री सहित, जिसके तहत संचार सेवा प्रदाताओं की

भूमिकाओं और जिम्मेदारियों को निर्धारित किया जा सके, और परिस्थितियां निर्धारित की जाएं ताकि सम्बद्ध अधिकारी उन परिस्थितियों के अंतर्गत ही इन सूचनाओं को देख सकें.

- कानून, नियमों या अभ्यास के कोड जो शासित करेंगे:

1. सीसीटीवी कैमरों के उपयोग को
2. साइबर कैफे के संचालन
3. डीएनए डेटाबेस सहित राष्ट्रीय पहचान प्रणाली, राष्ट्रीय बॉयोमेट्रिक प्रणाली और आईडी कार्ड प्रणाली की स्थापना
4. कार्यस्थल का अनुप्रवर्तन और निगरानी

- वित्तीय और बैंकिंग कानून
- · स्वास्थ्य सेवाओं विधान
- · व्यापार प्रथाओं और उपभोक्ता कानून
- · विधान या ई-गवर्नेंस और डेटा साझा प्रथाओं से संबंधित नियम

संस्कृतियों और संदर्भों में गोपनीयता

यद्यपि देशों के बीच गोपनीयता के अधिकार की अभिव्यक्ति और उसकी सुरक्षा प्राप्त करने के तरीके काफी भिन्न होते हैं, लगभग हर देश ने अपने घरेलू कानूनी व्यवस्था में गोपनीयता के कानून किसी न किसी रूप में शामिल किये हैं. गोपनीयता की स्पष्ट संवैधानिक अधिकार कम से कम 45 राष्ट्रीय संविधानों में विविध रूप में पाया जा सकता है, इन देशों में शामिल है

बुल्गारिया और बुरुंडी , चिली और क्रोएशिया, और निहित गोपनीयता के अधिकार कई और अधिक संविधानों में स्थापित किए गए हैं. अंतरराष्ट्रीय व्यापार और व्यापार व्यवस्था का एक महत्वपूर्ण तत्व है डेटा संरक्षण कानून को आत्मसात करना, खासकर जब यूरोपीय निगमों और सरकारों द्वारा उन देशों को आउटसोर्सिंग निषेध की हुई है जो यूरोपीय संघ के डेटा संरक्षण कानून के नियमों को नही मानते. समान रूप से, कई देशों में सीमा पार से संचार और साइबर सुरक्षा के मुद्दों की बढ़ती मान्यता से संबंधित कानून को आत्मसात करने के लिए नेतृत्व किया है.

हालांकि, गोपनीयता अधिवक्ताओं द्वारा सबसे प्रखर आलोचनाओं में से एक जिनका उन्हें सामना करना पड़ता है, ये वो है कि गोपनीयता का अधिकार एक पश्चिमी निर्माण है जो व्यक्तिपरक संस्कृतियों के लिए महत्वपूर्ण हो सकता है पर समूहवादी अर्थव्यवस्था वाली संस्कृतियों के लिए अप्रासंगिक है. आलोचकों का तर्क है कि निजता के अधिकार पश्चिमी उदार परंपरा के हिस्से के रूप में विकसित हुआ है, और एशियाई संस्कृतियों में इसे कोई प्रमुखता प्राप्त नहीं है.(1)(उदाहरण के लिए, जूली ई कोहेन देखें : Configuring the Networked Self: Law, Code and the Play of Everyday Practice, Yale University Press, 2012.) गोपनीयता के अधिकार की एक नारीवादी दृष्टिकोण से भी आलोचना की जाती है, जो कुछ मामलों में गोपनीयता के विचार को खतरनाक रूप में देखती है क्योंकि वो राज्य के गैर हस्तक्षेप को प्रोत्साहित करती है और घरेलू क्षेत्र में महिलाओं की अधीनता को बनाए रखती है .(2)([2] उदाहरण के लिए, देखें Catherine MacKinnon, *Toward a Feminist Theory of the State*, Harvard University Press, 1989.Page 5)

मानव अधिकारों के संभाषण में अन्य सांस्कृतिक रिलेटिविस्ट बहस की तरह, आलोचक अक्सर पिछले 50 वर्षों में एशिया भर में आई हुई सांस्कृतिक और सामाजिक परिवर्तन और विकास

की जटिल प्रक्रिया लेने के लिए उपेक्षा कर जाते हैं. इसके अलावा, वे एक जटिल मुद्दे को अत्यंत सरलता से प्रस्तुत करने का प्रयास करते हैं. उदाहरण के लिए, थाईलैंड में, गोपनीयता के प्रति उच्च जागरूकता है बनाम मतदाता गोपनीयता, पुलिस घुसपैठ और शारीरिक गोपनीयता, लेकिन कम जागरूकता है उपभोक्ता संरक्षण के संबंध के साथ. दूसरी ओर, बांग्लादेश में उपभोक्ता गोपनीयता के मुद्दों में विशेष दिलचस्पी है. चीन के अध्ययनों से पता चलता है कि वहां पर खासकर डेटा संरक्षण से संबंधित गोपनीयता के मुद्दों में रुचि बढ़ रही है.

विधायी व्यवस्थाएं और एशिया भर से स्थानीय न्यायशास्त्र के स्कैन से निष्कर्ष को समर्थन मिलता है कि गोपनीयता एशियाई समाजों के लिए प्रासंगिक और महत्वपूर्ण है. फिर भी, यह स्पष्ट है कि गोपनीयता की अवधारणाएं वे ऐतिहासिक अवधियों में भिन्न होती हैं और, संस्कृतियों और स्थानों में भी होती हैं अलग अलग तरह से विद्यमान होती हैं. चुनौती है कि गोपनीयता को सरलीकृत सांस्कृतिक तर्क से परे समझने के लिए प्रयास किया जाए स्थानीय सांस्कृतिक और लौकिक संदर्भों के भीतर. अंतरराष्ट्रीय मानवाधिकार उपकरणों में मुखर होने के बावजूद गोपनीयता को समाज से परे स्वतंत्र रूप से नहीं समझा जा सकता.

गोपनीयता के लिए चुनौतियां

निजता के अधिकार की प्राप्ति को हर कोण से चुनौतियों का सामना करता है. नए सुरक्षा खतरों और वास्तविकताओं, पहचान और रिश्तों को, तेजी से तकनीकी प्रगति, निजीकरण और आधुनिकीकरण की दिशा में सामाजिक व्यवहार बदल रहा है, और बढ़ती आबादी के लिए सार्वजनिक सेवाओं के वितरण की सभी चुनौतियों का हल ढूंढने के प्रयास में गोपनियता की अवधारणाओं को खतरे की स्थिति का सामना करना पड़ रहा है. गोपनीयता के लिए उत्पन्न हुई चुनौतियों में से कुछ नीचे विस्तृत रहे हैं:

डेटा संरक्षण

गोपनीयता के लिए प्रमुख चुनौतियों में से एक व्यक्तिगत डेटा और जानकारी की सुरक्षा है.आज भारी मात्रा में अभूतपूर्व गति और आवृत्तियों से व्यक्तियों के बारे में डेटा उत्पन्न किया जा रहा है. क्योंकि तकनीकी में नवोन्मेष से, डेटा जिस व्यक्ति से संबंधित हैं उसके लिए ही महत्वपूर्ण नहीं हैं, बल्कि विभिन्न प्रयोजनों के लिए विभिन्न किस्म से इस्तेमाल किया जा सकता है. उदाहरण के लिए, कंपनियों ने इस तरह ऑनलाइन डेटा का विश्लेषण करके, प्रवृत्तियों और पसंदों पर नज़र रख के ग्राहक वरीयताओं का विश्लेषण के रूप में प्रयोग करके वाणिज्यिक प्रयोजनों के लिए सक्षम कर लिया है. सरकारें, सरकारी एजेंसियों को उपलब्ध कराए गए आंकड़ों का विश्लेषण कर सकती हैं और अपने नागरिकों के बारे में बेहतर ज्ञान और नियंत्रण कर सकती हैं.

कई तरीके हैं जिनसे एक व्यक्ति के व्यक्तिगत डेटा का उपयोग करके व्यक्ति की गोपनीयता, और अन्य मानव अधिकारों के अपने आनंद, का उल्लंघन किया जा सकता है. अगर डेटा अपर्याप्त रूप से संग्रहीत और नियंत्रित किया जाता है, तो वे चोरी या धोखाधड़ी के परिवर्तन की चपेट में आ सकता है. एक कंपनी के लिए या सरकार के लिए गोपनीय आधार पर एक व्यक्ति द्वारा उपलब्ध कराई गई जानकारी को अगर साझा किया जाता है, तो वह व्यक्ति, उदाहरण के लिए, एक नौकरी के लिए आवेदन करते समय या एक ऋण लेने के समय, भेदभाव का अनुभव कर सकता है, या वित्तीय धोखाधड़ी के गंभीर रूपों का शिकार भी हो सकता है. अगर जानकारी को लंबी अवधि के लिए बनाए रखा जाता है, तो जानकारी के अन्य रूपों के साथ एक साथ एकत्र किया जा सकता है जिससे एक व्यक्ति की संचार, आंदोलनों, गतिविधियों और खरीद की पूरी प्रोफाइल बना सकते हैं. ये प्रोफाइल विज्ञापन और मूल्य

निर्धारण के बारे में निर्णय लेने के लिए निगमों द्वारा उपयोग किया जा सकता है. अगर एक व्यक्ति कानूनी कार्यवाही के अधीन है, तो ऐसी जानकारी को उनके खिलाफ इस्तेमाल किया जा सकता है .

पहचान के मुद्दे

आईडी कार्ड और बॉयोमीट्रिक और डीएनए डेटाबेस सहित पहचान प्रणाली, तेजी से नागरिकों का ट्रैक रखने और सार्वजनिक सेवाओं के वितरण में सुधार, कानून प्रवर्तन के प्रयासों के प्रभाव में वृद्धि, और प्रवास के प्रबंधन के लिए एक साधन के रूप में सरकारों द्वारा अपनाई जा रही है. आईडी सिस्टम निजता के अधिकार को चुनौती है इस प्रबंधन से प्राप्त जानकारी को वे, उस जानकारी की सत्यता की किसी गारंटी के बिना, बाद में अलग-अलग तरह से एकत्रित और विश्लेषित करते हैं. आईडी कार्ड के साथ जुड़ी सूचना के आधार पर, एक व्यक्ति के बारे में गंभीर निर्णय लिए जा सकते हैं जो उसके अन्य मानव अधिकारों के आनंद को संकट में डाल सकता है. आईडी कार्ड एक व्यक्ति की नस्ल या धर्म के रूप में संवेदनशील जानकारी रिकॉर्ड करते हैं जिसे किसी भी तरह के भेदभावपूर्ण उद्देश्यों के लिए इस्तेमाल किया जा सकता है. आईडी कार्ड भी धोखाधड़ी या दोहराव की चपेट में हैं. जब बायोमेट्रिक या डीएनए जानकारी पहचान प्रणाली से जुड़ा हुआ है, तो इससे आगे जोखिम की स्थिति उत्पन्न होती है. बायोमीट्रिक डेटा अक्सर अविश्वसनीय हैं और उनके उपयोग से अपवर्जनात्मक प्रभाव पड़ सकता है. डीएनए डेटा बेहद संवेदनशील होते हैं और मजबूत सुरक्षा उपायों के अभाव में चोरी और दुरुपयोग के लिए जोखिम रहता है. मानव अधिकारों के नजरिए से बॉयोमीट्रिक, डीएनए और केंद्रीकृत डेटाबेस में पहचान संबंधी जानकारी की बड़ी मात्रा का एकत्रीकरण विशेष रूप से चिंताजनक है. ऐसे डेटाबेस अविश्वसनीय रूप से मूल्यवान संसाधन है पर इसको चोरी या

धोखाधड़ी के खिलाफ सुरक्षित करना मुश्किल है. नतीजतन, उसमें निहित जानकारी के चोरी होने का खतरा होता है, धोखे से बदलने का खतरा होता है, दुरुपयोग या गलत प्रयोग का खतरा होता है.

निगरानी

निगरानी गोपनीयता के लिए एक गंभीर और बढ़ती चुनौती है. दोनों संचार निगरानी- ऑनलाइन गतिविधियों और टेलीफोन संचार के अवरोधन के द्वारा निगरानी - और शारीरिक निगरानी, अपराध, विकार और आतंकवाद का मुकाबला करने के साथ ही अन्य राष्ट्रीय सुरक्षा उद्देश्य को आगे बढ़ाने के लोकप्रिय साधन हैं. सीसीटीवी कैमरों का एक वैश्विक प्रसार किया गया है; अकेले ब्रिटेन में, एक अनुमान के अनुसार 300,000 सीसीटीवी कैमरे हैं.(3)(See Privacy International, “CCTV frequently asked questions”, available at www.privacyinternational.org/blog/cctv-frequently-asked-questions.) कैमरों की क्षमता और गुणवत्ता में सुधार के साथ उनके उपयोग की वृद्धि हद तक जारी है कई शहरों में वे अब निजी और साथ ही सार्वजनिक स्थानों में इस्तेमाल हो रहे हैं जैसे मशीनों, बसों, ट्रेनों, टैक्सियों वेंडिंग, फोन बूथ के अलावा, सड़कों और एटीएम के अंदर. सीसीटीवी की क्षमताओं को अब दुनिया भर में अपराध का पता लगाने और नियंत्रण रणनीतियों के लिए एक अनिवार्य हिस्सा हैं. वे तेजी से कार्यस्थल निगरानी की दिशा में एक व्यापक कदम के हिस्से के रूप में कार्यस्थलों में कार्यरत हैं. संचार निगरानी भी पता लगाने और अपराधों के अभियोग का एक तेजी से उभरता हुआ लोकप्रिय साधन है. पिछले एक दशक में राष्ट्रीय सुरक्षा के मुद्दों द्वारा प्रेरित होकर, विशेष रूप से आतंकवाद, कानून की प्रक्रियाएं धीरे-धीरे अधिक अनुमोदक बन गई हैं और संचार निगरानी की प्रथाओं और अधिक अंधाधुंध और आक्रामक. आज की तारीख में जब

आम व्यक्ति ऑनलाइन अपना समय ज्यादा व्यतीत कर रहा है, सरकारों की निगरानी करने और ऑनलाइन गतिविधियों अवरोधन करने के नए तरीकों का अधिग्रहण किया है. हालांकि निगरानी एक वैध उद्देश्य है,जब उसका कानून प्रवर्तन गतिविधियों के लिए उपयुक्त मामलों में इस्तेमाल किया जाता है, कई देशों में यह नियंत्रण और असंतोष दबाने के एक तंत्र के रूप में अधिक व्यापक रूप से इस्तेमाल किया जाता है. सरकारें प्रौद्योगिकियों के उपयोग से अब देश भर में बड़े पैमाने पर अवरोधन और संचार की निगरानी की सुविधा का प्रयोग करके व्यक्तियों के स्थान, और व्यवहार की रूपरेखा आवाज और की वर्ड्स के माध्यम से निगरानी कर सकते है. कुछ देशों के पास इस तरह की तकनीकी उपलब्ध है जिसके माध्यम से स्काइप कॉल के दौरान सुनने के लिए, ईमेल अवरोधन करने, हटाने और संशोधन करने के लिए और रिमोट जगह से लैपटॉप या स्मार्टफोन पर मौजूद माइक्रोफोन और कैमरे को ओन करने में सरकारों को सक्षम कर दिया है. इस तरह की तकनीकों को स्वतंत्र रूप से बेचा जाता है और मानव अधिकारों के रक्षक, राजनीतिक असंतुष्ट और कार्यकर्ता संगठनों पर नज़र रखने के प्रभावी साधन के रूप में इस्तेमाल किया जा रहा है.

कमजोर वर्ग

कुछ समूह जो ऐतिहासिक दृष्टि से हाशिए पर हैं, और काफी हद तक सरकार की नीतियों से जिन्हे अक्सर सताया जाता है निजता के अधिकार से उत्पन्न होने वाली चुनौतियोँ से असामान्य रूप से प्रभावित होते हैं. इस तरह के लोगों में शामिल हैं की महिलाओं के समूह, बच्चों, उनके राजनीतिक संबद्धता या एक जातीय या यौन अल्पसंख्यक की सदस्यता के आधार पर उत्पीड़न के अधीन व्यक्ति, और एचआईवी / एड्स के साथ जी रहे लोग. निगरानी विशेष रूप से महिलाओं को नुकसान पहुंचाती है, जिनकी आवाज पहले से ही खामोश कर दी गयी है

और जो संरचनात्मक भेदभाव और पारंपरिक पितृसत्तात्मक नजरिए से हाशिए पर हैं. डेटा संरक्षण के उल्लंघन विशेष रूप से जब वे इस तरह के स्वास्थ्य की देखभाल के रूप में सार्वजनिक सेवाओं के प्रावधान से संबंधित हैं, अक्सर महिलाओं के दूरगामी प्रभाव लेकर आती हैं, क्योंकि उनकी पहचान, उनके यौन और प्रजनन अधिकारों के संबंध में विकल्प और निर्णय राजनीतिक और धार्मिक ताकतों के हमले से प्रभावित होते हैं. एचआईवी / एड्स के साथ रहने वाले लोग भी गोपनीयता के उल्लंघन के बढे जोखिम का अनुभव करते हैं जब वे अक्सर सरकारी सेवाओं के संपर्क में आते हैं, जो असफल गोपनीयता के साथ उनके स्वास्थ्य की स्थिति का इलाज करते हैं.

गोपनीयता पर इंटरनेट और आईसीटी का प्रभाव

यह स्पष्ट है कि इंटरनेट और आईसीटी के आगमन के साथ निजता और गोपनीयता के हमारे अधिकार के समझने के मायने नाटकीय रूप से बदल गए हैं. इंटरनेट और आईसीटी ने मानव अधिकार, अभिव्यक्ति और जानकारी की स्वतंत्रता के संबंध में विशेष रूप से एक परिवर्तनकारी और सकारात्मक भूमिका निभाई है दूसरी तरफ, उसने वे भी गोपनीयता के मनोरंजन के लिए खतरे और जोखिम को बढ़ा दिया है. इंटरनेट (तकनीकी नवाचार और डिजिटलीकरण की प्रक्रिया जो उसके साथ विकसित हुई है) के आविर्भाव ने निजी व्यक्तियों के बारे में सूचना और संचार निगरानी के तंत्र के विस्तार के प्रसार में क्रांतिकारी भूमिका निभाई है. आईसीटी एक व्यक्ति के न केवल संचार के बारे में जानकारी और रिकॉर्ड उत्पन्न करता है, बल्कि साथ ही साथ उनके व्यवहार और खरीद ब्राउज़िंग, और उनके स्थान के बारे में भी सूचना एकत्रित करता है. तकनीकी प्रगति कानूनों और नियमों में परिवर्तन से आगे निकल गई है, और व्यक्तिगत जानकारी और इंटरनेट और आईसीटी के माध्यम से उत्पन्न डेटा असुरक्षित है और इसका

प्रयोग शोषण करने के लिए किया जा सकता है जो गोपनीयता के अधिकार के लिए गंभीर रूप से प्रतिकूल असर डाल सकता है. समय के साथ और विभिन्न समुदायों में निजता के अधिकार पर इंटरनेट और आईसीटी के प्रभाव पर परिप्रेक्ष्य मतभेद है. इंटरनेट और नए मीडिया के प्रारंभिक वर्षों के दौरान, और 1990 के दशक तक, यह बहस थी कि कुछ आधुनिक तकनीकों ने शायद बहुत ज्यादा गोपनीयता की अनुमति दी है.(4) [4] See, for example, Amitai Etzioni, *The Limits of Privacy,* Basic Books, 1999 है. प्रौद्योगिकी और, विशेष रूप से, क्रिप्टोग्राफी का उपयोग प्रभावी कानून प्रवर्तन रोकने के रूप में देखा गया था. 2000 के दशक में, गोपनीयता को बढे हुए राष्ट्रीय सुरक्षा के भय की स्थिति में, सुरक्षा में एक अवरोध करनेवाले के रूप में देखा गया था.(5) [5] See, for example, Richard Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency*, Oxford University Press, 2006. इस समय के दौरान, आईसीटी के लिए कानून प्रवर्तन दृष्टिकोण को स्थानांतरित कर दिया गया: वे और बडी निगरानी के लिए एक संबल बन गया प्रोफाइलिंग और ट्रैकिंग के नए रूपों की सुविधा को बढ़ावा देकर. सुरक्षा और गोपनीयता के बीच यह संतुलन इंटरनेट और मानव अधिकारों के आसपास बहस का एक अधिभावी फीचर बना हुआ है. इसी प्रकार, जबकि गोपनीयता के अधिकारों की वकालत करने वाले शुरू में सबसे आगे थे, इंटरनेट के लिए अनुकूल तकनीकी प्रगति के और समर्थन के मामले में, हाल के वर्षों में वे अक्सर नवीनता के विरोधी रूप में ऑनलाइन गोपनीयता के परिपेक्ष्य में जाने जाते हैं जब ऑनलाइन निजता के सन्दर्भ में नियमन और अंकुश लगाने की बात होती है. इस बदलाव ने मानव अधिकारों के समुदाय के भीतर भी दृष्टिकोण में मतभेद को उजागर किया है, जो समग्र रूप से इंटरनेट और आईसीटी को सभी मानव अधिकारों के संवर्धन और संरक्षण के परिवर्तनकारी उपकरण के रूप में देखता है. साथ ही साथ, APC के इंटरनेट राइट्स चार्टर जैसी पहल , जिसने इंटरनेट के निजता के

अधिकार को अन्य मानवाधिकारों के समकक्ष रखा है, इस पहल से दूरियों को कम करने का प्रयास करता है. नयी चुनौतियाँ नित नए रूप में उजागर हो रही हैं जो हमारी निजता के अधिकार की पुरानी समझ को नए दृष्टिकोण से देखने को मजबूर करती हैं, जिनमे शामिल हैं ऑनलाइन सूचना को साझा करने के बदलते हुए पैमाने और नयी तकनीकियों का आविर्भाव जो पर्यवेक्षण और ट्रैकिंग के नए रूपों को जन्म दे रही हैं जिनके बारे में पहले किसी ने सोचा भी नहीं होगा. गुमनामी ऑनलाइन अभिव्यक्ति की स्वतंत्रता का एक अनिवार्य तत्व है, और इसके बावजूद यह परंपरागत मानहानि कानूनों के आवेदन को रोकता है और गोपनीयता और प्रतिष्ठा की रक्षा के अधिकार के लिए खतरा हो सकता है. ऑनलाइन जानकारी का प्रावधान एक व्यक्ति की ब्राउज़िंग अनुभव को बढ़ाने और कार्यकुशलता में सुधार कर सकता है साथ ही साथ उन्हें गोपनीयता के उल्लंघनों के जोखिम की तरफ भी ले जा सकता है.

यह तो स्पष्ट है कि जैसे जैसे इन्टरनेट और ICT हमारी जिंदगी का अंतरंग हिस्सा बनते जा रहे है उसी तरह निजता की प्राचीन मान्यताओं के मायने भी पल प्रतिपल बदलते जा रहे हैं.(6)(David Souter for APC, “Human Rights and the Internet: A review of perceptions in human rights organisations”, 2012, available at)www.apc.org/en/system/files/HumanRightsAndTheInternet_20120627.pdf

Page 7. समान रूप से, मानव अधिकारों के दायित्वों की प्रकृति की समझ भी एक परिवर्तन के दौर से गुजर रही है. बल्कि सरकारों की तुलना में निजी क्षेत्र की कंपनियां प्राथमिक संग्राहकों और व्यक्तिगत जानकारी और डेटा के उपयोगकर्ता रहे हैं, पर अभी तक वे पारंपरिक रूप से सरकारों पर लागू किये गए मानव अधिकारों के दायित्वों के अधीन नहीं हैं। इस संदर्भ में, उदाहरण के लिए, गूगल की पारदर्शिता रिपोर्ट के रूप में पहल गोपनीयता और इंटरनेट के संदर्भ में कॉर्पोरेट जवाबदेही और पारदर्शिता के मुद्दों को संबोधित करने की दिशा में एक महत्वपूर्ण कदम है.

गोपनीयता के प्रति दृष्टिकोण, इंटरनेट और आईसीटी भी बदल रहे हैं। जैसे जैसे सरकार द्वारा व्यक्तियों की निगरानी और व्यक्तिगत डेटा के कॉर्पोरेट शोषण की वास्तविकता और अधिक स्पष्ट हो रही है, इंटरनेट के उपभोक्ता भी तेजी से ऑनलाइन, उनके बारे में उपलब्ध जानकारी की रक्षा के लिए कदम उठा रहे हैं. फेसबुक और इंस्टाग्राम(7) जैसे सामाजिक नेटवर्किंग साइटों

में निजता के दृष्टिकोण के पैमाने के खिलाफ बढ़ते आक्रोश और ऑनलाइन गोपनीयता के महत्व की वृद्धि निजता के प्रति जागरूकता का सबूत है. गोपनीयता "घोटालों" ने विनियामक परिवर्तन को उत्प्रेरित करने में प्रभावी भूमिका निभाई है और कारक रहा है कानूनी परिवर्तनों को क्रियान्वित करने में. इस तरह की घटनाओं के उदाहरण में शामिल है ऑक्टोपस पुरस्कार द्वारा बिक्री- हांगकांग के डिजीटल सार्वजनिक परिवहन भुगतान प्रणाली- 1.97 करोड़ पंजीकृत उपयोगकर्ताओं की व्यक्तिगत जानकारी की बिक्री और दक्षिण कोरिया के ऑनलाइन गेम कंपनी Nexcon द्वारा एक डेटा रिसाव जिसके कारण 13,200,000 का डेटा सार्वजनिक हो गया.

लोग अपनी गोपनीयता के लिए जोखिम के प्रति अधिक जागरूक हैं और वे इंटरनेट और आईसीटी के उपयोग के बारे में जागरूक निर्णय करने में अधिक सक्षम होते जा रहे हैं. फिर भी गोपनीयता और अन्य मानव अधिकारों के लिए सही के बीच तनाव बना हुआ है. आईसीटी के प्रसार, विशेष रूप से अफ्रीका में, अधिक से अधिक कनेक्टिविटी को सुविधाजनक बना रहा है और सक्षम सूचना के प्रवाह ने, समुदायों को आकर्षक और सशक्त बनाने में अहम भूमिका निभाई है. साथ ही साथ इसने गोपनीयता से सम्बंधित गम्भीर मुद्दों पर भी प्रकाश डाला है - उपकरणों की चोरी का जोखिम और उनका हैक किया जाना - और सबसे गरीब और सबसे उपेक्षित समूहों के ऊपर भेदभावपूर्ण प्रभाव छोड़ सकता है. इसी प्रकार ऑनलाइन गोपनीयता की सुरक्षा जैसे एन्क्रिप्शन उपकरण के निरंतर बढ़ते हुए का प्रयोग, पासवर्ड और एन्क्रिप्टेड साइट गोपनीयता की सुरक्षा का एक महत्वपूर्ण साधन रहे हैं, फिर भी वे सुरक्षा में गुणात्मक सुधार करने के के प्रयासों को विफल कर सकते हैं. ये मुद्दे निजता, इंटरनेट और मानव अधिकार सबंधित बहस के केंद्रबिंदु हैं.

निजता के अधिकार के कार्यान्वयन, प्रवर्तन, उपयोग और उल्लंघन

व्यक्तिगत जानकारी के लिए सरकार के उपयोग और पहुँच

गोपनीयता का अधिकार सामाजिक अनुबंध का एक आवश्यक घटक है; यह व्यक्ति और सरकार के बीच सत्ता के विभाजन की मध्यस्थता करता है. व्यक्तियों और सरकारों दोनों द्वारा अपने जीवन और गतिविधियों में इंटरनेट को एकीकृत रूप में आत्मसात करने का प्रयास अस्थिरता को स्थापित करता है, और सत्ता के विभाजन में अस्थिरता स्थापित करता है. बढ़ती आवृत्ति के साथ, सरकारें एक व्यक्ति की इंटरनेट गतिविधियों पर नजर रखने और इंटरनेट उपयोगकर्ताओं के बारे में ऑनलाइन जानकारी का उपयोग करने के लिए नियमों को अपना रहे हैं

को सौंपने के लिए कानून और संचार सेवा प्रदाताओं को व्यक्ति की इंटरनेट गतिविधियों के बारे में जानकारी देने के लिए मजबूर कर रही हैं. खुफिया सेवाओं को व्यापक अधिकार है जिसके द्वारा वे अक्सर संचार रिकॉर्ड और उसके प्रवाह को रोक सकते हैं, और कानून प्रवर्तन अधिकारी

नियमित रूप से रिकॉर्ड और ईमेल तक पहुंच के लिए,गूगल और फेसबुक जैसे ऑनलाइन सेवा प्रदाताओं की मदद ले रहे हैं. इनमें क्षमता है कि वे कई स्रोतों से प्राप्त या कई सरकारी विभागों के लिए उपलब्ध कराई गई जानकारी एकत्र करने की और उससे की व्यक्तियों के व्यापक प्रोफाइल उससे की. कुछ देशों में, सरकारों ने इस तरह की प्रौद्योगिकी हासिल कर ली है कि जिसके द्वारा वे विधीतर निगरानी सकते हैं जैसे कि संचार के बड़े पैमाने पर अवरोधन के रूप में. फलस्वरूप सत्ता का संतुलन तेजी से सरकार के पक्ष में आ गया है जब गोपनीयता के संरक्षण की बात आती है.

नागरिकों की जानकारी का संग्रह निजी डेटा पर सरकारी नियंत्रण का एक प्रमुख तत्व है. नागरिकों का निजी डेटा सरकारों द्वारा विभिन्न प्रयोजनों के लिए प्रयोग किया जाता है:

- **प्रशासन और सार्वजनिक सेवाओं की डिलिवरी**: सरकारों को सटीक जनसंख्या जानकारी मदद करती है सार्वजनिक सेवाओं और बजटीय आवंटन को प्राथमिकता के आधार पर निर्धारित करने के लिए और इसके द्वारा अन्य शासन फैसले को भी सूचित कर सकते हैं. सरकारें इंटरनेट का उपयोग करती हैं सेवाओं के प्रावधान को सुविधाजनक बनाने के लिए जैसे कि सामाजिक सुरक्षा प्रावधान, स्कूल नामांकन, मेडिकल रिकॉर्ड और ऑनलाइन आयकर रिटर्न दाखिल करना और ऑनलाइन सिस्टम में उपलब्ध कराए गए आंकड़ों का उपयोग कर सकती हैं के बंटवारे के रूप में इंटरनेट का उपयोग करते हैं, देश के नागरिकों की एक साफ तस्वीर हासिल करने के लिए और तदनुसार उनकी सेवाओं की डिलीवरी में सुधार के लिए.
- **कानून प्रवर्तन**: सरकारें कानून प्रवर्तन प्रयोजनों के लिए व्यक्तियों की निजी जानकारी का उपयोग कर सकती हैं. ऑनलाइन संचार और गतिविधियों का उपयोग करने के लिए राष्ट्रीय कानून में निर्धारित प्रक्रियाओं का पालन करके, सरकारें पड़ताल करने या अपराधों पर मुकदमा चलाने के क्रम में ईमेल, वित्तीय लेनदेन, सामाजिक नेटवर्किंग साइटों और अन्य ऑनलाइन गतिविधियों का उपयोग कर सकती हैं. सरकार डेटाबेस में एक व्यक्ति की पहचान के बारे में बनाए रखी जानकारी को आईसीटी से और सीसीटीवी फुटेज के साथ प्राप्त भू-स्थान की जानकारी के साथ मिलान कर के एक अपराधी का एक व्यापक प्रोफाइल बनाया जा सकता है.
- **पहचान प्रबंधन और सामाजिक छँटाई**: आईडी कार्ड और बायोमेट्रिक प्रणाली के उपयोग के माध्यम से, सरकारें नागरिकों की प्रोफाइल बना सकती हैं और उनका इस्तेमाल विभिन्न प्रयोजनों के लिए किया जा सकता है. पहचान प्रबंधन का इस्तेमाल किया जा सकता है व्यक्तियों की गतिविधियों पर नज़र रखने के लिए जिसमे शामिल हो सकती है जानकारी उनके रहन सहन , खान पान, यात्रा , इंटरनेट की आदतों, साइबर कैफ़े में इंटरनेट के

प्रयोग के स्वरुप किस तरह के आंदोलनों के प्रति उनकी सहानुभूति है और किस तरह के ऑनलाइन वाद-विवादों में वो हिस्सा लेते हैं. आईडी सिस्टम अधिक दखल देने के उद्देश्यों के लिए भी इस्तेमाल किया जा सकता है: एक व्यक्ति की नस्ल और धर्म के बारे में जानकारी के साथ और बायोमेट्रिक और डीएनए के बारे में जानकारी के साथ, सरकारों के पास क्षमता है समाज के चयनित क्षेत्रों को अलग करने और उनके खिलाफ भेदभाव करने की. जातीय और लैंगिक अल्पसंख्यकों, प्रवासियों और बेघर लोग इस संबंध में विशेष रूप से कमजोर हो सकते हैं.

- **संचार और व्यवहार की निगरानी**: • सरकारों के पास फेसबुक और ट्विटर जैसे सामाजिक नेटवर्किंग साइटों पर ऑनलाइन संचार और गतिविधियों पर नजर रखने के लिए तकनीकी क्षमता है. संचार और निगरानी के व्यवहार की वैधता में देश से देश के बीच भिन्नता है. कुछ देशों में, कानून प्रतिनिधियों द्वारा कानून प्रवर्तन एजेंसियों को जांच के व्यापक अधिकार प्रदान किये गए है जिसके आधार पर बिना न्यायिक निरीक्षण के संचार को रोकने और संचार की निगरानी करने के लिए वे सक्षम हैं. अन्य उदाहरणों में, कानून प्रवर्तन अधिकारियों को व्यक्तिगत संचार का उपयोग करने के क्रम में एक वारंट या सम्मन प्राप्त करना होगा. कुछ मामलों में विधायी परिवर्तन कानून तकनीकी प्रगति से कदम से कदम मिला कर नहीं चल पा रहा है तो ऐसी स्थितियों में प्रवर्तन द्वारा ऑनलाइन निगरानी केवल आंतरिक नीतियों और दिशा निर्देशों के द्वारा नियंत्रित की जाती है. नतीजतन, पुलिस और अन्य सरकारी अधिकारियों को विस्तृत विवेक है कि निगरानी के लिए चयन अपनी स्वच्छंदता के साथ कर सकते हैं .स्वतंत्र रूप से ऑनलाइन व्यक्तियों द्वारा उपलब्ध कराई गई सूचना को राजनीतिक या सामाजिक वरीयताओं को प्राप्त करने के लिए खनन किया जा सकता है और अवैध व्यवहार की पहचान करने के लिए प्रयोग में लाया जा सकता है. इस जानकारी को सीसीटीवी फुटेज और सरकारों द्वारा आयोजित अन्य व्यक्तिगत जानकारी के साथ जोड़ा जाता है, और एक व्यक्ति की गतिविधियों और व्यवहार पर आधारित एक व्यापक प्रोफाइल परिणामतः तैयार हो जाती है.

गोपनीयता डेटा संरक्षण कानून वह कानून है जिसके द्वारा यह सुनिश्चित किया जाता है कि सरकार द्वारा एकत्र आंकड़ों की गोपनीयता बनी रहे और उसे उच्चतम वर्ग की वरीयता मिले. यह कानून अलग अलग देशो में अलग अलग रूप में हैं, आम तौर पर गोपनीयता के संरक्षण पर अंतरराष्ट्रीय मानक ओईसीडी के दिशा निर्देशों और सीमा के आर पार का व्यक्तिगत डेटा का प्रवाह पर्सनल डाटा (भाग दो) के प्रवाह द्वारा दिशा निर्देशित होते हैं. यह निर्देश स्पष्तः रेखांकित करते हैं कि व्यक्तिगत जानकारी और डाटा प्रोसेसिंग संग्रह में

निम्न का पालन होना चाहिए:

· **संग्रह सीमा**: व्यक्ति की जानकारी या सहमति के साथ व्यक्तिगत डेटा का संग्रह करने की सीमा निर्धारित होनी चाहिए।, और उसे उचित वैध और उचित साधन, द्वारा प्राप्त किया जाना चाहिए.
· **डेटा गुणवत्ता**: व्यक्तिगत डेटा जिस उद्देश्य के लिए संग्रह किया गया है उसी के लिए प्रासंगिक और सटीक होना चाहिए, और नियमित रूप से अपडेट होते रहना चाहिए.
• **प्रयोजन विशिष्टता**: व्यक्तिगत डेटा जिस निर्दिष्ट उद्देश्य के लिए एकत्र कर रहे हैं उसी उद्देश्य के लिए उपयोग किया जाना चाहिए और किसी भी बाद के उपयोग कि विनिर्देश करने के लिए सीमित किया जाना चाहिए.

· **प्रयोग सीमा**: निर्दिष्ट के अलावा अन्य प्रयोजनों के लिए उपलब्ध डाटा का खुलासा या न उपयोग नहीं किया जाना चाहिए, है सिवाय, एक) कानून के अधिकार से या ख) व्यक्ति की सहमति के साथ.
· **सुरक्षा निगरानी**: डेटा को उचित सुरक्षा निगरानी द्वारा खोने, विनाश, उपयोग, संशोधन या प्रकटीकरण के खिलाफ संरक्षित किया जाना चाहिए.
· **खुलापन**: व्यक्तिगत डेटा के खुलेपन के बारे में एक सामान्य नीति होनी चाहिए.
· **व्यक्तिगत भागीदारी**: एक व्यक्ति अपने डेटा के बारे में जानकारी पता लगाने का अधिकार होना चाहिए और गलत डेटा को मिटाने या उसको संशोधित करने का अधिकार होना चाहिए.
· **जवाबदेही**: एक डेटा नियंत्रक इन उपायों के अनुपालन के लिए जवाबदेह है.

यद्यपि ओईसीडी के दिशा निर्देश स्पष्ट रूप से डेटा प्रतिधारण को रेखांकित नहीं करते है, गोपनीयता अधिवक्ताओं का यह मत है कि प्राप्त किया गया डेटा उद्देश्य को पूरा करने के बाद किसी भी लंबे समय तक बनाए रखा नहीं जाना चाहिए. विवादास्पद रूप से, 2006 में अपनाया यूरोपीय संघ के डेटा प्रतिधारण निर्देशक, यह निर्धारित करता है कि संचार प्रदाता छह महीने और दो साल के बीच जानकारी की कुछ श्रेणियों को बनाए रखें , और कानून प्रवर्तन अधिकारियों के अनुरोध पर इस जानकारी को उपलब्ध कराएं. डेटा प्रतिधारण दुनिया भर में विधायी चौखटे में तेजी से कानून लागू करने के प्रयासों की प्रभावशीलता में सुधार की आड़ में शामिल किया जा रहा है.

व्यक्तिगत जानकारी के लिए कॉर्पोरेट उपयोग और पहुँच

डेटा की बिक्री और व्यापार इन दिनों बड़ा व्यापार है. व्यक्तियों की व्यक्तिगत जानकारी के लिए निम्न विधियों और तंत्र के माध्यम से डाटा से लाभ उत्पन्न हो सकते हैं, जो निजी क्षेत्र के लिए अत्यंत मूल्यवान है:

· **व्यवहार संबंधी विज्ञापन और रूपरेखा**: अपने पिछले गतिविधियों के आधार पर इंटरनेट उपयोगकर्ताओं के लिए विज्ञापनों का वितरण. यह एकल सेवाओं के रूप में होता है, ऐसे अमेज़न और फेसबुक पर, जो आपकी पिछली गतिविधियों के अभिलेखों के आधार पर आपको नए उत्पाद बेचने का प्रयास करते हैं. विभिन्न वेबसाइटों पर कुकीज़ के उपयोग के माध्यम से भी उपयोगकर्ता के हितों का एक प्रोफाइल रहता है, जो उपयोगकर्ताओं के डेटा तीसरी पार्टी के विज्ञापन नेटवर्क से जो उपभोक्ता का एक प्रोफाइल उसकी आदतों के हिसाब से बना कर रखता है. बिना उपभोक्ता की सहमति के शेयर कर देते हैं एक व्यक्ति की निजी जानकारी इस प्रकार उनकी सहमति के बिना तीसरे पक्ष के साथ साझा किया जाता है, और यह जानकारी ग्राहकों को आकर्षित करने के इच्छुक कॉर्पोरेट संस्थाओं के लिए एक मूल्यवान संसाधन हो जाता है. वास्तव में, गूगल और फेसबुक सहित सबसे प्रमुख ऑनलाइन सेवा प्रदाताओं के व्यापार मॉडल, इस तरह की तकनीक के माध्यम से विज्ञापन राजस्व को अधिकतम करने के लिए विभिन्न प्रयोजन कर रहे हैं

- · **डाटा माइनिंग**: इस प्रक्रिया से डेटा के एक सेट से जानकारी या पैटर्न निकालने का प्रयास शामिल है। डाटा माइनिंग एक कंपनी के लिए अपने ग्राहकों को समझने और कुछ व्यक्तियों के लिए कुछ उत्पादों को और अधिक उचित रूप से बेचने में मदद कर सकते हैं. इसका इस्तेमाल, उदाहरण के लिए इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड में पैटर्न का पता लगाने के लिए, विज्ञान और इंजीनियरिंग, शैक्षिक अनुसंधान और चिकित्सा अनुसंधान के क्षेत्र में किया जा सकता है। संयुक्त राज्य अमेरिका की सरकार द्वारा विश्लेषण, प्रसार, विजुअलाइजेशन, अंतर्दृष्टि और सिमेंटिक संवर्धन (एडवाईस) कार्यक्रम के तहत डाटा माइनिंग का प्रयोग करके डेटा का बड़ी मात्रा में विश्लेषण करती है आतंकवादी के पैटर्न के खोज करने के लिए सरकार के रिकॉर्ड और खुफिया रिपोर्टों के ब्लॉग और ईमेल से.
- **बिग डेटा**: जबकि डाटा खनन प्रबंधनीय डेटासेट पर आयोजित किया जा सकता है, डेटा की जानकारी और उत्पादन की दर अब इतनी बढ़ गयी है कि डेटासेट बनाया जा रहा है जो कि इतना जटिल और वृहद है कि उसे पारंपरिक डेटाबेस प्रबंधन उपकरण का उपयोग कर संसाधित करना टेढ़ी खीर है. छोटे डेटासेट की तुलना में बड़े डेटासेट के विश्लेषण से

अधिक जानकारी का पता चलता है, और यह जानकारी निजी क्षेत्र, वैज्ञानिक अनुसंधान, और प्रशासन के लिए बहुमूल्य साबित हो सकती है. 2012 में, ओबामा प्रशासन ने बड़े डेटा अनुसंधान और विकास पहल की स्थापना की घोषणा की जिसका उद्देश्य था बड़े डेटा के विश्लेषण से शासन के मुद्दों को संबोधित करना. बड़े डेटा के विश्लेषण से चिकित्सा अनुसंधान के क्षेत्र के लिए भी दिव्य संभावनाएं हैं.

- व्यक्तिगत जानकारी के कॉर्पोरेट उपयोग के द्वारा उठाए गए कानूनी मुद्दों जटिल हैं. इस संबंध में निजी क्षेत्र के ऊपर विभिन्न तरह की कानूनी रूपरेखाएं लागू होती हैं

सेवा / उपयोगकर्ता समझौतों की शर्तें: ये निर्धारित करते हैं कि एक कंपनी और उपयोगकर्ता के बीच एक प्रवर्तनीय अनुबंध के रूप में उपयोगकर्ता की कौन सी जानकारी का इस्तेमाल किया जा सकता है और किसका नहीं. हालांकि, उपयोगकर्ताओं द्वारा सेवा सम्बंधित लम्बे और जटिल नियम शायद ही कभी पढ़ा जाता है, और प्रभाव स्वरुप कंपनियाँ अलग अलग तरीकों से व्यक्तिगत जानकारी का उपयोग कर लेती हैं.

- **डेटा संरक्षण**: बहुत सारे देशों में एक बढ़ती हुई संख्या में निजी क्षेत्र के ऊपर भी सार्वजनिक की तरह ही डेटा संरक्षण के नियमन लागू होते हैं. हालांकि, डेटा संरक्षण कानून अफ्रीका सहित विश्व के कई देशों में अनुपस्थित है. इस संबंध में नोट के लिए महत्वपूर्ण है कि विश्व स्तर पर किसी भी प्रकार का अंतरराष्ट्रीय डेटा संरक्षण शासन मौजूद नहीं है , और ऑनलाइन गतिविधियों के संचालन के समय संभव है कि,एक व्यक्ति की व्यक्तिगत जानकारी एक गैर डेटा संरक्षण देश में पंजीकृत एक कंपनी की इकाई को प्रदान कर दी जाएगी.
- ·**सरकार द्वारा कॉर्पोरेट डेटा का उपयोग**: सरकारें नियमित रूप से निगमों, विशेष रूप से प्रमुख ऑनलाइन सेवा प्रदाताओं द्वारा आयोजित डेटा का उपयोग करना चाहती हैं। उदाहरण के लिए, जनवरी से जून 2012 के बीच, विदेशी अधिकारियों से 20,000 से अधिक अनुरोध प्राप्त हुए गूगल प्रयोक्ताओं के ईमेल खातों या इंटरनेट खोजों के उपयोग की मांग को लेकर. अधिकांश देशों में, एक व्यक्ति के ईमेल के उपयोग के लिए या उनके फोन कॉल अवरोधन करने के लिए एक न्यायिक आदेश की आवश्यकता होती है जिसके लिए घरेलू कानून प्रवर्तन के क्रम में एक प्रक्रिया के अनुबंध का पालन होना चाहिए. हालांकि,व्यवहार में, कानून प्रवर्तन अधिकारी नियमित रूप से कॉर्पोरेट संस्थाओं से सीधे उपयोगकर्ता डेटा का अनुरोध कर लेते हैं. कुछ कंपनियाँ को बिना एक वारंट या सम्मन के उत्पादन की आवश्यकता के उपयोगकर्ता की जानकारी प्रदान कर देती हैं. यह न केवल एक देश के भीतर लेकिन सरकारों और विदेशी कॉर्पोरेट संस्थाओं के बीच भी होता है. कॉर्पोरेट संस्थाओं हमेशा

जानकारी नहीं प्रदान करती हैं; कई मामलों में अधिकारियों को परस्पर कानूनी सहायता संधि (परस्पर विधिक सहायता संधियाँ) (MLAT) की प्रक्रिया के माध्यम से एक औपचारिक आवेदन करके जानकारी मिलती है. हालांकि, कई बार उपयोगकर्ता डेटा अनौपचारिक रूप से सौंप दिया जाता है खासकर जहां एक नितांत आवश्यक मुद्दे के नतीजे को प्राप्त करने की जरूरत है.

अन्य व्यक्तियों और तृतीय पक्षों द्वारा व्यक्तिगत जानकारी के उपयोग और पहुँच

व्यक्तिगत जानकारी और आंकड़े भी ऑनलाइन धोखाधड़ी के दुरुपयोग या दुरुपयोग के अन्य रूपों का शिकार हो सकते हैं जैसे कि, हैकिंग, धोखाधड़ी उकसावा, धोखाधड़ी सुरक्षा सॉफ्टवेयर के वितरण, या पहचान की चोरी और धोखाधड़ी और गलत बयानी का वितरण. इन स्थितियों में से प्रत्येक की एक व्यक्ति की गोपनीयता के अधिकारों के गंभीर उल्लंघन का प्रतिनिधित्व करता है. इन कार्यों में से बहुत से ऐसे हैं जो कंप्यूटर दुरुपयोग या साइबर अपराध कानून के दायरे में आते हैं और हर देश का इस विषयक कानून दूसरे देश से आम तौर पर भिन्न होता है. इसके अलावा, प्रकार और ऑनलाइन हमलों की संभावनाएं विकसित होती जा रही हैं और कानून प्रवर्तन अधिकारियों को पर्याप्त रूप से प्रतिक्रिया करने में मुश्किल उत्पन्न कर रही हैं. उदाहरण चीन में "मानव मांस खोज इंजन" और " प्रतिशोध अश्लील" वेबसाईट्स शामिल हैं.

जब मीडिया निजी जानकारी का उपयोग और निजी जानकारी को प्रकाशित करता है तो उससे निजता के अधिकार को भी खतरा उत्पन्न होता है. अभिव्यक्ति की स्वतंत्रता और निजता के अधिकार और मीडिया और मानहानि और प्रतिष्ठा के सवाल की भूमिका के बीच संतुलन मुश्किल से स्थापित होता है. इसके अलावा, निजता के अधिकार का सम्मान करने के लिए मीडिया की जिम्मेदारी पर कोई अंतरराष्ट्रीय आम सहमति नहीं है, और दुनिया भर के देशों में अदालतों और विधायिकाओं के बीच इस सवाल के साथ संघर्ष जारी है. इंटरनेट गोपनीयता और अभिव्यक्ति की स्वतंत्रता पर 2012 में यूनेस्को वैश्विक सर्वेक्षण, विभिन्न राष्ट्रीय पदों का सार प्रस्तुत करता है और इस मुश्किल को हल करने के तरीके के बारे में सिफारिशें देता है.

जैंसे जैसे मीडिया ऑनलाइन हो रहा है, और ब्लॉगर्स और ट्विटर प्रयोक्ताओं के प्रकाशन मीडिया के परंपरागत रूपों स्वरूपों को कड़ी स्पर्धा प्रदान कर रहे हैं, ऐसी स्थिति में मानहानि का सवाल और भी अधिक जटिल हो जाता है. प्रकाशन के स्थल और उनके अधिकार क्षेत्र की मान्यताएं और ऑनलाइन गुमनामी और छद्मनाम का उपयोग इस मुद्दे

को और जटिल बनाती हैं. पहचान से सम्बंधित मुद्दे ऑनलाइन पर चल रहे निजता की विभिन्न संघर्षों में से सबसे प्रमुख हैं. इंटरनेट की स्थापना के बाद से ऑनलाइन क्षेत्र में नाम न छापना एक आदर्श स्थिति है, पर साइबर अपराध, साइबर बदमाशी और ट्रॉल्लिंग, बाल यौन शोषण और सौंदर्य, और आतंकवादी आशंका के बारे में चिंताओं को लेकर इंटरनेट उपयोगकर्ताओं के वास्तविक नाम पंजीकरण और पता लगाने की क्षमता की आवश्यकता की दिशा में एक मुहीम को समर्थन दिया गया है.

सारांश

इंटरनेट और आईसीटी ने निजता के अधिकार की सहमति के लिए नई और कठिन चुनौतियाँ आधुनिक युग के समक्ष रखी है. प्रौद्योगिकी के क्षेत्र में परिवर्तन और विधायी सुधार में उस गति से परिवर्तन के समावेश न हो सकने की स्थिति में व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करना एक विशेष चुनौती है. प्रभावी डेटा संरक्षण के अभाव में व्यक्ति को अपनी व्यक्तिगत जानकारी के सरकार और कॉरपोरेट जगत दोनों द्वारा शोषित किये जाने की दोहरी मार का सामना करना पड़ रहा है.
एक दूसरा व्यापक चिंता का विषय निगरानी प्रौद्योगिकियों और तकनीकों के विस्तार से सम्बंधित है. निगरानी और कानून प्रवर्तन अधिकारियों द्वारा संचार के अवरोधन अधिक से अधिक व्यापक हो रहे हैं. इस तरह के व्यवहार न केवल लगातार निजता के अधिकार का उल्लंघन है, लेकिन यह भी अभिव्यक्ति, संघ और आंदोलन की स्वतंत्रता सहित अन्य अधिकारों और स्वतंत्रता के आनंद के उपभोग को भी प्रभावित करते हैं.

गोपनीयता को सामाजिक मानदंडों और बदलते नजरिए के संदर्भ में समझना जरूरी है , और जैसे जैसे इंटरनेट का विकास होता है और उसमे परिवर्तन आते हैं, साथ ही साथ निजता के अधिकार और कंटेंट के स्वरुप में भी परिवर्तन आ रहा है. हालांकि, गोपनीयता के अधिकार का मूल एक उदार, लोकतांत्रिक समाज का एक महत्वपूर्ण तत्व है, और इसे संरक्षित रहना चाहिए. इस परिणाम की प्राप्ति के लिए, यह महत्वपूर्ण है कि मानव अधिकारों का समुदाय इंटरनेट और आईसीटी के समक्ष रखी गोपनीयता के जोखिम को समझे, और उन सारांशों को शामिल करे अपने काम के दायरे को आगे बढ़ने के लिए