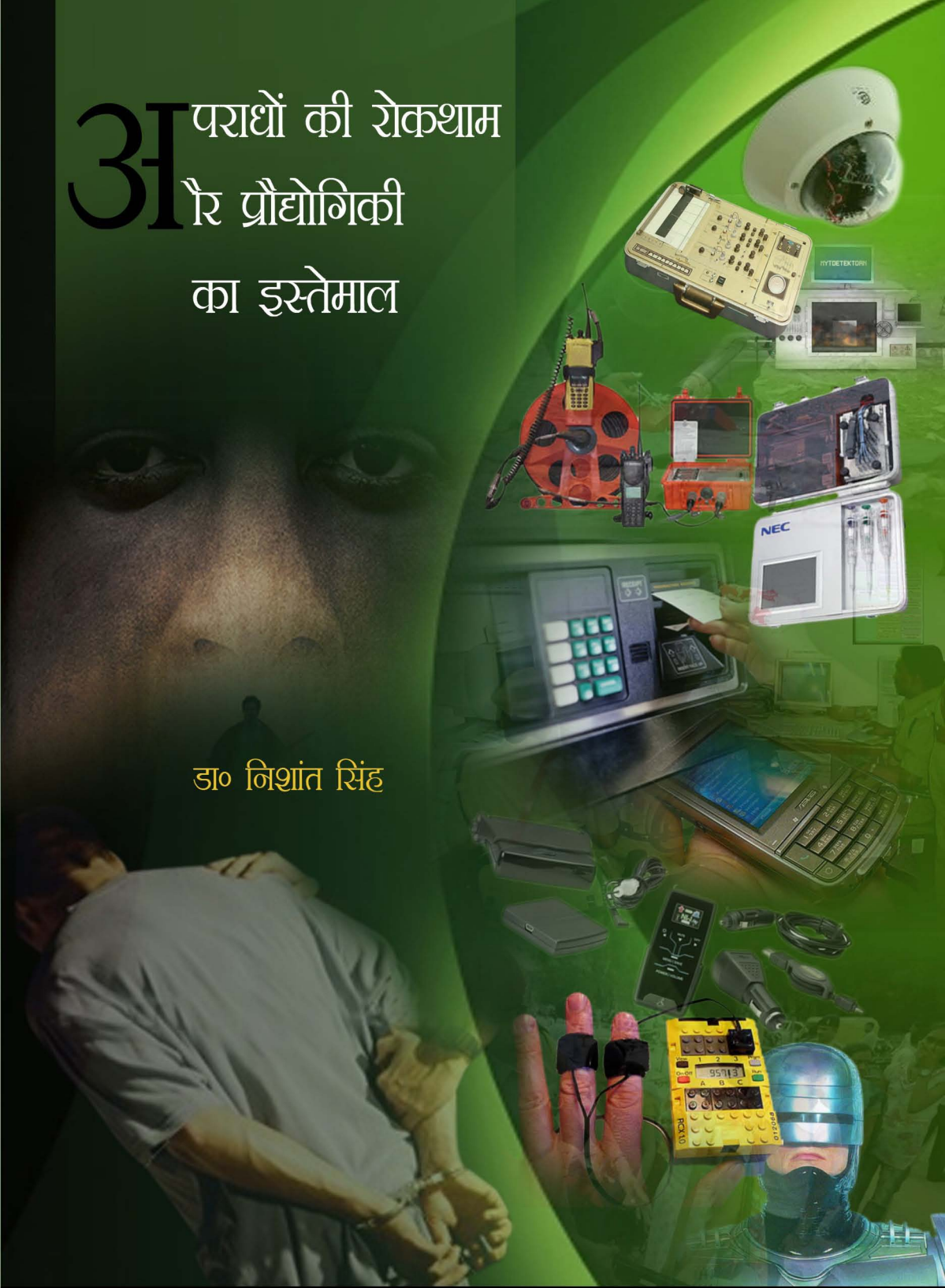
अपराधों की रोकथाम और प्रौद्योगिकी का इस्तेमाल



डा० निशांत सिंह

पुलिस अनुसंधान एवं विकास ब्यूरो, नई दिल्ली

अपराधोंकीरोकथाम
और
प्रौद्योगिकी का इस्तेमाल

(पं. गोविंद वल्लभ पंत पुरस्कार योजना के अंतर्गत पुरस्कृत)

लेखक

डा.निशांतसिंह

पुलिस अनुसंधान एवं विकास ब्यूरो

गृह मंत्रालय, भारत सरकार

मूल्य :

प्रकाशक : पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, भारत सरकार

संस्करण : प्रथम, 2009

अक्षरांकन एवं कवर डिजाइन : रचना इंटरप्राइजिज, दिल्ली-110032

APRADHON KI ROKTHAM AUR PRAUDYOGIKI KE ISTEMAL *by* Nishant Singh

मेरी ओर से...

प्रतिस्पर्धा के इस युग में व्यक्ति की आकांक्षाएं असीमित हो गई हैं। वह रातोंरात अमीर बनकर सारे सुख पा लेना चाहता है, सारी सुख-सुविधाएं जुटा लेना चाहता है। मानव की प्रवृत्ति में आए इस बदलाव के कारण आज समाज में अपराधों की संख्या और उनकी गंभीरता में भी लगातार वृद्धि हो रही है। चूंकि आज विज्ञान, प्रत्येक क्षेत्र में अपनी उपस्थिति दर्ज करा रहा है इसलिए अपराधियों द्वारा भी आज अपराध को अंजाम देने में अत्याधुनिक तकनीकों का खूब इस्तेमाल किया जा रहा है। एक तरफ अपराधियों द्वारा अत्याधुनिक तकनीकों का प्रयोग, समाज और मानवजाति के खिलाफ किया जा रहा है तो दूसरी ओर प्रौद्योगिकी ने पुलिस तथा अन्य सुरक्षा एजेंसियों को ऐसे उपकरण एवं विधियां भी उपलब्ध करा दी हैं, जिनकी सहायता से अपराध को घटित होने से रोका जा सकता है, अपराधों की रोकथाम की जा सकती है।

अपराधियों के खिलाफ प्रौद्योगिकी का प्रयोग दो प्रकार से किया जाता है। अपराध के घटित होने पर अपराध तथा अपराधी की पहचान करने में प्रयुक्त वैज्ञानिक तकनीकें, विधि विज्ञान या फॉरेंसिक विज्ञान के अंतर्गत आती हैं जैसे डी.एन.ए. विश्लेषण, नार्को परीक्षण, पॉलीग्राफ और ब्रेन मैपिंग आदि। विधि विज्ञान की महत्ता से आज कोई भी इंकार नहीं कर सकता लेकिन इससे भी ज्यादा महत्त्वपूर्ण है, अपराध को घटित होने से पहले ही रोकने वाली तकनीकें, अर्थात ऐसी तकनीकें जिनका प्रयोग अपराधों की रोकथाम में किया जाता है। विज्ञान ने आज इतनी तरक्की कर ली है, प्रौद्योगिकी का आज इतना विकास हो चुका है कि अपराध को घटित होने से पहले ही रोका जा सकता है।

विधि विज्ञान के रूप में अपराध व अपराधियों की पहचान करने में तो तकनीकों का प्रयोग काफी पहले से ही किया जा रहा है लेकिन आजकल

तकनीकों और प्रौद्योगिकी ने इतना विकास कर लिया है कि अब अपराध को घटित होने से पहले ही रोका जा सकता है। इलैक्ट्रॉनिक सर्विलांस, मोबाइल सर्विलांस, वीडियो सर्विलांस, मोबाइल ट्रैकर्स, बायोमैट्रिक्स और एंटी-हैकिंग उपकरण, कुछ ऐसे उपाय हैं जिनके सहारे अपराध को घटित होने से पहले ही रोका जा सकता है।

अब पुलिस भी *टेक्नो सैवी* हो गई है और वह तकनीक व प्रौद्योगिकी पर आधारित अत्याधुनिक उपकरणों व यंत्रों का प्रयोग करने लगी है। पहले पुलिस पर आरोप लगाया जाता था कि वह अपराध घटित होने के काफी देर बाद घटनास्थल पर पहुंचती है लेकिन अब पुलिस, अपराध के घटित होने से पहले ही अपराधियों तक पहुंचने लगी है और यह सब संभव हो पाया है पुलिस द्वारा तकनीक एवं प्रौद्योगिकी के इस्तेमाल के कारण।

आजकल अपराधों की रोकथाम के क्षेत्र में *'बायोमैट्रिक्स'* शब्द काफी चर्चा में है। *बायोमैट्रिक्स* का अर्थ है व्यक्ति के व्यवहार अथवा उसके द्वारा छोड़े गए अवशेषों की संबंधी जैविक विशेषताओं के आधार पर उसकी पहचान स्थापित करना। रेटिना एवं आइरिस स्कैनिंग, हथेली एवं अंगुलियों की ज्यामितीय, आवाज के प्रतिरूप, चेहरे को पहचानने के तरीके *(फेशियल रिकोगनिशन सिस्टम)* तथा अंगुलि-चिह्नों व हस्ताक्षरों को पहचानने की विधियां, *बायोमैट्रिक्स* के अंतर्गत आती हैं।

आज अगर आतंकवादी कंप्यूटर, इंटरनेट, मोबाइल और सैटेलाइट फोन जैसे अत्याधुनिक संचार साधनों का इस्तेमाल कर रहे हैं तो इलैक्ट्रॉनिक सर्विलांस द्वारा आतंकवाद की रोकथाम करना भी काफी सरल हो गया है। मोबाइल और वीडियो सर्विलांस के जरिए आतंकवाद के पर कतरना बेहद सुविधाजनक हो गया है। हाल ही में भारतीय प्रौद्योगिकी संस्थान, कानपुर ने *'ऑटोमैटिक वीडियो सर्विलांस'* नामक एक ऐसी तकनीक विकसित की है, जिसके जरिए संदिग्ध आतंकवादियों को दबोचना आसान हो जाएगा।

स्पष्ट है कि आपराधिक घटनाओं और आतंकी गतिविधियों की रोकथाम में तकनीक और प्रौद्योगिकी का प्रयोग, पुलिस और अन्य सुरक्षा एजेंसियों द्वारा बहुतायत से किया जाने लगा है। बायोमैट्रिक्स, इलैक्ट्रॉनिक सर्विलांस, डिजिटल हस्ताक्षर और मोबाइल सर्विलांस ऐसी ही कुछ अत्याधुनिक तकनीकें हैं तथा इन

सभी तकनीकों की विस्तृत चर्चा प्रस्तुत पुस्तक में की गई है।

पुस्तक में 'वैज्ञानिक एवं तकनीकी शब्दावली आयोग' द्वारा प्रमाणित शब्दावली का ही प्रयोग किया गया है लेकिन कुछ स्थानों पर भाषाई कट्टरता को छोड़ते हुए अधिक प्रचलित अंग्रेजी शब्दों का भी प्रयोग किया गया है ताकि आम पाठकों के लिए भी विषय को समझना, सरल व सुगम रहे। पुस्तक में सरल व आम बोलचाल की भाषा का प्रयोग किया गया है ताकि पुलिस तथा अन्य सुरक्षा एजेंसियों के छोटे कर्मियों के साथ-साथ आम जनता भी इससे लाभ उठा सके।

पुस्तक को 'पं. गोविंद वल्लभ पंत पुरस्कार' से सम्मानित करने के लिए मैं, पुरस्कार चयन समिति और पुलिस अनुसंधान एवं विकास ब्यूरो का हृदय से आभारी हूँ। श्री राजीव माथुर, निदेशक, राष्ट्रीय अपराध रिकॉर्ड ब्यूरो और श्री नासिर कमाल, संयुक्त निदेशक, रा. अ. रि. ब्यूरो को उनके मिलत्रत सहयोग व आशीर्वाद के लिए हार्दिक धन्यवाद देता हूँ।

निशांत सिंह

प्राक्कथन

आज के बदलते सामाजिक परिवेश में व्यक्तियों की अपेक्षाएं दिन-प्रतिदिन बढ़ती जा रही हैं और सही रूप में इनको पूरा कर पाना संभव नहीं हो पाता है। इसके लिए वह विभिन्न वैध व अवैध तरीके अपनाने लगता है। चूंकि आज का युग वैज्ञानिक युग है इसलिए अवैध तरीकों को अपनाने के लिए नित नए प्रयोग होने लगे हैं, जिसमें सफलता भी मिलने लगी है। यह सफलता कानून और व्यवस्था संभालने वाली संस्थाओं के लिए चुनौती बन गई है। जिस प्रकार नित नए अपराध गठित हो रहे हैं, उसी प्रकार उनके निदान के लिए नित नई तकनीकों की खोज की जा रही है। लेकिन अपराधी भी उसी गति से उन तकनीकों का तोड़ ढूँढने में लग जाते हैं। इसी समस्या को देखते हुए पं. गोविन्द वल्लभ पंत पुरस्कार योजना की मूल्यांकन समिति ने यह निर्णय लिया कि अपराधों की रोकथाम के लिए क्या प्रौद्योगिकी अपनाई जाने से संबंधित विषय पर लेखन कार्य कराया जाए। ताकि आम जन के साथ-साथ पुलिस कर्मी भी इनसे अवगत हो सके।

इसके लिए डा. निशांत सिंह को यह लेखन कार्य सौंपा गया। लेखक ने अपने अथक परिश्रम से इस समस्या के समाधान में कुछ ठोस आधार प्रस्तुत करने का प्रयास किया है। मैं समझता हूं कि इस प्रयास में कहीं न कहीं अपराध की प्रकृति को दिखाने के साथ, उन अपराधों से निपटने के लिए अपनाई जा रही विभिन्न प्रौद्योगिकियों का उल्लेख भी किया है, जो अपराधों के समाधान के लिए उपयोगी प्रतीत होता है। मैं आशा करता हूं कि यह पुस्तक सभी पुलिस अधिकारियों और पुलिसकर्मियों के लिए काफी उपयोगी होगी।

मैं डा. निशांत सिंह का आभार प्रकट करना चाहूंगा तथा इस पुस्तक के सफल प्रकाशन के लिए ब्यूरो के संपादक हिन्दी को धन्यवाद देना चाहूंगा।

मुझे विश्वास है कि यह पुस्तक सभी आम जन के लिए उपयोगी सिद्ध होगी, जिससे समाज में हो रही नवीन प्रौद्योगिकियों के विकास के बारे में जान कर, वे इस समस्या से होने वाले प्रभावों पर आत्म-मंथन कर सकेंगे।

प्रसून मुखर्जी
14.7.09.

(प्रसून मुखर्जी)
महानिदेशक
पुलिस अनुसंधान एवं विकास ब्यूरो

विषयक्रम

1

अपराध, अपराधी और प्रौद्योगिकी

आधुनिकता और भौतिकवाद के इस युग में व्यक्ति की इच्छाएं असीमित हो गई हैं और वह रातोंरात धनवान बनकर समस्त ऐशो-आराम पा लेना चाहता है, सारी सुविधाएं प्राप्त कर लेना चाहता है। लोगों की मानसिकता में आए इस बदलाव के कारण भारत सहित समूचे विश्व में अपराधों की संख्या और उनकी गंभीरता में लगातार वृद्धि हो रही है। अपराधों के अलावा आतंकवाद ने भी दुनियाभर को अपनी गिरफ्त में ले रखा है। दुनिया का शायद ही कोई देश हो जो आतंकवाद के साए से मुक्त हो। 9/11 की दुस्साहसिक घटना ने साबित कर दिया कि संयुक्त राष्ट्र अमेरिका जैसे शक्तिशाली राष्ट्र की सुरक्षा व्यवस्था भी अभेद नहीं है। आतंकवाद और अपराध का एक दुर्भाग्यपूर्ण और खतरनाक पहलू यह है कि अब आतंकवादी और अपराधी भी तकनीक एवं प्रौद्योगिकी का इस्तेमाल, मानवता और समाज के खिलाफ करने लगे हैं।

चाहे मुम्बई हो या मैनहट्टन, अहमदाबाद हो या एमस्टर्डम, हर जगह आतंकवादी और अपराधी, अत्याधुनिक तकनीक से लैस हो रहे हैं जिस कारण मानवता के इन दुश्मनों का मुकाबला करना काफी कठिन हो गया है। आतंकवाद और आपराधिकता के इस युग में अगर समाज-विरोधी तत्व, तकनीक का इस्तेमाल कर रहे हैं तो तकनीक एवं प्रौद्योगिकी ने सुरक्षा एजेंसियों को भी ऐसे उपकरण उपलब्ध करवा दिए हैं, जिनके सहारे अपराध को घटित होने से पहले ही रोकना भी संभव हो गया है। अपराधियों के खिलाफ प्रौद्योगिकी का इस्तेमाल दो प्रकार से किया जाता है। अपराध के घटित होने पर अपराध तथा अपराधी की पहचान करने में प्रयुक्त वैज्ञानिक तकनीकें,

विधि विज्ञान या फॉरेंसिक विज्ञान *(फॉरेंसिक्स)* के अंतर्गत आती हैं जैसे नारको विश्लेषण, डी.एन. ए. फिंगर प्रिंटिंग, ब्रैन मैपिंग और पॉलीग्राफ आदि। विधि विज्ञान की महत्ता से आज कोई भी इंकार नहीं कर सकता लेकिन इससे भी ज्यादा महत्त्वपूर्ण हैं, अपराध को घटित होने से पहले ही रोकने वाली वैज्ञानिक तकनीकें अर्थात् वे तकनीकें जिनका प्रयोग अपराधों की रोकथाम में किया जा सकता है। यह एक सुखद तथ्य है कि विज्ञान ने आज इतनी तरक्की कर ली है, प्रौद्योगिकी का इतना विकास हो चुका है कि अपराध को अब घटित होने से पहले भी रोका जा सकता है।

सबसे पहले बात अपराध की। अपराध एक सार्वभौमिक प्रक्रिया है और यह उसी समय से प्रचलन में है जबसे सभ्यता विकसित हुई। वस्तुतः अपराध तभी से होने प्रारंभ हो गए थे जबसे मानव ने धीरे-धीरे सभ्य होना शुरू किया था। अपराध प्रत्येक युग और हर समाज में पाई जाने वाली घटना है। कुछ उदारवादी विद्वान मानते हैं कि अपराध एक मानव-व्यवहार है। साथ ही ये विद्वान यह भी कहते हैं कि सभी मानव-व्यवहार, अपराध नहीं होते हैं। केवल उन्हीं मानव-व्यवहारों को अपराध कहा जा सकता है जो सामाजिक मान्यताओं और नैतिकता के प्रतिकूल होंाध एक सार्वभौमिक घटना है लेकिन इसकी परिभाषा/व्याख्या में सार्वभौमिकता का अभाव पाया जाता है। इसका कारण यह है कि अपराध की अवधारणा, स्थान, समय, परिस्थितियों और आदर्शों से संबंधित होती है। अक्सर ऐसा भी देखा गया है कि कोई अपराध विशेष, शेष विश्व के लिए तो अपराध होता है लेकिन किसी क्षेत्र विशेष या वर्ग विशेष में उसे अपराध नहीं माना जाता है।

अपराध, *'CRIME'* का हिन्दी पर्याय है। *क्राइम* एक फ्रेंच शब्द है जिसे जुर्म, कसूर, पाप और गुनाह आदि के पर्यायवाची के रूप में इस्तेमाल किया जाता है। वास्तव में 'CRIME' शब्द लैटिन भाषा के शब्द 'CRIMEN' से उत्पन्न हुआ है जिसका शाब्दिक अर्थ होता है विलगाव अथवा अलगाव। इस प्रकार अपराध एक ऐसी घटना है जिसके करने से अपराधी, समाज से विलग हो जाता है अर्थात् उसके मन में समाज के प्रति अलगाव पैदा हो जाता है। विभिन्न राष्ट्रीय-अंतर्राष्ट्रीय विद्वानों ने अपराध शब्द को अपने-अपने तरीके से परिभाषित किया है। अपराध को परिभाषित करते हुए ***आसबर्न*** कहते हैं

कि ''अपराध वह कृत्य या अपकृत्य है जो समाज के समुदाय के हित के विरुद्ध है और जो विधि द्वारा निषिद्ध है, जिसको करने पर सरकार को दंड देने का भी अधिकार होता है।'' ***मोरर*** के मुताबिक ''अपराध किसी भी कानून का उल्लंघन करने की प्रक्रिया है।'' ***जानगिलिन*** के मुताबिक ''अपराध वे कार्य हैं जो समाज के लिए वास्तव में अहितकर बताए गए हैं या जो उन व्यक्तियों के समुदाय द्वारा जिसको अपने विश्वास को कार्यान्वित करने की शक्ति है, समाज के लिए अहितकर बताए गए हैं और जिसको उन्होंने दंड द्वारा रोक दिया है।''

सदरलैंड के मुताबिक ''अपराधी आचरण वह आचरण है, जिससे अपराधी कानून भंग होता है।'' ***जानएस.मैकेन्जी*** कहते हैं कि ''अपराध, समाज के विरुद्ध, उन समस्त असंतोषों को प्रकट करता है जिन्हें राष्ट्रीय कानून द्वारा स्वीकार किया गया है तथा जिनका कर्ता दंड का भागी है।'' अपराध को परिभाषित करते हुए ***टेफ्ट*** कहते हैं कि ''अपराध वे कार्य हैं जिनको करना कानून द्वारा रोका गया है और जो विधि द्वारा दंडनीय माने गए हैं।'' ***हत्सबरी*** के मुताबिक ''अपराध एक ऐसा कार्य या दोष है जो जनता के विरुद्ध असंतोष है और जो कार्य के कर्ता या दोषी को दंड का भागी बनाता है।'' ***लैंडिस*** एवं ***लैंडिस*** कहते हैं कि ''अपराध वह कार्य है जिसे राज्य ने सामूहिक कल्याण के लिए हानिप्रद घोषित किया है और जिसके लिए दंड देने के लिए राज्य शक्ति रखता है।'

स्वप्निल भारत' के कार्यकारी निदेशक डा. ***निशातंसिंह*** के मुताबिक ''नैतिकता और समाज के विरुद्ध किया गया ऐसा प्रत्येक कार्य जिससे कि आधारभूत सामाजिक सिद्धांतों को ठेस पहुंचती हो, अपराध की श्रेणी में आता है और जरूरी नहीं कि ऐसा प्रत्येक आपराधिक कुकृत्य किसी राष्ट्र विशेष द्वारा कानूनन प्रतिबंधित किया ही गया हो।''

अपराध को परिभाषित करने के लिए विभिन्न वैज्ञानिकों ने कुछ अवधारणाओं का प्रयोग किया है। प्रेत संबंधी अवधारणा के मुताबिक कोई व्यक्ति भूत-प्रेत का साया होने के कारण अपराध करता है। अपराध की विधिशास्त्रीय अवधारणा के मुताबिक कोई सार्वजनिक कानून जो किसी व्यवहार के करने पर प्रतिबंध लगाता है या ऐसा करने की अवज्ञा देता है, उसके

उल्लंघनस्वरूप किया गया व्यवहार अपराध है। इस अवधारणा के आधार पर अपराध को परिभाषित करते हुए ***हेकरवाल*** कहते हैं कि ''अपराध, कानून का उल्लंघन है।'' इसी के आधार पर ***टैपन*** कहते हैं कि ''अपराध कानून संहिता के उल्लंघन में एक जान-बूझकर किया गया व्यवहार है, जो बिना किसी आरक्षण के किया गया तथा राज्य द्वारा दंडनीय है।'' इस प्रकार अपराध की विधिशास्त्रीय अवधारणा कहती है कि अपराध कानून द्वारा प्रतिबंधित होता है। अपराध की समाजशास्त्रीय अवधारणा के आधार पर भी विभिन्न विद्वानों ने अपराध शब्द को परिभाषित किया है। ये सभी विद्वान मानते हैं कि अपराध एक ऐसा कार्य है जिससे समाज को क्षति पहुंचती है और जो सामाजिक आदर्शों के विरुद्ध होता है। इस आधार पर ***इलियट*** और ***मेरिल*** कहते हैं कि ''जब किसी व्यक्ति का आचरण असामाजिक ठहराया जाता है तो उसका आचरण उस मान्य आचरण से, जो उस समूह के द्वारा उस स्थिति में निश्चित होता है, भिन्न होता है।'' इसी प्रकार ***प्रो.रेकलेस*** कहते हैं कि ''समाज के बनाए और माने हुए रास्ते को तोड़ने का नाम अपराध है। अपराध, समाजशास्त्रीय दृष्टिकोण से उन कृत्यों का नाम है जो सामाजिक रूढ़ियों एवं प्रथाओं को तोड़ते हैं लेकिन इसके लिए यह आवश्यक नहीं है कि आधुनिक युग की कानून की किताबों में इसका जिक्र हो ही।''

अपराध की मनोवैज्ञानिक अवधारणा भी बेहद महत्त्वपूर्ण है। इसमें वृत्ति तथा अपराधी-व्यवहार के विश्लेषण पर विशेष बल दिया गया है। अपराध का संबंध मानव-व्यवहार से है। इस अवधारणा के मुताबिक किसी व्यक्ति को अपराधी बनाने में सबसे ज्यादा दोषी है उसका सामाजिक परिवेश। स्थितिजन्य अपराध व्यक्ति जानबूझ कर नहीं करता है अपितु ऐसी परिस्थितियां आ जाती हैं जिनमें अपराध हो जाते हैं। प्रसिद्ध न्यायशास्त्री ***हॉल*** ने कभी कहा था कि किसी भी कृत्य को अपराध घोषित करने से पूर्व उस कृत्य विशेष को निम्नलिखित बिंदुओं के आधार पर जांच-परख लेना चाहिए :

(1) समाज के हित के लिए कृत्य विशेष के कुल परिणाम हानिकारक हों अर्थात् उस कृत्य से अंततः समाज के हितों को नुकसान पहुंचता हो।

(2) कृत्य संवैधानिक रूप से निषिद्ध हो अर्थात् असंवैधानिक हो।

(3) कृत्य हानिकारक परिणाम वाला हो तथा सज्ञान हो।
(4) दंड क्रिया के लिए दंड देने की वैधानिक व्यवस्था हो।
(5) अपराध उद्देश्यात्मक कृत्य में हानि पहुंचाने के संकलित प्रयोजनापूर्ण हो।

'अपराध' शब्द को परिभाषित करते हुए ***टैपन*** कहते हैं कि ''अपराध, आपराधिक विधि का सोद्देश्य कृत्य है जो बिना किसी औचित्य एवं बचाव के किया जाता है और जिसको करने पर व्यक्ति को राज्य द्वारा दंडित किया जा सकता है।'' टैपन द्वारा अपराध की दी गई उपरोक्त परिभाषा, विधिक दृष्टिकोण को व्यापक तथा विस्तृत स्वरूप प्रदान करती है। टैपन की उपरोक्त परिभाषा में जिन तत्त्वों के आधार पर किसी कृत्य को अपराध माना गया है, वे निम्नलिखित हैं :

(1) किसी भी कार्य को अपराध घोषित करने के लिए जरूरी है कि वह कृत्य कानून के खिलाफ किया गया हो।
(2) किसी आपराधिक कानून का उल्लंघन करने पर ही कोई कृत्य अपराध कहलाता है।
(3) वैधानिक औचित्य के अंतर्गत किया गया कार्य अपराध की श्रेणी में नहीं आता है।
(4) बिना किसी उद्देश्य के किया गया कार्य, अपराध की श्रेणी में नहीं आएगा।
(5) बिना क्षमता के किया गया कार्य भी अपराध की श्रेणी में नहीं आएगा।
(6) सभी हानिकारक कृत्य अपराध नहीं होते हैं वरन् केवल वे ही हानिकारक कृत्य अपराध कहलाते हैं जो विधि द्वारा निषिद्ध हैं और कानून द्वारा हानिकारक घोषित किए गए हैं।
(7) जिस कृत्य को करने पर विधि-विधान में दंड का प्रावधान किया गया होता है, वही कृत्य अपराध की श्रेणी में आता है, चाहे दंड देने का उद्देश्य प्रतिशोधात्मक, निरोधात्मक, प्रतीकात्मक, क्षतिपूर्त्यात्मक या सुधारात्मक कुछ भी रहा हो।

इस प्रकार हम कह सकते हैं कि केवल वही कार्य अपराध की परिभाषा

के अंतर्गत आते हैं जिनको करना राज्य या सरकार द्वारा मना किया गया हो या सरकार द्वारा प्रतिबंधित हो। इसके अलावा अन्य कार्य, चाहे वे सामाजिक व नैतिक रूप से अहितकर ही क्यों न हों, अपराध नहीं माने जाते हैं। अपराध की परिभाषा समय-समय पर बदलती रहती है। उदाहरण के लिए, बहुविवाह प्राचीनकाल में वैध था और एक सर्वमान्य प्रथा के रूप में था लेकिन आज यह कानूनन अवैध है। जिस प्रकार अपराध की परिभाषा समय के साथ बदलती रहती है, ठीक उसी प्रकार भौगोलिक क्षेत्र के अनुरूप भी अपराध की परिभाषा बदलती रहती है। कई ऐसे कृत्य हैं जिन्हें एक राष्ट्र का कानून तो अवैध मानता है लेकिन दूसरे देश का कानून उस कृत्य को मान्यता देता है। इस संदर्भ में हम वेश्यावृत्ति और शराब पीने को उदाहरण के रूप में प्रस्तुत कर सकते हैं। हमारे देश में वेश्यावृत्ति एक कानूनन जुर्म है जबकि मलेशिया जैसे अनेक देशों में इसे कानूनी मान्यता प्राप्त है और इसे एक उद्योग का दर्जा दिया गया है। इसी प्रकार भारत में शराब पीना गलत नहीं है लेकिन अनेक अरब देशों में इसे एक अपराध की संज्ञा दी गई है। अपराध का एक दुर्भाग्यपूर्ण पहलू यह है कि न्यायालय, मनोवैज्ञानिक, अभियोजन अधिकारी, पुलिस आदि सभी अपराधों को रोकने में जुटे हैं लेकिन अपराधों का ग्राफ लगातार बढ़ता जा रहा है।

यदि कोई व्यक्ति मात्र कर्तव्यों या अधिकारों का उल्लंघन करता है तो उसे अपराधी नहीं माना जा सकता क्योंकि जीवन में ऐसी बहुत सी चीजें होती हैं जो कर्तव्य की सीमा में तो आती हैं लेकिन जिनका उल्लंघन करना अपराध नहीं माना जा सकता, अपराध नहीं माना जाता। इसी प्रकार अपराध और नीयत में भी गहरा संबंध है। यदि किसी व्यक्ति से कोई गलत काम हो जाए लेकिन उसकी नीयत बुरी नहीं थी तो उसे अपराधी नहीं माना जा सकता। अक्सर डाक्टर, रोगी को दवा देता है ताकि वह ठीक हो जाए लेकिन दवा की प्रतिक्रिया से रोगी की मौत भी हो सकती है। क्या ऐसे में डाक्टर को हत्यारा कहा जा सकता है? डाक्टर को अपराधी (हत्यारा) नहीं माना जा सकता क्योंकि उसकी नीयत खराब नहीं थी। यही कारण है कि किसी कृत्य को अपराध घोषित करने से पूर्व कर्ता की नीयत भी देखी जाती है। नीयत का अपराध में कितना महत्त्व होता है यह इसी से समझा जा सकता है कि प्राचीन भारतीय संस्कृति में 'दुर्भावना' और 'बुरी नीयत' को भी दंडनीय माना गया था।

हम जानते हैं कि वह कृत्य अपराध कहलाता है जिसे उस देश के कानून ने प्रतिबंधित कर रखा है। इसी प्रकार अपराधी वह है जो अपराध करता है। जिस प्रकार अपराध कई प्रकार के होते हैं, ठीक उसी प्रकार अपराधियों के भी कई वर्ग निर्धारित किए गए हैं। सवाल है कि अपराध और अपराधियों के कौन-कौन से वर्ग हैं और इन्हें किस आधार पर वर्गीकृत किया जाता है? अपराधशास्त्रियों और न्यायालयिक विज्ञानियों के मुताबिक प्रत्येक अपराधी एक वर्ग विशेष का प्रतिनिधित्व करता है अर्थात् वह अपने आप में एक 'टाइप' होता है। इस आधार पर विद्वानों ने अपराधियों के कई वर्गीकरण प्रस्तुत किए हैं।

महान अपराधशास्त्री लोम्ब्रासो के मुताबिक कुल 4 प्रकार के अपराधी पाए जाते हैं। उनके अनुसार जन्मजात अपराधियों का ही एक प्रकार के अपस्मारी अपराधी होते हैं। जन्मजात और अपस्मारी अपराधियों के मस्तिष्क में जन्म से ही एक विशेष प्रकार का दोष होता है जिसके चलते वे अनुकूल परिस्थितियां पैदा होने पर आसानी से अपराध की ओर उन्मुख हो जाते हैं। ***लोम्ब्रासो*** ने अपराधियों को निम्नलिखित 4 वर्गों में विभाजित किया था :

(1) जन्मजात अपराधी *(बोर्न क्रिमिनल)*

(2) अपस्मारी अपराधी *(एपिलेप्टिक क्रिमिनल)*

(3) आकस्मिक अपराधी *(आक्केजनल क्रिमिनल)*

(4) काम अपराधी *(क्रिमिनल बाई पैशन)*

उपरोक्त वर्गीकरण के विपरीत **गैरोफैलो** का मानना है कि अपराधियों के वर्गीकरण में मानवीय पक्ष का भी ध्यान रखना चाहिए और अपराधियों के मनोवैज्ञानिक पक्ष की अवहेलना कदापि नहीं करनी चाहिए। गैरोफैलो ने अपराधियों के 4 वर्ग बताए थे विचित्र अपराधी, विचित्र हत्यारे, बेईमान अपराधी और लंपट अपराधी। ***हेंज*** ने अपने वर्गीकरण में निम्नलिखित 4 प्रकार के अपराधी बताए थे :

☆ प्रथम दोषी अपराधी

☆ आकस्मिक अपराधी

☆ अभ्यस्त अपराधी

☆ पेशागत अपराधी

कुछ विद्वानों ने अपराधियों को उनके आर्थिक स्तर के आधार पर विभाजित किया है। सदरलैंड ने केवल दो ही प्रकार के अपराधी बताए हैं निम्नवर्गीय अपराधी और उच्चवर्गीय अपराधी। सदरलैंड ने उच्चवर्गीय अपराधियों को सफेदपोश अपराधी भी कहा था। सदरलैंड के मुताबिक निम्नवर्गीय अपराधी वे होते हैं जिनका सामाजिक व आर्थिक स्तर बेहद निम्न स्तर का होता है जबकि उच्चवर्गीय अपराधी वे होते हैं जिनका सामाजिक-आर्थिक स्तर बेहद उच्च प्रकार का होता है। चूंकि सफेदपोश अपराधियों की आपराधिक गतिविधियां समाज से छिपी रहती हैं इसलिए उन्हें समाज में सम्मानजनक स्थान प्राप्त होता है। ***बोन्जर*** ने अपराधियों का वर्गीकरण, अपराधियों के उद्देश्यों के आधार पर किया है। इसी आधार पर बोन्जर ने निम्नलिखित 5 प्रकार के अपराध बताए हैं :

(1) सामाजिक अपराध
(2) राजनैतिक अपराध
(3) आर्थिक अपराध
(4) काम संबंधी अपराध
(5) मिश्रित अपराध

उपरोक्त चर्चा के आधार पर हम कह सकते हैं कि विभिन्न विद्वानों ने अपराधियों के भिन्न-भिन्न वर्गीकरण प्रस्तुत किए हैं लेकिन कोई भी वर्गीकरण न तो पूरी तरह से सही है और न ही सर्वमान्य। मनोवैज्ञानिकों ने मनोविश्लेषण के आधार पर अपराधियों को 3 भागों में विभाजित किया है आत्मसम्मोही अपराधी, मनस्ताप वाले अपराधी और बहिर्मुखी अपराधी।

(1) ***आत्मसम्मोहीअपराधी:*** इन्हें *नारसिस्टक टाइप* भी कहा जाता है। इस वर्ग के अपराधी स्वभाव से शांतिप्रिय और स्वार्थी किस्म के होते हैं। आत्मसम्मोही अपराधी, अपने व्यक्तिगत स्वार्थों के लिए समाज को नुकसान पहुंचाने से भी पीछे नहीं हटते और अपराध कर बैठते हैं। ऐसे अपराधी परवाह नहीं करते हैं कि उनके कृत्य से समाज, परिजनों या मित्रों को कितना नुकसान हो सकता है। नारसिस्टक टाइप के अपराधियों की एक प्रमुख विशेषता यह होती है कि ये प्रत्येक अपराध काफी सोच-समझकर पूरे शातिराना तरीके से करते हैं न कि क्षणिक आवेश में।

आत्मसम्मोही अपराधी, अपराधविज्ञानियों के लिए सदैव से शोध का विषय रहे हैं। इस प्रकार के अपराधियों का विश्लेषण करने पर पता चलता है कि इस तरह के अपराधियों की कामवृत्ति का किसी न किसी रूप में दमन हुआ रहता है अर्थात् ऐसे व्यक्तियों की कामवासना अतृप्त होती है। इस प्रकार के अधिकतर अपराधी सेक्स को लेकर किसी मानसिक बीमारी से पीड़ित होते हैं। कारण चाहे जो भी हों, लेकिन इतना निश्चित है कि इस प्रकार के अपराधियों की कामशक्ति का ह्रास हुआ रहता है अर्थात् वे शारीरिक रूप से निर्बल होते हैं, अशक्त होते हैं। हाल ही में उत्तर प्रदेश के नोएडा का निठारी कांड काफी सुर्खियों में रहा था। इसका एक अभियुक्त सुरेन्द्र कोली तथाकथित रूप से अबोध बच्चों को पकड़कर उनके साथ सेक्स करने की कोशिश करता था लेकिन अपनी नपुंसकता के चलते जब वह अपने मंसूबों में सफल नहीं हो पाता था तो वह खीझ में बच्चों की हत्या कर देता था। सुरेन्द्र कोली बेहद शातिराना तरीके से बच्चों के अंगों को काटकर फेंक देता था। सुरेन्द्र कोली आत्मसम्मोही वर्ग के अपराधियों का ही प्रतिनिधित्व करता है।

(2) ***मनस्तापवालेअपराधी:*** इन्हें 'न्यूरोटिक टाइप' भी कहा जाता है। ये ऐसे अपराधी होते हैं जो क्षणभर के लिए आए आवेग के कारण अपराध कर बैठते हैं। ऐसे व्यक्ति अपराध करने से पहले न तो सोचते-विचारते हैं और न ही तर्क-वितर्क करते हैं। स्पष्ट है कि ये क्रोध आदि की गर्मी में अपराध कर बैठते हैं न कि ठंडे दिमाग से। ऐसे अपराधी अधिकतर बहुव्यक्तित्व के स्वामी होते हैं। बलात्कार और हत्या के अधिकतर अपराध इसी प्रकार के अपराधियों द्वारा किए जाते हैं।

(3) ***बहिर्मुखीअपराधी:*** ऐसे अपराधियों को 'एक्ट्रोवर्ट टाइप' के अपराधी भी कहा जाता है। इस प्रकार के अपराधी अधिकतर गिरोह या गैंग बनाकर सामूहिक रूप से अपराध करते हैं। एक विशेष बात यह कि इस प्रकार के अपराधियों द्वारा किए गए अपराधों का उद्देश्य अपने मित्र, सगे-संबंधियों को लाभ पहुंचाना होता है न कि स्वयं को लाभ पहुंचाना।

आमतौर पर उपरोक्त तीन प्रकार के अपराधी ही समाज में पाए जाते हैं। वैसे कुछ विद्वानों ने अपराधियों की आयु के आधार पर भी अपराधियों का वर्गीकरण किया है। इस आधार पर दो प्रकार के अपराधी होते हैं बाल

और प्रौढ़ अपराधी। बचपन या किशोरावस्था में जो व्यक्ति अपराध करते हैं उन्हें बाल अपराधी *(जुवेनाइल क्रिमिनल)* कहा जाता है। लगभग सभी देशों में बाल अपराधियों के निर्धारण के लिए 16 वर्ष तक की आयु निर्धारित की गई है। सामान्यतः माना जाता है कि बाल अपराधियों द्वारा छोटे-मोटे प्रकार के अपराधों को ही अंजाम दिया जाता है लेकिन आजकल देखा गया है कि कई जघन्य प्रकार के अपराध भी बाल-अपराधियों द्वारा किए जाने लगे हैं। लूटमार, राहजनी और चोरी के अलावा बाल अपराधी आजकल विभिन्न प्रकार के यौन अपराध भी करने लगे हैं। महिलाओं से छेड़खानी, बलात्कार और बलात्कार के प्रयास जैसे अपराधों में भी बच्चे संलग्न रहने लगे हैं।

समाजविज्ञानी चिंतित हैं कि क्यों बच्चे अपराध की ओर बढ़ रहे हैं। दरअसल इसका एक प्रमुख कारण आधुनिक दिखावे वाली जीवन-शैली और भोग-विलास की प्रवृत्ति भी है। बच्चों तथा किशोरों द्वारा किए जाने वाले अपराध आज एक गंभीर सामाजिक समस्या का रूप लेते जा रहे हैं। इस प्रकार के अपराधों का विश्लेषण करने पर पता चलता है कि इसके मूल में परिवार संबंधी समस्याएं ही होती हैं। निम्नलिखित पारिवारिक परिस्थितियों के कारण बच्चे अपराध की दुनिया में प्रवेश करते हैं :

(1) माता-पिता का बच्चों के प्रति असंतुलित व्यवहार
(2) माता-पिता द्वारा लगातार आपस में लड़ना
(3) परिवार की आर्थिक दरिद्रता
(4) परिवार की नैतिक क्षीणता
(5) परिवार के किसी अपराधी का अनुकरण
(6) अभिभावक द्वारा दिए गए अनुचित निर्देश
(7) विभिन्न प्रकार के मानसिक रोग, दुर्बलता या दोष।

अबबातप्रौढ़अपराधियोंकी। 16 वर्ष से ऊपर के सभी अपराधी, प्रौढ़ अपराधी कहलाते हैं। प्रौढ़ अपराधियों के साथ न्यायालय अपेक्षाकृत अधिक सख्ती बरतता है चाहे उसका अपराध किसी बालक द्वारा किए गए अपराध से कम संगीन ही क्यों न हो। प्रौढ़ अपराधियों द्वारा लगभग सभी प्रकार के अपराधों को अंजाम दिया जाता है।

अपराधकामनोवैज्ञानिकविश्लेषणः इस सिद्धांत के समर्थक मानते

हैं कि वास्तव में अपराध का मूल कारण मानसिक दुर्बलता तथा मानसिक हीनता ही है। सन् 1905 में विने ने एक *विने-साइमन* पैमाना बनाया जिससे व्यक्ति की बुद्धिमत्ता का स्तर तथा मानसिक हीनता को मापा जा सकता है। इसके बाद 1919 में गोड्डा ने व्यक्ति के मंदबुद्धि व्यवहार को आपराधिकता से जोड़ने का प्रयत्न किया।

मनोविकार विश्लेषण पर आधारित सिद्धांतः इस सिद्धांत का प्रतिपादन व्हीले तथा कानर ने किया। इन दोनों विद्वानों ने अपराध के कारणों को शारीरिक व मानसिक लक्षणों के स्थान पर संवेगात्मक व्याकुलता और व्यक्तित्व संघर्ष में खोजने का प्रयत्न किया था। इसी सिद्धांत को आगे बढ़ाते हुए हीतों ने कहा कि निराशा तथा अवसाद, व्यक्ति को अपराध की ओर खींच ले जाते हैं। इस सिद्धांत के अधिकतर समर्थकों का मानना है कि व्यक्ति विभिन्न प्रकार के मनोविकारों के कारण ही अपराध करने को प्रेरित होता है और व्यक्ति के मनोविकारों का विश्लेषण करके उसकी आपराधिकता के संबंध में भविष्यवाणी की जा सकती है।

अपराध का नियंत्रण सिद्धांतः सन् 1970 में इस सिद्धांत का प्रतिपादन करने वाले हेश ने अपराध के नियंत्रण का एक सिद्धांत दिया जो आपराधिक व्यवहार सीखने की स्वीकारात्मक तथा निषेधात्मक प्रवृत्तियों के आधार पर बनाया गया था। हेश ने कहा कि विशेष परिस्थितियों में ही व्यक्ति विधि के अनुरूप कार्य करता है, आचरण करता है। इसी प्रकार व्यक्ति आपराधिक कुकृत्य भी तभी करता है जब उसके लिए कुछ विशेष परिस्थितियां पैदा हो जाती हैं। इस सिद्धांत के अनुसार व्यक्ति का आपराधिक व्यवहार, क्रिया के प्रति प्रतिक्रिया मात्र है और कुछ भी नहीं तथा व्यक्ति वही कार्य शीघ्र सीखता है, शीघ्र करता है, जिसके एवज में उसे कुछ लाभ मिलने की आशा हो। इसलिए अपराध पर तभी नियंत्रण पाया जा सकता है जब व्यक्ति को लगे कि अपराध करने पर उसे नुकसान होगा, दंड मिलेगा।

बहुकारवादी सिद्धांतः इस सिद्धांत के प्रणेताओं में मुख्य रूप से हीले, सिरिलबर्ट और अबराहन्सन का नाम लिया जा सकता है। इस सिद्धांत के अनुसार कई उपादानों के संयुक्त प्रभाव के कारण ही किसी व्यक्ति में आपराधिक प्रवृत्ति पैदा होती है। इन कारणों को बहुत अधिक स्पष्ट रूप से

परिभाषित नहीं किया जा सकता है। इस प्रकार हम कह सकते हैं कि अपराध की घटनाएं, विभिन्न विशिष्ट परिस्थितियों के संयोग के परिणामस्वरूप होती हैं। विलियम हीले के अनुसार यदि कोई बालक कोई अपराध करता है तो उसके पीछे कोई एक-दो कारण ही नहीं होते हैं अपितु यह क्रिया कई कारकों की वजह से होती है। इसी प्रकार सिरिलबर्ट का भी मानना है कि किन्हीं दो-तीन कारकों के आधार पर ही किसी अपराध की व्याख्या नहीं की जा सकती क्योंकि कोई भी अपराध वास्तव में कई विभिन्न कारणों के संयोग से ही घटित होता है। इस सिद्धांत का समर्थन करते हुए बिल एलियर का कहना है कि किसी एक ही कारण से व्यक्ति में आपराधिक प्रवृत्ति का उदय नहीं हो सकता।

अपराधकासंघर्षताकासिद्धांतः इस सिद्धांत का प्रतिपादन करने वाले प्रमुख अपराधशास्त्री क्वैली ने अपराध की परिभाषा, परिभाषा निर्णय तथा परिभाषा क्रियान्वयनहीन सैद्धांतिक परिकल्पनाएं प्रस्तुत कीं जिनके अनुसार अपराधी व्यक्ति, समाज की राजनैतिक व आर्थिक परिस्थितियों के उत्पाद होते हैं और उन्हीं के अधीन रहते हैं। इस प्रकार देखा जाए तो अपराध का संघर्षता का यह सिद्धांत, कार्ल मार्क्स की विचारधारा के ही कुछ अधिक करीब है। लेकिन इस सिद्धांत की सबसे बड़ी कमी यह है कि वस्तुतः सामाजिक मान्यताएं, राजनैतिक मान्यताओं की पर्यायवाची नहीं होती हैं।

मानदंडधारणासिद्धांतः इस सिद्धांत को प्रस्तुत करने वाले रेकलेस (1962) के मुताबिक अपराध नियंत्रण के दो मानदंड होते हैं बाह्य और आंतरिक मानदंड। सामाजिक-न्यायिक तंत्र को तो बाह्य मानदंड कहा जाता है जबकि समूह के मानदंड आंतरिक मानदंडों की श्रेणी में आते हैं। रेकलेस के अनुसार जो व्यक्ति बाह्य एवं आंतरिक मानदंड नियंत्रकों को धारण करने की शक्ति रखते हैं, मनोवृत्ति रखते हैं, उनमें आपराधिक प्रवृत्ति उत्पन्न होने की आशंका कम होती है जबकि जो व्यक्ति इस धारणा के अयोग्य होते हैं या कमजोर होते हैं उनमें आपराधिक प्रवृत्ति पैदा होने की आशंका काफी प्रबल होती है।

आरोपणसिद्धांतः इस सिद्धांत का प्रणेता फ्रेंक (1938) को माना जाता है तथा इस सिद्धांत में समाज के सदस्यों की प्रतिक्रिया के आधार पर अपराध को संभालने का विचार दिया गया था। बाद में इसी सिद्धांत को एडविन लेमट (1959) ने विकसित किया, जिनके अनुसार औपचारिक अथवा

आपराधिकता, सामाजिक प्रतिक्रिया द्वारा परिभाषित की जाती है और इस आपराधिकता का स्वभाव और दर, अपराधी की भूमिका के साथ सामाजिक प्रतिक्रिया द्वारा ही स्वरूप ग्रहण करते हैं।

अपराध के विभिन्न सिद्धांतों में हम पढ़ चुके हैं कि अपराध का सबसे बड़ा कारण, व्यक्ति की मानसिक तथा बौद्धिक दुर्बलता ही होता है। इस संदर्भ में गॉडर्ड ने ठीक ही कहा है कि ''अपराध का सबसे बड़ा अकेला कारण सिर्फ और सिर्फ बौद्धिक दुर्बलता ही है।'' इसी क्रम में इटली के चिकित्सक लौमब्रोसो ने अपराधियों की शारीरिक संरचना का अध्ययन किया और बताया कि आपराधिक मानसिकता वाले व्यक्ति का सिर नीचा होता है और ललाट अपेक्षाकृत कुछ पीछे की ओर होता है। इसी प्रकार ऐसे व्यक्तियों का जबड़ा कुछ भारी और बाहर को निकला होता है। बाद में 1913 में चार्ल्स बोरिंग ने लौमब्रोसो की उपरोक्त धारणा को सिरे से नकारते हुए बताया कि अपराधी और निरपराधी व्यक्ति को उनकी शारीरिक संरचना के आधार पर नहीं पहचाना जा सकता। कुछ भी हो, इतना तो निश्चित है कि व्यक्ति की आपराधिक प्रवृत्ति के पीछे उसकी मनोवृत्ति और मानसिक स्थिति का भी महत्त्वपूर्ण हाथ होता है।

शिकागो के विद्वान हीले ने अपने एक अध्ययन में पाया कि लगभग 28 प्रतिशत अपराधी निरे मूर्ख होते हैं। इसी प्रकार कैलीफोर्निया के समाजशास्त्री विलियम ने बाल-अपराधियों के बीच एक सर्वेक्षण किया और पाया कि 32 प्रतिशत से भी अधिक बाल-अपराधी मंद बुद्धि वाले थे। इसके बाद कई मनोवैज्ञानिकों ने इसी प्रकार के अध्ययन किए और पाया कि मंद बुद्धि तथा मानसिक कमजोरी, आपराधिकता का एक प्रमुख कारण तो है लेकिन साथ ही कुछ कुशाग्र बुद्धि वाले व्यक्ति भी अपराधी होते हैं। अध्ययन बताते हैं कि जालसाजी, तस्करी और धोखाधड़ी जैसे अपराध अधिकतर तीव्र बुद्धि वाले अपराधी ही करते हैं। कुछ अत्यधिक तीक्ष्ण बुद्धि वाले अपराधियों का अध्ययन करने पर पाया गया कि ऐसे व्यक्ति का रुझान, किशोरावस्था से ही अपराध की ओर था और जब उन्हें अपराध के लिए अवसर व उपयुक्त परिस्थितियां मिलीं तो उन्होंने अपनी बुद्धि का प्रयोग, आपराधिक कुकृत्यों को करने में किया।

जब व्यक्ति अपनी आंतरिक इच्छाओं को दबा लेता है तो ऊपर से भले

ही यह लगता है कि उसने अपनी इच्छाओं को दबा लिया है लेकिन वास्तव में ऐसा होता नहीं है। वस्तुतः दमित इच्छाएं, मन-मस्तिष्क के किसी कोने में जाकर सुप्तावस्था में बैठ जाती हैं। जब कभी व्यक्ति को आपराधिक माहौल मिलता है अथवा दमित इच्छाएं को फलने-फूलने का अवसर मिलता है तो व्यक्ति आपराधिक कुकृत्य करने लगता है, अपनी इच्छाएं पूरी करने लगता है। उदाहरणस्वरूप, हम देखते हैं कि किसी कामुक व्यक्ति की काम से संबंधित इच्छाएं दबाने पर भी नष्ट नहीं होती हैं। यदि व्यक्ति की काम-इच्छाओं को दमित किया जाता है, दबाया जाता है तो वे विकृत स्वरूप में अपना सिर उठाने लगती हैं परिणामस्वरूप व्यक्ति छेड़खानी, यौन-उत्पीड़न जैसे कुकृत्य करने लगता है। बलात्कार करने वाला व्यक्ति पीड़िता को दुःख पहुंचाकर खुद सुख का अनुभव करता है अर्थात् उसकी मानसिकता विकृत हो जाती है। मनोवैज्ञानिकों का मानना है कि कई बार व्यक्ति, अपने मानसिक दोषों के चलते भी अपराध करने लगता है। यदि व्यक्ति में बौद्धिकता की कमी होगी तो वह अपराध की ओर अधिक तेजी से और अधिक सरलता से मुड़ जाता है।

मनोवैज्ञानिक सर्वेक्षणों में पाया गया है कि मानसिक रूप से दुर्बल व्यक्ति और दुर्बल इच्छाशक्ति वाले व्यक्ति, आसानी से किसी के भी कहने में आ जाते हैं। ऐसे व्यक्ति को यदि अपराध करने के लिए प्रेरित किया जाए तो वह आसानी से आपराधिक निर्देशों को मान लेता है। मानसिक दुर्बलता के कारण व्यक्ति यह निर्णय नहीं कर पाता कि जिस कार्य को उसे करने के लिए प्रेरित किया जा रहा है वह सही है या गलत। कुछ व्यक्तियों में किसी एक वृत्ति या मानसिक इच्छा का अत्यधिक विकास हो जाता है जिस कारण वह एक विशेष प्रकार के अपराध ही करने लगता है। किसी दूसरे व्यक्ति की देखादेखी भी कुछ व्यक्तियों में आपराधिक प्रवृत्ति पनप जाती है। इस प्रकार अनुकरण के कारण भी कुछ लोग अपराध की ओर उन्मुख हो जाते हैं। जब कोई व्यक्ति गैर-कानूनी धंधे करके ऐशोआराम से रहता है तो उसके आसपास के लोग उसका अनुकरण करने लगते हैं। इस प्रकार अनुकरण भी आपराधिक प्रवृत्ति के लिए जिम्मेदार होता है। इस प्रकार स्पष्ट है कि मनोवैज्ञानिक कारणों से भी व्यक्ति अपराध करने लगता है। मनोवैज्ञानिकों ने अपराध के निम्नलिखित मनोवैज्ञानिक आधारों की पहचान की है :

(1) मानसिक दोष (2) मानसिक दुर्बलता
(3) पैतृक विशेषताएं (4) दमित इच्छा
(5) अनुकरण (6) प्रवृत्तिशीलता
(7) पारिवारिक कारण (8) निर्धनता
(9) भौतिकतावादी संस्कृति (10) आधुनिकता

विभिन्न प्रकार के मानसिक रोगों को भी अपराध का एक प्रमुख कारण माना जाता है। मनोविज्ञान में कई ऐसे रोगों की पहचान की गई है जिनका रोगी, अपराध करने को अधिक उन्मुख होता है। आज के भौतिक और आधुनिक जीवन में व्यक्ति की इच्छाएं असीमित हो गई हैं, वह रातोंरात अमीर बनकर सारे ऐशोआराम पा लेना चाहता है, सारी सुख-सुविधाएं जुटा लेना चाहता है। ऐसे भौतिकतावादी इच्छाओं के कारण व्यक्ति तनाव का शिकार होकर कई ऐसे मानसिक रोगों का शिकार हो जाता है जिनके कारण वह अपराध करने लगता है। चूंकि निम्नवर्गीय लोगों के जीवन में जटिलताएं अधिक होती हैं, उन्हें अधिक संघर्ष करने पड़ते हैं और उनके पास चिकित्सा की सुविधाएं भी कम होती हैं इसलिए उनमें मानसिक रोग अधिक पाए जाते हैं। इसके विपरीत उच्चवर्गीय व्यक्तियों का जीवन अपेक्षाकृत सरल होता है और उनके पास सारी सुख-सुविधाएं उपलब्ध होती हैं इसलिए उन्हें मानसिक रोगों का शिकार कम ही होना पड़ता है। यही कारण है कि अधिकतर अपराधी निम्नवर्ग से संबंधित होते हैं। वैसे आजकल इस तथ्य में काफी विचलन देखने को मिल रहे हैं। महानगरों में उच्चवर्ग के धनाढ्य युवक-युवतियां भी अब गंभीर किस्म के अपराध करने लगे हैं।

इसमें कोई शक नहीं है कि अधिकतर अपराधियों का व्यक्तित्व, असामान्य तथा कुछ विकृत होता है। सभी आदतन अपराधियों में किसी-न-किसी प्रकार का कोई मानसिक विकार अवश्य पाया जाता है। मनोवैज्ञानिक अध्ययन बताते हैं कि अपराधियों में स्वच्छंदता, विद्रोह, ध्वंसात्मक प्रवृत्ति और उत्पात मचाने की प्रवृत्ति, अपेक्षाकृत अधिक होती है। कहा जाता है कि अपराधी अपेक्षाकृत जल्दी ही आवेश में आ जाते हैं और बात-बात पर वे उत्तेजित भी हो जाते हैं।

मानसिक रोग या मनोविकार जन्मजात भी हो सकते हैं और जन्म के बाद भी कभी पैदा हो सकते हैं। इस संदर्भ में चोरी की प्रवृत्ति को उदाहरणस्वरूप लिया जा सकता है। कुछ व्यक्तियों में बचपन से ही चोरी की प्रवृत्ति होती है और वे

बिना कुछ किए ही कोई वस्तु पा लेना चाहते हैं अर्थात् वस्तु को चुरा लेना चाहते हैं। यह मानसिक प्रवृत्ति ही उन्हें चोरी के लिए प्रेरित करती है। एक दिलचस्प शोध-निष्कर्ष के मुताबिक यदि जुड़वां बच्चों में से कोई भी आपराधिक प्रवृत्ति का होता है तो निश्चित रूप से दूसरा बच्चा भी आपराधिक प्रवृत्ति का ही होगा।

विभिन्नमानसिकरोगः वैज्ञानिकों के अनुसार मानसिक रोग दो प्रकार के होते हैं मानसिक दौर्बल्य और मनोविक्षेप। मानसिक दौर्बल्य कुल छह प्रकार के माने जाते हैं स्नायु रोग, औत्सुक्य विकलता *(ऐंनजाईटी)*, भीति *(फोबिया)*, कल्पनागृह *(ओबसेशन)*, अनियंत्रित अभ्यास *(कम्पल्शन)* और *हिस्टीरिया*। ठीक इसी प्रकार मनोविक्षेप के भी तीन प्रकार बताए गए हैं स्थिर भ्रम रोग, असामयिक मनोहास्र और उत्साह विषादमय उन्माद *(मैनिकडिप्रेसिव साइकोसिस)*।

क्रोध और प्रतिशोध व्यक्ति की मानसिक अवस्थाएं हैं और उन्हीं के वशीभूत व्यक्ति कभी-कभी गंभीर अपराध कर बैठता है। शरीर-क्रिया विज्ञान के अनुसार जब व्यक्ति की कोई इच्छा पूरी नहीं हो पाती है या वह अपना मनचाहा कार्य नहीं कर पाता है तो *डक्टलैस ग्लैंड* नामक ग्रंथि से एक हार्मोन का स्रावण होता है जिस कारण व्यक्ति के रक्त में शर्करा (शुगर) की मात्रा बढ़ जाती है और रक्त-संचार तीव्र होने लगता है। इसका परिणाम यह होता है कि व्यक्ति स्वयं को अत्यधिक शक्तिशाली और सामर्थ्यवान समझने लगता है। क्षणिक शक्ति के अहसास से इस समय व्यक्ति का अपने ऊपर से नियंत्रण समाप्त हो जाता है और उसे पता नहीं रहता कि वह क्या कर रहा है। इस मानसिक स्थिति को क्रोध कहते हैं और क्रोधावस्था में व्यक्ति, आपराधिक कुकृत्य कर बैठता है। क्रोधावस्था की कुल 4 अवस्थाएं होती हैं आवेश, झुंझलाहट, रूदन और शांत्यातिरेक। आवेश, क्रोध की अत्याधिक खतरनाक स्थिति होती है। आवेश में व्यक्ति का अपने ऊपर से नियंत्रण बिल्कुल समाप्त हो जाता है और इस अवस्था में वह हत्या जैसा जघन्य अपराध भी कर बैठता है। जब व्यक्ति अपने क्रोध, अपने दुख को प्रकट नहीं कर पाता है तो वह झुंझला उठता है। झुंझलावस्था की इस अवस्था में व्यक्ति अपने बाल नोचने लगता है, बुदबुदाने लगता है और आसपास की वस्तुओं को इधर-उधर फेंकने लगता है। क्रोधावस्था की इस अवस्था की विशिष्टता यह है कि इसमें व्यक्ति, दूसरे को

कोई गंभीर क्षति नहीं पहुंचा पाता है और अंदर ही अंदर घुटकर रह जाता है।

अत्याधिक क्रोध के बावजूद जब व्यक्ति कुछ नहीं कर पाता है, असहाय हो जाता है तो वह रोने लगता है। इसी से मिलती-जुलती क्रोधावस्था, शांत्यातिरेक कहलाती है जिसमें व्यक्ति कुछ नहीं कर पाता है और सारा क्रोध अपने सीने में ही दबा लेता है। कहा जाता है कि महात्मा गांधी, शांत्यातिरेक के अभ्यास के कारण ही अपने को क्रोधित होने से बचा लेते थे। यदि गहराई से अध्ययन करें तो पता चलता है कि क्रोध की केवल एक अवस्था ही ऐसी है जिसमें व्यक्ति अपराध करता है और वह अवस्था है आवेश की अवस्था। बाकी की तीन क्रोधावस्थाओं में व्यक्ति समाज के लिए खतरनाक नहीं होता है अपितु अपना ही नुकसान कर बैठता है।

प्रतिशोध नामक मानसिक अवस्था भी कई व्यक्तियों में पाई जाती है। वस्तुतः क्रोध के कारण ही व्यक्ति प्रतिशोध लेने को आतुर हो जाता है। क्रोध और प्रतिशोध में मुख्य अंतर यही है कि क्रोध तो एक अस्थायी अवस्था है, क्षणिक आवेश की अवस्था है जबकि प्रतिशोध एक स्थायी अवस्था है। वास्तव में प्रतिशोध एक स्थायी मनोविकार है, एक स्थायी मनोरोग है। प्रतिशोध में व्यक्ति अंदर ही अंदर तब तक आवेशित रहता है जब तक कि वह अपना प्रतिशोध पूरा नहीं कर लेता। प्रतिशोध की एक विशिष्टता यह भी है कि प्रतिशोध प्रवृत्ति वाले लोग अपने आवेश को प्रकट नहीं करते हैं और समय आने पर प्रतिशोध ले लेते हैं पूरे ठंडे दिमाग से। वस्तुतः प्रतिशोध दो प्रकार के होते हैं आवेग-प्रधान और ईर्ष्या-प्रधान। आवेग-प्रधान प्रतिशोध में व्यक्ति दूसरे को शारीरिक हानि पहुंचाकर अपने को शांत करना चाहता है जबकि ईर्ष्या-प्रधान प्रतिशोध में व्यक्ति षड्यंत्र रचकर दूसरे पक्ष को नीचा दिखाना चाहता है, उसकी बेइज्जती करना चाहता है।

अपराध का प्राणिशास्त्र

व्यक्ति की शारीरिक रचना, शरीर क्रियाविधि और उसके संपूर्ण शरीर का अध्ययन प्राणिशास्त्र के अंतर्गत किया जाता है। जैसे-जैसे प्राणिशास्त्र का विकास होता गया वैज्ञानिक कहने लगे कि प्राणिशास्त्र के आधार पर भी किसी व्यक्ति की आपराधिक प्रवृत्ति की भविष्यवाणी की जा सकती है। लेकिन

वास्तव में सच्चाई यह है कि केवल प्राणिशास्त्र के आधार पर ही इस संदर्भ में कुछ नहीं कहा जा सकता। इसके लिए भूगोल, पर्यावरण और व्यक्ति के सांस्कृतिक विकास का भी सहारा लेना पड़ता है।

प्रो. नोयलपेटन ने एक सर्वेक्षण में पाया कि किसानों के बच्चे, शहरी बच्चों की अपेक्षा अधिक तेजी से बड़े होते हैं और अपेक्षाकृत अधिक होशियार होते हैं। फिर डा. शुबसाल ने बताया कि भिन्न-भिन्न देशों की भिन्न-भिन्न जातियों में व्यक्ति की शारीरिक रचनाएं भिन्न-भिन्न प्रकार की होती हैं और इनमें अलग-अलग प्रकार की बीमारियां होती हैं। डा. बैरी और पोरटियस ने 6 हजार बच्चों के बीच अध्ययन करने पर बताया कि 13 वर्ष तक के बच्चे के मस्तिष्क का औसतन वजन 1352 क्यूबिक सेंटीमीटर होता है और इसी उम्र के मानसिक दोष वाले बच्चों के मस्तिष्क का वजन केवल 1292 क्यूबिक सेंटीमीटर ही होता है। इन दोनों वैज्ञानिकों ने यह भी बताया कि अपराधियों के मस्तिष्क का वजन अपेक्षाकृत कम होता है। बाद में कुछ वैज्ञानिकों ने यह भी बताया कि सिर के गठन का भी अपराध से बेहद गहरा संबंध होता है। डा. लोम्ब्रासो ने बताया कि एक विशेष प्रकार की लंबाई-चौड़ाई वाली नाक तथा ललाट, व्यक्ति की आपराधिक प्रवृत्ति के द्योतक होते हैं। इस सिद्धांत का समर्थन बाद में क्वैतेलेते तथा बरटिलॉन ने भी किया।

यह एक स्थापित तथ्य है कि पृथ्वी पर प्रत्येक व्यक्ति के रूप-रंग तथा चेहरे के नक्शे में काफी विभिन्नताएं होती हैं। व्यक्तियों के ललाट, नाक तथा चेहरे में पहचानने योग्य भिन्नताएं पाई जाती हैं। प्राणिविज्ञान और भूगोल के आधार पर हम कह सकते हैं कि समान प्रकार के भौगोलिक क्षेत्र में रहने वाले लोगों की शारीरिक संरचना लगभग समान होती है। कुछ प्राणिशास्त्रियों का यह भी मानना है कि व्यक्ति की आपराधिक प्रवृत्ति आनुवंशिक होती है अर्थात् यह आपराधिक प्रवृत्ति उसे अपने माता-पिता से विरासत में मिलती है। लेकिन इस सिद्धांत का समर्थन करने वाले बहुत कम हैं। अक्सर देखा गया है कि अपराधी मां-बापों के बच्चे अच्छा माहौल मिलने पर एक अच्छे नागरिक साबित होते हैं।

हमारा देश विभिन्न जातियों, धर्मों में बंटा हुआ है और हमारे यहां कई ऐसी जातियां हैं जिनका पेशा ही अपराध करना है। ऐसी आपराधिक जातियों में बच्चे, आपराधिक माहौल में ही पलते-बढ़ते हैं और बाद में अपराध को ही

अपना पेशा बना लेते हैं। कई जातियों में तो अपराध करने को कला के रूप में लिया जाता है। जिस प्रकार कुम्हार का बच्चा, कुल्हड़ बनाना अपने पिता से सीखता है ठीक उसी प्रकार इन आपराधिक जातियों के बच्चे अपराध की कला अपने बुजुर्गों से सीखते हैं। इस संदर्भ में यह भी उल्लेखनीय है कि अधिकतर जातियां किसी एक विशिष्ट अपराध में ही सिद्धहस्त होती हैं। कुछ जातियां चोरी को पेशे के रूप में अपनाती हैं तो कुछ जातियां लूटमार को वरीयता देती हैं। ठीक इसी प्रकार कई जातियों में लड़कियां तथा महिलाएं वेश्यावृत्ति में संलग्न रहकर पूरे परिवार का पेट पालती हैं।

कुछ प्राणिशास्त्रियों का मानना है कि यदि आपराधिक जाति के व्यक्तियों की नाप-तोल कर ली जाए तो अपराधियों के शारीरिक गठन के बारे में महत्त्वपूर्ण निष्कर्ष निकाले जा सकते हैं। कुछ विद्वानों ने आपराधिक जातियों की खोपड़ी की माप, नाक की माप तथा औसतन शारीरिक ऊंचाई का अध्ययन किया और बताया कि डोम, हबूड़ा तथा भन्तू जैसी आपराधिक जातियों में खोपड़ी का अंक क्रमशः 73.79, 73.71 और 78.43 होता है जबकि इनमें नाक का अंक क्रमशः 75.7, 71.29 और 68.46 होता है। इसी प्रकार इन तीन जातियों में औसत शारीरिक ऊंचाई क्रमशः 166.53, 164.91 और 163.13 सेंटीमीटर होती है। आजकल के आधुनिक अध्ययनों से निष्कर्ष निकलता है कि आपराधिक जातियों में शारीरिक रूप-रंग कुछ अलग प्रकार का नहीं होता है।

अपराधियों द्वारा प्रौद्योगिकी का इस्तेमाल

यह एक दुर्भाग्यपूर्ण तथ्य है कि अब प्रौद्योगिकी का इस्तेमाल आतंकवादियों और अपराधियों द्वारा भी खूब किया जाने लगा है। प्रौद्योगिकी ने हमारे जीवन को बेहद तेज गति प्रदान कर दी है, हर चीज बहुत तेजी से भाग रही है। दो-तीन दशक पहले तक दूरभाष जैसी वस्तु इतनी असामान्य थी कि किसी के घर में दूरभाष होना एक प्रतिष्ठा की चीज माना जाता था लेकिन अब हमारा देश संचार-क्रांति के दौर से गुजर रहा है और अब दूरभाष की सुविधा, गांव-गांव तक पहुंच गई है। दूरभाष के बाद अब मोबाइल फोन भी आम आदमी के हाथों तक पहुंच गए हैं। मोबाइल फोन ने आम जनता की जिंदगी में अपनी जगह बना ली है तो अपराधी भी मोबाइल फोन का खूब इस्तेमाल करने लगे हैं। फिरौती

की मांग करने, धमकी देकर वसूली करने, अपने गिरोह के सदस्यों से बात करने आदि में आपराधिक तत्व, मोबाइल फोन का ही इस्तेमाल करने लगे हैं। मोबाइल फोन के कारण अपराधियों के बहुत से काम बेहद आसान हो गए हैं तो इसके कारण अपराध की प्रक्रिया को गति भी मिली है। संचार क्रांति का लाभ अपराधी तो उठा ही रहे हैं साथ ही कुछ असामाजिक तत्व भी मोबाइल फोन या पी.सी.ओ. के दूरभाष के जरिए, बम आदि रखे होने की झूठी सूचना *(हॉक्स-कॉल)* देकर सुरक्षा एजेंसियों को खूब छकाते हैं। बम रखे होने की इन सूचनाओं के कारण सुरक्षा एजेंसियां बेवजह दबाव में आ जाती हैं तो आम आदमी का तो जीवन ही जैसे कुछ समय के लिए ठहर सा जाता है।

इंटरनेट क्रांति का लाभ भी आपराधिक तत्व खूब उठा रहे हैं। दुनिया के अनेक आतंकी संगठन, इंटरनेट के जरिए ही अपने सदस्यों से संपर्क में रहते हैं। दुनिया का सबसे खतरनाक आतंकवादी संगठन 'अल कायदा' और उसका सरगना ओसामा-बिन-लादेन, इंटरनेट के जरिए ही अपने सदस्यों को कूट-भाषा में निर्देश देता है और उनसे बातचीत करता है। इंटरनेट के कारण कुछ प्रकार के सामाजिक अपराधों को भी बढ़ावा मिला है। आजकल जमाना *'सोशल नेटवर्किंग साइट्स'* का है। *'आरकुट', 'भारत स्टूडेंट'* और *'फेसबुक'* जैसी सोशल नेटवर्किंग साइट्स से युवतियों के व्यक्तिगत विवरण चुरा कर उन्हें परेशान करना, ब्लैकमेल करना या किसी के अश्लील चित्रों, वीडियो क्लिपों को इन सोशल नेटवर्किंग साइट्स पर डाल देने के मामले अब खूब सामने आ रहे हैं। इसके अलावा देह-व्यापार का धंधा भी इंटरनेट के सहारे ही चल रहा है। सभी हाई-प्रोफाइल सेक्स रेकैट्स, इंटरनेट के पहिये पर ही दौड़ रहे हैं।

यह सच है कि सूचना-क्रांति (संचार साधनों, कंप्यूटर एवं इंटरनेट का प्रयोग) ने आज हमारे जीवन में क्रांति सी स्थिति पैदा कर दी है। इसके कारण हमारा जीवन अब काफी सरल व सुविधाजनक हो गया है लेकिन तस्वीर का दूसरा रुख बेहद स्याह है। इस सूचना क्रांति ने हमारे समाज में जहर घोलने का काम भी किया है। सूचना क्रांति ने बच्चों से उनकी मासूमियत और स्वाभाविक मानसिक विकास-प्रक्रिया छीन ली है। इंटरनेट का राक्षस, बच्चों की जिंदगी में जहर घोलने का काम कर रहा है। इस समय दुनियाभर में लगभग पचास हजार ऐसी वेबसाइटें काम कर रही हैं, जिनका एकमात्र उद्देश्य इन बच्चों को यौन-उत्पीड़न व शोषण

के शिकंजे में कसना है। हाल ही में *यूनेस्को* ने *'वर्ल्ड मूवमेंट ऑफ सिटीजन्स टू प्रोटेक्ट इनोसेंस इन डेंजर'* शीर्षक से एक पुस्तिका प्रकाशित की है, जिसमें इंटरनेट के खतरे के प्रति आगाह किया गया है। पुस्तिका के मुताबिक दुनियाभर में इस समय लगभग 40 हजार ऐसे चैटरूम कार्यरत हैं जिनमें बालकों व बालिकाओं के प्रति कुंठित यौन मानसिकता से ग्रसित व्यक्ति, स्वयं को किशोरवय का बताकर बच्चों से मिलने की इच्छा प्रकट करते हैं। बाद में ये कुंठित व्यक्ति, बच्चों का यौन शोषण करते हैं।

चैटरूमों के अलावा इंटरनेट पर तकरीबन 25 हजार ऐसी साइटें भी हैं, जिनमें बच्चों व अधेड़ों के यौन-संबंधों को लेकर चित्र, कहानियां व समाचारों का संग्रह है। इन सभी साइटों पर यौन-संबंधों को काफी चटपटे व मसालेदार रूप में परोसा जाता है। विभिन्न स्रोतों से प्राप्त इन अश्लील सूचनाओं से बाल-मन में इनके प्रति स्वाभाविक जिज्ञासा उत्पन्न हो जाती है, जिसकी परिणति उनके यौन-शोषण के रूप में होती है। अश्लील वेबसाइटों तक आसान पहुंच के कारण अब छोटे-छोटे बच्चे भी यौन-अपराधों में संलिप्त पाए जाने लगे हैं। कुछ वर्ष पूर्व घटे *'डी.पी.एस. एम.एम.एस. कांड'* के जहर को असानी से नहीं भुलाया जा सकता। इस कांड में दिल्ली के रामाकृष्णा पुरम् स्थित अत्याधिक प्रतिष्ठित, दिल्ली पब्लिक स्कूल के एक छात्र ने अपनी एक सहपाठिनी को घर बुला कर उसके साथ यौनाचार किया और किशोरी द्वारा मुख-मैथुन करती तस्वीरें अपने मोबाइल फोन के कैमरे में उतार लीं। बाद में आरोपी छात्र ने वे तस्वीरें, एम.एम.एस. *(मल्टीमीडिया शॉर्ट मैसेजेज)* के जरिए अपने दोस्तों को भी भेज दीं। सालों पहले घटी यह घटना ही यह बताने के लिए काफी है कि इंटरनेट व सूचनाक्रांति का कितना बुरा असर हमारे समाज पर पड़ रहा है और इनके सहारे कैसे-कैसे अपराधों को अंजाम दिया जा रहा है।

इंटरनेट का प्रयोग बढ़ रहा है तो इंटरनेट-अपराधों की भी बाढ़ सी आ गई है। इंटरनेट पर धोखाधड़ी और ब्रांड का दुरुपयोग अब एक आम सी बात हो गई है। 'मार्क मॉनीटर ब्रांड जैकिंग इंडेक्स स्प्रिंग, 2008' ने करोड़ों वेब पेजों और लाखों ई-मेल का अध्ययन करने के बाद अपनी रिपोर्ट में बताया है कि सन् 2008 की पहली तिमाही (जनवरी मार्च) में ही साइबर-धोखाधड़ी के 40 हजार से भी अधिक मामले दर्ज किए जा चुके हैं जो पिछले वर्ष (सन् 2007) की प्रथम

तिमाही की तुलना में 40 फीसदी ज्यादा हैं। सन् 2008 की पहली तिमाही में ही फ्रॉड-एसोसिएशन के 78,562 मामले, पे-पर-क्लिक घोटाले के 29,504 मामले, डोमेन काइटिंग के 19,737 मामले और आपत्तिजनक सामग्री डाल कर ब्रांड जैकिंग करने के कुल 1464 मामले थानों में दर्ज हो चुके हैं। रिपोर्ट में कहा गया है कि फिशिंग आज भी ब्रांड जैकिंग का सबसे कुख्यात तरीका है।

इंटरनेट का प्रयोग आतंकवादी और अपराधी तो करते ही हैं, कभी-कभी हमारे दुश्मन देश भी इंटरनेट के द्वारा हमारी समूची व्यवस्था को ध्वस्त करने की कोशिश करते रहते हैं। अप्रैल, 2008 में भारतीय विदेश मंत्रालय की वेबसाइट को हैक करने की कोशिश हमारे पड़ोसी देश चीन की ओर से की गई। दरअसल कई देश इस तरह की कोशिशें अक्सर करते रहते हैं। वैसे हैकिंग के दौरान किसी तरह की जानकारी लीक नहीं हुई क्योंकि विदेश मंत्रालय अपनी वेबसाइट की सुरक्षा दीवार को अक्सर बदलता रहता है और विशेष महत्त्व की गोपनीय बातों का मंत्रालय वेबसाइट के जरिए आदान-प्रदान ही नहीं करता है। विदेश और रक्षा मंत्रालयों के अलावा अन्य महत्त्वपूर्ण सरकारी संगठनों की वेबसाइटों को भी हैक करने की कोशिशें अक्सर की जाती रहती हैं। अभी कुछ समय पहले *'नेशनल इनफॉरमेटिक्स सेंटर'* (एन.आई.सी.) की वेबसाइट और उसके सर्वर से भी छेड़छाड़ करने की कोशिश की गई थी। नेशनल इनफॉरमेटिक्स सेंटर, केंद्र व राज्य सरकारों को नेटवर्क उपलब्ध कराता है। सरकारी योजनाओं से जुड़े आंकड़े व सारा लेखा-जोखा भी एन.आई.सी. के सर्वर में ही सुरक्षित रहता है। यदि एन.आई.सी. का सर्वर ठप हो जाए तो सरकार का सारा सूचना-तंत्र ध्वस्त हो सकता है। इसके अलावा सरकारी कामकाज और यहां तक कि पुलिस मुख्यालयों के डाटाबेस पर भी खतरा पैदा हो सकता है।

तकनीक और प्रौद्योगिकी का इस्तेमाल आतंकवादी भी कर रहे हैं। कहा जा सकता है कि आतंकियों का नया हथियार *'साइबर वार'* बन चुका है। *'साइबर-वार'* के तहत खुफिया एजेंसियों और पुलिस को *ई-मेल* भेज कर बम विस्फोटों की धमकियां दी जाती हैं जिस कारण हमारी सुरक्षा एजेंसियां उलझ कर रह जाती हैं। हमारे देश में अत्याधुनिक तकनीक से लैस आतंकियों के हौसले कितने बुलंद हो चुके हैं इसका अंदाजा इसी बात से लगाया जा सकता है कि देश के लगभग सभी प्रमुख नगरों में आतंकवादियों के *'टेरर मॉड्यूल'* हैं। टेरर मॉड्यूल

में एक 'बम मेकर' होता है। यह एक तकनीकी व्यक्ति होता है जिसका नाम गोपनीय रखा जाता है। यहां तक कि पूरे ऑपरेशन को अंजाम देने वाले भी उसे नहीं जानते। यह बम बनाने वाला मॉड्यूल, गोपनीय स्थान से आता है और फिर वहीं वापस लौट जाता है। इसके बाद *'होल्डर'* सक्रिय होते हैं जिन्हें बम रखने का काम सौंपा जाता है। *'होल्डर'* को बम चालू करने की तकनीक बताई जाती है। मॉड्यूल में दो से चार लोग और होते हैं जो पुलिस को बम की जानकारी देने का काम करते हैं ताकि बम फटने से ठीक पहले अफरा-तफरी मच जाए।

हाल ही में भारत सरकार के गृह मंत्रालय ने पाया कि आतंकवादियों और नक्सलवादियों द्वारा अत्याधुनिक तकनीकों का खूब इस्तेमाल किया जा रहा है। अभी कुछ समय पूर्व केंद्रीय गृह राज्यमंत्री ने लोकसभा में भी स्वीकारा था कि आज आतंकवादी, *'टेक्नोसैवी'* हो रहे हैं। अपने नापाक इरादों को अंजाम देने के लिए ये लोग सैटेलाइट फोन, इंटरनेट, अत्याधुनिक वायरलैस उपकरण और अन्य हाईटेक सुविधाओं का इस्तेमाल कर रहे हैं। इन माध्यमों के जरिए आतंकवादी पैसा और समर्थन तो जुटा ही रहे हैं साथ ही नई भर्ती भी कर रहे हैं। तकनीक के प्रयोग में आतंकवादी, सरकार से चार कदम आगे चल रहे हैं। कई नक्सली संगठनों की वेबसाइटें धड़ल्ले से चल रही हैं।

ई-टिकटिंग ने हमारे जीवन को बेहद सुविधाजनक बना दिया है लेकिन आजकल ई-टिकटिंग से जालसाजी भी होने लगी है। एक समय था जब रेलवे का टिकट आरक्षित कराने के लिए घंटों लाइन में लगना पड़ता था और एयरलाइनों का टिकट लेने के लिए महानगरों में धक्के खाने पड़ते थे लेकिन ई-टिकटिंग की सुविधा ने हमारी सारी मुश्किलें आसान कर दी हैं। अब आप इंटरनेट के जरिए घर बैठे ही किसी भी रेलगाड़ी और किसी भी हवाई उड़ान का टिकट ले सकते हैं। ई-टिकटिंग ने सुविधा तो दी है लेकिन इसके कारण जालसाजी और धोखाधड़ी के मामले भी काफी बढ़ गए हैं। इस अपराध में किसी और के क्रेडिट कार्ड के माध्यम से इंटरनेट पर एयरलाइनों की टिकट बुक कराई जाती हैं। दरअसल ई-टिकटिंग के जरिए जालसाजी करने वाले लोग थाइलैंड और सिंगापुर जैसे देशों के निवासियों के क्रेडिट कार्डों का डाटा चुरा लेते हैं और फिर इस डाटा के आधार पर वे किसी भी एयरलाइन के टिकट बुक करा लेते हैं। इस प्रकार ये साइबर अपराधी, करोड़ों रुपये का चूना

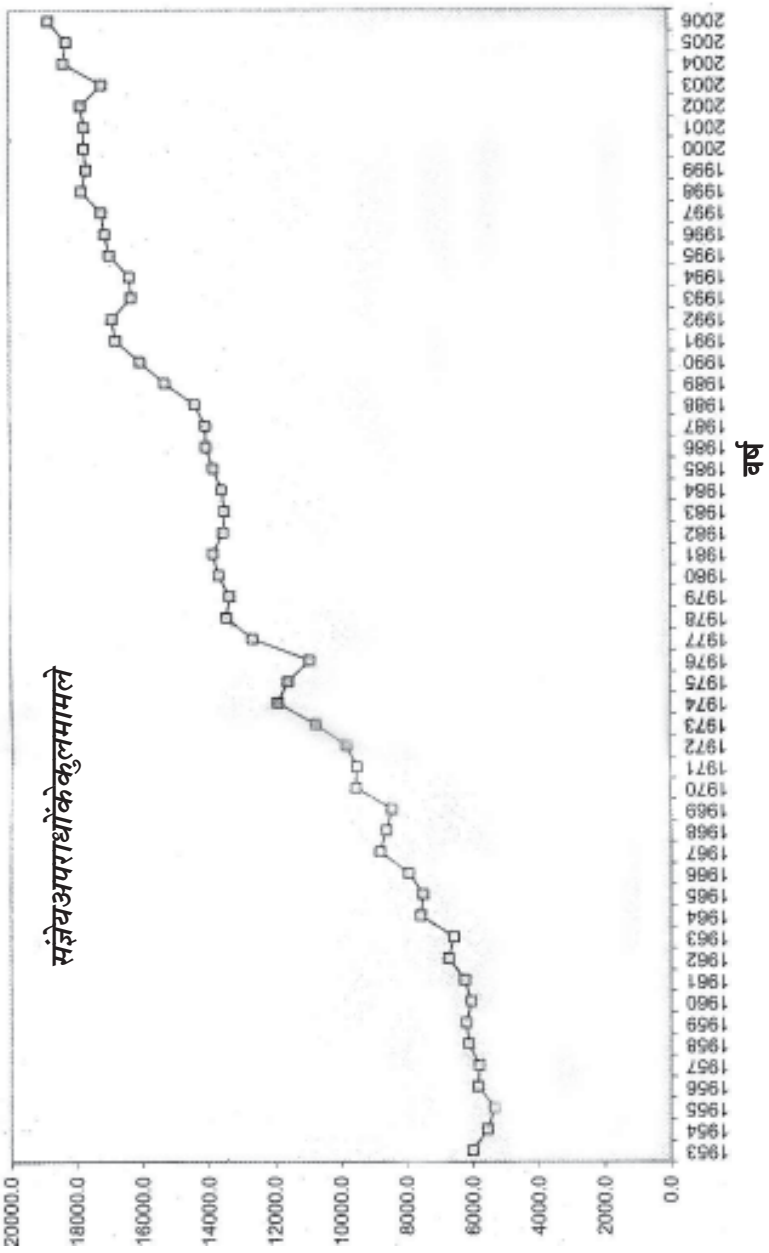
एयरलाइनों और क्रेडिट कार्ड धारकों को लगा देते हैं।

लगभग यही हाल प्लास्टिक कार्ड (डेबिट/क्रेडिट कार्ड) के द्वारा की जाने वाली चोरी धोखाधड़ी का भी है। किसी का क्रेडिट कार्ड चुरा कर बाजार से लाखों की खरीददारी करने का अपराध तो सामान्यतः होता ही है लेकिन अब तो कुछ आपराधिक मानसिकता वाले कंप्यूटर विशेषज्ञ, फर्जी क्रेडिट कार्ड (क्लोन काड) तक बना लेते हैं जिस कारण एक झटके में ही आपकी लाखों की गाढ़ी कमाई, अपराधियों की जेब में चली जाती है। इसके अलावा प्लास्टिक कार्डों के पासवर्ड को हैक करना भी एक ऐसा गंभीर अपराध है, जिसके काफी मामले अब सामने आ रहे हैं।

लगातार बढ़ते अपराध

अपराध एक ऐसी घटना है जिसका अस्तित्व प्रत्येक काल और युग में रहा है लेकिन पिछले कुछ वर्षों के दौरान अपराधों और आतंकवादी घटनाओं में बहुत तेजी से वृद्धि हुई है। समाज में कौन से अपराध, कितनी संख्या में हो रहे हैं, इसकी बहुत कुछ वास्तविक तस्वीर, राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (गृह मंत्रालय, भारत सरकार) के वार्षिक प्रकाशन, *'क्राइम इन इंडिया'* में दिए गए आंकड़ों से प्राप्त की जा सकती है। नई दिल्ली स्थित राष्ट्रीय अपराध रिकार्ड ब्यूरो द्वारा समूचे भारतवर्ष के सभी राज्यों और केंद्रशासित प्रदेशों से अपराध संबंधी आंकड़े इकट्ठे किए जाते हैं और फिर उन्हें *'क्राइम इन इंडिया'* के रूप में प्रकाशित किया जाता है। *'क्राइम इन इंडिया'* में दिए गए आंकड़ों को भारत सरकार के अधिकृत व प्रमाणिक आंकड़े माना जाता है।

'क्राइम इन इंडिया-2006' के मुताबिक सन् 2006 के दौरान देशभर में भारतीय दंड संहिता के अंतर्गत कुल 18,78,293 मामले विभिन्न थानों में दर्ज किए गए जबकि विशेष एवं स्थानीय कानूनों *(एस.एल.एल.)* के तहत कुल 32,24,167 मामले पंजीकृत किए गए। इस प्रकार भारतवर्ष में कुल 51,02,460 मामले सन् 2006 के दौरान दर्ज किए गए जबकि सन् 2005 के दौरान कुल 50,26,337 मामले ही प्रकाश में आए थे। इस प्रकार सन् 2005 के मुकाबले सन् 2006 में अपराधों की कुल संख्या में लगभग 1.5 फीसदी की बढ़ोत्तरी दर्ज की गई। भारतीय दंड संहिता के अंतर्गत वर्षभर में सबसे अधिक मामले मध्य


संज्ञेयअपराधोंकेकुलमामले
20000.0
18000.0
16000.0
14000.0
12000.0
10000.0
8000.0
6000.0
4000.0
2000.0
0.0
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
वर्ष
आपराधिक घटनाएं

प्रदेश में दर्ज किए गए। यहां देशभर में घटित कुल अपराधों के लगभग 10. 4 प्रतिशत मामले दर्ज किए गए। 10.2 प्रतिशत मामलों के साथ महाराष्ट्र दूसरे स्थान पर और 9.3 फीसदी मामलों के साथ आंध्र प्रदेश तीसरे स्थान पर रहा।

वर्ष 2006 के दौरान सबसे अधिक अपराध दर (444.7) पांडिचेरी में दर्ज की गई जो राष्ट्रीय अपराध दर (167.7) के मुकाबले 2.7 गुना अधिक थी। भारत के सबसे अधिक साक्षरता-दर वाले राज्य केरल में अपराध-दर भी सर्वाधिक (राज्यों में) थी। यहां की अपराध-दर 312.5 दर्ज की गई। इस तथ्य से पता चलता है कि आजकल शिक्षित लोग भी अपराध की स्याह दुनिया में खूब कदम रख रहे हैं। विभिन्न महानगरों में सबसे अधिक अपराध दिल्ली (16. 2 प्रतिशत), मुम्बई (9.5 प्रतिशत) और बंगलुरु (8.1 प्रतिशत) में दर्ज किए गए। महानगरों में सबसे अधिक अपराध-दर इंदौर में दर्ज की गई। इंदौर की अपराध-दर 769.1 थी जबकि 719.5 की अपराध-दर के साथ भोपाल दूसरे स्थान पर और 597.1 की अपराध-दर के साथ जयपुर तीसरे स्थान पर रहा।

वर्ष	*भा.द.सं. के कुल अपराध*	*हत्या*	*बला-त्कार*	*अपराध*	*डकैती*	*लूट*	*चोरी*	*दंगे*
1953	6,01,964	9,802	2,487	5,261	5,579	8,407	1,47,379	20,529
2006	18,78,293	32,481	19,348	23,991	4,747	18,456	91,666	56,641
1953 के मु-काबले 2006 में % अंतर	212.0	231.0	678.0	350.0	150	120.0	380	176.0

स्रोत : 'क्राइम इन इंडिया'

तालिका : सन् 1953-2006 के दौरान अपराधों की प्रवृत्ति

सन् 2006 के दौरान भारतीय दंड संहिता की विभिन्न धाराओं के अंतर्गत कुल 26,53,683 व्यक्तियों को गिरफ्तार किया गया जबकि इसी अवधि के दौरान कुल 35,54,222 व्यक्तियों को विशेष अधिनियमों के तहत गिरफ्तार किया गया। कुल गिरफ्तार व्यक्तियों में से 44.6 प्रतिशत गिरफ्तार व्यक्ति, 18-30 वर्ष के आयु वर्ग के थे, जिससे पता चलता है कि अब युवा और किशोर लोग, अपराध की दुनिया में तेजी से कदम रख रहे हैं। यहां यह बताना प्रासंगिक रहेगा कि किशोर व युवा अपराधी, आपराधिक घटनाओं को अंजाम देने में तकनीक एवं प्रौद्योगिकी का जमकर इस्तेमाल करते हैं।

हालांकि आजकल अपराधी लगभग सभी तरह के अपराधों में तकनीक एवं प्रौद्योगिकी का इस्तेमाल करते हैं लेकिन साइबर-अपराध तो विशुद्ध रूप से तकनीक एव प्रौद्योगिकी आधारित ही होते हैं। पिछले कुछ वर्षों के दौरान देशभर में साइबर अपराध भी काफी तेजी से बढ़े हैं। सूचना-प्रौद्योगिकी अधिनियम एवं भारतीय दंड संहिता की विभिन्न धाराओं के अंतर्गत सन् 2005 में कुल 481 साइबर अपराध के मामले दर्ज किए गए थे जबकि सन् 2006 के दौरान देशभर के थानों में साइबर अपराध के कुल 453 मामले पंजीकृत किए गए। साइबर अपराधों को अंजाम देने वाले कुल अपराधियों में से 70 फीसदी से भी अधिक अपराधी, 18-30 वर्ष के आयु वर्ग के थे। इस तथ्य से पता चलता है कि तकनीक आधारित साइबर अपराधों को अधिकतर युवा अपराधियों द्वारा ही अंजाम दिया जाता है।

स्पष्ट है कि चूंकि विज्ञान आज जीवन के प्रत्येक क्षेत्र में अपनी उपस्थिति दर्ज करा रहा है इसलिए अपराधियों द्वारा भी आज अपराध को अंजाम देने में अत्याधुनिक तकनीकों का खूब इस्तेमाल किया जा रहा है। अपराधियों द्वारा आमतौर पर मोबाइल फोन, इंटरनेट, कंप्यूटर और रात में देखने वाले उपकरणों का अधिक इस्तेमाल किया जाता है। तकनीक और प्रौद्योगिकी से आतंकवादी और अपराधी इस कदर लैस हो चुके हैं कि वे अब किसी राष्ट्र की महत्त्वपूर्ण वेबसाइटों को हैक करने लगे हैं और आतंक फैलाने के लिए जैविक-हथियारों तक का प्रयोग करने लगे हैं। आधुनिक तकनीक से लैस अपराधियों के मंसूबों को ध्वस्त करने के लिए पुलिस तथा अन्य सुरक्षा एजेंसियों द्वारा प्रौद्योगिकी का इस्तेमाल आज वक्त की जरूरत है, समय की मांग है।

●

2

अपराध निरोध में प्रौद्योगिकी का प्रयोग

हम चर्चा कर चुके हैं कि आजकल आतंकवादी और अपराधी, तकनीक एवं प्रौद्योगिकी का खूब इस्तेमाल कर रहे हैं। आधुनिक तकनीक से लैस अपराधियों के मंसूबों को ध्वस्त करने के लिए आवश्यक है कि पुलिस तथा अन्य सुरक्षा एजेंसियों द्वारा भी अत्याधुनिक प्रौद्योगिकी उपकरणों व यंत्रों का प्रयोग अपराध व अपराधियों से लड़ने के लिए किया जाना चाहिए। सौभाग्य से आज हमारी सुरक्षा एजेंसियां भी प्रौद्योगिकी का इस्तेमाल खूब करने लगी हैं और इसके सकारात्मक परिणाम भी हमारे सामने आने लगे हैं। आजकल बड़े से बड़े अपराधी, इलैक्ट्रॉनिक सर्विलांस के जरिए पकड़े जा रहे हैं तो इसका श्रेय तकनीक एवं प्रौद्योगिकी को ही दिया जा सकता है।

विधि विज्ञान के रूप में अपराध व अपराधियों की पहचान करने में तो तकनीकों का प्रयोग काफी पहले से ही किया जा रहा है लेकिन आजकल तकनीकों और प्रौद्योगिकी ने इतना विकास कर लिया है कि अब अपराध को घटित होने से पहले ही रोका जा सकता है। इलैक्ट्रॉनिक सर्विलांस, मोबाइल सर्विलांस, वीडियो सर्विलांस, मोबाइल ट्रैकर्स, बायोमैट्रिक्स और एंटी-हैकिंग उपकरण, कुछ ऐसे उपाय हैं जिनके सहारे अपराध को घटित होने से पहले ही रोका जा सकता है। क्लोज सर्किट टेलीविजन, मेटल डिटेक्टर और बम-निष्क्रिय करने की तकनीकों के कारण भी अपराधों की रोकथाम करना काफी आसान हो गया है। ऐसी ही कुछ तकनीकों के कारण अब संसद भवन जैसी इमारतों की सुरक्षा को लगभग अभेद्य बना दिया गया है। भारतीय संसद के बाद अब दिल्ली सचिवालय में भी एक हाई-फाई सुरक्षा तंत्र स्थापित किया जा रहा है

जिसके जरिए न केवल पूरी इमारत पर नजर रखी जा सकेगी अपितु वहां प्रवेश करने वालों की पहचान, उनकी आंखों की पुतलियों (आयरिश) से की जाएगी। तकनीक व प्रौद्योगिकी का इस्तेमाल किस प्रकार अपराध को घटित होने से रोक सकता है, इसकी पड़ताल करने के लिए हम भारतीय संसद की सुरक्षा व्यवस्था का उल्लेख कर सकते हैं। संसद की सुरक्षा व्यवस्था के संदर्भ में निम्नलिखित तथ्यों का उल्लेख प्रासंगिक रहेगा :

(1) संसदीय परिसर का एक-एक इंच, क्लोज सर्किट टेलीविजन की नजर में रहता है। परिसर में लगे सभी क्लोज सर्किट टेलीविजन, नियंत्रण-कक्ष में लगे मॉनीटरों से जुड़े हैं जिस कारण संसद के चप्पे-चप्पे पर सुरक्षा एजेंसियों की नजर रहती है और कहीं पर भी कोई असामान्य गतिविधि या हलचल देखते ही सुरक्षा एजेंसियों के जवान वहां पहुंच जाते हैं।

(2) संसद भवन के सभी प्रवेश द्वारों पर बायोमैट्रिक उपकरण लगाए गए हैं जो आगंतुक की आंखों की पुतलियों (आयरिश/रेटिना) के आधार पर किसी व्यक्ति की पहचान करते हैं। इस कारण कोई भी संदिग्ध व्यक्ति, भेष बदल कर भी संसद के परिसर में प्रवेश नहीं कर सकता है।

(3) संसद के सभी प्रवेश द्वारों पर धातु-खोजक (मेटल डिटेक्टर) और बारूद खोजक (एक्सप्लोसिव डिटेक्टर) लगाए गए हैं। प्रत्येक व्यक्ति को इन खोजक यंत्रों से होकर गुजरना पड़ता है जिस कारण किसी भी संदिग्ध वस्तु को भीतर ले जाना लगभग असंभव है।

(4) संसद भवन में नियमित रूप से आने वाली गाड़ियों के लिए फ्लैप बैरियर लगाए गए हैं जिस कारण केवल वही वाहन, संसदीय परिसर में प्रवेश कर सकता है, जिसे पहले से ही अधिकृत किया गया हो। वाहनों के लिए विशेष बार-कोड युक्त स्टीकर जारी किए गए हैं, ये स्टीकर इस प्रकार के हैं कि उन्हें जाली तरीके से नहीं बनाया जा सकता।

(5) संसदीय परिसर में कार्य करने वाले सरकारी अधिकारियों व कर्मचारियों की पहचान के लिए विभिन्न बायोमैट्रिक उपकरणों का प्रयोग किया

जाता है। इस विधि से केवल 3 सेकेंड में किसी व्यक्ति की ठीक पहचान स्थापित की जा सकती है। बायोमैट्रिक उपकरणों को धोखा देना लगभग असंभव है इसलिए अब संसद की सुरक्षा को भेद पाना, असंभव हो गया है।

(6) परिसर में कभी-कभी आने वाले लोगों के लिए बनने वाले प्रवेश-पत्रों में भी बार-कोड का इस्तेमाल किया जाता है जिस कारण जाली प्रवेश-पत्र बनाकर कोई भी संसदीय परिसर में प्रवेश नहीं कर सकता। इससे प्रवेश-पत्र धारक के प्रवेश और निकास का समय भी कंप्यूटर में दर्ज हो जाता है।

(7) प्रत्येक प्रवेश-द्वार पर 'बैगेज स्क्रीनिंग सिस्टम' लगाए गए हैं जिसमें बेहद संवेदनशील एक्सरे मशीनों की सहायता से आगंतुक के सामान की जांच की जाती है।

आतंकवादियों के हौसले पस्त करने के लिए भी तकनीक एवं प्रौद्योगिकी का इस्तेमाल अब दुनियाभर के बड़े देश करने लगे हैं। इस संदर्भ में दुनियाभर में नये-नये प्रयोग किए जा रहे हैं। संयुक्त राज्य अमेरिका की मियामी पुलिस, सर्वप्रथम एक चालक रहित आकाश में उड़ने वाले एक ऐसे यंत्र का प्रयोग करने जा रही है जो आसमान में रहते हुए, अपराध व आतंकवाद पर नियंत्रण स्थापित करेगा। इस उपकरण का आकार, मधुमक्खी के आकार जैसा है और इस तकनीक का आविष्कार 'होनेइवेल इंटरनेशनल एस ओ एन.एन.' ने किया है। इस उपकरण के हवा में घूमने और आकाश में स्थिर रहने हेतु इसमें इलैक्ट्रो-ऑपटिक अथवा इनफ्रारेड सेंसारेस का इस्तेमाल किया गया है। अभी तो इस उपकरण को फ्लोरिडा के आकाश में तैनात करने की योजना है ताकि फ्लोरिडा शहर में अपराधों पर नियंत्रण स्थापित किया जा सके लेकिन बाद में इस उपकरण को अरब क्षेत्रों के आकाश में भी उड़ाने की तैयारी की जा रही है ताकि आतंकवादी गतिविधियों पर पूरी तरह से निगरानी रखी जा सके। बाद में इस उपकरण का प्रयोग अमेरिकी सेना भी करेगी।

हमारे देश का लगभग प्रत्येक हिस्सा आज आतंकवाद के साए में है। आतंकवाद से लड़ने के लिए नये-नये तकनीकी आविष्कार किए जा रहे हैं। जिस देश में कुल 833 लोगों पर मात्र एक पुलिसकर्मी हो, वहां आतंकवाद की

रीढ़ मात्र तकनीक के इस्तेमाल तथा बेहतर योजनाबद्ध रणनीति से ही तोड़ी जा सकती है। इस दिशा में काफी शोध व अनुसंधान किए जा रहे हैं।

उत्तर प्रदेश की एक कम्पनी ने एक ऐसा सॉफ्टवेयर तैयार किया है जो साइबर-कैफे का इस्तेमाल करने वाले लोगों की पहचान का रिकॉर्ड रखेगा। 'जी आई बायोमैट्रिक्स' नामक लखनऊ में आधारित इस कम्पनी ने *'क्रिस' (कस्टमर रजिस्ट्रेशन एण्ड आइडेंटिफिकेशन सिस्टम)* नामक एक बेहद उपयोगी सॉफ्टवेयर तैयार किया है। इस सॉफ्टवेयर के लगने के बाद साइबर कैफे जाने वाले व्यक्ति को अपना पहचान-पत्र दिखाने के अलावा अंगूठे का निशान भी देना होगा। इसके बाद वेबकैम (कंप्यूटर से जुड़ा कैमरा) से उस व्यक्ति या ग्राहक का चित्र भी अपने आप ही खिंच जाएगा। इस प्रकार ग्राहक के पहचान-पत्र की सारी जानकारियां, उसके अंगूठे के निशान (अंगुलि चिह्न) और उसका चित्र, कंप्यूटर के डाटाबेस में दर्ज हो जाएगा। इसके बाद कभी भी यह आसानी से पता लगाया जा सकेगा कि किसने किस समय किस कंप्यूटर पर लॉग-ऑन किया। इस सॉफ्टवेयर के डाटाबेस से कोई भी छेड़खानी नहीं की जा सकती क्योंकि ग्राहक का अंगुलि चिह्न व चित्र, *'एनक्रिप्टेड फार्म'* (बाइट/आंकड़े) में बदल जाते हैं और जिन्हें परिवर्तित नहीं किया जा सकता। सॉफ्टवेयर में पुलिस एजेंसी के लिए एक अलग से सेक्शन है, जिसमें सिर्फ रिपोर्ट तैयार की जा सकेगी। मात्र एक बटन दबाते ही सारी जानकारी पुलिसकर्मी निकाल कर पता कर सकता है कि किसने और कब इंटरनेट का इस्तेमाल किया। आजकल आतंकवादी अपने सदस्यों से बात करने और बम विस्फोटों की झूठी सूचना देने के लिए इंटरनेट/साइबर कैफे का खूब इस्तेमाल करने लगे हैं। ऐसे आतंकवादियों पर नकेल कसने के लिए *'क्रिस'* नामक यह सॉफ्टवेयर निश्चित रूप से बेहद कारगर साबित होगा।

जैसे-जैसे आज विज्ञान और तकनीक के क्षेत्र में नित नये विकास हो रहे हैं, वैसे-वैसे उसका लाभ अब पुलिस तथा अन्य सुरक्षा एजेंसियों को भी मिलने लगा है। अपराधों की रोकथाम के लिए तकनीक एवं प्रौद्योगिकी का इस्तेमाल दो प्रकार से किया जाता है। पहला, पुलिस एवं अन्य सुरक्षा एजेंसियों द्वारा तकनीक एवं प्रौद्योगिकी का इस्तेमाल। उदाहरण के लिए, इलैक्ट्रॉनिक तथा मोबाइल सर्विलांस का प्रयोग आजकल पुलिस द्वारा अपराधों

की रोकथाम के लिए बहुतायत से किया जा रहा है और इसके बेहद सकारात्मक नतीजे भी सामने आ रहे हैं। दूसरा, आम नागरिकों द्वारा तकनीक एवं प्रौद्योगिकी पर आधारित ऐसे अत्याधुनिक उपकरणों का इस्तेमाल किया जाता है, जिनकी सहायता से अपराध को घटित होने से पहले ही रोका जा सकता है। कार को चोरी होने से बचाने के लिए और आवास (अपार्टमेंट्स) की सुरक्षा के लिए लगाए गए अत्याधुनिक उपकरण इसी श्रेणी में आते हैं। बैंकिंग क्षेत्र द्वारा भी बहुत सी ऐसी तकनीकों का इस्तेमाल किया जाता है जिनकी सहायता से किसी अपराध को घटित होने से पहले ही रोका जा सकता है। इस संदर्भ में हम प्लास्टिक कार्डों (डेबिट एवं क्रेडिट कार्ड) पर *मैग्नेटिक स्ट्रिप* और ग्राहक के चित्र के उपयोग के साथ-साथ इन कार्डों के इस्तेमाल के लिए जरूरी पासवर्ड, ई-पिन, टी-पिन आदि का उल्लेख कर सकते हैं।

पुलिस द्वारा प्रौद्योगिकी का इस्तेमाल

एक समय था जब पुलिस का नाम लेते ही एक कठोर, संवेदनहीन और लगभग अल्पबुद्धि व्यक्ति का चेहरा हमारी नजरों के सामने कौंध जाता था लेकिन तकनीक और प्रौद्योगिकी के इस युग में पुलिस का चेहरा भी बदल गया है। अब पुलिस भी *टेक्नो सैवी* हो गई है और वह तकनीक व प्रौद्योगिकी पर आधारित अत्याधुनिक उपकरणों व यंत्रों का प्रयोग करने लगी है। पहले पुलिस पर आरोप लगाया जाता था कि वह अपराध घटित होने के काफी देर बाद घटनास्थल पर पहुंचती है लेकिन अब पुलिस, अपराध के घटित होने से पहले ही अपराधियों तक पहुंचने लगी है और यह सब संभव हो पाया है पुलिस द्वारा तकनीक एवं प्रौद्योगिकी के इस्तेमाल के कारण।

अब लगभग हर राज्य और प्रत्येक महानगर की पुलिस के पास साइबर अपराध शाखा और सर्विलांस-शाखा जैसे विभाग हैं जिनमें प्रशिक्षित पुलिस अधिकारी व कर्मचारी, अत्याधुनिक उपकरणों के सहारे अपराधों की रोकथाम करते नजर आते हैं। पुलिस द्वारा सभी प्रमुख और संवेदनशील स्थानों पर क्लोज-सर्किट कैमरे और वीडियो कैमरे लगाए गए हैं जिनकी सहायता से पूरे क्षेत्र की हर छोटी से छोटी गतिविधि पर भी नजर रखी जाती है। पुलिस

के विशेषज्ञ इलैक्ट्रॉनिक और मोबाइल सर्विलांस के जरिए पूरे संचार-तंत्र पर पैनी नजर रखते हैं जिस कारण आतंकवादियों और अपराधियों द्वारा आपस में की गई बातचीत को भी सुनना संभव हो गया है। मोबाइल सर्विलांस के जरिए बहुत सी खतरनाक घटनाओं को होने से पहले ही रोकना संभव हो गया है। अक्सर हम मीडिया में पढ़ते और सुनते रहते हैं कि फलां शहर में फलां आतंकवादी प्रवेश कर गया है और वो फलां स्थान पर फलां तारीख को बम विस्फोट करेगा। यह सब इलैक्ट्रॉनिक सर्विलांस के कारण ही संभव हो पाया है। संदिग्ध आतंकवादियों के फोन, सुरक्षा एजेंसियां सर्विलांस पर रखती हैं जिस कारण आतंकवादियों की प्रत्येक गतिविधि का पता पुलिस या सुरक्षा एजेंसी को लग जाता है। अपराधों की रोकथाम के लिए पुलिस द्वारा निम्नलिखित तकनीक आधारित उपकरणों/तकनीकों का उपयोग सफलतापूर्वक किया जा रहा है :

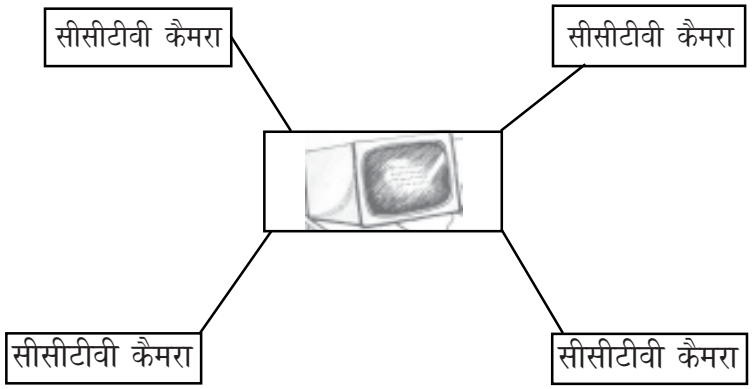
1. क्लोज-सर्किट टेलीविजन (सी.सी.टी.वी.)
2. टेलीफोन वार्तालाप सुनने वाले यंत्र (टैपिंग यंत्र)
3. जी.पी.एस. ट्रैकिंग व्यवस्था
4. डायरेक्टनल माइक्रोफोन
5. कर्वर लिस्टिंग डिवाइस
6. अंधेरे में देखने वाले उपकरण (नाइट विजन डिवाइस)
7. कंप्यूटर सर्विलांस
8. इंटरनेट सर्विलांस
9. मोबाइल सर्विलांस
10. इलैक्ट्रॉनिक डाटा पर नजर रखने वाले यंत्र (इलैक्ट्रॉनिक्स-ट्रायल्स)
11. स्वचालित वीडियो सर्विलांस तकनीक
12. धातु-खोजक यंत्र (मेटल डिटेक्टर)
13. बारूद-खोजक यंत्र (एक्सप्लोसिव डिटेक्टर)
14. अत्याधुनिक प्रशिक्षण प्राप्त खोजी कुत्ते (डॉग स्कवायड)

उपरोक्त सभी उपकरणों व तकनीकों का इस्तेमाल करने में पुलिसकर्मियों को पारंगत बनाने के लिए दुनिया के अन्य देशों के साथ-साथ हमारे देश में भी अत्याधुनिक प्रशिक्षण कार्यक्रम चलाए जा रहे हैं और कार्यशालाएं आयोजित

की जा रही हैं। तकनीक एवं प्रौद्योगिकी आधारित अत्याधुनिक उपकरणों व यंत्रों के कुशल उपयोग के लिए प्रशिक्षित पुलिसकर्मियों की जरूरत होती है। अप्रशिक्षित पुलिसकर्मियों के कारण अपराधियों के हौसले किस प्रकार बुलंद होते हैं, यह जानने के लिए हम नौएडा के आरुषि-हेमराज हत्याकांड का उल्लेख कर सकते हैं। हत्याकांड के समय दो-तीन लोगों ने घटनास्थल पर बैठकर शराब पी और फिर आरुषि अरोरा व उसके नौकर हेमराज की गला रेत कर हत्या कर दी जिससे चारों तरफ खून फैल गया। बाद में हत्यारे/हत्यारों ने घर की छत पर रखे कूलर के पानी से खून से लथपथ हाथ भी धोए। स्पष्ट है कि घटनास्थल पर बहुत सारे वैज्ञानिक प्रमाण *(साइंटिफिक एवीडेंस)* छूटे होंगे। मामले की जांच करने वाले पुलिस दल की अज्ञानता के कारण घटनास्थल से एक भी वैज्ञानिक प्रमाण नहीं मिल पाया। रही-सही कसर मीडियाकर्मियों ने पूरी कर दी और सभी सबूत पैरों तले रौंद डाले। यदि घटनास्थल पर सबसे पहले पहुंचने वाला पुलिसदल पर्याप्त प्रशिक्षित होता तो वहां से काफी वैज्ञानिक प्रमाण जुटाए जा सकते थे और उनके आधार पर वास्तविक अपराधियों तक पहुंचना काफी आसान रहता।

पुलिसद्वाराक्लोज-सर्किटटेलीविजनकाप्रयोग:अपराधों की रोकथाम के लिए पुलिस द्वारा प्रयुक्त किया जाने वाला बेहद आम उपकरण है क्लोज-सर्किट टेलीविजन। क्लोज-सर्किट टेलीविजन में कुछ वीडियो कैमरे होते हैं जो एक मॉनीटर (कंप्यूटर) से जुड़े होते हैं। इन वीडियो कैमरों द्वारा खींची गई तस्वीरों का सीधा प्रसारण उनसे जुड़े मॉनीटरों पर होता रहता है। यह मॉनीटर एक नियंत्रण-कक्ष में स्थापित होता है जहां बैठा पुलिसकर्मी पूरे क्षेत्र के चप्पे-चप्पे पर नजर रख सकता है। अपराधों की रोकथाम में क्लोज-सर्किट टेलीविजन बेहद महत्त्वपूर्ण भूमिका अदा करते हैं।

क्लोज-सर्किट टेलीविजन को हम आमतौर पर 'सी.सी.टी.वी.' के नाम से जानते और पहचानते हैं। सीसीटीवी, अन्य प्रसारण टेलीविजन से इस मायने में अलग होते हैं कि इनके द्वारा खींची गई तस्वीरों का प्रसारण न होकर, वे तस्वीरें एक निश्चित मॉनीटर तक ही जाती हैं। इसके विपरीत आम टेलीविजन प्रसारण पूरी तरह से खुला होता है और कोई भी अपने टेलीविजन उपकरण से उस प्रसारण को देख सकता है।



क्लोज-सर्किट टेलीविजन का उपयोग पुलिस तथा अन्य सुरक्षा एजेंसियों द्वारा ऐसे स्थानों पर किया जाता है, जहां आने-जाने व्यक्तियों के व्यवहार पर नजर रखना, सुरक्षा की दृष्टि से आवश्यक होता है। सुरक्षा की दृष्टि से संवेदनशील स्थानों जैसे हवाई अड्डों, बंदरगाहों, बैंक, कैसिनो, सैनिक क्षेत्र व परिसर, रेलवे स्टेशनों, बस अड्डों और अन्य भीड़-भाड़ वाले स्थानों पर क्लोज-सर्किट टेलीविजनों का प्रयोग, बहुतायत से किया जाता है। पुलिस के अलावा निजी उपयोग हेतु भी आजकल क्लोज-सर्किट टेलीविजनों का इस्तेमाल खूब किया जा रहा है। उद्योगों, फैक्टरियों, गहनों की दुकानों आदि में निजी व्यक्तियों द्वारा क्लोज-सर्किट टेलीविजनों का प्रयोग किया जाता है और यह प्रयोग भी किसी आशंकित अपराध (चोरी आदि) को रोकने के लिए ही किया जाता है।

क्लोज-सर्किट टेलीविजन की तकनीक में भी अब काफी बदलाव आ चुके हैं। अत्याधुनिक क्लोज-सर्किट टेलीविजन बेहद संवेदनशील होते हैं और ये अपने नियंत्रण वाले क्षेत्र में होने वाली छोटी से छोटी गतिविधि को भी रेकॉर्ड कर लेते हैं। सबसे पहला क्लोज-सर्किट टेलीविजन, सन् 1942 में जर्मन कम्पनी *सीमेंस* ने बनाया था और उसे जर्मनी के रॉकेट प्रक्षेपण केंद्र में लगाया गया था ताकि 'वी-2 रॉकेट' के प्रक्षेपण पर नजर रखी जा सके। इस पहले क्लोज-सर्किट टेलीविजन का डिजायन बनाने का श्रेय ख्यातिप्राप्त जर्मन अभियंता वाल्टर ब्रूक को जाता है। इसके बाद से हरेक विकसित देश, क्लोज सर्किट

टेलीविजनों का प्रयोग करने लगा। हमारे देश में क्लोज-सर्किट टेलीविजनों का इस्तेमाल न तो बहुत पुराना है और न ही हर शहर में इनका प्रयोग होता है लेकिन संयुक्त राज्य अमेरिका और इंग्लैंड जैसे विकसित देशों में सीसीटीवी का प्रयोग बहुतायत से होता है। हमारे यहां महानगरों और कुछ अन्य महत्त्वपूर्ण स्थलों पर ही क्लोज-सर्किट टेलीविजनों का प्रयोग किया जाता है।

न्यूयार्क, वाशिंगटन, मियामी, फ्लोरिडा, लंदन और म्यूनिख जैसे विदेशी शहरों में क्लोज-सर्किट टेलीविजनों का प्रयोग लगभग प्रत्येक सार्वजनिक स्थल पर किया जाता है। इन क्लोज-सर्किट टेलीविजनों से जुड़े मॉनीटरों पर पुलिसकर्मी सावधानी पूर्वक नजर गड़ाए बैठे रहते हैं। यही कारण है कि इन शहरों में आमतौर पर सार्वजनिक स्थलों पर पुलिसकर्मी दिखाई नहीं देते हैं लेकिन क्षेत्र में जरा सी भी कोई असामान्य हरकत होते ही तुरंत पुलिसकर्मी मौके पर पहुंच जाते हैं। संयुक्त राज्य अमेरिका, इंग्लैण्ड और आस्ट्रेलिया के लगभग प्रत्येक भीड़भाड़ वाले स्थान, रेलवे स्टेशन, बस अड्डे, सिनेमाघरों, कार पार्किंग स्थलों, स्कूलों, कॉलेजों और धार्मिक स्थलों में, क्लोज-सर्किट टेलीविजन स्थापित किए गए हैं जिस कारण यहां किसी भी तरह के अपराध को रोका जाना काफी आसान है और अगर फिर भी कोई अपराध घटित हो जाए तो क्लोज-सर्किट टेलीविजन की मेमोरी से रिकार्डिंग देख कर अपराधी की पहचान आसानी से की जा सकती है।

एक अनुमान के मुताबिक सन् 2002 में अकेले लंदन में निजी परिसरों में लगभग 5 लाख क्लोज-सर्किट टेलीविजन स्थापित थे जबकि पूरे इंग्लैंड में इन सीसीटीवी कैमरों की संख्या 42 लाख से भी अधिक थी। इंग्लैंड में हर 14 लोगों पर एक सर्विलांस कैमरा (सीसीटीवी) लगा है। इंग्लैंड के मुकाबले संयुक्त राज्य अमेरिका में सर्विलांस कैमरों का उपयोग कम किया जाता है क्योंकि अमेरिकी लोग इसे अपनी निजता में घुसपैठ मानते हैं। हमारे देश में भी अब क्लोज-सर्किट टेलीविजनों का प्रयोग काफी बढ़ गया है। लगभग सभी भारतीय महानगरों के प्रत्येक महत्त्वपूर्ण व संवेदनशील स्थल पर क्लोज-सर्किट टेलीविजन लगे हैं। संसद, राष्ट्रपति भवन, इंडिया गेट और चारमीनार जैसी महत्त्वपूर्ण इमारतों की सुरक्षा में भी क्लोज-सर्किट टेलीविजन का खूब इस्तेमाल किया जाता है। अब तो शो-रूमों, मॉल, फैक्टरियों, उद्योगों, रेलवे स्टेशनों, बस अड्डों

और धार्मिक स्थलों पर भी क्लोज-सर्किट टेलीविजन लगा दिए गए हैं। राजधानी दिल्ली के मुख्य चौराहों पर भी क्लोज-सर्किट टेलीविजन लगे हैं ताकि यातायात के नियमों का उल्लंघन करने वाले वाहनों की पहचान सुनिश्चित की जा सके। कुछ विदेशी शहरों की तो टैक्सियों तक में क्लोज-सर्किट टेलीविजन लगे हुए हैं ताकि चालक के खिलाफ होने वाले किसी अपराध को घटित होने से पहले ही रोका जा सके।

क्लोज-सर्किट टेलीविजन अपराधों की रोकथाम में तो कारगर भूमिका निभाते ही हैं साथ ही ये अपराध घटित हो जाने के बाद अपराधी की पहचान स्थापित करने में भी काफी महत्त्वपूर्ण होते हैं। 7 जुलाई के लंदन हमले के अंतर्गत वहां की ट्यूब ट्रेन स्टेशनों पर एक के बाद एक कई बम विस्फोट हुए इन धमाकों के आरोपियों की पहचान बाद में, वहां लगे क्लोज-सर्किट टेलीविजनों की *फुटेज* देख कर ही की गई। स्वयं हमारे देश में ही अक्सर मीडिया में खबरें आती रहती हैं कि किस प्रकार किसी गहनों की दुकान या मॉल में हुई चोरी के आरोपी की पहचान वहां लगे क्लोज-सर्किट टेलीविजन की फुटेज देख कर की गई।

क्लोज-सर्किट डिटिजल फोटोग्राफी अर्थात् 'सी.सी.डी.पी.' जैसी अत्याधुनिक तकनीक का भी विकास अब हो चुका है। इस तकनीक के अंतर्गत मेगापिक्सल डिजिटल स्थिर कैमरों के जरिए 1600 × 1200 पिक्सल आवर्धता वाले स्थिर चित्र लिए जाते हैं। ये स्थिर चित्र, परंपरागत विडियो फुटेज के मुकाबले काफी स्पष्ट होते हैं इसलिए इनका इस्तेमाल कहीं अधिक उपयोगी व कारगर रहता है। *सीसीडीपी* कैमरों से खींची गई स्थिर तस्वीरों को पलभर में संबंधित कंप्यूटर तक पहुंचा दिया जाता है जहां से चित्रों की निगरानी की जा सकती है। यदि सर्विलांस कैमरे से संबंधित कंप्यूटर किसी नेटवर्क से जुड़ा हो तो दुनिया के किसी भी हिस्से में बैठ कर एक क्षेत्र विशेष पर नजर रखी जा सकती है।

क्लोज-सर्किट टेलीविजन की तकनीक में आज काफी बदलाव आ गए हैं। प्रारंभिक सीसीटीवी, श्वेत-श्याम *(ब्लैक एण्ड व्हाइट)* तो होते ही थे साथ ही उनकी आवर्द्धता भी बेहद कम होती थी। इसके अलावा उनमें जूम (किसी वस्तु को नजदीक से देखने की सुविधा) और 'पैन' (कैमरे को घुमाने की

क्षमता) जैसी आवश्यक सुविधाएं भी नहीं होती थीं। अत्याधुनिक क्लोज-सर्किट कैमरे रंगीन विडियो चित्र खींचते हैं और ये किसी सूक्ष्म वस्तु को भी बड़े आकार में देख सकते हैं। अत्याधुनिक तकनीक के तहत क्लोज सर्किट कैमरों को 'चेहरा पहचान तंत्र' *(फेशियल रिकोगनिशन सिस्टम)* से जोड़ दिया गया है जिस कारण यदि क्लोज सर्किट कैमरे से किसी संदिग्ध व्यक्ति की तस्वीर मिलती है तो उसका मिलान तुरंत फेशियल रिकोगनिशन सिस्टम में उपलब्ध डाटाबेस से किया जा सकता है और संदिग्ध व्यक्ति की पहचान स्थापित की जा सकती है।

आजकल चर्चा है कि अन्य ग्रहों के प्राणी *(एलियंस)* यदाकदा पृथ्वी पर आते रहते हैं और वे कभी भी हमारी धरती पर हमला कर सकते हैं। एलियंस की तथाकथित उपस्थिति आमजनता के बीच तो कौतुहल का विषय है ही, साथ ही वैज्ञानिक भी एलियंस के अस्तित्व पर एक मत नहीं हैं। अक्सर मीडिया में समाचार आते रहते हैं कि फलां स्थान पर एलियंस देखे गए हैं। अभी हाल ही में इंग्लैंड के हैसडेलेन में एक क्लोज-सर्किट टेलीविजन, एलियंस की खोज के लिए ही स्थापित किया गया है। एलियंस के अलावा यह क्लोज-सर्किट कैमरा, अनजान उड़ने वाली वस्तु (यू.एफ.ओ.) पर भी नजर रखेगा। उपरोक्त चर्चा के आधार पर हम कह सकते हैं कि अपराधों की रोकथाम के कार्य में क्लोज-सर्किट टेलीविजन काफी महत्त्वपूर्ण भूमिका अदा कर सकते हैं और वस्तुतः वे ऐसा कर भी रहे हैं।

टेलीफोनटैपिंगउपकरण: तकनीक के इस युग में अपराधियों द्वारा परस्पर संपर्क में रहने के लिए टेलीफोन और मोबाइल फोन का इस्तेमाल काफी ज्यादा किया जाता है। अपराधों की रोकथाम के लिए पुलिस तथा अन्य सुरक्षा एजेंसियों द्वारा टेलीफोन टैपिंग उपकरणों का इस्तेमाल भी अब काफी होने लगा है। ये ऐसे यंत्र होते हैं जिनकी सहायता से दो व्यक्तियों के मध्य हो रही टेलीफोन वार्ता को सुना जा सकता है। अपराधियों द्वारा आपस में की जा रही बातचीत को सुन कर सुरक्षा एजेंसियां सतर्क हो जाती हैं और आशंकित अपराध को घटित होने से पहले ही रोक देती हैं।

टैपिंग एक अंग्रेजी शब्द है लेकिन यहां हम 'टैपिंग' शब्द का ही प्रयोग करेंगे क्योंकि भारत में पुलिस के साथ-साथ आम लोगों के बीच भी यही शब्द

प्रचलित हैं। टेलीफोन टैपिंग को 'वायर-टैपिंग' भी कहा जाता है और इसका अर्थ है टेलीफोन (मोबाइल फोन सहित) पर हो रही बातचीत को किसी तीसरे व्यक्ति द्वारा सुना जाना या रिकॉर्ड किया जाना। टैपिंग को यह नाम इसलिए मिला क्योंकि शुरुआती समय में जब किसी व्यक्ति की टेलीफोन वार्ता को सुना जाना होता था तो उसके टेलीफोन तारों में एक दूसरा टेलीफोन तार जोड़ दिया जाता था। इस नये तार में भी कुछ रेडियो-संकेत आ जाते थे जिस कारण उस व्यक्ति के वार्तालाप को सुना जाना संभव हो पाता था। टैपिंग शब्द का प्रयोग आमतौर पर तब किया जाता है जब दो व्यक्तियों के मध्य होने वाले वार्तालाप को अनाधिकृत (गैर-कानूनी) रूप से सुना जाता है। जब पुलिस या अन्य कोई सरकारी एजेंसी विधिक रूप से किन्हीं व्यक्तियों की बातचीत को छिप कर सुनती है तो उसे टैपिंग के स्थान पर *'इंटरसेप्शन'* कहा जाता है।

अब बात टेलीफोन टैपिंग की वैधानिक स्थिति की : दुनिया के अधिकतर देशों में टेलीफोन टैपिंग को विधिक मान्यता प्राप्त नहीं है और किसी विशेष परिस्थिति में ही पुलिस या अन्य सुरक्षा एजेंसी को किसी व्यक्ति के टेलीफोन को छिप कर सुनने (टैप) की इजाजत मिलती है। दुनिया के अधिकतर लोकतांत्रिक देशों में टेलीफोन-टैपिंग की यही वैधानिक स्थिति है। टेलीफोन टैपिंग पर यह नियंत्रण इसलिए रखा गया है ताकि किसी व्यक्ति के व्यक्तिगत जीवन और उसकी निजता (*प्राइवेसी*) में किसी बाहरी व्यक्ति की घुसपैठ न हो। सैद्धांतिक रूप से किसी व्यक्ति द्वारा टेलीफोन पर की जा रही बातचीत को सुनने के लिए न्यायालय की अनुमति लेनी चाहिए और अधिकतर देशों में ऐसा किया भी जाता है। न्यायालय जब इस तथ्य से संतुष्ट हो जाता है कि उस व्यक्ति के अपराध के प्रमाण, टेलीफोन टैपिंग से ही मिल सकते हैं अथवा कोई व्यक्ति विशेष संदिग्ध आचरण वाला है तो न्यायालय सुरक्षा/जांच एजेंसी को किसी व्यक्ति के टेलीफोन को टैप करने की अनुमति दे देते हैं। यह बात और है कि किसी देश में यह अनुमति सरलता से मिल जाती है तो कुछ देशों में टेलीफोन टैपिंग हेतु अनुमति लेने के लिए पुलिस व सुरक्षा एजेंसियों को काफी पापड़ बेलने पड़ते हैं। जर्मनी जैसे कुछेक देशों में तो गैरकानूनी रूप से किसी व्यक्ति के टेलीफोन को टैप करके उसकी बातचीत की रिकॉर्डिंग को

न्यायालय द्वारा सबूत के रूप में भी स्वीकार कर लिया जाता है।

संयुक्त राज्य अमेरिका में किसी व्यक्ति के टेलीफोन को टैप करने की अनुमति आसानी से नहीं मिलती है। संघीय एजेंसियों को टेलीफोन टैपिंग के लिए *'यूनाइटेड स्टेट्स फॉरेन इंटेलीजेंस सर्विलांस कोर्ट'* से विशेष अनुमति लेनी पड़ती है। संयुक्त राज्य अमेरिका के कुछ राज्यों के कानून के मुताबिक टेलीफोन टैपिंग की अनुमति केवल उसी परिस्थिति में मिल सकती है जब टेलीफोन वार्तालाप करने वाले दो व्यक्तियों में से कम से कम एक व्यक्ति को इस बात की जानकारी हो कि उनके वार्तालाप को किसी पुलिस एजेंसी द्वारा छिप कर सुना जाएगा। अमेरिका के कुछ राज्यों में टेलीफोन टैपिंग के द्वारा वार्तालाप को रिकॉर्ड भी किया जा सकता है जबकि कुछ दूसरे राज्यों में वार्तालाप को केवल सुना जा सकता है, उसे रिकॉर्ड नहीं किया जा सकता है। इसी प्रकार कुछ अमेरिकी राज्यों में टैपिंग द्वारा की गई रिकॉर्डिंग को न्यायालय सबूत मानते हैं तो अन्य राज्यों में ऐसे किसी भी सबूत को विधिक मान्यता प्राप्त नहीं है।

हमारे देश में भी टेलीफोन टैपिंग के मामले में वैधानिक स्थिति, अन्य लोकतांत्रिक देशों की तरह ही है। भारत में आमतौर पर टेलीफोन टैपिंग के लिए न्यायालय अनुमति नहीं देते हैं लेकिन कुछ महत्त्वपूर्ण मामलों में ऐसी अनुमति दे दी जाती है। राजधानी दिल्ली जैसे कुछ महानगरों में तो पुलिस अधिकारी को ही किसी व्यक्ति के टेलीफोन को टैप करने की अनुमति देने का अधिकार मिला हुआ है। दिल्ली में पुलिस उपायुक्त (डी.सी.पी.) स्तर का अधिकारी अपने अधीनस्थ अधिकारी या कर्मचारी को किसी व्यक्ति का टेलीफोन टैप करने की अनुमति दे सकता है। हमारे देश में राजनैतिक क्षेत्र में अनाधिकृत रूप से राजनेताओं के टेलीफोन टैप करने की खबरें मीडिया में आती रहती हैं। विपक्ष आरोप लगाता रहता है कि सरकार विभिन्न सुरक्षा एजेंसियों से उसके नेताओं के टेलीफोन टैप करवा रही है। 1990 के दशक में चन्द्रशेखर सरकार मात्र इसलिए गिर गई थी क्योंकि चन्द्रशेखर सरकार को समर्थन दे रही कांग्रेस पार्टी का आरोप था कि सरकार, उसके नेता राजीव गांधी का टेलीफोन टैप करवा रही है और खुफिया विभाग के अधिकारी, श्री राजीव गांधी की गतिविधियों की निगरानी कर रहे हैं।

स्पष्ट है कि हमारे देश में किसी व्यक्ति का टेलीफोन टैप करने के लिए प्राधिकृत अधिकारी से अनुमति लेना आवश्यक है अन्यथा टेलीफोन टैपिंग भारतीय कानून के अंतर्गत एक अपराध है। वैसे आतंकवाद और अपराध के युग में पुलिस द्वारा टेलीफोन टैपिंग को काफी प्राथमिकता दी जाती है और पुलिस एजेंसियां बिना किसी अनुमति के भी टेलीफोन टैप करती रहती हैं।

अब सवाल है कि किसी व्यक्ति के टेलीफोन को किस प्रकार टैप किया जाता है और किस प्रकार उसकी बातचीत को सुना जा सकता है। आमतौर पर टेलीफोन या मोबाइल सेवा प्रदाता कंपनी को सरकार से संचार सेवा प्रदान करने के लिए लायसेंस लेना आवश्यक होता है। विधिक रूप से लायसेंस प्राप्त कर लेने के बाद ही कोई कम्पनी अपने उपभोक्ताओं को टेलीफोन सेवा प्रदान कर सकती है। भारत सहित कुछ देशों में लायसेंस के अंतर्गत ही सरकार की यह शर्त होती है कि आवश्यक होने पर टेलीफोन सेवा प्रदाता कम्पनी को ही, सरकारी एजेंसियों और पुलिस को किसी व्यक्ति के टेलीफोन को टैप करके सुनाना होगा और जरूरत पड़ने पर वार्तालाप की रिकॉर्डिंग भी करनी होगी। संयुक्त राज्य अमेरिका में भी लगभग ऐसी ही व्यवस्था है। यही कारण है कि टेलीफोन सेवा प्रदाता कम्पनी ही टेलीफोन टैपिंग के लिए आवश्यक यंत्रों का इंतजाम करके रखती है और जैसे ही उसे प्राधिकृत एजेंसी या अधिकारी से निर्देश मिलता है, वह अपने किसी भी ग्राहक का टेलीफोन टैप कर देती है।

जब दूरभाष केन्द्र यांत्रिक होते थे तब किसी व्यक्ति के टेलीफोन को टैप करने के लिए उस व्यक्ति की टेलीफोन लाइनों में एक छोटा सा टैपिंग यंत्र जोड़ना पड़ता था लेकिन अब लगभग सभी टेलीफोन केन्द्रों का डिजिटीकरण (कंप्यूटरीकरण) हो चुका है जिस कारण टेलीफोन टैप करना अपेक्षाकृत काफी आसान हो गया है। अब कंप्यूटरीकृत टेलीफोन केन्द्र से ही उस केंद्र से संबद्ध किसी भी टेलीफोन लाइन को टैप किया जा सकता है। इसी प्रकार मोबाइल सेवा प्रदाता कंपनी के नियंत्रण कक्ष (स्विच रूम) से भी किसी भी मोबाइल ग्राहक का टेलीफोन टैप किया जा सकता है। तकनीक के इस युग में टेलीफोन सेवा प्रदान करने वाली केबल टेलीविजन कंपनियां भी डिजिटल स्विचिंग तकनीक का इस्तेमाल करती हैं जिस कारण वे भी आसानी से किसी टेलीफोन को टैप

कर सकती है। डिजिटल स्विचिंग तकनीक में बोले गए शब्द कंप्यूटर द्वारा बिट्स में परिवर्तित होते हैं और इन बिट्स को ही टेलीफोन रिसीवर तक भेजा जाता है जहां ये बिट्स पुनः ध्वनि (स्वर) में बदल जाती हैं। टेलीफोन टैपिंग की कमाण्ड (निर्देश) पाकर कंप्यूटर, वार्तालाप की बिट्स को कॉपी कर लेता है जिसे कोई तीसरा व्यक्ति सुन भी सकता है और उसकी रिकॉर्डिंग भी की जा सकती है। इस तकनीक द्वारा टेलीफोन टैप करने पर, वार्तालाप करने वाले व्यक्तियों को पता ही नहीं चलता कि उनका फोन टैप हो रहा है।

जब भी दो व्यक्ति परस्पर टेलीफोन पर वार्तालाप कर रहे होते हैं तो दोनों टेलीफोनों का पूरा डाटा, टेलीफोन सेवा प्रदाता कम्पनी के कंप्यूटर में दर्ज होता रहता है। किसी टेलीफोन से किस नंबर पर बातचीत की गई, वार्तालाप किस समय प्रारंभ हुआ, वार्तालाप किस समय समाप्त हुआ, वार्तालाप कुल कितने समय चला और उस टेलीफोन पर किन-किन नंबरों से फोन किए गए, ये सभी जानकारियां स्वतः ही कंप्यूटर में दर्ज होती रहती हैं। इस जानकारी का प्रयोग, बाद में टेलीफोन सेवा प्रदाता कम्पनी, अपने ग्राहक का बिल तैयार करने के लिए करती है। यदि वार्तालाप मोबाइल फोन से किया जा रहा हो तो मोबाइल सेवा प्रदाता कम्पनी के कंप्यूटर में यह भी दर्ज हो जाता है कि वार्तालाप के समय मोबाइल-धारक ग्राहक, भौगोलिक रूप से किस क्षेत्र में था। टेलीफोन सेवा प्रदाता कंपनी को कंप्यूटर में दर्ज ये जानकारियां भी पुलिस तथा अन्य जांच एजेंसियों के लिए बेहद उपयोगी साबित होती हैं। इन सारी जानकारियों को इकट्ठा करने के लिए *'पेन रजिस्टर'* नामक एक छोटे से उपकरण का इस्तेमाल किया जाता है और मामूली सी औपचारिकताएं पूरी करके ये जानकारियां आसानी से प्राप्त की जा सकती हैं। वार्तालाप की विषयवस्तु को छोड़ कर उपरोक्त जानकारियां प्राप्त करने को *'पैन रजिस्टर टैपिंग'* कहा जाता है। यह तो रही बात अधिकृत और वैधानिक फोन टैपिंग की। बाजार में कुछ ऐसे यंत्र भी उपलब्ध हैं जिनकी सहायता से कोई भी व्यक्ति, किसी व्यक्ति का टेलीफोन टैप कर सकता है। इसके अलावा अत्याधुनिक मोबाइल फोनों में ऐसी भी सुविधा उपलब्ध है कि आप अपने फोन से की जाने वाली अथवा आपके फोन पर आने वाली टेलीफोन कॉल को रिकॉर्ड भी कर सकते हैं। मोबाइल फोन पर अश्लील बातें करने या धमकी देने वाले

व्यक्ति की बातचीत को इस सुविधा से रिकॉर्ड किया जा सकता है। बाजार में *'कॉइल टैप'* (टेलीफोन पिकअप कॉइल) नामक एक यंत्र उपलब्ध है जिसका प्रयोग करके आप अपने फोन से की जाने वाली या उस पर आने वाली किसी भी टेलीफोन कॉल को रिकॉर्ड कर सकते हैं ताकि भविष्य में उसका उपयोग किया जा सके। आजकल बाजार में कॉल रिकार्डिंग सॉफ्टवेयर भी उपलब्ध हैं जिसके अंतर्गत किसी टेलीफोन को कंप्यूटर से जोड़ा जा सकता है और फिर उस टेलीफोन से की जाने वाली किसी भी बातचीत को कंप्यूटर में रिकॉर्ड किया जा सकता है। इसके अलावा *'बट सेट'*, *'बेजे बॉक्स'* और *'इंडेक्शन कॉइल'* ऐसे उपकरण हैं जिन्हें सीधे टेलीफोन लाइन में जोड़ना पड़ता है और फिर सारी बातचीत को कंप्यूटर या टेप रिकॉर्डर में रिकॉर्ड किया जा सकता है। इस विधि से टैपिंग करने पर रिकॉर्डिंग की गुणवत्ता कुछ खराब किस्म की आती है।

टेलीफोन टैपिंग अपराधों की रोकथाम में काफी मददगार साबित होती है। पुलिस तथा अन्य सुरक्षा एजेंसियां अक्सर संचार के लिए प्रयुक्त होने वाले रेडियो संकेतों पर नजर रखती हैं और जैसे ही उसे कोई संदिग्ध बात सुनाई देती है वह पूरी बातचीत को रिकॉर्ड कर लेती है। यही कारण है कि अक्सर पुलिस को पहले से ही पता चल जाता है कि कोई अपराधी या आतंकवादी कब और कहां किस वारदात को अंजाम देने वाला है। सुरक्षा एजेंसियों की टैपिंग के खतरे से बचाने के लिए आपराधिक गिरोह और आतंकवादी संगठन, अपने सदस्यों से टेलीफोन पर बातचीत करते समय गुप्त कूट (कोडवर्ड) का इस्तेमाल करते हैं लेकिन अपने सामान्य ज्ञान और लगातार विश्लेषण से पुलिस अधिकारी गुप्त कूट में की गई बातचीत को भी डीकोड कर लेते हैं। अभी हाल ही में मुंबई पुलिस ने कार चोरों के एक बड़े गिरोह को फोन टैपिंग की सहायता से ही पकड़ा था। ये कार चोर आपस में वार्तालाप करते समय 'कोडवर्ड' का इस्तेमाल करते थे। उदाहरण के लिए, वे सैन्ट्रो कार के लिए 'संतरा', मारुति जेन कार के लिए 'जामुन', मारुति वैन के लिए 'बनाना' आदि शब्दों का प्रयोग किया करते थे।

सुरक्षाएजेंसियोंद्वाराइंटरनेटटैपिंग:संचार क्रांति के इस युग में अपराधी और आतंकवादी संगठन अपने सदस्यों से बातचीत करने के लिए

इंटरनेट का इस्तेमाल करने लगे हैं। वे *ई-मेल* और *चैटिंग* आदि के द्वारा आवश्यक दिशा-निर्देश अपने सदस्यों को देते हैं। अल-कायदा नामक खतरनाक आतंकवादी संगठन का सरगना, ओसामा-बिन-लादेन तो अपने सदस्यों को निर्देश देने के लिए हमेशा इंटरनेट का ही प्रयोग करता है। अपराधियों और आतंकवादियों द्वारा इंटरनेट के अत्याधिक इस्तेमाल के कारण पुलिस तथा सुरक्षा एजेंसियों के लिए 'इंटरनेट टैपिंग' आज वक्त की जरूरत बन गई है ताकि दहशतगर्दों के हौसलों को पस्त किया जा सके।

इंटरनेट-टैपिंग या इंटरनेट-वायरटैप का सबसे पहले इस्तेमाल संयुक्त राज्य अमेरिका के एक विशेष एजेंट पीटर गारजा ने सन् 1996 में किया था। सुरक्षा एजेंसियों और खुफिया विभाग के अधिकारी, इंटरनेट से किए जाने वाले ई-मेलों की निगरानी करते रहते हैं और जैसे ही उन्हें कोई संदिग्ध ई-मेल मिलता है तो वे सतर्क हो जाते हैं। इंटरनेट-टैपिंग के बाद अब वेब-टैपिंग भी सुरक्षा एजेंसियों द्वारा की जाने लगी है। इंटरनेट-टैपिंग और वेब-टैपिंग में कुछ मूलभूत अंतर होते हैं। वेब-टैपिंग के अंतर्गत निश्चित वेबसाइटों तक पहुंचने वाले इंटरनेट प्रयोगकर्ता के *'आई.पी. एड्रेस'* तक पहुंचने और प्रयोगकर्ता की पहचान करने का कार्य सुरक्षा एजेंसियों द्वारा किया जाता है। वेब-टैपिंग के अंतर्गत कुछ ऐसी वेबसाइटों पर निगरानी रखी जाती है जो खतरनाक, संवेदनशील और आतंकवाद को प्रोत्साहन देने वाली उत्तेजक सामग्री का संकलन करती हैं। ऐसी वेबसाइटें आमतौर पर किसी आतंकवादी संगठन द्वारा ही संचालित की जाती हैं। जैसे ही कोई इंटरनेट प्रयोगकर्ता इस प्रकार की किसी संदिग्ध वेबसाइट तक पहुंचता है तो सुरक्षा एजेंसियां उस प्रयोगकर्ता के आई. पी. एड्रेस को खोज निकालने के कार्य को अंजाम दे देती हैं।

दुश्मन देश की गतिविधियों पर नजर रखने के लिए भी कुछ देश वेब-टैपिंग करते हैं। वैसे इसका अधिकतर प्रयोग सुरक्षा एजेंसियों द्वारा अपराधियों और आतंकवादियों के विरुद्ध ही किया जाता है। वेब-टैपिंग इस लिहाज से बेहद महत्त्वपूर्ण है कि इसके कारण असामाजिक तत्वों की संचार व्यवस्था पूरी तरह से ध्वस्त हो जाती है और वे अपने खतरनाक मंसूबों को अंजाम नहीं दे पाते हैं। भारत में भी वेब-टैपिंग का प्रचलन प्रारंभ हो चुका है और इसके द्वारा अपराधियों व आतंकवादियों पर कड़ी नजर रखी जा रही है।

अपराधोंकीरोकथामऔरइलैक्ट्रॉनिकसर्विलांसः इलैक्ट्रॉनिक सर्विलांस, अपराधों की रोकथाम की सबसे कारगर विधि है। इसके द्वारा अपराधियों द्वारा अंजाम दी जाने वाली घटना की जानकारी पहले से ही सुरक्षा एजेंसियों को मिल जाती है और वे सतर्क होकर, घटना (अपराध) को घटित होने से पहले ही रोक देते हैं। भारत में इलैक्ट्रॉनिक सर्विलांस एक नई तकनीक है लेकिन अब हमारे यहां इस तकनीक का काफी बड़े स्तर पर प्रयोग होने लगा है। इलैक्ट्रॉनिक सर्विलांस के कारण अब बेहद गंभीर किस्म के अपराधों को रोकना भी संभव हो गया है।

'सर्विलांस' फ्रेंच भाषा का शब्द है जिसका अर्थ होता है, अतिरिक्त नजर। इसे हम सरल शब्दों में निगरानी भी कह सकते हैं। हिन्दी भाषा में सर्विलांस को 'निगरानी तंत्र' नाम दिया गया है। सर्विलांस के अंतर्गत व्यक्ति के व्यवहार पर निगरानी रखी जाती है। आज हमारे देश में सभी प्रमुख पर्यटक व धार्मिक स्थलों, हवाई अड्डों, बंदरगाहों, रेलवे स्टेशनों, बस अड्डों, मेट्रो स्टेशनों, राजनीतिक व सामरिक महत्त्व की इमारतों, रक्षा परिसरों और बाजार आदि की निगरानी, क्लोज-सर्किट टेलीविजन कैमरों के जरिए की जा रही है। यह निगरानी-तंत्र (सर्विलांस सिस्टम) का ही एक भाग है।

इलैक्ट्रॉनिक सर्विलांस के अंतर्गत कुछ अत्याधुनिक इलैक्ट्रॉनिक उपकरणों के जरिए आसपास के क्षेत्र पर निगरानी की जाती है। इलैक्ट्रॉनिक सर्विलांस के लिए विभिन्न प्रकार के यंत्रों, उपकरणों आदि का प्रयोग किया जाता है और इन्हें सर्विलांस माध्यम कहा जाता है। हमारे देश में इलैक्ट्रॉनिक सर्विलांस के क्षेत्र में काफी शोध व अनुसंधान किए जा रहे हैं। अभी हाल ही में कानपुर स्थित भारतीय प्रौद्योगिकी संस्थान (आई.आई.टी.) द्वारा एक अत्याधुनिक विकसित और कारगर, स्वचालित वीडियो-निगरानी-तंत्र *(ऑटोमैटिक वीडियो सर्विलांस सिस्टम)* का विकास किया गया है जिसके जरिए संदिग्ध आतंकवादियों और अपराधियों को पकड़ने में सहायता मिलेगी। एक समझौते के तहत भारतीय प्रौद्योगिकी संस्थान (कानपुर) इस निगरानी तंत्र को मुम्बई स्थित भाभा परमाणु अनुसंधान केंद्र (बार्क) में स्थापित कर रहा है। इस सर्विलांस-तंत्र की मदद से भाभा परमाणु अनुसंधान केंद्र के परिसर में हर आने-जाने वाले व्यक्ति पर नजर रखी जा सकेगी। हमारे यहां इलैक्ट्रॉनिक सर्विलांस के माध्यम के रूप में

क्लोज-सर्किट टेलीविजन कैमरों, डारेक्शनल माइक्रोफोनों, कर्वर लिस्टिंग डिवाइस, जी.पी.एस. ट्रैकिंग उपकरणों, इलैक्ट्रॉनिक ट्रायल्स और रात के अंधेरे में भी देखने की क्षमता प्रदान करने वाले उपकरणों का खूब प्रयोग हो रहा है।

भारत में संदिग्ध लोगों और संवेदनशील स्थलों पर निगरानी रखने के लिए परंपरागत उपकरणों व विधियों जैसे सीधी निगरानी, दूरदर्शी और बाइनोक्यूलर द्वारा निगरानी और *पोस्टल-इंटरसेप्शन* आदि का प्रयोग तो काफी पहले से किया जाता रहा है लेकिन अब इन परंपरागत साधनों के साथ-साथ अत्याधुनिक कंप्यूटरीकृत निगरानी माध्यमों का भी प्रयोग किया जाने लगा है। क्लोज-सर्किट टेलीविजन कैमरों, फोन व वेबसाइट टैपिंग यंत्रों आदि के अलावा निम्नलिखित अत्याधुनिक तकनीकों/उपकरणों का इस्तेमाल भी अपराधों की रोकथाम के लिए किया जाने लगा है :

- ☆ बग्स (कवर्ट लिसनिंग डिवाइस)
- ☆ मिनोक्स सब मिनियेचर कैमरा
- ☆ बैट कार
- ☆ इलैक्ट्रॉनिक टैगिंग
- ☆ सी.सी.टी.वी. स्थिर डिजिटल चित्र
- ☆ रिकोनैसेंस एयरक्राफ्ट
- ☆ रिकोनैसेंस उपग्रह
- ☆ 'ट्रस्टेड' नामक कंप्यूटर उपकरण
- ☆ बायोमैट्रिक सर्विलांस
- ☆ इलैक्ट्रॉनिक ट्रेल्स
- ☆ काउंटर सर्विलांस
- ☆ इनवर्स सर्विलांस

मोबाइलसर्विलांसकाइस्तेमालः हमारे देश में मोबाइल फोन सेवा 1990 के दशक के अंतिम वर्षों में ही प्रारंभ हो पायी थी लेकिन देखते ही देखते मोबाइल फोन हर हाथ की शान बन चुके हैं। भारत में मोबाइल फोन सेवा की तकनीक में भी निरंतर सुधार हुआ है। पहले हमारे यहां *जी एस एम* मोबाइल फोन (एयरटेल, वोडाफोन, आइडिया, डॉल्फिन, ट्रम्प, सेलवन आदि ब्रांड नाम वाली सेवाएं) ही उपलब्ध थे लेकिन अब *सीडीएमए* तकनीक आधारित

मोबाइल फोन (रिलायंस, टाटा इंडिकॉम, गरुड़ ब्रांड नाम वाली सेवाएं) भी अस्तित्व में आ चुकी हैं।

मोबाइल क्रांति के साथ ही हमारी सुरक्षा व्यवस्था को एक बड़ा खतरा पैदा हो गया था क्योंकि अपराधी और आतंकवादी मोबाइल फोन के जरिए अपने खतरनाक मंसूबों को बेहद तेजी के साथ अंजाम देने लगे थे लेकिन मोबाइल सर्विलांस ने अब सारा खेल ही बदल दिया है। मोबाइल सर्विलांस के चलते मोबाइल फोन अपराधियों के लिए एक मुसीबत बन चुके हैं। आतंकवादियों के लिए जहां मोबाइल फोन बेहद आसान हथियार है वहीं सुरक्षा एजेंसियों के लिए यह एक वरदान की तरह साबित हो रहा है। हालांकि मोबाइल सर्विलांस के जरिए अपराधी तक पहुंचना पुलिस के लिए बेहद आसान हो गया है लेकिन यहां हम मोबाइल सर्विलांस के उस पक्ष की चर्चा करेंगे जिसके चलते अपराध को घटित होने से पहले ही रोका जा सकता है, अपराधों की रोकथाम की जा सकती है।

मोबाइल-सर्विलांस का अर्थ है किसी संदिग्ध व्यक्ति से संबंधित सूचनाएं एकत्रित करने के लिए उसके मोबाइल फोन की निगरानी करना। मोबाइल-सर्विलांस के अंतर्गत जिस मोबाइल नंबर की निगरानी की जाती है, उसके संबंध में अग्रलिखित ब्यौरा आसानी से उपलब्ध हो जाता है :

(क) कॉलडिटेलरिकॉर्ड (सीडीआर) : अर्थात् प्रयोगकर्ता ने किस नंबर पर कब और कितनी देर बात की और प्रयोगकर्ता के मोबाइल फोन पर किस-किस नंबर से कब-कब फोन आए, यह सब जानकारी कॉल-डिटेल-रिकॉर्ड के जरिए उपलब्ध हो जाती हैं।

(ख) ग्लोबलपॉजिशिनिंगसिस्टमद्वारालोकेशनकीपहचान: इस तकनीक (जी.पी.एस.) का प्रयोग करके आसानी से पता लगाया जा सकता है कि किस समय विशेष पर मोबाइल धारक किस क्षेत्र (इलाके) में था और वर्तमान में वह कहां (क्षेत्र) है।

(ग) बातचीतकाब्यौरा: मोबाइल सर्विलांस के अंतर्गत दो व्यक्तियों द्वारा आपस में की गई या की जा रही बातचीत को सुना भी जा सकता है और उस बातचीत को रिकॉर्ड भी किया जा सकता

है। किसी मोबाइल से की जा रही बातचीत को सुनने तथा उसे रिकॉर्ड करने के लिए *'लिसनिंग वॉच'* नामक प्रणाली/तकनीक का प्रयोग किया जाता है।

मोबाइल सर्विलांस कितनी महत्त्वपूर्ण तकनीक है, इसका अंदाजा इसी बात से लगाया जा सकता है कि प्रतिदिन अनेक हत्यारे, अपहरणकर्ता और लुटेरे, इस तकनीक के कारण पुलिस की गिरफ्त में आ जाते हैं। विभिन्न जांच एजेंसियों के लिए मोबाइल फोनों की 'कॉल डिटेल्स' एक अहम सबूत का कार्य कर रही है। कई हाई-प्रोफाइल आपराधिक मामलों में मोबाइल सर्विलांस के कारण ही अपराधियों पर अदालत में आरोप सिद्ध हो पाए। पत्रकार शिवानी भटनागर हत्याकाण्ड में शिवानी भटनागर के मोबाइल फोन डिटेल्स से एक ओर जहां शिवानी भटनागर और अभियुक्त आर.के. शर्मा के नजदीकी रिश्ते साबित हुए तो वहीं दूसरी ओर आर.के. शर्मा और अन्य अभियुक्तों के मोबाइल फोन के ब्यौरे से पता चला कि हत्या वाले दिन सभी अभियुक्त परस्पर संपर्क में थे। मोबाइल फोन के ब्यौरे से ही अभियोजन पक्ष ने अदालत में साबित कर दिया कि अभियुक्त आर.के. शर्मा और जयभगवान न केवल एक-दूसरे को जानते थे अपितु वे अक्सर बातचीत भी करते रहते थे। अदालत ने मोबाइल कॉल ब्यौरे को सबूत मानते हुए भारतीय पुलिस सेवा के अधिकारी रहे आर.के. शर्मा और उसके तीन साथियों को पत्रकार शिवानी भटनागर की हत्या का दोषी मानते हुए उन्हें आजीवन कारावास की सजा सुनाई।

लगभग ऐसा ही दिल्ली के पार्षद आत्माराम गुप्ता हत्याकांड में भी हुआ। मृतक आत्माराम गुप्ता के मोबाइल फोन के ब्यौरे ने साबित कर दिया कि अपनी मौत के समय वे गाजियाबाद के पास कहीं थे। उनके फोन से एक अन्य महिला पार्षद को लगातार और दिन में कई-कई बार फोन किए जाते थे इसलिए पुलिस ने उस महिला पार्षद के मोबाइल फोन का ब्यौरा निकलवाया तो पाया कि आत्माराम गुप्ता की हत्या के समय वह महिला पार्षद भी लगभग उसी स्थान पर थी जहां आत्माराम का शव पड़ा मिला था। इन सब तथ्यों के कारण अभियोजन पक्ष को परिस्थितिजन्य साक्ष्यों की कड़ियों को जोड़ने का अवसर मिला और न्यायालय ने महिला पार्षद को दोषी करार दे दिया।

हाल ही में कानपुर के भारतीय प्रौद्योगिकी संस्थान (आई॰आई॰टी॰) ने

'मोबाइल ट्रैकिंग डिवाइस' नामक तकनीक का विकास किया है जिसकी सहायता से मोबाइल धारक अपराधी या संदिग्ध व्यक्ति की स्थायी व ठीक लोकेशन प्राप्त हो सकेगी अर्थात् पुलिस पता लगा सकेगी कि मोबाइल धारक व्यक्ति/अपराधी किस क्षेत्र की किस इमारत में है। इससे पहले भी मोबाइल धारक की लोकेशन तो पता चलती थी लेकिन मात्र यह पता चल पाता था कि मोबाइल धारक, किस मोबाइल सिग्नल टॉवर के आसपास स्थित है। इस तकनीक का सफल परीक्षण किया जा चुका है और अब इसे इंटेलीजैंस ब्यूरो, रॉ, केंद्रीय अन्वेषण ब्यूरो सहित गृह मंत्रालय को मुहैया कराने की कोशिश की जा रही है।

भारत के लगभग सभी राज्यों में मोबाइल फोन सेवा प्रदान करने वाली प्रमुख कम्पनी एयरटेल ने अपने ग्राहकों के लिए *'लॉस्ट मोबाइल ट्रैकिंग सिस्टम'* नामक एक अनोखी सुविधा प्रारंभ की है। एयरटेल यह सुविधा (तकनीक) 'माइक्रो-टेक्नोलॉजी' नामक एक सॉफ्टवेयर कम्पनी के साथ मिलकर उपलब्ध करा रही है। इस सुविधा की मदद से मोबाइल फोन ग्राहक, अपने चोरी हो गए या खो गए मोबाइल फोन की लोकेशन (क्षेत्र) का तो पता लगा ही सकेंगे साथ ही यह भी आसानी से पता लगा लिया जाएगा कि वर्तमान में गुमशुदा/चोरीशुदा मोबाइल फोन पर कौन से नंबर का सिमकार्ड लगा है। इस तकनीक के अंतर्गत जब गुमशुदा/चोरीशुदा मोबाइल फोन में से उसका मूल सिमकार्ड निकाल कर उसमें कोई दूसरा सिमकार्ड डाला जाएगा तो मोबाइल फोन में लगा सॉफ्टवेयर वास्तविक उपभोक्ता (ग्राहक) को नये लगे सिम कार्ड के नंबर की जानकारी उसके ई-मेल के जरिए भेज देगा। इसके अतिरिक्त मोबाइल फोन की लोकेशन की जानकारी भी ई-मेल के द्वारा वास्तविक ग्राहक को दे दी जाएगी। इस प्रकार चोरी शुदा मोबाइल को ढूंढ़ना और चोर को पकड़ना आसान हो जाएगा।

धातुखोजक(मेटलडिटेक्टर) औरअपराधोंकीरोकथाम : अपराधों की रोकथाम में धातु-खोजक या मेटल डिटेक्टर बेहद महत्त्वपूर्ण भूमिका अदा करते हैं। मेटल डिटेक्टर से आसानी से पता चल जाता है कि किसी व्यक्ति ने अपने कपड़ों के भीतर या बैग आदि के अंदर धातु का कोई हथियार जैसे चाकू, पिस्टल, रिवाल्वर, लाइटर आदि तो नहीं छिपा रखा है।

आज लगभग सभी प्रमुख सार्वजनिक स्थलों, इमारतों में प्रवेश द्वार पर ही मेटल डिटेक्टर लगा होता है। हवाई अड्डे, रेलवे स्टेशन, शॉपिंग-मॉल, सिनेमाघरों और प्रमुख इमारतों में मेटल डिटेक्टर का इस्तेमाल आसानी से देखा जा सकता है। मेटल डिटेक्टर की सहायता से उन सभी छिपी हुई वस्तुओं का पता लगाया जा सकता है जिनमें मेटल (धातु) का प्रयोग होता है या जिनमें कुछ धातु लगी हुई हो। सवाल है कि मेटल डिटेक्टर यह कैसे पता लगा लेता है कि किसी बैग आदि के भीतर कोई धातु की वस्तु (हथियार आदि) है या नहीं?

आमतौर पर प्रयोग में लाया जाने वाला मेटल डिटेक्टर, वैद्युत-चुम्बकत्व के सिद्धांत पर काम करता है। चूंकि मेटल डिटेक्टर का इस्तेमाल अलग-अलग जगहों पर भिन्न-भिन्न वस्तुओं की खोज के लिए किया जाता है इसलिए आवश्यकता के अनुरूप इसकी संवेदनशीलता अलग-अलग बनाई जाती है। प्रत्येक मेटल डिटेक्टर में एक दोलक होता है जो अल्टरनेटिंग विद्युत धारा पैदा करता है। यह विद्युत धारा एक कुण्डली में प्रवाहित होती है जिस कारण एक चुम्बकीय क्षेत्र उत्पन्न हो जाता है। इसमें एक अन्य कुण्डली का इस्तेमाल, चुम्बकीय क्षेत्र को मापने के लिए किया जाता है। चुम्बकीय पदार्थ होने पर चुम्बकीय क्षेत्र में होने वाले परिवर्तन के आधार पर इसको मापा जाता है। प्रत्येक मेटल-डिटेक्टर में एक छोटा सा माइक्रो- प्रोसेसर भी लगा होता है जो यह पता लगाता है कि खोजी गई धातु कौन सी है अर्थात् वह लोहे या पीतल की है अथवा तांबे, स्टील आदि की है। सैद्धांतिक रूप से मेटल-डिटेक्टर का आविष्कार काफी पहले ही कर लिया गया था। उन्नीसवीं शताब्दी से ही वैज्ञानिक एक ऐसे यंत्र या उपकरण को विकसित करने का प्रयास कर रहे थे जिससे धातुओं को खोजा जा सके। प्रारंभिक दौर में धातुओं की खोज के लिए जो उपकरण बनाए गए उनकी क्षमता बेहद सीमित थी। इसके अलावा उन उपकरणों में ऊर्जा (विद्युत धारा) का खर्च भी ज्यादा होता था। यही कारण है कि प्रारंभिक धातु-खोजक यंत्र अधिक कारगर नहीं थे। भारी वजन और बड़े आकार के कारण उन्हें एक स्थान से दूसरे स्थान तक ले जाने में भी दिक्कत का सामना करना पड़ता था।

सन् 1937 में जेरार्ड फिशर नामक वैज्ञानिक ने एक ऐसे यंत्र का आविष्कार

किया जिसमें ध्यान रखा गया कि अगर रेडियो, किसी धातु की खोज में खराब हो जाए तो भी उसे फ्रीक्वेंसी के आधार पर खोजा जा सके। उन्होंने सफलतापूर्वक ऐसे यंत्र का आविष्कार कर लिया और बाद में जेरार्ड फिशर ने अपने आविष्कार का पेटेंट भी प्राप्त कर लिया। आजकल के मेटल डिटेक्टर बेहद संवेदनशील होते हैं और वे बालू, मिट्टी या लकड़ी के भीतर छिपा कर रखी गई धातु को भी खोज निकालते हैं। सुरक्षा के अतिरिक्त, पुरातत्व विज्ञान, ट्रेजर-हंटिंग और सुरक्षा संबंधी स्क्रीनिंग के लिए भी मेटल डिटेक्टर बेहद उपयोगी होते हैं। किसी आशंकित आतंकवादी कार्रवाई को रोकने में भी ये मेटल डिटेक्टर बेहद कारगर होते हैं। सिनेमाघर जैसी जगह पर आतंकवादियों द्वारा बम विस्फोट करना बेहद आसान होता है लेकिन सिनेमाघरों के प्रवेश-द्वार पर ही अब मेटल-डिटेक्टर लगा दिए गए हैं जिस कारण किसी आपत्तिजनक या खतरनाक वस्तु को सिनेमाघर के भीतर ले जाना संभव नहीं हो पाता है। ऐसा ही हवाई अड्डों, रेलवे स्टेशनों और शॉपिंग-मॉल आदि के मामले में भी होता है। दिल्ली मेट्रो रेल कार्पोरेशन के स्टेशन और मेट्रो रेल अपनी सुरक्षा के लिए प्रसिद्ध हैं। यहां की सुरक्षा व्यवस्था बेहद मजबूत किस्म की है जिस कारण कोई भी आतंकवादी गुट मेट्रो-परिसर में कोई आतंकी कार्रवाई को अंजाम देने में डरता है। प्रत्येक मेट्रो स्टेशन में प्रवेश करने पर सुरक्षाकर्मी मेटल डिटेक्टर से प्रत्येक यात्री की भलीभांति तलाशी लेते हैं जिस कारण मेट्रो स्टेशन पर खतरे की संभावना कम है।

अपराधोंकीरोकथामऔरसेलफोनजैमरः संचार क्रांति के इस दौर में सेल फोन या मोबाइल फोन हर व्यक्ति की जरूरत बन गया है। आम आदमी के बीच सेल फोन का उपयोग बढ़ा है तो आतंकवादी और अपराधी भी सेल फोन का खूब इस्तेमाल करने लगे हैं। यही कारण है कि मोबाइल फोन के कारण आज महत्त्वपूर्ण इमारतों जैसे संसद भवन, राज्य विधानसभाओं और राष्ट्रपति भवन आदि की सुरक्षा को खतरा पैदा हो गया है।

मोबाइल फोन के इस्तेमाल के कारण महत्त्वपूर्ण इमारतों की सुरक्षा व्यवस्था को पैदा हुए खतरे को रोकने के लिए आजकल सेल फोन जैमर का प्रयोग किया जाने लगा है। जब किसी स्थान पर सेल फोन जैमर स्थापित कर दिया जाता है तो उस स्थान के आसपास के सभी मोबाइल फोन काम करना

बंद कर देते हैं क्योंकि उनका नेटवर्क बाधित हो जाता है। सेल फोन जैमर एक ऐसा इलैक्ट्रॉनिक उपकरण है जो इस्तेमाल किए जा रहे सेल फोन के समान आवृत्ति के रेडियो-संकेत (सिगनल) छोड़ता है जिस कारण तरंगों का ट्रांसमिशन बंद हो जाता है फलस्वरूप मोबाइल फोन का नेटवर्क बाधित हो जाता है और मोबाइल फोन काम करना बंद कर देता है।

सेल फोन जैमर किस प्रकार काम करता है, यह जानने से पहले यह समझना आवश्यक है कि सेल फोन किस प्रकार की आवृत्तियों का इस्तेमाल करता है। जिन मोबाइल फोनों का हम आमतौर पर इस्तेमाल करते हैं वे दो अलग-अलग आवृत्तियों का इस्तेमाल करते हैं। एक आवृत्ति, बोलने वाली आवाज (ट्रांसमिशन) के लिए और दूसरी आवृत्ति, सुनने वाली आवाज (रिसीविंग) के लिए। सेल फोन से उत्पन्न संकेतों को सबसे पहले बेस स्टेशन भेजा जाता है और बेस स्टेशन से उन संकेतों को प्राप्तकर्ता के मोबाइल फोन तक भेजा जाता है। जब हम किसी स्थान पर सेल फोन जैमर का इस्तेमाल करते हैं तो जैमर भी उसी आवृत्ति के संकेत प्रेषित करता है जिस आवृत्ति के संकेत, मोबाइल फोन द्वारा बेस स्टेशन को प्रेषित किए जाते हैं। जब समान आवृत्ति के दो संकेत बेस स्टेशन तक पहुंचते हैं तो समान आवृत्ति के दोनों संकेत रद्द हो जाते हैं जिस कारण सेल फोन काम करना बंद कर देता है।

मोबाइल जैमर मुख्यत: 3 भागों में विभाजित होता है। दर्द एंटीना, मुख्य सर्किट और ऊर्जा स्रोत। मोबाइल फोन जैमर विभिन्न आवृत्ति के रेडियो संकेत छोड़ते हैं। किसी क्षेत्र विशेष में मोबाइल सेवा ठप करने की शक्ति के आधार पर जैमर अलग-अलग आकार-प्रकार के होते हैं। कुछ जैमर, सेल फोन के आकार के ही होते हैं। ये 30 से 100 फीट की दूरी तक के सभी मोबाइल फोनों को जैम (बाधित) कर देते हैं। कुछ दूसरे जैमर, ब्रीफकेस के आकार के होते हैं और ये डेढ़ से दो किलोमीटर तक के क्षेत्र में मोबाइल फोन नेटवर्क को बाधित कर देते हैं। एक सेल फोन जैमर उस क्षेत्र में काम कर रहे सभी मोबाइल नेटवर्कों को बाधित कर देता है। आजकल आतंकवादी धमकियों को देखते हुए, सुरक्षा के लिहाज से सेल फोन जैमर का प्रयोग बहुतायत से किया जाता है। भारतीय संसद, विभिन्न राज्यों की विधानसभाओं और राष्ट्रपति भवन जैसी महत्त्वपूर्ण इमारतों में मोबाइल फोन जैमर का प्रयोग किया जाता

है। ऐसा करने से उस महत्त्वपूर्ण इमारत के आसपास आतंकवादी या अपराधी आपस में संपर्क में नहीं रह पाते हैं जिस कारण किसी वारदात की उनकी योजना सफल नहीं हो पाती है।

अपराधोंकीरोकथामऔरबायोमैट्रिक्सः अपराधों की रोकथाम के लिए आजकल विभिन्न बायोमैट्रिक तकनीकों का भी खूब इस्तेमाल किया जा रहा है और ये तकनीकें काफी सफल भी हो रही हैं। सबसे पहले बात बायोमैट्रिक्स की परिभाषा की। बायोमैट्रिक्स के अंतर्गत हम व्यक्ति की जैविक विशेषताओं के आधार पर उसकी पहचान स्थापित करते हैं। इस प्रकार बायोमैट्रिक्स का प्रयोग करके हम किसी अनाधिकृत व्यक्ति को किसी महत्त्वपूर्ण स्थान, आवास आदि में प्रवेश करने से रोक सकते हैं। बायोमैट्रिक्स के अंतर्गत व्यक्ति की निम्नलिखित किसी एक जैविक विशेषता को आधार बनाया जा सकता है :

1. अंगुलि चिह्न
2. आंखों का रेटिना
3. चेहरे के कटाव
4. बालों की विशेषताएं

अंगुलि चिह्नों को बायोमैट्रिक्स का सबसे महत्त्वपूर्ण अवयव माना जाता है तो इसका कारण यह है कि दुनियाभर में यह बात वैज्ञानिक आधार पर स्थापित हो चुकी है कि किन्हीं भी दो व्यक्तियों के अथवा एक ही व्यक्ति की दो अंगुलियों के चिह्न एक समान नहीं हो सकते हैं। इसके अलावा अंगुलि चिह्नों को दुनियाभर में न्यायालयिक मान्यता भी प्राप्त है। आजकल अत्याधुनिक आवासों में प्रवेश के लिए और कार्यालय में उपस्थिति दर्ज कराने के लिए भी अंगुलि चिह्नों का प्रयोग किया जाता है। इसके अलावा महंगी कारों के दरवाजों में भी बायोमैट्रिक्स का प्रयोग करके ऐसी व्यवस्था की गई है कि कार-स्वामी के अलावा अन्य कोई व्यक्ति कार में प्रवेश नहीं कर सकता है। इस प्रकार कार को चोरी होने से बचाया जा सकता है।

अंगुलि चिह्नों के अलावा आंखों के रेटिना का प्रयोग भी व्यक्ति की पहचान स्थापित करने के लिए किया जाता है। जिस प्रकार दो व्यक्तियों के अंगुलि चिह्न एक जैसे नहीं होते हैं ठीक उसी प्रकार दो व्यक्तियों के आंखों के

रेटिना भी एक समान नहीं होते हैं। इस विधि में किसी व्यक्ति के रेटिना के चित्र को कंप्यूटर की मेमोरी में संरक्षित कर लिया जाता है और फिर जरूरत पड़ने पर वास्तविक रेटिना और पहले से रखे गए रेटिना के चित्र का मिलान करके बताया जा सकता है कि व्यक्ति वही है जिसके रेटिना के चित्र को पहले से ही संरक्षित करके रखा गया था अथवा नहीं। हमारे देश में व्यक्ति की पहचान स्थापित करने के लिए रेटिना का प्रयोग अभी बहुत कम किया जाता है लेकिन पश्चिम के विकसित देशों में इसका खूब प्रयोग होने लगा है।

चेहरापहचाननेकीतकनीकऔरआतंकवादपररोक: आज समूची दुनिया आतंकवाद के साए में जीने को अभिशप्त है। भारत के अलावा संयुक्त राज्य अमेरिका में भी आतंकवाद से लड़ने के लिए तकनीक और प्रौद्योगिकी का इस्तेमाल किया जा रहा है। अक्सर देखा गया है कि कोई खूंखार आतंकवादी भेष बदल कर एक देश से दूसरे देश तक पहुंच जाता है और सुरक्षा एजेंसियां उसे पहचान नहीं पाती हैं। इस समस्या के समाधान के लिए संयुक्त राज्य अमेरिका ने एक नई तकनीक का विकास किया है जिसके अंतर्गत आतंकवादी विशेष के चेहरे के तकनीकी चित्र को उपकरण में स्टोर कर लिया जाता है और इस उपकरण से संबंधित कैमरे हवाई अड्डे, रेलवे स्टेशन आदि पर लगा दिए जाते हैं। सैद्धांतिक रूप से, जब भी वह आतंकवादी विशेष उस कैमरे के सामने से गुजरेगा तो सुरक्षा एजेंसियों को तत्काल उसका पता चल जाएगा और उसे गिरफ्तार किया जा सकेगा।

आजकल चेहरा पहचानने की कई अत्याधुनिक तकनीकों का प्रयोग भी किया जा रहा है। ऐसा ही एक नया सिस्टम कुछ हवाई अड्डों पर परीक्षण के तौर पर लगाया गया है। इस सिस्टम के लिए सॉफ्टवेयर बनाते समय फोटो का विश्लेषण करते हुए हजारों चेहरों को 128 अलग-अलग इमेजों में तोड़ दिया जाता है। इन इमेजों को *'इंजीन फेसेज'* कहते हैं। इन्हें एक साथ मिलाकर *फेशियल फिजियोनॉमी* की एक पूरी रेंज उभर आती है और फिर सामान्य इमेज का मिलान सभी इंजीन फेसेज से किया जाता है। अब इस सिस्टम के द्वारा वास्तविक व्यक्ति और उसके टेम्पलेट का मिलान किया जा सकता है। इस सिस्टम द्वारा किसी व्यक्ति विशेष को विमान में चढ़ने से रोका जा सकता है। उदाहरण के लिए, यदि हवाई अड्डा अधिकारियों को किसी आतंकवादी

विशेष के विमान में उड़ने का अंदेशा हो तो अधिकारी, विमान में प्रवेश करने वाले यात्रियों के चेहरे का मिलान, कंप्यूटर सिस्टम में मौजूद उस आतंकवादी के इंजीन फेस से करता है। यह तकनीक अभी परीक्षण के दौर में ही है और इसमें बहुत सी दिक्कतें भी हैं। सबसे बड़ी दिक्कत तो है एक कारगर डेटाबेस बनाने की। हालांकि कुख्यात आतंकवादियों की तस्वीरें सिस्टम में डाली जा सकती हैं लेकिन केवल कुछेक आतंकवादियों की तस्वीरें ही उपलब्ध हैं। इसके अलावा डेटाबेस में आतंकवादी की तस्वीर मौजूद होने के बावजूद किन्हीं दूसरे कारणों से भी मिलान में दिक्कत आ सकती हैं। उम्र बढ़ने पर चेहरे का रूप-रंग बदल जाता है जिस कारण यह सिस्टम फेल हो सकता है। यदि कोई आतंकवादी, प्लास्टिक सर्जरी आदि के द्वारा अपना भेष बदल ले, तो भी यह तंत्र असफल हो सकता है।

तकनीककेप्रयोगसेकारचोरोंसेसुरक्षाः आज हम वैश्वीकरण और भूमंडलीकरण के दौर से गुजर रहे हैं। हमारी आर्थिक विकास-दर तेजी से बढ़ रही है जिस कारण आम लोगों की खरीदारी करने की क्षमता भी बढ़ने लगी है। यही कारण है कि भारत में यात्री कारों का उद्योग बहुत तेजी से विकास कर रहा है। एक समय था जब हमारे यहां यात्री कारों के दो ही ब्राण्ड, अम्बेसडर और फिएट उपलब्ध थे लेकिन आज सैकड़ों कार कम्पनियां अपनी कारें भारतीय बाजार में बेच रही हैं। कार आज मध्यम वर्ग की आवश्यकता बन गई है। महानगर दिल्ली में सबसे अधिक कारें हैं। महानगर दिल्ली में कारों की संख्या, अन्य तीन महानगरों मुम्बई, चेन्नई व कोलकाता में उपलब्ध कारों की कुल संख्या से भी अधिक है। हमारे यहां कारों की खरीददारी और उनका उपयोग बढ़ा है तो कार चोरी के मामले भी तेजी से बढ़े हैं।

एक समय था जब कार को चोरी हो जाने से बचाने के लिए ताले का प्रयोग किया जाता था लेकिन अब कार चोरी रोकने के लिए एक से एक आधुनिक इलैक्ट्रॉनिक उपकरण बाजार में आ गए हैं। कोई उपकरण कार को किसी संदिग्ध व्यक्ति द्वारा छूने पर तेज आवाज में सायरन बजाने लगता है तो कुछ उपकरण कार के चोरी हो जाने पर कार मालिक को *एस.एम.एस.* करके कार की वास्तविक स्थिति (लोकेशन) के बारे में बताते रहते हैं। इसके अलावा कार में प्रवेश के लिए भी एक सुरक्षा उपकरण *(एक्सेस कन्ट्रोल*

सिस्टम) लगाया जाने लगा है। यह व्यवस्था, बायोमैट्रिक विधि पर आधारित होती है। इसमें कार स्वामी के अंगूठे के निशान को उपकरण के माइक्रोप्रोसेसर में संरक्षित करके रख दिया जाता है। अब कार के दरवाजे केवल तभी खुलेंगे जब उसका स्वामी, दरवाजे के हैंडिल पर अपना 'अंगूठा' रखेगा। यह एक्सेस कन्ट्रोल सिस्टम, कार-स्वामी के अंगूठे के निशान को ही पहचानता है और कार स्वामी के अलावा अन्य किसी व्यक्ति को कार में प्रवेश नहीं करने देता है।

हाल ही में गुड़गांव पुलिस ने कार-चोरी के एक मामले को महज 5 घंटे में ही सुलझा लिया था। दरअसल चोरी गई कार में एक माइक्रो चिप लगा था। ग्लोबल पॉजिशिनिंग सिस्टम के जरिए कार का माइक्रो-चिप, कार स्वामी के मोबाइल फोन से जुड़ा था जिस कारण कार स्वामी को अपनी कार की भौगोलिक स्थिति (पोजिशन) लगातार पता चलती रहती थी। जैसे ही कार चोरी हुई, कार-स्वामी को उसके मोबाइल फोन पर संकेत मिलने लगे कि उसकी कार चोरी हो गई है। कार-स्वामी ने तुरंत कार के चोरी हो जाने की जानकारी पुलिस को दे दी। पुलिस तुरंत हरकत में आई और कार में लगे *ग्लोबल पॉजिशिनिंग सिस्टम* के आधार पर पुलिस ने कार को दिल्ली के मायापुरी इलाके से बरामद कर लिया। यह तकनीक और प्रौद्योगिकी का ही कमाल है कि अब कार-चोर, महंगी कारों को चुराने से डरने लगे हैं क्योंकि उन्हें लगता है कि कार में लगा 'सुरक्षा उपकरण' उन्हें पकड़वा देगा। कार में लगे *ग्लोबल पॉजिशिनिंग सिस्टम* के कारण टैक्सी चालकों द्वारा यात्रियों के साथ किए जाने वाले अपराधों में भी कमी आई है। आज राष्ट्रीय राजधानी दिल्ली समेत मुम्बई, बंगलुरु और हैदराबाद जैसे महानगरों में सैकड़ों रेडियो-टैक्सियां दौड़ रही हैं जिनमें 'ग्लोबल पॉजिशिनिंग सिस्टम' लगा है। टैक्सी की स्थिति (लोकेशन) का पता बताने वाले इस तंत्र के कारण टैक्सी-चालक, यात्रियों के साथ किसी प्रकार का कोई अपराध कारित करने के बारे में सोच भी नहीं पाते हैं।

तकनीक और प्रौद्योगिकी ने आज इतनी तरक्की कर ली है कि अब कारों की सुरक्षा के लिए एक से एक अभिनव उपकरण बाजार में आ गए हैं। कुछ कारों में प्रवेश केवल बायोमैट्रिक पहचान स्थापित हो जाने के बाद ही

संभव हो पाता है तो कुछ सुरक्षा-उपकरण ऐसे हैं जो किसी अनाधिकृत व्यक्ति द्वारा कार में प्रवेश करने पर कार के सभी दरवाजों को जाम कर देता है। इसके अलावा ऐसे सुरक्षा-उपकरण भी बेहद लोकप्रिय हैं जो कार के साथ की जाने वाली किसी भी छेड़छाड़ पर तेजी से अलार्म बजाने लगते हैं। इस प्रकार तकनीक व प्रौद्योगिकी ने कार चोरों के हौसलों को काफी पस्त कर दिया है।

कार चोरों को हतोत्साहित करने के लिए राष्ट्रीय अपराध रिकार्ड ब्यूरो ने भी एक शानदार तकनीकी पहल की है। अक्सर देखा गया है कि कार चोर किसी कार को चुरा कर उसके फर्जी दस्तावेज बना कर उसे किसी दूसरे राज्य में बेच दिया करते हैं। कार चोरों की इस प्रवृत्ति को रोकने के लिए राष्ट्रीय अपराध रिकार्ड ब्यूरो ने चोरीशुदा कारों का एक कंप्यूटरीकृत डाटाबेस तैयार किया है और प्रत्येक जिले की पुलिस को यह निर्देश दिया गया है कि उनके क्षेत्र में यदि कोई कार चोरी होती है तो उसकी सूचना, विस्तृत विवरण (कार पंजीकरण संख्या, इंजिन संख्या, चेसिस संख्या आदि) के साथ तुरंत राष्ट्रीय अपराध रिकार्ड ब्यूरो को दी जाए। एक ओर तो राष्ट्रीय अपराध रिकार्ड ब्यूरो ने चोरीशुदा कारों का डेटाबेस तैयार किया है तो दूसरी ओर वह प्रयुक्त (*सैकिंड हैंड*) कार खरीदने वाले ग्राहकों से अनुरोध कर रहा है कि प्रयुक्त कार खरीदने से पहले वे उस कार विशेष के आपराधिक इतिहास (यदि कोई हो) की जानकारी, ब्यूरो से प्राप्त कर लें। राष्ट्रीय राजधानी दिल्ली में तो प्रयुक्त कार के हस्तांतरण से पहले यह आवश्यक कर दिया गया है कि कार खरीदने वाला व्यक्ति, राष्ट्रीय अपराध रिकार्ड ब्यूरो से इस आशय का प्रमाण-पत्र जारी करवाए कि कार चोरी की नहीं है और उस कार का प्रयोग किसी आपराधिक कर्म में नहीं किया गया है। राष्ट्रीय अपराध रिकार्ड ब्यूरो, पूर्वी खण्ड-7, रामाकृष्णा पुरम्, नई दिल्ली के काउंटर से यह प्रमाण पत्र प्राप्त किया जा सकता है। राष्ट्रीय अपराध रिकार्ड ब्यूरो की इस पहल के कारण चोरीशुदा कारों के फर्जी ढंग से स्वामित्व परिवर्तन के काम में प्रभावी रोक लगी है।

बैंकिंगअपराधऔरतकनीकः भूमंडलीकरण और व्यावसायिकता के इस दौर में बैंकिंग क्षेत्र का अत्याधिक तेजी से विकास हुआ है। बैंकिंग

क्षेत्र का विस्तार हुआ है तो बैंकिंग अपराधों में भी खासी बढ़ोत्तरी हुई है। यहां एक सकारात्मक तथ्य यह है कि तकनीक व प्रौद्योगिकी का इस्तेमाल, बैंकिंग संबंधी अपराधों की रोकथाम में महत्त्वपूर्ण भूमिका अदा कर रहा है। बैंकिंग संबंधी अपराधों की रोकथाम में तकनीक और प्रौद्योगिकी किस प्रकार एक कारगर भूमिका अदा कर रही है, इसे हम निम्नलिखित तथ्यों से समझ सकते हैं :

(1)डी-मैटखातेकाप्रयोग: एक समय था जब शेयर बाजार में शेयरों की खरीद-फरोख्त करने वाले लोगों, दलालों आदि के मानवीकृत (भौतिक) शेयर खाते हुआ करते थे। चूंकि इन शेयर खातों का कंप्यूटरीकरण नहीं हुआ था इसलिए इन खातों के कारण कई प्रकार के फर्जीवाडे व धोखाधड़ी के मामले सामने आते रहते थे। चूंकि उस समय शेयर बाजार में तकनीक व प्रौद्योगिकी का इस्तेमाल लगभग न के बराबर होता था इसीलिए हर्षद मेहता जैसा दलाल अरबों रुपये का शेयर घोटाला करने में कामयाब रहा था।

शेयर बाजार में तकनीक व प्रौद्योगिकी के इस्तेमाल के कारण अब तस्वीर बदल चुकी है। अब सभी शेयर खातों का कंप्यूटरीकरण करके उन्हें *डी-मैट* खातों में बदल दिया गया है जिस कारण किसी भी प्रकार के फर्जीवाडे या धोखाधड़ी की आशंका बहुत कम हो गई है। प्रौद्योगिकी ने शेयर बाजार की तस्वीर ही बदल कर रख दी है।

(2)सी.बी.एस.बैंकशाखा: आजकल सभी बैंकों की शाखाओं के कंप्यूटरीकरण करने और उन्हें आपस में जोड़ने (नेटवर्किंग) का काम किया जा रहा है। पूर्णतया कंप्यूटरीकृत और संबंधित बैंक के मुख्य डाटाबेस से नेटवर्किंग के द्वारा जुड़ी शाखा को 'सी.बी.एस.' *(कोर बैंकिंग सॉल्यूशन)* शाखा कहा जाता है। इस प्रकार की शाखाओं के अस्तित्व में आ जाने के बाद बेनामी और फर्जी बैंक खातों के परिचालन पर प्रभावी रोक लगी है।

(3)प्लास्टिककार्डोंकाइस्तेमाल: वे जमाने अब लद गए जब लोगों की जेबें सिक्कों और करेंसी नोटों से भरी रहती थीं जिस कारण लूट, चोरी जैसी मामले खूब होते थे। अब जमाना प्लास्टिक-मुद्रा का है। मात्र एक प्लास्टिक के कार्ड (डेबिट या क्रेडिट कार्ड) में पूरी दुनिया समाई होती है। इन प्लास्टिक कार्डों से कहीं से भी धन की निकासी की जा सकती है और किसी

के भी बैंक खाते में धन का हस्तांतरण किया जा सकता है।

आज अगर प्लास्टिक-मुद्रा का चलन बढ़ा है तो इनसे संबंधित अपराध भी बढ़े हैं लेकिन तकनीक और प्रौद्योगिकी के इस्तेमाल के कारण डेबिट/क्रेडिट कार्ड संबंधी अपराधों पर प्रभावी अंकुश लगा लिया गया है। प्रत्येक प्लास्टिक कार्ड पर पीछे की तरफ एक *मैग्नेटिक-स्ट्रिप* लगी होती है जिसमें उपभोक्ता का पूरा विवरण दर्ज होता है जिस कारण प्लास्टिक कार्ड के दुरुपयोग की आशंका न्यूनतम हो जाती है। इसके अलावा प्लास्टिक कार्ड का उपयोग ए.टी.एम. *(ऑटोमैटिक ट्रेलर मशीन)* में करने के लिए एक 'पासवर्ड' (पी.आई.एन./पर्सनल आइडेंडिफिकेशन नंबर/ व्यक्तिगत पहचान संख्या) की आवश्यकता पड़ती है जिस कारण किसी अनाधिकृत व्यक्ति द्वारा कार्ड (डेबिट या क्रेडिट कार्ड) का प्रयोग नहीं किया जा सकता।

(4)ए.टी.एम.कक्षमेंसुरक्षाव्यवस्थाः प्लास्टिक कार्डों (डेबिट/क्रेडिट) का प्रयोग धन-निकासी के लिए 'ए.टी.एम.' (ऑटोमैटिक ट्रेलर मशीन) में किया जाता है। यदि कोई अनाधिकृत व्यक्ति किसी दूसरे के प्लास्टिक कार्ड का प्रयोग इन ए.टी.एम. कक्षों में करने की चेष्टा करें तो उसे रोकने के लिए आधुनिक प्रौद्योगिकी ने कई तकनीकें उपलब्ध करा दी हैं।

यदि कोई अनाधिकृत व्यक्ति लगातार तीन या अधिक बार गलत पासवर्ड (पिन) का प्रयोग करता है तो कंप्यूटर उस कार्ड को ब्लॉक कर देता है और अनाधिकृत व्यक्ति चोरी के कार्ड से धन-निकासी नहीं कर पाता है। इसके अलावा प्रत्येक ए.टी.एम कक्ष में क्लोज-सर्किट कैमरे लगे होते हैं जो मशीन का प्रयोग करने वाले व्यक्ति की एक-एक गतिविधि पर नजर रखते हैं। ऐसे कई मामले प्रकाश में आए हैं जिनमें ए.टी.एम. कक्ष में लगे कैमरों की फुटेज देखकर ही अपराधी की पहचान कर ली गई।

तकनीक के इस युग में कंप्यूटरों का प्रयोग बढ़ा है तो कंप्यूटर संबंधित अपराधों (साइबर अपराधों) के मामले भी प्रकाश में आने लगे हैं। विभिन्न प्रकार के साइबर अपराधों की रोकथाम के लिए तकनीक व प्रौद्योगिकी ने कई प्रकार के उपकरण व यंत्र भी हमें उपलब्ध करा दिए हैं। इसके अलावा अत्याधुनिक तकनीक से लैस साइबर-सुरक्षा विशेषज्ञों को प्रशिक्षित करने का कार्य भी किया जा रहा है। गाजियाबाद स्थित प्रबंधन प्रौद्योगिकी संस्थान

(आई.एम.टी.) ने विश्वविख्यात साइबर सुरक्षा विशेषज्ञ अंकित फाडिया के साथ मिलकर 'साइबर सुरक्षा' में एक वर्षीय स्नातकोत्तर डिप्लोमा कार्यक्रम प्रारंभ किया है। इस पाठ्यक्रम में विद्यार्थियों को इंटरनेट हैकिंग, सॉफ्टवेयर हैकिंग, मोबाइल हैकिंग और नेटवर्क हैकिंग जैसी समस्याओं से निपटने के तकनीकी गुर सिखाए जाएंगे। प्रबंधन प्रौद्योगिकी संस्थान (गाजियाबाद) के अतिरिक्त अन्य बहुत से संस्थानों में भी साइबर सुरक्षा से संबंधित पाठ्यक्रम प्रारंभ किए गए हैं। इन सब प्रयासों से विभिन्न प्रकार के साइबर अपराधों की रोकथाम में काफी मदद मिलेगी।

विभिन्न क्षेत्रों में आपराधिक कृत्य कर रहे हैकर्स आज के साइबर विश्व की सबसे बड़ी समस्या है। इन हैकर्स के कारण देश की सुरक्षा-व्यवस्था तो खतरे में पड़ती ही है साथ ही आतंकी गतिविधियों को भी प्रोत्साहन मिलता है। लेकिन अब तकनीक व प्रौद्योगिकी के सहारे *हैकर्स* को मुंहतोड़ जवाब देने की तैयारी कर ली गई है। अभी कुछ समय पूर्व ही एक वेबसाइट पर, अमेरिका, स्वीडन, चीन, इटली, जर्मनी सहित कई अन्य देशों में भारत के राजदूतों सहित 'राष्ट्रीय रक्षा अकादमी' और 'रक्षा अनुसंधान एवं विकास संगठन' (डी.आर.डी.ओ.) के कई उच्चाधिकारियों के ई-मेल अकाउंट और पासवर्ड डाल दिए गए थे। जांच के दौरान पता चला कि हैकर्स ने ई-मेल हैक कर लिया था। हैकर ने 'पोस्ट ऑफिस प्रोटोकॉल' (पी॰ओ॰पी॰) मेल सर्वर की कमियों का फायदा उठा कर ऐसा कुकृत्य किया था। यह एक गंभीर अपराध था क्योंकि हैकर्स भविष्य में राष्ट्रीय सुरक्षा से संबंधित दस्तावेजों को भी हैक कर सकते हैं। इस समस्या के समाधान के लिए भी तकनीक खोज निकाली गई है।

भारत की एक सूचना प्रौद्योगिकी प्रमाणन कम्पनी *'अप्पीन'* ने हैकर्स की समस्या से छुटकारा दिलाने के लिए 'इंटरटेक' नामक सॉफ्टवेयर कम्पनी से समझौता किया है। समझौते के मुताबिक दोनों कम्पनियां, *'एपीपीएसईसी'* नाम से 'सॉफ्टवेयर ऐप्लीकेशन सिक्युरिटी सर्टिफिकेट' प्रदान करेंगी। प्रमाणपत्र प्रदान करने से पहले 'अप्पीन' और 'इंटरटेक' मिल कर 20 मानदंडों पर सॉफ्टवेयर का परीक्षण करेंगी। इस सॉफ्टवेयर (एपीपीएसईसी) को संयुक्त राज्य अमेरिका, इंग्लैंड और आस्ट्रेलिया सहित कई यूरोपियन देशों में पहले से

ही मान्यता प्राप्त है।

हैकर्स के अलावा 'स्पैम मेल' भी इंटरनेट प्रयोगकर्ताओं के लिए एक बहुत बड़ी समस्या है। हालांकि कंप्यूटर विशेषज्ञ स्पैम मेल को फिल्टर करने के प्रयास कर रहे हैं लेकिन फिर भी स्पैम मेल एक बड़ी समस्या है। वैसे तकनीक का प्रयोग करके स्पैम मेल के खतरे से आसानी से बचा जा सकता है। कभी भी स्पैम मेल का जवाब न दें क्योंकि ऐसा करते ही आपके ई-मेल एकाउंट पर स्पैम मेल की बमबारी शुरू हो जाएगी। इसके अलावा वे दूसरे स्पैमर्स को भी आपका ई-मेल का पता बांट देंगे। स्पैमर्स से बचने के लिए जरूरी है कि किसी भी स्पैम-मेल का जवाब न दें। इसके अलावा जरूरत इस बात की भी है कि आप अपने ब्राउजर में सुरक्षा संबंधी सेटिंग को एडजस्ट करें तथा अपना नाम, पता और अन्य जानकारियां वेबसाइट पर न डालें।

उपरोक्त चर्चा से स्पष्ट है कि यदि विज्ञान ने अपराधियों और आतंकवादियों के हाथ में कुछ नये हथियार दिए हैं तो तकनीक और प्रौद्योगिकी ने सुरक्षा एजेंसियों के हाथ भी मजबूत किए हैं। अत्याधुनिक तकनीक के बल पर अपराध को घटित होने से पहले ही रोका जा सकता है। प्रौद्योगिकी ने हमें कुछ ऐसी महत्त्वपूर्ण व उपयोगी तकनीकें उपलब्ध करा दी हैं जिनकी सहायता से अपराधों की रोकथाम की जा सकती है। हमारे पास तकनीक भी हैं और उपकरण भी हैं, कमी है तो बस प्रशिक्षित पुलिसकर्मियों की और उच्च गुणवत्ता वाले प्रशिक्षण कार्यक्रमों की। प्रौद्योगिकी के बल पर अपराधों की रोकथाम बेहद सरल है, जरूरत है तो बस प्रौद्योगिकी के प्रयोग की, उसके दोहन की। ●

3

अपराध निरोध और बायोमैट्रिक्स

पहले अंगुलि चिह्नों का प्रयोग, अपराधी की पहचान स्थापित करने तक ही सीमित था लेकिन अब इनका प्रयोग, अपराधों की रोकथाम में भी किया जाने लगा है। अंगुलि चिह्न, बायोमैट्रिक्स का एक प्रमुख अवयव है। आजकल अपराधों की रोकथाम के क्षेत्र में *'बायोमैट्रिक्स'* शब्द काफी चर्चा में है। *बायोमैट्रिक्स* का अर्थ है व्यक्ति के व्यवहार अथवा उसकी कार्यिकी संबंधी जैविक विशेषताओं के आधार पर उसकी पहचान स्थापित करना। रेटिना एवं आइरिस स्कैनिंग, हथेली एवं अंगुलियों की ज्यामितीय, आवाज के प्रतिरूप, चेहरे को पहचानने के तरीके *(फेशियल रिकोगनिशन सिस्टम)* तथा अंगुलि-चिह्नों व हस्ताक्षरों को पहचानने की विधियां, *बायोमैट्रिक्स* के अंतर्गत आती हैं।

बायोमैट्रिक्सः बायोमैट्रिक्स वह विधि या तकनीक है जिसमें व्यक्ति की जैविक विशेषताओं (कार्यिकी अथवा व्यवहार संबंधी विशेषताओं) के आधार पर उसकी पहचान स्थपित की जाती है। किसी व्यक्ति के अंगुलि चिह्नों को देखकर बताया जा सकता है कि वे उस व्यक्ति-विशेष के हैं या नहीं। ठीक इसी प्रकार व्यक्ति के हस्ताक्षरों से भी उसकी पहचान स्थापित की जा सकती है। ऐसी इसलिए हो पाता है क्योंकि अंगुलि चिह्न और हस्ताक्षर, किन्हीं दो व्यक्तियों के समान नहीं हो सकते। आजकल वैज्ञानिकों ने कुछ और ऐसी जैविक विशेषताओं की पहचान कर ली है, जिनके आधार पर व्यक्ति की पहचान स्थापित की जा सकती है। बायोमैट्रिक्स के अंतर्गत निम्नलिखित विशेषताएं सम्मिलित होती हैं :

☆ अंगुलि चिह्न

☆ रेटिना स्कैनिंग
☆ आइरिस स्कैनिंग
☆ हाथों की ज्यामितिय
☆ अंगुलियों की ज्यामितिय
☆ आवाज प्रतिरूप (पैटर्न)
☆ चेहरे के कटाव
☆ हस्तलिखित हस्ताक्षर

बायोमैट्रिक्सकेअनुप्रयोगः बायोमैट्रिक्स के अंतर्गत ऐसी तकनीकें आती हैं जिनके आधार पर हम व्यक्ति की पहचान स्थापित कर सकते हैं। इस प्रकार बायोमैट्रिक्स का उपयोग आजकल विभिन्न प्रकार के अपराधों की रोकथाम में भी खूब हो रहा है। यदि हम किसी अनाधिकृत व्यक्ति को किसी स्थान विशेष में प्रवेश करने से रोक दें तो कई प्रकार के अपराधों को रोका जा सकता है। इस प्रकार बायोमैट्रिक्स का अनुप्रयोग निम्नलिखित क्षेत्रों में किया जाता है अथवा किया जा सकता है :

(1)हवाईअड्डोंकीसुरक्षामेंः आतंकवाद के इस दौर में हवाई अड्डे आतंकियों के मुख्य निशाने पर हैं लेकिन बायोमैट्रिक्स का प्रयोग करके हम इनकी सुरक्षा व्यवस्था को और पुख्ता कर सकते हैं। हवाई अड्डों के प्रवेश द्वार पर ऐसे स्कैनर लगाए जा सकते हैं जो व्यक्ति के अंगुलि चिह्नों, रेटिना या उसके चेहरे के कटाव के आधार पर उसकी पहचान स्थापित करें और केवल अधिकृत व्यक्ति को ही प्रवेश करने दें। कुछ मामलों में देखा गया है कि आतंकी या आपराधिक तत्व, किसी अन्य व्यक्ति के पासपोर्ट से छेड़छाड़ करके उसमें अपना चित्र चिपका देते हैं और फिर हवाई अड्डे की सारी सुरक्षा व्यवस्था को लांघते हुए उसके भीतर प्रवेश कर जाते हैं। यदि पासपोर्ट पर धारक का अंगुलि चिह्न भी हो और हवाई अड्डे आदि में प्रवेश करते समय पासपोर्ट पर अंकित अंगुलि चिह्न का मिलान, धारक के वास्तविक अंगुलि चिह्न से किया जाए तो संवेदनशील स्थानों पर अनाधिकृत व्यक्तियों के प्रवेश को रोका जा सकता है।

कुछ देशों में इस प्रकार के प्रयोग प्रारंभ भी हो चुके हैं और वहां प्रत्येक पासपोर्ट पर धारक का अंगुलि चिह्न भी होता है। इन देशों में हवाई अड्डों आदि में प्रवेश करते समय, बायोमैट्रिक्स के आधार पर पहले व्यक्ति की पहचान

स्थापित की जाती है और उसके बाद ही उसे प्रवेश दिया जाता है। संयुक्त राज्य अमेरिका के कुछ हवाई अड्डों पर परीक्षण के तौर पर एक ऐसी बायोमैट्रिक व्यवस्था संस्थापित की गई है जो चेहरे के कटाव से किसी व्यक्ति की पहचान करती है। इस व्यवस्था में *'इंजीन फेसेज'* तकनीक का इस्तेमाल किया जाता है।

(2)अंतर्राष्ट्रीयसीमाओंकीसुरक्षा: कुछ देश अपनी सीमाओं की रक्षा के लिए भी बायोमैट्रिक्स का प्रयोग करते हैं। हमारे देश में भी ऐसा किया जा सकता है। भारत में बांग्लादेशियों द्वारा अवैध रूप से घुसपैठ एक बड़ी समस्या है। भारत में रहकर ये बांग्लादेशी विभिन्न आतंकी व आपराधिक गतिविधियों में संलग्न रहते हैं। चूंकि ये बांग्लादेशी देखने, सुनने, व्यवहार करने आदि में हमारे सीमावर्ती राज्यों के निवासियों के समान ही हैं इसलिए इनकी पहचान करना बेहद कठिन कार्य है। लेकिन बायोमैट्रिक्स द्वारा इनकी पहचान आसानी से की जा सकती है। सीमावर्ती राज्यों के निवासियों को ऐसे पहचान-पत्र या स्मार्ट कार्ड दिए जा सकते हैं जिन पर धारक का अंगुलि चिह्न भी अंकित हो। ऐसा किए जाने पर अवैध रूप से भारत की सीमाओं में घुस आए बांग्लादेशियों की पहचान आसानी से की जा सकती है। लगभग इसी व्यवस्था का लाभ, जम्मू एवं कश्मीर राज्य में भी उठाया जा सकता है। इस विधि का अनुप्रयोग प्रारंभ भी हो चुका है और प्रत्येक भारतीय नागरिक को 'राष्ट्रीय पहचान पत्र' दिए जा रहे हैं, जिनमें बायोमैट्रिक्स का प्रयोग भी किया गया है।

(3)पासपोर्टएवंयात्रा-दस्तावेज़ोंकीसुरक्षा: किसी एक देश के नागरिक द्वारा किसी दूसरे देश में प्रवेश करने के लिए पासपोर्ट एक अहम एवं अत्यावश्यक दस्तावेज़ है। इसके बिना किसी दूसरे देश में प्रवेश नहीं किया जा सकता। फर्जी दस्तावेज़ों के सहारे किसी दूसरे देश में प्रवेश करने के मामले अक्सर प्रकाश में आते रहते हैं। बायोमैट्रिक्स के इस्तेमाल से इस प्रकार के अपराधों की रोकथाम बेहद आसान है।

कुछ भारतीय सुरक्षा एजेंसियां काफी लंबे समय से मांग कर रही हैं कि भारत सरकार द्वारा जारी किए जाने वाले पासपोर्टों पर धारक के अंगुलि चिह्न भी अंकित किए जाने चाहिएं ताकि पासपोर्टों के साथ किए जाने वाले किसी भी फर्जीवाड़े पर प्रभावी अंकुश लगाया जा सके। कुछ पश्चिमी देश ऐसा करना प्रारंभ भी कर चुके हैं। यदि पासपोर्ट पर धारक का अंगुलि चिह्न अंकित

हो तो हवाई अड्डे पर प्रवेश करते समय ही धारक की पहचान को परखा जा सकेगा। आजकल ऐसे आधुनिक उपकरण अस्तित्व में आ चुके हैं जो जीवित व्यक्ति के अंगुलि चिह्नों का मिलान, दस्तावेज़ पर अंकित अंगुलि चिह्न से कर सकते हैं। *'लाइव स्कैनर'* नामक उपकरण की सहायता से ऐसा आसानी से किया जा सकता है। *'लाइव स्कैनर'* के बारे में हम विस्तृत चर्चा, अगले पृष्ठों पर करेंगे।

(4) चोरी से बचाव: बायोमैट्रिक्स का उपयोग करके बड़ी चोरी की घटनाओं को भी आसानी से रोका जा सकता है। अक्सर ऐसे मामले सामने आते रहते हैं कि किसी व्यक्ति ने नकली चाबियां बनवा कर किसी बैंक के *स्ट्रांग-रूम* से वहां रखा सारा पैसा चुरा लिया। आजकल ऐसे ताले अस्तित्व में आ चुके हैं जो केवल स्वामी के अंगुलि चिह्नों को पहचान कर ही खुलते हैं। यदि बैंक के स्ट्रांग-रूम में बायोमैट्रिक्स आधारित ताला लगा दिया जाए तो नकली या डुप्लीकेट चाबियों की सहायता से चोरी कर पाना संभव नहीं हो पाएगा। बायोमैट्रिक्स-तालों का उपयोग निम्नलिखित स्थानों पर किया जा सकता है :

☆ बैंक के स्ट्रांग-रूम में
☆ डाकघर के नगद-कक्ष में
☆ आवास के प्रवेश-द्वार पर
☆ कार के दरवाजों में
☆ बहुमूल्य वस्तुओं के संग्रहालय में।

(5) बायोमैट्रिक्स और स्मार्ट कार्ड: किसी व्यक्ति की जैविक विशेषताओं के विवरण वाले स्मार्ट-कार्ड, विभिन्न प्रकार के अपराधों की रोकथाम कर सकते हैं। ऐसे ही स्मार्ट कार्डों का प्रयोग आजकल वाहन-चालन लायसेंसों के लिए भी किया जाता है। राष्ट्रीय राजधानी दिल्ली सहित और भी कई राज्यों में अब ऐसे स्मार्ट-कार्ड वाले ड्राइविंग लायसेंस ही जारी किए जाते हैं। इन स्मार्ट कार्डों पर अब फर्जी पहचान के जरिए ड्राइविंग लायसेंस प्राप्त करने के मामलों पर प्रभावी रोक लग गई है। जरूरत इस बात की है कि इन स्मार्ट कार्डों का प्रयोग जीवन के अन्य क्षेत्रों में भी किया जाए।

राजधानी दिल्ली में परिवहन विभाग द्वारा वाहन चालकों को जो लायसेंस जारी किए जाते हैं, उन पर धारक का अंगुलि चिह्न भी अंकित रहता है, ताकि

किसी प्रकार का कोई फर्जीवाड़ा नहीं किया जा सके।

(6)बैंकिंगमेंबायोमैट्रिक्सः बैंकिंग और वित्तीय क्षेत्र ऐसे हैं जहां व्यक्तिगत अधिकारिता काफी महत्त्व रखती है। बैंकिंग जैसे क्षेत्रों में आजकल व्यक्तिगत अधिकारिता के लिए *'पासवर्ड'* या *'पिन'* के स्थान पर बायोमैट्रिक लक्षणों का उपयोग कहीं अधिक सुविधाजनक और सुरक्षित है। चूंकि *'पासवर्ड'* या *'पिन'* का उपयोग अनाधिकृत रूप से कोई अन्य व्यक्ति भी कर सकता है इसलिए अंगुलि-चिह्न, रेटिना स्कैन आदि बायोमैट्रिक लक्षणों का प्रयोग बैंकिंग क्षेत्र में अधिक होने लगा है। व्यक्तिगत अधिकारिता (पहचान) के लिए बायोमैट्रिक्स के बढ़ते इस्तेमाल का एक प्रमुख कारण यह भी है कि इसे न तो याद रखने की जरूरत है (पासवर्ड की तरह) और न ही कोई दूसरा व्यक्ति इसका अनाधिकृत रूप से इस्तेमाल ही कर सकता है।

बायोमैट्रिक्सउपकरणः हम पढ़ चुके हैं कि बायोमैट्रिक्स के अंतर्गत किसी व्यक्ति की पहचान स्थापित करने के लिए उसके जैविक लक्षणों या विशेषताओं को आधार बनाया जाता है। बायोमैट्रिक्स नामक अत्याधुनिक तकनीक का उपयोग किन-किन क्षेत्रों में किया जा सकता है, इसकी चर्चा भी हम कर चुके हैं। बायोमैट्रिक्स का उपयोग करने के लिए बहुत से उपकरणों का प्रयोग किया जाता है। इसके लिए अंगुलि चिह्न, आइरिश स्कैन, हस्ताक्षर प्रमाणीकरण, चेहरे के कटाव और आवाज के प्रतिरूप जैसी विशेषताओं (उपकरणों) का प्रयोग किया जाता है।

अंगुलिचिह्नपहचानः बायोमैट्रिक्स की विभिन्न तकनीकों में अंगुलि चिह्न सबसे लोकप्रिय हैं। अधिकतर बायोमैट्रिक तकनीकों में अंगुलि चिह्नों का इस्तेमाल ही किया जाता है तो इसके पीछे निम्नलिखित कारण हैं :

1. अंगुलि चिह्न बेहद सरल एवं सुविधाजनक होते हैं
2. अपेक्षाकृत काफी सस्ता होता है अंगुलि चिह्नों का मिलान
3. अंगुलि चिह्नों को विश्व भर में विधिक मान्यता प्राप्त है
4. अंगुलि चिह्न उपयोग में अत्याधिक सुविधाजनक होते हैं

बायोमैट्रिक्स में अंगुलि चिह्नों का इस्तेमाल करने के लिए 'एकल चिह्न स्कैनर' का प्रयोग किया जाता है। बायोमैट्रिक्स में सभी दस अंगुलियों के चिह्न लेने की आवश्यकता नहीं है। आमतौर पर अंगूठे या तर्जनी अंगुलि को स्कैन

करके उसे डाटाबेस में स्टोर करके रख लिया जाता है। जब कोई ऐसा व्यक्ति, जिसका अंगुलि चिह्न पहले से ही डाटाबेस में है, किसी स्थान तक पहुंचने का प्रयास करता है अथवा किसी कंप्यूटर-तंत्र तक पहुंचने की कोशिश करता है तो सबसे पहले उसे अपनी अंगुलि एक उच्च-आवर्धता वाले स्कैनर पर रखनी होती है। स्कैनर उस व्यक्ति की अंगुलियों की डिजीकृत छवि उतार लेता है। अब कंप्यूटर, इस डिजीकृत छवि का मिलान, डाटाबेस में रखे अंगुलि चिह्न से करता है। यदि दोनों चिह्न, एक ही व्यक्ति से संबंधित होते हैं तो बायोमैट्रिक-तंत्र उस व्यक्ति को आगे बढ़ने की अनुमति दे देता है अन्यथा नहीं। इस प्रकार एक अधिकृत व्यक्ति ही किसी स्थान विशेष में प्रवेश कर सकता है अथवा किसी कंप्यूटर-तंत्र तक पहुंच सकता है। आजकल अंगुलि चिह्न बायोमैट्रिक्स का प्रयोग आवास की सुरक्षा, कार की सुरक्षा और महत्त्वपूर्ण इलैक्ट्रॉनिक डाटा तक किसी व्यक्ति को पहुंचने की अनुमति आदि देने के लिए किया जाता है।

आइरिससेपहचानः आंख के उस गोल भाग को आइरिस कहते हैं जो आमतौर पर काला या ब्राउन होता है और पुतलियों से सुरक्षित रहता है। आइरिस पर एक विशेष प्रकार का प्रतिरूप (पैटर्न) बना होता है। जिस प्रकार दो व्यक्तियों के अंगुलि चिह्न एक समान नहीं हो सकते, ठीक उसी प्रकार दो व्यक्तियों की आंखों के आइरिस भी एक-समान नहीं होते हैं। प्रत्येक व्यक्ति का आइरिस एक विशिष्ट प्रकार का होता है इसलिए आइरिस के आधार पर भी किसी व्यक्ति की व्यक्तिगत पहचान स्थापित की जा सकती है।

आइरिस बायोमैट्रिक्स में सबसे पहले व्यक्ति की आंखों का एक चित्र लिया जाता है। चित्र लेते समय कैमरे को आंखों के बेहद नजदीक रखा जाता है और चित्र लेते समय इंफ्रारेड प्रकाश का प्रयोग किया जाता है ताकि आंखों की छोटी से छोटी विशेषताएं भी चमकने लगें। इस प्रकार एक उच्च आवर्धन *(रिजोल्यूशन)* वाला आंखों का चित्र तैयार हो जाता है। इस प्रकार का आइरिस का चित्र खींचने में मात्र दो से तीन सेकेंड का समय ही लगता है। इस प्रकार के चित्र से आइरिस का जो विवरण प्राप्त होता है उससे आइरिस का एक मानचित्र तैयार कर लिया जाता है जिसमें आइरिस की सभी विशेषताएं उपस्थित रहती हैं।

आइरिस का विशिष्ट प्रतिरूप उसी समय आकार ले लेता है जब शिशु

मां के गर्भ में ही होता है। इस प्रकार आइरिस की विशिष्टताएं, जन्म से पहले ही निर्धारित हो जाती हैं। आइरिस की विशिष्टताएं व्यक्ति के पूरे जीवनभर एक समान ही रहती हैं और उनमें मृत्युपर्यंत कोई बदलाव नहीं आता है। केवल किसी दुर्घटना आदि के कारण ही आइरिस की विशिष्टताएं परिवर्तित हो सकती हैं। आइरिस का प्रतिरूप (पैटर्न) बेहद जटिल प्रकार का होता है और इसमें लगभग 200 अद्वितीय प्रकार के चिह्न होते हैं जिनके आधार पर आइरिस को एक विशिष्टता प्राप्त होती है। प्रत्येक व्यक्ति की दायीं और बायीं आंखों के आइरिस भी अलग-अलग प्रतिरूप वाले होते हैं अर्थात् एक ही व्यक्ति के दोनों आइरिस भी समान नहीं होते हैं।

आइरिस की अद्वितीयता के आधार पर ही व्यक्ति की पहचान की जाती है। आइरिस के आधार पर व्यक्ति की पहचान करने में गलती होने की आशंका लगभग न के बराबर होती है। विभिन्न शोधों से यह प्रमाणित हो गया है कि 1.2 मिलियन में से मात्र एक मामले में ही आइरिस स्कैनर व मैचर गलती कर सकता है। सन् 1997 से ही इंग्लैण्ड, संयुक्त राज्य अमेरिका, जापान और जर्मनी में *'ऑटोमैटिक ट्रेलर मशीन'* (ए.टी.एम.) में आइरिस बायोमैट्रिक्स का इस्तेमाल किया जा रहा है ताकि कोई अनाधिकृत व्यक्ति, एटीएम का परिचालन न कर सके। भारत में भी अब इस अत्याधुनिक तकनीक का इस्तेमाल किया जाने लगा है। दिल्ली स्थित तिहाड़ जेल में हाल ही में आइरिस और स्कैन तकनीक का इस्तेमाल, कैदियों की पहचान के लिए किया जाने लगा है।

अधिकृतहस्ताक्षरः किसी व्यक्ति की पहचान स्थापित करने के लिए हस्ताक्षर, बेहद सुगम और सरल साधन हैं और इसीलिए दुनियाभर में हस्तलिखित हस्ताक्षरों का प्रयोग विभिन्न बैंकिंग, विधिक और अन्य कामों के लिए किया जाता है। किसी व्यक्ति के दो हस्ताक्षरों का मिलान करने के लिए हस्ताक्षर की विभिन्न विशिष्टताओं को ध्यान में रखा जाता है। आधुनिक प्रौद्योगिकी ने ऐसी तकनीकें प्रस्तुत कर दी हैं कि किन्हीं दो हस्ताक्षरों का क्षणभर में ही मिलान किया जा सकता है। हस्ताक्षरों का मिलान करने वाले इस अत्याधुनिक उपकरण को 'डी.एस.वी.टी.' *(डायनामिक सिग्नेचर वैरीफिकेशन टेक्नोलॉजी)* का नाम दिया गया है।

हालांकि साधारण हस्ताक्षर मिलान विधियां और *'डायनामिक सिग्नेचर*

वैरीफिकेशन टेक्नोलॉजी' दोनों को कंप्यूटरीकृत किया जा सकता है लेकिन दोनों में एक मूलभूत अंतर भी होता है। साधारण हस्ताक्षर मिलान विधियों में यह देखा जाता है कि हस्ताक्षर दिखने में कैसे हैं और उनमें क्या अंतर हैं। इसके विपरीत *'डायनामिक सिग्नेचर वैरीफिकेशन टेक्नोलॉजी'* में यह देखा जाता है कि हस्ताक्षर किस प्रकार बनाए गए हैं। इस अत्याधुनिक तकनीक में मिलाए जाने वाले हस्तक्षरों के संदर्भ में अग्रलिखित पक्षों का अध्ययन किया जाता है :

- ☆ हस्ताक्षर लेखन की गति में परिवर्तन
- ☆ हस्ताक्षर लेखन के समय कागज पर लगाया गया दबाव
- ☆ हस्ताक्षर करने में लगा कुल समय

'डायनामिक सिग्नेचर वैरीफिकेशन टेक्नोलॉजी' एक प्राकृतिक और मौलिक प्रकार की तकनीक है जिसमें विज्ञान और प्रौद्योगिकी का इस्तेमाल भी किया जाता है। यह तकनीक बेहद आसान है और इस पर विश्वास किया जा सकता है। आजकल इस तकनीक का इस्तेमाल काफी अधिक किया जा रहा है जिस कारण फर्जी हस्ताक्षरों के कारण होने वाले फर्जीवाड़ों की रोकथाम करना काफी सरल हो गया है।

चेहरापहचानतंत्र(फेशियलरिकोगनिशनसिस्टम): आजकल कई ऐसे कंप्यूटरीकृत तंत्र अस्तित्व में आ चुके हैं जो कंप्यूटर प्रोग्राम के द्वारा मानवीय चेहरों के चित्रों का विश्लेषण करते हैं ताकि संबंधित व्यक्तियों को पहचाना जा सके। यह कंप्यूटर प्रोग्राम, सबसे पहले किसी चेहरे के चित्र को लेता है और फिर चेहरे की विभिन्न विशेषताओं (जैसे आंखों के बीच की दूरी, नाक की लंबाई, जबड़े का कोण और ठोडी की बनावट आदि) का विश्लेषण करता है और फिर एक अद्वितीय कंप्यूटर फाइल बनाता है जिसे 'टेम्पलेट' कहते हैं। इसके बाद कंप्यूटर सॉफ्टवेयर (प्रोग्राम) दूसरे चेहरों के भी टेम्पलेट तैयार करता है और फिर इन टेम्पलेटों का परस्पर मिलान करके बताता है कि दो चेहरे किस प्रकार एक-दूसरे से समान हैं। इस तंत्र के लिए चेहरे के चित्रों का प्राथमिक स्रोत, वीडियो कैसेट्स में उपलब्ध चित्र और ड्राइविंग लायसेंस व पहचान-पत्रों पर लगे व्यक्ति के चित्र हो सकते हैं।

अन्य बायोमैट्रिक्स तकनीकों के विपरीत 'फेशियल रिकोगनिशन टेक्नॉलॉजी' का प्रयोग साधारण सर्विलांस के लिए सार्वजनिक स्थलों पर भी किया जा

सकता है। यदि चेहरा पहचानने के इस तंत्र को सार्वजनिक वीडियो कैमरों (क्लोज सर्किट कैमरे) से जोड़ दिया जाए तो किसी व्यक्ति विशेष (कोई खूंखार अपराधी या आतंकवादी) को भारी भीड़ के बीच से भी पहचानना संभव हो जाएगा।

आजकल चेहरा पहचानने की कई अत्याधुनिक तकनीकों का प्रयोग भी किया जा रहा है। ऐसा ही एक नया सिस्टम कुछ हवाई अड्डों पर परीक्षण के तौर पर लगाया गया है। इस सिस्टम के लिए सॉफ्टवेयर बनाते समय फोटो का विश्लेषण करते हुए हजारों चेहरों को 128 अलग-अलग इमेजों में तोड़ दिया जाता है। इन इमेजों को 'इंजीन फेसेज' कहते हैं। इन्हें एक साथ मिलाकर फेशियल फिजियोनॉमी की एक पूरी रेंज उभर आती है और फिर सामान्य इमेज का मिलान सभी इंजीन फेसेज से किया जाता है। अब इस सिस्टम के द्वारा वास्तविक व्यक्ति और उसके टेम्पलेट का मिलान किया जा सकता है। इस सिस्टम द्वारा किसी व्यक्ति विशेष को विमान में चढ़ने से रोका जा सकता है। उदाहरण के लिए, यदि हवाई अड्डा अधिकारियों को किसी आतंकवादी विशेष के विमान में उड़ने का अंदेशा हो तो अधिकारी, विमान में प्रवेश करने वाले यात्रियों के चेहरे का मिलान, कंप्यूटर सिस्टम में मौजूद उस आतंकवादी के इंजीन फेस से करता है। यह तकनीक अभी परीक्षण के दौर में ही है और इसमें बहुत सी दिक्कतें भी हैं। सबसे बड़ी दिक्कत तो है एक कारगर डेटाबेस बनाने की। हालांकि कुख्यात आतंकवादियों की तस्वीरें सिस्टम में डाली जा सकती हैं लेकिन केवल कुछेक आतंकवादियों की तस्वीरें ही उपलब्ध हैं। इसके अलावा डेटाबेस में आतंकवादी की तस्वीर मौजूद होने के बावजूद किन्हीं दूसरे कारणों से भी मिलान में दिक्कत आ सकती हैं। उम्र बढ़ने पर चेहरे का रूप-रंग बदल जाता है जिस कारण यह सिस्टम फेल हो सकता है।

आवाज/स्वरपहचान: आजकल ऐसी तकनीकें भी अस्तित्व में आ चुकी हैं जो प्रयोगकर्ता को यह सुविधा प्रदान करती हैं कि प्रयोगकर्ता अपनी आवाज के आधार पर ही किसी स्थान तक पहुंच सके। इस स्वर-पहचान आधारित बायोमैट्रिक तकनीक में सबसे पहले किसी व्यक्ति की आवाज/स्वर को कंप्यूटर में रखा जाता है। कंप्यूटर का सॉफ्टवेयर इस आवाज की पहचान कर लेता है। बाद में वह केवल उसी व्यक्ति को उस स्थल पर प्रवेश करने की

अनुमति देगा, जिसकी आवाज पहले से ही कंप्यूटर में दर्ज होगी।

इस अत्याधुनिक तकनीक का उपयोग आजकल फोन-बैंकिंग में आमतौर पर किया जाने लगा है। फोन-बैंकिंग के अंतर्गत बैंक का ग्राहक, बैंक के ग्राहक-सेवा केन्द्र को फोन करता है और फिर वह फोन के सहारे ही अपने खाते को संचालित करता है। ग्राहक, फोन-बैंकिंग द्वारा धनादेश बनाने का निर्देश दे सकता है और खाते से धनराशि को स्थानांतरित भी करवा सकता है। फोन बैंकिंग के सहारे बैंक का ग्राहक वह सारे कार्य कर सकता है जो वह बैंक की खिड़की/काउंटर पर जाकर करता है। इस प्रकार किसी अनाधिकृत व्यक्ति द्वारा फोन-बैंकिंग की सुविधा का इस्तेमाल करके किसी अन्य के खाते को संचालित करने की आशंका सदैव बनी रहती है लेकिन स्वर-पहचानने वाली नई तकनीक के प्रयोग से ऐसी किसी भी आशंका से बचा जा सकता है। स्वर-पहचान की तकनीक के अंतर्गत ग्राहक के स्वर (आवाज) को बैंक के कंप्यूटर में दर्ज कर लिया जाता है। जब भी कोई ग्राहक, अपने बैंक से फोन-बैंकिंग द्वारा संपर्क करता है तो बैंक का कंप्यूटर, फोन करने वाले व्यक्ति के स्वर का मिलान उस ग्राहक विशेष के कंप्यूटर में पहले से दर्ज स्वर से करता है। यदि दोनों स्वर समान होते हैं तो ग्राहक-सेवा-अधिकारी, बैंक के ग्राहक को उसका खाता संचालित करने की अनुमति दे देता है और यदि दोनों स्वरों में समानता नहीं होती है तो तथाकथित ग्राहक को फोन-बैंकिंग सुविधा का लाभ लेने से वंचित कर दिया जाता है।

हाथएवंअंगुलिपहचानः विभिन्न बायोमैट्रिक तकनीकों की सहायता से किसी व्यक्ति के हाथों और उसकी अंगुलियों को पहचानना भी संभव हो गया है। हाथ व अंगुलि पहचान की इस तकनीक के अंतर्गत हाथों की ज्यामितिय रचना के आधार पर किस व्यक्ति की पहचान स्थापित की जाती है। इस विधि के कार्यान्वयन के लिए प्रयोग में लाए जाने वाले कुछ उपकरण तो हाथ की दो-तीन अंगुलियों का ही विश्लेषण करते हैं जबकि कुछ उपकरण, व्यक्ति के पूरे हाथ का गहराई से विश्लेषण करते हैं। इसी प्रकार कुछ पहचान-तंत्र, हाथों की अंगुलियों की ज्यामितीय के आधार पर भी व्यक्ति की पहचान स्थापित करते हैं।

अंतर्राष्ट्रीय स्तर पर, कुछ हवाई अड्डों पर ऐसी सुविधा है कि काफी

अधिक संख्या में यात्रा करने वाले ग्राहकों को मात्र *'हैंड स्कैन डिवाइस'* की जांच से ही गुजरना पड़ता है और ऐसे यात्री अन्य सुरक्षा व दस्तावेज़ जांच से बच जाते हैं। इस पहचान तंत्र का उपयोग, अन्य बायोमैट्रिक तंत्रों के साथ सम्मिलित रूप से भी किया जा सकता है। इस विधि का इस्तेमाल, किसी व्यक्ति विशेष को किसी स्थल विशेष में प्रवेश देने या नहीं देने के लिए भी किया जा सकता है।

विभिन्न बायोमैट्रिक तंत्रों/विशेषताओं का तुलनात्मक अध्ययन : बायोमैट्रिक्स आजकल काफी चर्चा में है क्योंकि इसके द्वारा किसी अपराध को कारित होने से पहले ही रोका जा सकता है। वास्तव में अपराधों की रोकथाम में विभिन्न बायोमैट्रिक उपकरण व विशेषताएं, महत्त्वपूर्ण भूमिका अदा कर रही हैं। इनमें से कुछ विशेषताओं को दुनियाभर में विधिक मान्यता मिली हुई है (जैसे अंगुलि चिह्न) तो कुछ विशेषताएं अपने इस्तेमाल के शैशव-काल में ही हैं।

लक्षण	*अंगुलि चिह्न*	*हाथ की ज्यामितीय*	*आइरिस स्कैन*	*चेहरा पहचान*	*हस्ताक्षर*	*स्वर*
प्रयोग में सरलता	उच्च	उच्च	मध्यम	मध्यम	उच्च	उच्च
गलती की आशंका	सूखापन, गंदगी, आयु	हाथ में चोट, आयु	कम प्रकाश	प्रकाश, आयु, चश्मा, बाल	हस्ताक्षरों में परिवर्तन	शोर जुकाम, मौसम
शुद्धता	उच्च	उच्च	अत्याधिक उच्च	उच्च	उच्च	उच्च
प्रयोग में मान्यता	मध्यम	मध्यम	मध्यम	मध्यम	मध्यम	उच्च
आवश्यक सुरक्षा स्तर	उच्च	मध्यम	अत्याधिक उच्च	मध्यम	मध्यम	मध्यम
दीर्घकालिक स्थायित्व	उच्च	मध्यम	उच्च	मध्यम	मध्यम	मध्यम

सारणी : विभिन्न बायोमैट्रिक तंत्रों की तुलना

लाइव-स्कैनर : एक महत्त्वपूर्ण उपकरण

लाइव-स्कैनर, एक महत्त्वपूर्ण बायोमैट्रिक उपकरण है। इसका वास्तविक नाम, *'पोर्टेल लाइव फिंगरप्रिंट वर्कस्टेशन'* है लेकिन सुविधा की दृष्टि से सामान्य रूप से इसे *'लाइव स्कैनर'* ही कहा जाता है। यह एक प्रकाश-वैद्युत उपकरण है जिसमें प्रकाशिकी और वैद्युतिकी के मूल सिद्धांतों का प्रयोग किया जाता है। इसे 'वर्क-स्टेशन' इसलिए कहा जाता है क्योंकि इसमें कई उपकरणों का एक साथ इस्तेमाल किया जाता है। लाइव-स्कैनर के प्रमुख अवयव निम्नलिखित हैं :

- ☆ एक लैपटॉप (कंप्यूटर)
- ☆ छोटा स्कैनर
- ☆ वेब कैमरा (वैकल्पिक)

यह पूरा तंत्र इतना सुविधाजनक होता है कि इसे एक आम कार्यालय-बैग (ऑफिस बैग) में रखकर कहीं भी ले जाया जा सकता है। इसके अलावा इसे परिचालित करने के लिए विद्युत ऊर्जा की आवश्यकता भी नहीं होती है। एक आम लैपटॉप में जो बैटरी पहले से ही लगी होती है, यह तंत्र उसी बैटरी से चलता है। लाइव-स्कैनर की सहायता से उच्च गुणवत्ता वाली साफ, दस अंगुलि चिह्न युक्त पर्ची (10 डिजिट स्लिप) बेहद आसानी और तीव्र गति से तैयार की जा सकती है। इसमें किसी भी प्रकार की किसी स्याही का इस्तेमाल नहीं किया जाता है। इस प्रकार यह अत्याधुनिक उपकरण (विधि) पूर्णतया स्याही-मुक्त होता है।

परंपरागतविधिकीसमस्याएं: लाइव-स्कैनर का उपयोग किसी व्यक्ति की दसों अंगुलियों के चिह्न युक्त एक पर्ची (स्लिप) तैयार करने में किया जाता है। वैसे परंपरागत रूप से भी ऐसी स्लिप बनाई जा सकती है लेकिन उसमें अपेक्षाकृत निम्नलिखित समस्याएं सामने आती हैं :

(1) स्याही, कागज आदि की खरीद में समस्या
(2) उपयुक्त प्रकार से स्याहीयुक्त अंगुलि चिह्न लेने के प्रशिक्षण की कमी
(3) अशुद्धता एवं कम गुणवत्ता की आशंका

लाइव-स्कैनर का प्रयोग करने के लिए जरूरी नहीं है कि कोई अंगुलि चिह्न

विशेषज्ञ ही उसे संचालित करे। एक साधारण कंप्यूटर ऑपरेटर भी लाइव-स्कैनर को परिचालित कर सकता है। इसका सबसे बड़ा लाभ यह है कि इसकी सहायता से तुरंत, अंगुलि चिह्नों का मिलान करके, परिणाम घोषित किया जा सकता है।

लाइवस्कैनरकीतकनीकीविशिष्टताएं: लाइव स्कैनर के अधिकतम और अनुकूलतम उपयोग के लिए आवश्यक है कि उसमें निम्नलिखित तकनीकी विशिष्टताएं आवश्यक रूप से हों :

रोल-फिंगरस्कैनर:

सिद्धांत : प्रकाश-वैद्युत आधारित
विंडो आकार : 40 मि.मी. × 40 मि.मी.
आवर्द्धता : 512 डीपीआई
छवि प्रकार : 256 ग्रे पैमाना
स्कैनिंग समय : 0.01 सेकेंड से कम

आवश्यक हार्डवेयर :

इंटेल पेंटियम-IV
40 जी. बी. हार्ड डिस्क
64 एम. बी. वीडियो मेमोरी
512 एम.बी. रैम
न्यूनतम 3 यू.एस.बी. पोर्ट
चपटा स्क्रीन मैट्रिक्स एल.सी.डी. मॉनीटर (15 इंच न्यूनतम)
उच्च आवर्द्धता वाला वीडियो कैमरा (हैंडीकैम)

अन्य आवश्यकताएं :

220 वोल्ट ए.सी. वैद्युत धारा
5 एम्पियर, 50 हर्टज की धारा
0^0 से लेकर 45^0 सेंटीग्रेड तक का तापमान
90 प्रतिशत आर्द्रता
माइक्रोसॉफ्ट विंडोज-2000 का ऑपरेटिंग सिस्टम
I Bio S-CJ संस्करण का स्कैन इंजिन

लाइवस्कैनरकेअनुप्रयोग: विभिन्न बायोमैट्रिक विधियों के लिए अंगुलि चिह्न डाटाबेस की आवश्यकता पड़ती है और इस महत्त्वपूर्ण कार्य को

लाइव स्कैनर की सहायता से संपादित किया जा सकता है। भारत सरकार की एक परियोजना के अंतर्गत सभी नागरिकों को एक 'राष्ट्रीय पहचान-पत्र' (स्मार्ट कार्ड) जारी करने की योजना है। इस महत्त्वपूर्ण योजना के क्रियान्वयन के लिए सभी भारतीय नागरिकों के अंगुलि चिह्न लिए जाने आवश्यक हैं। लाइव स्कैनर की सहायता से काम को सफलतापूर्वक अपेक्षाकृत कम समय में पूरा किया जा सकता है।

लाइव स्कैनर इतना अधिक सुविधाजनक होता है कि इसे किसी गांव में ले जाकर वहां के निवासियों के अंगुलि चिह्नों का डाटाबेस भी तैयार किया जा सकता है। एक 40 जी.बी. हार्डडिस्क क्षमता वाले लैपटॉप में लगभग 10 हजार अंगुलि चिह्नों को दर्ज किया जा सकता है। आजकल विभिन्न परिवहन प्राधिकरणों द्वारा जारी किए जाने वाले ड्राइविंग लायसेंसों में धारक के अंगूठे के निशान को भी अंकित किया जाता है और यह कार्य विभिन्न परिवहन प्राधिकरणों में लाइव स्कैनर की सहायता से ही किया जा रहा है। लाइव स्कैनर को उपयोग में लाना इतना सरल है कि विभिन्न परिवहन प्राधिकरणों में साधारण कंप्यूटर परिचालक ही इस कार्य को बिना किसी बाधा के कर रहे हैं। लाइव स्कैनर की सहायता से अंगुलि चिह्न लेने के लिए किसी विशेष प्रशिक्षण की आवश्यकता नहीं है। यह भी जरूरी नहीं है कि कोई अंगुलि चिह्न विशेषज्ञ ही लाइव स्कैनर को परिचालित करे इसलिए स्थानीय पुलिस थानों में कार्य कर रहे पुलिसकर्मी भी सरलतापूर्वक इस उपकरण का इस्तेमाल कर सकते हैं।

तथ्यों में बायोमैट्रिक्स

(1) संयुक्त राज्य अमेरिका की *'फेडरल ब्यूरो ऑफ इन्वेस्टीगेशन'* (एफ.बी.आई.) ने लगभग 50 मिलियन अपराधियों के अंगुलि चिह्नों को अभिलेखित (रिकॉर्ड) कर रखा है ताकि उनका उपयोग अपराधों की रोकथाम में किया जा सके।

(2) विश्व भर में बायोमैट्रिक्स का सर्वाधिक प्रयोग निम्नलिखित कार्यों में किया जाता है :
- ☆ पहचान-पत्र कार्यक्रम
- ☆ फर्जीवाडा रोकने के लिए

- ☆ व्यक्ति की पृष्ठभूमि का पता लगाने के लिए
- ☆ भौतिक प्रमाणीकरण के लिए
- ☆ यात्रियों की जांच के लिए
- ☆ आगंतुकों को खोज निकालने के लिए
- ☆ आतंकवाद से सुरक्षा में
- ☆ कानून एवं व्यवस्था की स्थिति बनाए रखने के लिए
- ☆ संयुक्त राज्य अमेरिका आने वाले प्रत्येक पर्यटक की पहचान प्रत्येक हवाई अड्डे, बंदरगाह और सीमा पर बने केंद्रों पर की जाती है।
- ☆ अंतर्राष्ट्रीय नागरिक उड्डयन संगठन (इंटरनेशनल सिविल एवीएशन आर्गेनाइजेशन) ने यात्रा-दस्तावेज़ों में चेहरा-पहचान तंत्र के प्रयोग हेतु मानदंड तैयार किए हैं।
- ☆ कुछ पश्चिमी देशों में 'ऑटोमैटिक ट्रेलर मशीन' को परिचालित करने के लिए प्रयोगकर्ता को रेटिना-स्कैन से गुजरना पड़ता है।
- ☆ भारत सरकार द्वारा जारी किए जाने वाले 'राष्ट्रीय नागरिक पहचान-पत्र' में भी अंगूठे के चिह्न का अंकन किया जा रहा है।

बायोमैट्रिक्स में हृदय की धड़कन का प्रयोग

भारतीय वैज्ञानिकों ने एक ऐसी तकनीक विकसित कर ली है जिसमें हृदय की धड़कन के आधार पर किसी व्यक्ति की पहचान स्थापित की जाएगी। जी हां, हृदय की धड़कनें ही अब हमारी पहचान बनने जा रही हैं। लखनऊ स्थित इंस्टीटयूट ऑफ इंजीनियरिंग एंड टेक्नोलॉजी ने भारतीय प्रौद्योगिकी संस्थान के सहयोग से एक ऐसी तकनीक विकसित की है जिसमें हृदय की धड़कनों को डिजिटल आई.डी. में परिवर्तित किया जाएगा ताकि अंतर्राष्ट्रीय हैकर्स और आतंकी गतिविधियों पर प्रभावी अंकुश लगाया जा सके।

इंस्टीटयूट ऑफ इंजीनियरिंग एंड टेक्नोलॉजी (लखनऊ) के वरिष्ठ वैज्ञानिक वाई. एन. सिंह द्वारा विकसित इस तकनीक को अंतर्राष्ट्रीय संस्था *'इंस्टीटयूट*

ऑफ इलैक्ट्रॉनिक्स इंजीनियर्स' अर्थात 'आई.ई.ई.' ने भी अपनी मान्यता प्रदान कर दी है। इस तकनीक को विकसित करने की प्रेरणा, बायोमैट्रिक्स पहचान में अंगुलि चिह्नों से लेकर चेहरे के कटावों (विशेषताओं) तक की तकनीकी समस्याओं के प्रकाश में आने से मिली। इस तकनीक से संबंधित शोध में एम.आई.टी. कैम्ब्रिज और संयुक्त राज्य अमेरिका के डाटाबेस का इस्तेमाल किया गया है। इस शोध में सामान्य व्यक्तियों और रोगियों के हृदय की धड़कनों का अध्ययन इलैक्ट्रोकार्डियोग्राम संकेतों से किया गया था। बाद में *'टाइम डेरिवेटिव एंड एडेप्टिव थ्रीसोल्ड'* (टीडीएटी) तकनीक से इन धड़कनों का प्रयोग बायोमैट्रिक तंत्र में किया गया।

उपरोक्त चर्चा से स्पष्ट है कि बायोमैट्रिक्स टेक्नोलॉजी एक ऐसा क्षेत्र है जिसकी उपेक्षा करने का खतरा, विधि विज्ञान (न्यायालयिक विज्ञान) और सूचना-प्रौद्योगिकी उद्योग, नहीं उठा सकता। बायोमैट्रिक्स के कारण घर, दुकान, व्यावसायिक परिसरों, कार और ए.टी.एम. आदि की सुरक्षा के साथ-साथ विभिन्न प्रकार के आतंकी खतरों से भी समाज को बचाया जा सकता है। सारतः अपराधों की रोकथाम में बायोमैट्रिक्स आज एक प्रमुख उपकरण के रूप में सामने आ रहा है।

●

4

अपराध-निरोध और अंगुलि चिह्न

अंगुलि चिह्नों का प्रयोग अत्यंत प्राचीन काल से ही व्यक्ति की पहचान स्थापित करने के लिए किया जाता रहा है। बाद में इनका प्रयोग, अपराधियों की पहचान स्थापित करने के लिए भी किया जाने लगा और इस कार्य में अंगुलि चिह्नों की कोई काट आज तक उपलब्ध नहीं हो पाई है। वैज्ञानिक प्रमाणों की लंबी सूची में अंगुलि चिह्न अकेले ऐसे प्रमाण हैं जिन्हें दुनियाभर के न्यायालयों में वैधानिक मान्यता प्राप्त है। पहले अंगुलि चिह्नों का प्रयोग मात्र अपराधी की पहचान तक ही सीमित था लेकिन अब इनका उपयोग अपराधों की रोकथाम के लिए भी किया जाने लगा है। अपराधों की रोकथाम में अंगुलि चिह्न किस प्रकार महत्त्वपूर्ण भूमिका अदा करते हैं, यह चर्चा करने से पहले यह जान लेना प्रासंगिक रहेगा कि अंगुलि चिह्न कहते किसे हैं और इनका महत्त्व क्या है।

व्यक्ति चाहे किसी भी जाति, वंश, लिंग, राष्ट्र या महाद्वीप का हो, उसकी हथेली और अंगुलियों पर कुछ विशिष्ट प्रकार की रेखाएं एक निश्चित विन्यास में सजी दिखाई देती हैं। अंगुलियों पर पाई जाने वाली इन्हीं विशिष्ट रेखाओं को 'अंगुलि चिह्न' कहते हैं। यहां ध्यान देने योग्य बात यह है कि ये अंगुलि चिह्न, अति-प्राचीन काल के मानव में भी पाए जाते थे। मानव-विकास विज्ञान के शोधों से ज्ञात होता है कि वानरों और आधुनिक मानव के बीच की पीढ़ी, आदिमानव की अंगुलियों पर भी इसी प्रकार के अंगुलि चिह्न पाए जाते थे। यदि हम अंगुलि चिह्नों के इतिहास के पन्ने पलटें तो पाएंगे कि मानव, पृथ्वी पर अपने प्रादुर्भाव के कुछ समय बाद से ही अंगुलि चिह्नों का प्रयोग किसी न किसी रूप में कर रहा है। ईसा से भी हजारों वर्ष पूर्व से ही

निर्माता का संकेत देने के लिए पकी मिट्टी की मूर्तियों *(टेराकोटा)* और मिट्टी के बर्तनों *(पॉटरी)* पर अंगुलि चिह्नों का प्रयोग किया जाता था। मिस्र के राजा *'तुत-एन-खामेन'* के मकबरे में लगभग 3000 वर्ष पुरानी, अंगुलि चिह्न युक्त चूने के पट्टिकाएं *(स्लैब)* पाई गई हैं। भारत में भी सदियों पूर्व से ही पंजे के चिह्न (Palm Prints) का प्रयोग विभिन्न प्रयोजनों हेतु किया जाता रहा है। चीन में तांग के शासनकाल (618 ई.पू. से 906 ई.पू.) में अंगुलि चिह्नों का प्रयोग, राजकीय मुहरों के रूप में किया जाता था।

ज्योतिष-शास्त्र में अंगुलियों तथा हथेली की रेखाओं के आधार पर ही सटीक भविष्यवाणियां कर दी जाती हैं। ज्योतिष-शास्त्र वास्तव में एक विज्ञान ही है और इसी प्राचीन विज्ञान से मिलता-जुलता आज का 'अंगुलि चिह्न विज्ञान' है। दोनों में अंतर है तो मात्र इतना कि अंगुलि चिह्न विज्ञान की सहायता से 'भविष्य' के स्थान पर अपराधियों की पहचान का निर्धारण किया जाता है। व्यक्तिगत पहचान के माध्यम के रूप में अंगुलि चिह्नों का प्रयोग सर्वप्रथम कब और कहां किया गया, यह एक रहस्य ही है लेकिन इतना निश्चित है कि हस्त-रेखाओं और अंगुलि चिह्नों का प्रयोग प्राचीनतम मानव सभ्यताओं में भी किसी न किसी रूप में अवश्य किया जाता था।

प्रागैतिहासिक काल के मिट्टी के बर्तनों और पकी मिट्टी की मूर्तियों पर हाथ तथा अंगुलियों के चिह्न (निशान) पाए गए हैं। पुरातत्वविद् कर्नल जी. मैलारी ने नोवास्कोसिया पर्वत-शृंखला की चोटी पर इसी प्रकार की प्रागैतिहासिक काल की कुछ मिट्टी की मूर्तियां प्राप्त की हैं। इन मूर्तियों पर अंगुलि चिह्न किस उद्देश्य से अंकित किए गए थे, इस बारे में तो कर्नल मैलारी कुछ नहीं बता पाए लेकिन उनका स्पष्ट रूप से मानना है कि अंगुलि चिह्न युक्त मिट्टी की ये मूर्तियां, ईसा से भी हजारों वर्ष पूर्व, प्रागैतिहासिक काल की हैं। कार्बन-डेटिंग पद्धति द्वारा सिद्ध किया जा चुका है कि मिस्र के राजा *'तुत-एन-खामेन'* के मकबरे से प्राप्त अंगुलि चिह्न युक्त चूना-पत्थर की बनी पट्टिकाएं (स्लैब) लगभग 3000 वर्ष पुरानी हैं। तत्कालीन कोरिया का इतिहास बताता है कि वहां प्राचीन काल में गुलाम-प्रथा काफी प्रचलित थी और उस समय वहां गुलामों के क्रय-विक्रय से संबंधित दस्तावेजों पर संबंधित व्यक्ति (गुलाम) के अंगुलि चिह्न ले लिए जाते थे ताकि उनकी पहचान की जा सके। लगभग 1200 वर्ष पूर्व तक

कोरिया में भी ऐसा किए जाने के प्रमाण मिलते हैं।

सिंधु सभ्यता के मोहनजोदड़ो और हड़प्पा आदि नगरों की खुदाई में भी ऐसी कुछ टेराकोटा की मूर्तियां और पकी मिट्टी के बर्तन आदि मिले हैं जिनसे ज्ञात होता है कि सिंधु-मानव विभिन्न उद्देश्यों की पूर्ति के लिए अंगुलि चिह्नों का प्रयोग करता था। स्पष्ट है कि अंगुलि चिह्नों का प्रयोग प्रागैतिहासिक काल से ही आदिमानव द्वारा किया जाता रहा है लेकिन उनका सही-सही, वास्तविक उद्देश्य अभी तक अल्पज्ञात ही है। व्यक्तिगत पहचान हेतु अंगुलि चिह्नों का प्रयोग सर्वप्रथम कहां और किसके द्वारा किया गया, इस संबंध में विद्वानों में मतभेद हैं। कुछ लोगों के अनुसार इसकी खोज चीन में की गई जबकि कुछ विद्वान मानते हैं कि व्यक्तिगत पहचान स्थापित करने में अंगुलि चिह्नों का उपयोग करने का श्रेय प्राचीन भारतीयों को जाता है। अति-प्राचीन काल में चीनी अनपढ़ नागरिक भूमि संबंधी अभिलेखों में हस्ताक्षर के स्थान पर अंगुलि चिह्न ही अंकित करते थे, ठीक वैसे ही जैसे आज भी भारत के ग्रामीण इलाकों में 'अंगूठा लगाया' जाता है। कहा जाता है कि जब लिखाई (लिपि) का आविष्कार नहीं हुआ था तब चीन के अनाथाश्रमों में किसी बच्चे को भर्ती करते समय उसके अंगुलि चिह्न ले लिए जाते थे और इन अंगुलि चिह्नों की विशिष्ट बनावट के आधार पर ही अनाथ बच्चों की पहचान निश्चित की जाती थी।

भारत में भी अत्यंत प्राचीन काल से ही व्यक्ति की पहचान स्थापित करने के लिए अंगुलि चिह्नों का प्रयोग किया जाता रहा है। यहां विभिन्न उद्देश्यों की पूर्ति के लिए अंगूठे और हथेली की चिह्न का प्रयोग प्रागैतिहासिक काल से ही किया जाता रहा है। प्राचीन भारतीय, रिजों (रघीनों) के विशिष्ट विन्यास से भी परिचित थे और वे इन्हें **'चक्र'** और **'जावा'** जैसे वर्गों में वर्गीकृत करते थे। हस्तरेखा विज्ञान का उद्गम भी भारत की पावनभूमि में ही हुआ था। इस पूर्णतया वैज्ञानिक कला का आधार, अंगुलियों और हथेली पर उपस्थित विशिष्ट प्रकार की रिजें ही होती हैं। अपने समय की सर्वाधिक आधुनिक सिंधु सभ्यता, भारतीय सिंधु नदी की घाटी में ही पुष्पित-पल्लवित हुई थी। हड़प्पा, मोहनजोदड़ो, लोथल आदि प्राचीन नगरों की पुरातात्विक खुदाई से पता चलता है कि सिंधु सभ्यता के लोग अंगुलि चिह्नों के महत्त्व से भलीभांति परिचित थे।

246-210 ई.पू. चीन के सम्राट टी-एन-शी ने अंगुलि चिह्न युक्त राजकीय

मुहरें (पकी मिट्टी की) जारी की थीं। इन राजकीय मुहरों के एक ओर सम्राट के अंगूठे का चिह्न छपा (खुदा) रहता था जिससे आम जनता को पता चल जाता था कि ये मोहरें राजकीय हैं अथवा नहीं। चीन में इस प्रकार की अंगुलि चिह्न युक्त राजकीय मुहरों का उपयोग सम्राट वू के शासनकाल (147-156 ई.पू.) तक निर्बाध रूप से चलता रहा। स्पष्ट है कि प्राचीन काल में ही चीनियों को अंगुलि चिह्नों के विशिष्ट विन्यास का ज्ञान था लेकिन दुर्भाग्य से उन्होंने इनके किसी नियमबद्ध वर्गीकरण का कोई प्रयास नहीं किया।

भारत तथा चीन के अलावा अन्य कई प्राचीन सभ्यताओं में भी अंगुलि चिह्नों का उपयोग विभिन्न उद्देश्यों के लिए अत्यंत प्राचीनकाल से ही किया जाता रहा है। प्राचीन सीरिया में महत्त्वपूर्ण अभिलेखों की प्रमाणिकता स्थापित करने के लिए उन पर अंगुलि चिह्नों का प्रयोग किया जाता था। ये अंगुलि चिह्न, चूने या चूना-पत्थर की बनी पट्टिकाओं पर उत्कीर्ण होते थे। प्राचीन सीरिया के इस प्रकार के अंगुलि चिह्न युक्त चूने-पत्थर के नमूने आज भी 'ब्रिटिश संग्रहालय' में देखे जा सकते हैं। जापान में भी इस प्रकार के अंगुलि चिह्नों का प्रयोग काफी लंबे समय से किया जाता रहा है। जापानी सम्राट तेहो के शासनकाल (702 ई.पू.) में अपनी पत्नी से तलाक चाहने वाले व्यक्ति को तलाक के प्रार्थनापत्र पर नीचे हस्ताक्षर के साथ-साथ अपनी तर्जनी अंगुली का चिह्न भी अंकित करना पड़ता था ताकि वास्तविक पति की पहचान स्थापित की जा सके।

अरब देश के एक व्यापारी सुलेमान ने अपनी चीन-यात्रा के प्रसंगों को एक पुस्तक के रूप में संकलित किया था। सुलेमान की इस पुस्तक के अनुसार तत्कालीन चीन में कर्ज लेते समय कर्जदार को कर्ज के दस्तावेजों पर अपनी अंगुलियों के चिह्न लगाने पड़ते थे। इतिहासकारों ने इस प्रसंग का समय 851 ई. निर्धारित किया है। साक्ष्य बताते हैं कि 1000 ई. के आसपास चीन में सम्राट सुंग के शासनकाल के दौरान चल-अचल संपत्ति की खरीद-फरोख्त से संबंधित कागजात पर क्रेता और विक्रेता द्वारा अंगुलि चिह्न लगाए जाते थे। इंग्लैण्ड के प्रसिद्ध शेयर बाजार 'रॉयल सोसायटी ऑफ लंदन' में 1684 ई. में अंगुलि चिह्न युक्त एक शेयर देखा गया जिसे आज भी वहां संरक्षित करके रखा गया है। इसका प्रयोजन अभी तक अज्ञात है।

इंग्लैण्ड में अंगुलि चिह्नों का प्रयोग सजावटी वस्तुओं पर भी किया जाता था। प्रसिद्ध अंग्रेजी लेखक और चिंतक थॉमस बेविक ने 1770 ई. में अपनी तीन पुस्तकों के आवरण पर लोगों का ध्यान आकर्षित करने के लिए अपने अंगुलि चिह्नों का प्रयोग किया। लोकप्रिय लेखक के अंगुलि चिह्नों से युक्त ये पुस्तकें इंग्लैण्ड में हाथों-हाथ बिक गईं। इसी प्रकार 1882 ई. में अमेरिकी भूगर्भ शास्त्री गिलवर्ट थॉमसन ने मैक्सिको में पुरातात्विक खुदाई का कार्य कर रहे श्रमिकों को भुगतान के बाद रसीदों पर उनके अंगुलि चिह्न लिए।

अंगुलि चिह्न विज्ञान और भारत

स्पष्ट है कि अंगुलि चिह्नों का प्रयोग अति प्राचीनकाल से ही समूचे विश्व में किया जाता रहा है लेकिन अंगुलि चिह्नों के विभिन्न विन्यासों को विधिपूर्वक निश्चित वर्गों में विभाजित करने का श्रेय भारतीयों को ही दिया जाता है। मुगल बादशाह शाहजहां के शासनकाल में ही अंगुलि चिह्नों को विधिवत वर्गीकृत करने का सर्वप्रथम प्रयास किया गया था लेकिन सीमित साधनों के कारण ये प्रयास अधिक सफल नहीं हो सके। वैसे मुगल बादशाह शाहजहां की हथेली तथा अंगुलि चिह्नों से युक्त कई राजकीय अभिलेख मिले हैं जिन्हें राष्ट्रीय संग्रहालय में आज भी देखा जा सकता है।

यह एक सर्वमान्य तथ्य है कि अंगुलि चिह्न विज्ञान का सर्वप्रथम प्रादुर्भाव हमारे देश की धरती पर ही हुआ था। इतिहास के पन्ने पलटने पर पता चलता है कि इंग्लैण्ड के एक प्रशासक सर फ्रांसिस गाल्टन ने 1899 ई. में उस समय ही भारत में क्रमबद्ध अंगुलि चिह्न विज्ञान की नींव रख दी थी जब उनकी पहल पर भारतीय डाक-तार विभाग के अराजपत्रित कर्मचारियों का रिकॉर्ड रखने के लिए उनके अंगुलि चिह्न लेने को अनिवार्य कर दिया गया था। इसी वर्ष ब्रिटिश सरकार ने सभी भारतीय चिकित्सा पार्षदों और चिकित्सकों को निर्देश दिया कि किसी भी व्यक्ति को चिकित्सकीय-प्रमाणपत्र देते समय उसके अंगूठे का चिह्न अवश्य ले लिया जाए ताकि आवश्यकता पड़ने पर व्यक्ति की पहचान निश्चित की जा सके। चिकित्सा-प्रमाणपत्र पर उपचारित व्यक्ति के अंगूठे की चिह्न लेने की यह परंपरा आज भी बदस्तूर जारी है।

भारत में अंगुलि चिह्न विज्ञान को अंकुरित और पुष्पित-पल्लवित करने का श्रेय सर हेनरी को दिया जा सकता है। उन्होंने अंगुलि चिह्न विज्ञान द्वारा किसी व्यक्ति की पहचान स्थापित करने की उपयोगिता को समझते हुए 1896 में भारत सरकार से अनुरोध किया कि अंगुलि चिह्न विज्ञान को जनोपयोगी बनाने के लिए एक समिति बनाई जाए। सर हेनरी के अनुरोध को स्वीकार करते हुए तत्कालीन भारत सरकार ने एक समिति गठित की। सी. स्टानहान, आर. ई. सरवेयर और एलेक्स पेडलर को इस समिति का सदस्य नियुक्त किया गया। समिति ने अंगुलि चिह्न विज्ञान के अनुप्रयोगों और इसकी उपयोगिता का गहराई से अध्ययन किया और अपनी रिपोर्ट में अंगुलि चिह्न पद्धति को अंगीकार करने का अनुमोदन किया। समिति की सिफारिशों के अनुरूप विश्व का सबसे पहला 'अंगुलि चिह्न ब्यूरो', 1897 ई. को कोलकाता में स्थापित किया गया। इस ऐतिहासिक अंगुलि चिह्न ब्यूरो की स्थापना में सर हेनरी के योगदान को कभी भी भुलाया नहीं जा सकता है। इस प्रकार स्पष्ट है कि अंगुलि चिह्न को एक विधिवत विज्ञान का रूप सर्वप्रथम भारत में ही दिया गया।

भारत में अंगुलि चिह्न विज्ञान को संवर्द्धित करने में सर विलियम जे. हरशेल ने भी महत्त्वपूर्ण योगदान दिया। हरशेल भारतीय सिविल सेवा के वरिष्ठ अधिकारी थे और उन दिनों हुगली (बंगाल) में कलेक्टर के रूप में तैनात थे। इसी दौरान उन्होंने अपने प्रयोगों द्वारा सिद्ध कर दिया कि अंगुलियों पर उपस्थित रिजें, अपरिवर्तनशील होती हैं। उन्होंने सन 1858-1880 ई. के दौरान बंगाल की हुगली जेल में अंगुलि चिह्नों का प्रयोग अनिवार्य कर दिया। राजाधर कोनाई नामक एक ठेकेदार के अंगुलि चिह्न एक ठेके के अनुबंध-पत्र पर लेकर हरशेल ने अंगुलि चिह्न लेने का श्रीगणेश किया। यह ऐतिहासिक अनुबंध-पत्र आज भी सुरक्षित है। माना जाता है कि अंगुलि चिह्न विज्ञान की वर्तमान इमारत, श्री हरशेल के प्रयत्नों की नींव पर ही खड़ी है।

अंगुलि चिह्नों को विभिन्न पैटर्नों (प्रतिरूपों) में सर्वप्रथम वर्गीकृत करने का श्रेय भी भारतीयों को ही जाता है। हस्त-रेखा विज्ञान में उपयोग हेतु सर्वप्रथम हिंदुओं ने अंगुलि चिह्नों को *'चक्र'*, *'जावा'* आदि पैटर्नों में विभाजित किया। इसके बाद ही चीनियों ने इन्हें *'लो'* और *'की'* आदि श्रेणियों में विभाजित किया। भारत के बंगाल प्रांत में अशिक्षित व्यक्तियों द्वारा महत्त्वपूर्ण

दस्तावेजों पर अंगूठे का निशान लगाने की परंपरा सदियों पूर्व से चली आ रही है। प्राचीन काल में इन्हीं अंगुलि चिह्नों (अंगूठे के निशान) से पहचाना जाता था कि अमुक अभिलेख किसी व्यक्ति विशेष से ही संबंधित है या नहीं। डा. हेनरी फाल्ड्स ने 1872 ई. में अपने अल्प समय के बंगाल प्रवास के दौरान देखा कि वहां हस्ताक्षरों के स्थान पर अंगूठे के निशानों का ही अधिक प्रयोग किया जाता था। बाद में अपने अनेक लेखों में हेनरी फाल्ड्स ने इस तथ्य का उल्लेख किया।

सर हेनरी के प्रयत्नों के फलस्वरूप जब बंगाल (भारत) में विश्व का पहला अंगुलि चिह्न ब्यूरो स्थापित कर दिया गया और समूचे भारतवर्ष में अंगुलि चिह्नों का उपयोग किया जाने लगा तो शेष विश्व की आंखें भी खुलीं और उसने इस दिशा में प्रयोग करने प्रारंभ किए। 1751 में जर्मन वैज्ञानिक हिर्टज ने और 1764 में गौटिंगटन ने कार्यिकी के आधार पर रिजों का अध्ययन किया और बताया कि किसी व्यक्ति की अंगुलियों पर पाई जाने वाली रिजें जीवनपर्यंत एकसमान रहती हैं अर्थात अपरिवर्तनशील होती हैं।

यह तथ्य अब निर्विवाद रूप से स्वीकार किया जा चुका है कि एक विज्ञान के रूप में अंगुलि चिह्न पद्धति का प्रयोग भारत में ही प्रारंभ हुआ और यहीं की भूमि में यह महत्त्वपूर्ण विज्ञान फला-फूला। अपराधियों की पहचान के लिए अंगुलि चिह्नों का प्रयोग भी सर्वप्रथम भारत में ही प्रारंभ हुआ। गाल्टन प्रणाली के आधार पर अपराधियों की पहचान सर्वप्रथम भारत में 1893 में शुरू हुई। इस पद्धति की उपयोगिता, वैज्ञानिकता और निष्पक्षता के कारण ही अगले वर्ष से ही इंग्लैंड में भी अपराधियों की पहचान के लिए अंगुलि चिह्नों का उपयोग किया जाने लगा। इसके बाद 1901 में स्काटलैंड यार्ड (इंग्लैंड) और वेल्स ने भी इस पद्धति को स्वीकार कर लिया।

अंगुलि चिह्न विज्ञान के पुरोधा

विलियम हरशेल

अंगुलि चिह्न को एक विज्ञान के रूप में मान्यता दिलवाने का श्रेय विलियम हरशेल को दिया जा सकता है। इनका जन्म 9 जनवरी 1833 को स्लो (इंग्लैण्ड)

के एक प्रसिद्ध वैज्ञानिक परिवार में हुआ था। इनके पितामह सर विलियम हरशेल एक प्रसिद्ध खगोल-विज्ञानी थे। हरशेल के पिता चाहते थे कि वे खगोल-विज्ञान के अतिरिक्त किसी अन्य क्षेत्र को अपने कैरियर के रूप में चुनें और तदुपरांत हरशेल को शिक्षा ग्रहण करने के लिए ब्रिटेन के प्रतिष्ठित हेलीबरी कॉलेज में भेज दिया गया। इस कॉलेज में ईस्ट इंडिया कम्पनी की सेवा के लिए लड़कों को शिक्षित-प्रशिक्षित किया जाता था।

पढ़ाई पूरी करने के बाद 1853 में मात्र बीस वर्ष की आयु में ही ईस्ट इंडिया कंपनी ने उन्हें बंगाल (भारत) में तैनात कर दिया। 1858 में हरशेल भारतीय सिविल सेवा में प्रवेश पा गए। मात्र 25 वर्ष की आयु में हरशेल को जुंगीपुर (हुगली) का कलेक्टर बना दिया गया। भारत में अपनी नियुक्ति के दौरान हरशेल ने अंगुलि-चिह्नों को लेकर काफी प्रयोग किए। अंगुलि चिह्नों की व्यक्तिगतृता (विशिष्टता) को सर्वप्रथम पहचानने का श्रेय विलियम हरशेल को ही है।

अपने प्रयोगों से हरशेल ने सिद्ध कर दिया कि किसी व्यक्ति के अंगुलि-चिह्नों की बनावट विशिष्ट और स्थायी होती है। इस तथ्य से हरशेल काफी उत्साहित थे और व्यक्ति की पहचान स्थापित करने के लिए विश्व में सबसे पहले हरशेल ने ही हुगली जेल में अंगुलि-चिह्न लेने अनिवार्य कर दिए। उनके द्वारा लिए गए सबसे पहले अंगुलि-चिह्न एक अनुबंध-पत्र के रूप में आज भी सुरक्षित हैं। राजाधर वास्तव में सड़क निर्माण की सामग्री की आपूर्ति करने वाला एक ठेकेदार था। एक ठेके के अनुबंध-पत्र पर राजाधर के हस्ताक्षर लेने के स्थान पर हरशेल ने उसके अंगुलि-चिह्न ले लिए। हरशेल द्वारा अंगुलि-चिह्न लेने के प्रयोजन पर विद्वान एकमत नहीं हैं लेकिन इतना तो निश्चित है कि ये अंगुलि-चिह्न पहचान स्थापित करने के लिए ही लिए गए थे।

वास्तव में व्यक्तिगत पहचान के लिए अंगुलि-चिह्नों का विश्व में सर्वप्रथम उपयोग विलियम हरशेल द्वारा ही 1858 में किया गया था। अपने प्रयोगों के आधार पर हरशेल ने पाया कि पूरी हथेली के स्थान पर केवल अंगुलियों की चिह्न का प्रयोग, व्यक्तिगत पहचान में अधिक उपयोगी है। कुछ समय बाद विलियम हरशेल को बंगाल के उत्तरी-पश्चिमी जिले, आरा का मजिस्ट्रेट नियुक्त कर दिया गया। यहां भी हरशेल ने अंगुलि-चिह्न पुनः लिए गए और फिर नये

तथा पुराने अंगुलि-चिह्नों की तुलना की गई। इस प्रयोग के आधार पर हरशेल ने सिद्ध किया कि किसी व्यक्ति के अंगुलि-चिह्न स्थायी और अपरिवर्तनशील होते हैं। इसी दौरान हरशेल ने तीस वर्षों के अंतराल पर अपनी बांयी हथेली के चिह्न दो बार लिए और पाया कि 30 वर्षों के बाद भी हथेली की चिह्न और अंगुलि-चिह्नों में लेशमात्र भी अंतर नहीं आया है। इस प्रकार सर्वप्रथम हरशेल ने ही सिद्ध किया कि किसी व्यक्ति के अंगुलि-चिह्न जीवन पर्यंत अपरिवर्तनशील होते हैं।

1860 से लेकर 1862 तक की दो वर्षों की अवधि में विलियम हरशेल ने जिन प्रमुख व्यक्तियों के अंगुलि चिह्न लिए उनमें से कुछ प्रमुख निम्नलिखित हैं :

(1) नाडिया के महाराजा
(2) बंगाल के पुलिस प्रमुख कैप्टन रबन
(3) नाडिया के पुलिस अधीक्षक सर चार्ल्स हॉवर्ड
(4) न्यायमूर्ति ओगिल्वी टेम्पल
(5) न्यायमूर्ति निनियन एच. थॉमसन
(6) ब्रिटिश प्रशासक एफ. के. हेवलिट
(7) ब्रिटिश प्रशासक ई. ग्रे
(8) ब्रिटिश प्रशासक एफ. डी.
(9) कोलकाता के व्यापारी क्लाउड ब्राउन

1877 में हरशेल जब चीन गए तो मंगोलिया में भी उन्होंने बहुत से लोगों के अंगुलि-चिह्न प्राप्त किए।

1860 में हरशेल को नाडिया जिले का मजिस्ट्रेट बना दिया गया। यहां भी हरशेल ने अंगुलि-चिह्न पर अपने प्रयोग जारी रखे। यहां हरशेल ने बंगाल सरकार के अनुरोध किया कि सभी अदालती अभिलेखों में वादी-प्रतिवादियों के अंगुलि-चिह्न लेने अनिवार्य कर देने चाहिएं। दुर्भाग्य से सरकार द्वारा हरशेल का यह अनुरोध अस्वीकार कर दिया गया क्योंकि इस समय नाडिया में नील-आंदोलन चल रहा था और भारतीय जनता अंग्रेज सरकार से कुपित थी और सरकार नहीं चाहती थी कि अंगुलि-चिह्न लेने को अनिवार्य कर दिए जाने का आदेश देकर एक और विवाद मोल ले लिया जाए।

1877 में जब हरशेल को हुगली का मजिस्ट्रेट बनाया गया तब उन्हें अंगुलि-चिह्न का उपयोग करने के काफी अवसर मिले क्योंकि यहां उन्हें आपराधिक न्यायालयों के नियंत्रण और शासकीय पेंशन के भुगतान के पर्याप्त अवसर मिले। विलियम हरशेल ही पहले व्यक्ति थे जिन्होंने सरकारी पेंशन प्राप्त करने वाले व्यक्तियों के अंगुलि-चिह्नों को रिकॉर्ड में रखना अनिवार्य कर दिया। इस परंपरा के बाद पेंशन प्राप्तकर्ता की मृत्यु के बाद किसी अन्य व्यक्ति द्वारा उसकी पेंशन प्राप्त कर लेने के मामलों पर रोक लग गई। 1877-1880 के दौरान हरशेल ने हुगली जेल के सभी कैदियों के अंगुलि-चिह्न लेकर उन्हें रिकॉर्ड में रखने को अनिवार्य कर दिया। उस समय अक्सर ऐसा होता था कि किसी बड़े परिवार का कोई अपराधी, न्यायालय द्वारा सजा सुनाए जाने पर अपने स्थान पर धन का लालच देकर किसी गरीब व्यक्ति को जेल भिजवा देता था। हरशेल ने सजा सुनाए जाने के तुरंत बाद न्यायालय के रिकॉर्ड-रूम में ही दोषी व्यक्ति के अंगुलि-चिह्न लेने अनिवार्य कर दिए। इससे अपने स्थान पर किसी अन्य व्यक्ति को जेल भेजे जाने के मामलों पर पूर्णतया रोक लग गई। इस प्रकार स्पष्ट है कि अंगुलि-चिह्न विज्ञान में विलियम हरशेल का योगदान अविस्मरणीय है।

डा. हेनरी फाल्ड्स

डा. हेनरी फाल्ड्स टोकियो (जापान) के तुसकजो अस्पताल में चिकित्सक के रूप में तैनात थे। 1879 में अंगुलि-चिह्नों में हेनरी फाल्ड्स की रुचि यकायक जागी और उन्होंने अंगुलि-चिह्न विज्ञान पर शोध कार्य प्रारंभ कर दिया। हेनरी फाल्ड्स का जन्म 1 जून 1843 को बीथ (आयरशायर) में हुआ था। 12 वर्ष की आयु से ही उन्होंने अपने चाचा के साथ उनके व्यापार में हाथ बंटाना शुरू कर दिया। इसके कुछ समय बाद उन्होंने शॉल और तैयार परिधान के निर्माण में भी भाग्य आजमाया। व्यापार में जब उनका मन नहीं रमा तो उन्होंने पढ़ाई जारी रखने का निर्णय किया और 1871 में फाल्ड्स ने एंडरसन कॉलेज, ग्लासगो से चिकित्सक की उपाधि प्राप्त की और उन्होंने अपनी प्रैक्टिस प्रारंभ कर दी।

चूंकि हेनरी फाल्ड्स धार्मिक प्रवृत्ति के व्यक्ति थे इसलिए वे निजी प्रैक्टिस छोड़कर स्कॉटलैंड चर्च के 'मिशन' में सम्मिलित हो गए। चर्च समिति ने नवंबर,

1871 में उनकी नियुक्ति दार्जिलिंग (असम, भारत) के एक चर्च में कर दी लेकिन एक वर्ष के भीतर ही चर्च के प्रभार को लेकर उनकी मिशनरों से अनबन हो गई। इसके बाद उनकी नियुक्ति जापान के एक चर्च में कर दी गई। जापान पहुंचने से पूर्व ही उन्होंने ग्लासगो की एक सुंदरी इसाबेला विल्सन से विवाह कर लिया।

1879 में ओमोरी तथा यूदू (जापान) की खाड़ी में पाए गए प्रागैतिहासिक बर्तनों पर अंगुलियों की चिह्न देखकर फाल्ड्स की रुचि अंगुलि-चिह्न विज्ञान में जागृत हुई। इसके बाद उन्होंने बंदरों के पंजों की चिह्न लेकर उनका अध्ययन प्रारंभ किया। कालांतर में उन्होंने मानव के हथेली व अंगुलि-चिह्नों पर भी शोध-कार्य प्रारंभ किया। अपनी शंकाओं के समाधान के लिए उन्होंने उत्परिवर्तनवाद के कारण प्रसिद्धि पाए चार्ल्स डार्विन से संपर्क साधा और उनके शोध कार्यों का प्रयोग किया। इसके बाद 1923 में फाल्ड्स ने *'मैन्युअल ऑफ प्रैक्टिकल डेक्टाइलोग्राफी'* नामक पुस्तक प्रकाशित की। फिर उनका एक शोध-पत्र विश्व प्रसिद्ध विज्ञान जर्नल *'नेचर'* में *'ऑन द स्किन-फुरोज ऑफ द हैंड'* नामक शीर्षक से प्रकाशित हुआ। इस महत्त्वपूर्ण शोध-पत्र में फाल्ड्स ने बताया कि कैसे उन्होंने प्रागैतिहासिक बर्तनों पर देख गए अंगुलि-चिह्नों के बाद बंदरों और मनुष्यों के अंगुलि-चिह्नों पर प्रयोग प्रारंभ किए। इसके बाद 'नेचर' में फाल्ड्स का एक और शोध-पत्र प्रकाशित हुई जिसमें उन्होंने छपाई की स्याही से अंगुलि-चिह्न लेने की विधि बताई। फाल्ड्स द्वारा बताई गई छपाई की स्याही से ही आज भी भारत सहित विश्व के अधिकतर देशों में अंगुलि-चिह्न लिए जाते हैं।

सर फ्रांसिस गाल्टन

अंगुलि-चिह्नों की व्याख्या के आधार पर सर्वप्रथम व्यक्ति की पहचान स्थापित करने का श्रेय फ्रांसिस गाल्टन को दिया जाता है। फ्रांसिस गाल्टन उन्नीसवीं सदी के महानतम् वैज्ञानिक थे और उनका जन्म 16 फरवरी, 1822 को बिरमिंघम में हुआ था। बालक गाल्टन की अति कुशाग्र बुद्धि को देखते हुए उनके अभिभावकों ने उन्हें चिकित्सक बनाने का फैसला लिया। इसके लिए उनका प्रवेश किंग्स कॉलेज, लंदन में करा दिया गया लेकिन अचानक पिता की मृत्यु से

उत्पन्न आर्थिक संकट के कारण उनकी मेडिकल की पढ़ाई अधूरी रह गई।

1844 में गाल्टन ने ट्रिनिटी कॉलेज, कैम्ब्रिज से बी.ए. की उपाधि प्राप्त की। 1858 में वे *'रॉयल ज्योग्राफिकल सोसायटी'* के फैलो चुने गए और तीन वर्ष बाद ही 34 वर्ष की आयु में उन्हें अति-प्रतिष्ठित 'रॉयल सोसायटी' का फैलो नियुक्त कर दिया गया। 1888 में रॉयल इंस्टीट्यूशन के अनुरोध पर गाल्टन ने एक शोध-पत्र *'पर्सनल आइडेंटीफिकेशन एंड डेसक्रिप्शन'* के नाम से पढ़ा। इस शोध-पत्र को तैयार करने में गाल्टन की सहायता *'नेचर'* के संपादक और सर विलियम हरशेल ने की। इस शोध-पत्र को पढ़ते समय गाल्टन ने हरेशल के 28 वर्षों के अंतराल पर लिए गए दो अंगुलि-चिह्न प्रस्तुत किए और बताया कि रिजों के लक्षण (उनका आकार-प्रकार व विन्यास) अपरिवर्तित व स्थायी होते हैं।

इसके बाद अगले सात वर्षों तक गाल्टन ने अंगुलि-चिह्न के क्षेत्र में जी-तोड़ मेहनत की। इस दौरान उन्होंने विभिन्न लोगों के अंगुलि-चिह्नों का एक विराट संग्रह एकत्रित कर लिया। गाल्टन के इस संग्रह में अंग्रेजों के अलावा वेल्स, हिन्दू, जावा, नीग्रो और कुछ विशिष्ट वर्ग के लोगों जैसे-मूर्ख व अपराधियों के अंगुलि-चिह्न सम्मिलित थे। 1892 में फ्रांसिस की पुस्तक *'फिंगर प्रिंट्स'* प्रकाशित हुई। यह इस विषय की पहली पुस्तक मानी जाती है।

बाद के वर्षों में गाल्टन ने अंगुलि-चिह्नों के स्थायित्व, विशिष्टता और असमानता के संबंध में काफी प्रयोग किए। इसी दौरान फ्रांसिस गाल्टन ने लंदन में एक ब्यूरो स्थापित किया जो *'सिविल ब्यूरो फॉर पर्सनल आइडेन्टीफिकेशन'* कहलाया। यह ब्यूरो अपने आप में विश्व का सबसे पहला ब्यूरो था इसलिए विश्व का सबसे पहला अंगुलि-चिह्न ब्यूरो स्थापित करने का श्रेय गाल्टन को ही जाता है। वैसे कुछ विद्वान इस ब्यूरो को अंगुलि-चिह्नों के रिकॉर्ड का ब्यूरो नहीं मानते। उनका मानना है कि विश्व का सबसे पहला अंगुलि-चिह्न ब्यूरो, 1897 में कोलकता (भारत) में स्थापित किया गया। गाल्टन के इस ब्यूरो ने लंदनवासियों के अंगुलि-चिह्नों के आधार पर उनका पंजीकरण किया ताकि अपराधों पर लगाम कसी जा सके।

उपरोक्त ब्यूरो में रहते हुए गाल्टन ने अपना पूरा समय अंगुलि-चिह्नों की गणना, शोध आदि पर लगाया और गणितिय विधि से उन्होंने सिद्ध कर दिया कि दो अलग-अलग व्यक्तियों के अंगुलि-चिह्नों में समानता का योग

60,000,000,000 व्यक्तियों में से मात्र एक है। गाल्टन पहले व्यक्ति थे जिन्होंने वैज्ञानिक विधि से प्रमाणित किया कि दो व्यक्तियों के अंगुलि-चिह्न कभी भी एक-समान नहीं हो सकते। अपने प्रयोगों और शोध-कार्य के आधार पर फ्रांसिस गाल्टन ने अंगुलि-चिह्न विज्ञान के संबंध में निम्नलिखित सिद्धांत प्रतिपादित किए :

(1) व्यक्ति की अंगुलियों पर पाई जाने वाली रिजें (रघीनें) स्थायी प्रकृति की होती हैं और जीवन पर्यंत इनके विन्यास में कोई परिवर्तन नहीं आता है।

(2) व्यक्ति की आयु बढ़ने के साथ-साथ रिजों का आकार तो बढ़ता जाता है लेकिन उनकी स्थिति तथा विन्यास में कोई भी परिवर्तन असंभव है।

(3) किसी व्यक्ति की विभिन्न अंगुलियों की रिजों की बनावट और उनका विन्यास भी भिन्न-भिन्न होता है अर्थात किसी व्यक्ति की दो अंगुलियों के चिह्न भी समान नहीं हो सकते हैं।

(4) अंगुलि-चिह्नों का निर्माण भ्रूणावस्था में ही हो जाता है और एक बार इनका निर्माण हो जाने के बाद इन्हें किसी भी विधि से परिवर्तित नहीं किया जा सकता है।

(5) अंगुलि-चिह्न, व्यक्ति की जाति, वंश या स्वभाव से प्रभावित नहीं होते हैं।

सर एडवर्ड रिचर्ड हेनरी

अंगुलि-चिह्न पहचान पद्धति को अंतिम रूप से विकसित करने का श्रेय सर एडवर्ड रिचर्ड हेनरी को दिया जाता है। समूचे विश्व में आज भी उन्हीं के द्वारा विकसित अंगुलि-चिह्न वर्गीकरण पद्धति को अपनाया गया है। हेनरी का जन्म 26 जुलाई, 1850 को शेडवैल (इंग्लैंड) के एक चिकित्सक के घर में हुआ था। वेयर के सेंट एडमंड कॉलेज से शिक्षा प्राप्त करने के बाद हेनरी 1867 में लॉयड्स की एक फर्म में जूनियर क्लर्क बन गए। ज्ञानोपार्जन की उनकी अदम्य इच्छा ही थी जिसके कारण वे नौकरी करने के साथ-साथ यूनिवर्सिटी कॉलेज, लंदन से उच्च-शिक्षा भी ग्रहण करते रहे। अगले वर्षों की मेहनत के फलस्वरूप

एक प्रतियोगी परीक्षा के द्वारा वे भारतीय सिविल सेवा के लिए चुन लिए गए। हैलीबरी कॉलेज से प्रशासनिक प्रशिक्षण करने के बाद उनकी नियुक्ति भारत के उत्तरी-पश्चिमी क्षेत्र में कर दी गई।

1891 में रिचर्ड हेनरी को बंगाल (लोअर प्रोविंसिज) का पुलिस महानिदेशक बना दिया गया। उस समय शातिर अपराधियों की पहचान के लिए बेहद बर्बर और अमानवीय तरीके प्रयोग में लाए जाते थे। किसी शातिर अपराधी को जब सजा पूरी होने पर जेल से छोड़ा जाता था तो उसके कंधों को गर्म सलाखों से दाग दिया जाता था ताकि उसकी पहचान आवश्यकता पड़ने पर की जा सके। हेनरी इस परंपरा से काफी आहत हुए और उन्होंने इसका विकल्प ढूंढने का निश्चय किया। 1892 में हेनरी ने *एंथ्रोपोमेट्रिक* पद्धति पर प्रयोग प्रारंभ किया जिसमें उन्होंने दसों अंगुलियों की माप और आंखों के रंग को सम्मिलित किया। जनवरी 1893 में हेनरी ने केवल छह अंगुलियों की माप को ही रिकॉर्ड के उपयुक्त पाया जिनमें बांया अंगूठा भी सम्मिलित था। इसमें बांयें अंगूठे के चिह्न को काफी महत्त्वपूर्ण माना गया क्योंकि अधिकतर व्यक्ति सीधे हाथ से अपने दैनिक कार्य निबटाते हैं जिस कारण दांये हाथ के अंगूठे की चिह्न अपेक्षाकृत अस्पष्ट होती है। अंगुलि-चिह्नों पर अपने ज्ञान को बढ़ाने के लिए हेनरी ने फ्रांसिस गाल्टन को एक पत्र लिखा, फलस्वरूप हेनरी और गाल्टन अच्छे मित्र बन गए और उन्होंने अंगुलि-चिह्न के अपने अनुभवों का आदान-प्रदान कर अंगुलि-चिह्न विज्ञान को काफी समृद्ध किया। 1894 में हेनरी अवकाश पर इंग्लैंड वापस आए और उन्होंने अपना पूरा समय गाल्टन के साथ उनकी प्रयोगशाला में बिताया। जब हेनरी वापस भारत पहुंचे तो वे एक ऐसे फार्मूले के विकास का निश्चय कर चुके थे जिसके आधार पर हजारों अंगुलि-चिह्नों को एक क्रम से संग्रहित किया जा सके।

भारत पहुंचने पर रिचर्ड हेनरी ने सभी कैदियों की दसों अंगुलियों के चिह्न (चिह्न) लेने को अनिवार्य कर दिया। उस समय हेनरी *एन्थ्रोपोमेट्रिक ब्यूरो* कलकत्ता में तैनात थे। यहीं हेनरी को दो भारतीयों अज़ीजुल हक और राय बहादुर हेम चन्द्र बोस का सक्रिय सहयोग प्राप्त हुआ। अज़ीजुल हक उस समय *एन्थ्रोपोमेट्रिक ब्यूरो* के प्रभारी अधिकारी थे जबकि हेम चन्द्र बोस उनके सहयोगी थे। वास्तव में अज़ीजुल हक और हेम चन्द्र बोस के अविस्मरणीय सहयोग और अथक

परिश्रम के कारण ही बाद में रिचर्ड हेनरी अंगुलि-चिह्न वर्गीकरण की एक नई पद्धति प्रतिपादित करने में सफल रहे। अत्यंत कठिन परिश्रम के बाद रिचर्ड हेनरी, अज़ीजुल हक और हेमचन्द्र बोस ने अंगुलि-चिह्नों को वर्गीकृत करने की एक अत्यंत सरल पद्धति का विकास किया। इसे दुर्भाग्य ही कहा जाएगा कि इस महान कार्य का तनिक सा भी श्रेय हेनरी ने अज़ीजुल हक और हेमचन्द्र बोस को नहीं दिया और उपरोक्त वर्गीकरण पद्धति 'हेनरी वर्गीकरण पद्धति' कहलायी। हेनरी ने इस वर्गीकरण पद्धति के सार-संक्षेप को एक शोध-पत्र *(फिंगर प्रिंट एंड डिटेक्शन ऑफ क्राइम इन इंडिया)* के रूप में ब्रिटिश एसोसिएशन की डोभर में आयोजित सभा (1899 ई.) में प्रस्तुत किया। तदुपरांत ब्रिटिश सरकार ने लॉर्ड बेल्पर की अध्यक्षता में 5 जुलाई, 1900 ई. में एक जांच समिति गठित की। बेल्पर समिति की सिफारिशों के आधार पर 1901 ई. में भारत की ब्रिटिश सरकार ने रिचर्ड हेनरी, अज़ीजुल हक और हेमचन्द्र बोस द्वारा विकसित अंगुलि-चिह्न वर्गीकरण पद्धति को विधिक मान्यता प्रदान कर दी। अपराधियों की पहचान हेतु विकसित यह पद्धति, अंगुलि-चिह्नों के वर्गीकरण एवं फाइलिंग (रिकॉर्डिंग) की 'हेनरी विधि' के नाम से लोकप्रिय है। भारत के साथ-साथ स्कॉटलैंड यार्ड और वेल्स ने भी 'हेनरी पद्धति' को अपना लिया। सर हेनरी ने इस पद्धति का प्रदर्शन 1905 ई. में अमेरिका में किया फलस्वरूप अमेरिका का सेंट लुइस मिसौरी के पुलिस विभाग ने भी व्यक्ति की पहचान स्थापित करने हेतु अंगुलि-चिह्न वर्गीकरण की 'हेनरी पद्धति' को अंगीकार कर लिया।

सैय्यद अज़ीजुल हक

आज समूचे विश्व में अंगुलि-चिह्न वर्गीकरण की जिस 'हेनरी पद्धति' को उपयोग में लाया जा रहा है उसका विकास करने का वास्तविक श्रेय एक भारतीय सैय्यद अज़ीजुल हक को ही है। जब रिचर्ड हेनरी अंगुलि-चिह्न विज्ञान पर अपने प्रयोग कर रहे थे तब एन्थ्रोपोमेट्रिक ब्यूरो, कोलकाता के प्रभारी अज़ीजुल हक और उनके एक सहयोगी हेमचन्द्र बोस ने अपना अमूल्य सहयोग उन्हें दिया। बाद में अज़ीजुल हक पूर्णतया अंगुलि-चिह्न विज्ञान को ही समर्पित हो गए और वे सर रिचर्ड एडवर्ड हेनरी के अधीन अंगुलि-चिह्न विज्ञान पर शोध कार्यों में जुट गए।

उस समय के पुलिस उप-निरीक्षक सैय्यद अज़ीजुल हक की गणित तथा ज्यामिती में विशेष रुचि थी। अपने अथक परिश्रम, लगन और गणित के गहरे ज्ञान के आधार पर अज़ीजुल हक ने दोनों हाथों की सभी 10 अंगुलियों के वर्गीकरण का एक सूत्र खोज निकाला जिसका संपूर्ण श्रेय वरिष्ठ अंग्रेज अधिकारी होने के नाते रिचर्ड हेनरी ने ले लिया। अज़ीजुल हक ने 10 अंगुलियों के 5 जोड़ों हेतु 5 अंकों का निर्धारण किया और 16, 8, 4, 2 एवं 1 अंक देकर 16+8+4+2+1=31, और फिर इस 31 में एक जोड़ कर 31+1=32×32=1024 छोटे खण्डों (पिजन होल्स) में वर्गीकृत, अंगुलि-चिह्न पत्रों को रिकॉर्ड (संग्रहीत) करने की पद्धति विकसित की। अज़ीजुल हक की इसी रूपरेखा के आधार पर 1/1 से लेकर 32/32 के प्राथमिक समूहों के वर्गीकरण की पद्धति ने रूप ग्रहण किया।

अज़ीजुल हक द्वारा विकसित इस वर्गीकरण और संग्रहण (फाइलिंग) पद्धति का सबसे महत्त्वपूर्ण लाभ यह था कि हजारों अंगुलि-चिह्न पत्रों (फिंगर प्रिंट स्लिप) को आसानी से संग्रहित किया जा सकता था और आवश्यकता पड़ने पर किसी पत्रक (स्लिप) विशेष को बहुत आसानी से वापस निकाला (रिट्राइव) जा सकता था। केन्द्रिय अंगुलि-चिह्न ब्यूरो (C.F.P.B.) सहित विश्व के अधिकतर अंगुलि-चिह्न ब्यूरो में आज भी अज़ीजुल हक की इसी पद्धति के आधार पर अंगुलि-चिह्न स्लिपों को संग्रहित (फाईल) किया जाता है।

अज़ीजुल हक द्वारा विकसित 'हेनरी वर्गीकरण पद्धति' से पूर्व सर फ्रांसिस गाल्टन द्वारा भी एक वर्गीकरण पद्धति प्रस्तुत की गई थी लेकिन गाल्टन की इस पद्धति को ट्रूप-कमेटी (Troop Committee) ने अस्वीकार कर दिया था क्योंकि गाल्टन द्वारा प्रस्तावित इस पद्धति में प्राथमिक-वर्गीकरण' का सर्वथा अभाव था। 1894 में गाल्टन द्वारा प्रस्तावित पद्धति की कमियों को अज़ीजुल हक की पद्धति ने बिल्कुल दूर कर दिया था। बाद में अज़ीजुल हक की वर्गीकरण प्रणाली को अधिक सरल, सुगम व सुविधाजनक बनाने की दृष्टि से सभी अंगुलि-चिह्नों को 4 मुख्य वर्गों में विभाजित किया गया आर्च (arch), लूप (loop), व्हर्ल (whorl) और कम्पोजिट (Composite)। प्रारंभ में इस पद्धति के आधार पर वर्गीकरण तथा संग्रहण में कुछ कठिनाइयां आईं लेकिन अज़ीजुल हक और हेमचन्द्र बोस ने अपने अथक परिश्रम से इन प्रारंभिक कठिनाइयों को भी दूर कर दिया।

हम पढ़ चुके हैं कि विश्व का सबसे पहला 'अंगुलि-चिह्न ब्यूरो' कोलकाता (भारत) में ही स्थापित किया गया था। इस ऐतिहासिक ब्यूरो की स्थापना में भी अज़ीजुल हक ने अपना अविस्मरणीय योगदान दिया। सर रिचर्ड हेनरी, अज़ीजुल हक और हेमचन्द्र बोस के सामूहिक प्रयासों के चलते विश्व का सबसे पहला अंगुलि-चिह्न ब्यूरो, कोलकाता की 'राइटर्स बिल्डिग' में 12 जून, 1897 को स्थापित किया गया। अंगुलि-चिह्न विज्ञान में अज़ीजुल हक के महत्त्वपूर्ण योगदान को देखते हुए 1900 ई. में अज़ीजुल हक को उप-निरीक्षक से प्रोन्नत कर निरीक्षक बना दिया गया। फिर सराहनीय सेवाओं के लिए 1909 ई. में अज़ीजुल हक को भारत सरकार ने पुरस्कारस्वरूप सोने की घड़ी और गले की चेन भेंट की और उन्हें उपाधीक्षक (डी.एस. पी.) के रूप में पदोन्नति दे दी गई जो उस समय किसी भी भारतीय के लिए असाधारण गौरव की बात थी।

सैय्यद अज़ीजुल हक ने अपना संपूर्ण जीवन अंगुलि-चिह्न विज्ञान को ही समर्पित कर दिया था। इसके एवज में तत्कालीन ब्रिटिश सरकार ने उन्हें 1913 में 'खान साहब' की महत्त्वपूर्ण उपाधि से नवाजा। सेवानिवृत्ति के बाद 3 जून, 1924 को ब्रिटिश सरकार ने उन्हें 'खान बहादुर' की अत्यंत प्रतिष्ठित उपाधि प्रदान की। इसके बाद 11 नवंबर, 1926 को अज़ीजुल की विशिष्ठ सेवाओं के बदले उन्हें ब्रिटिश सरकार ने 5000 रुपये का नकद पुरस्कार दिया जो एक 'पराधीन' देश के नागरिक के लिए उस समय सर्वोत्तम पुरस्कार था।

स्वतंत्र भारत की सरकार भी अज़ीजुल हक के महत्त्वपूर्ण योगदान को भूली नहीं और 27 अप्रैल, 1988 को केंद्रिय अंगुलि-चिह्न ब्यूरो, कोलकाता के रिकॉर्ड-हॉल में स्वर्गीय अज़ीजुल हक के रंगीन तैल-चित्र का अनावरण किया गया। केंद्रीय अंगुलि-चिह्न ब्यूरो द्वारा प्रतिवर्ष आयोजित 'ऑल इंडिया बोर्ड एग्जामिनेशन फॉर फिंगरप्रिंट एक्सपर्टशिप' परीक्षा में सर्वाधिक अंक प्राप्त करने वाले पुलिस अधिकारी को अज़ीजुल हक की पुण्य स्मृति में 'खान बहादुर स्मृति शील्ड' भी प्रदान की जाती है। सैय्यद अज़ीजुल हक ने अपना संपूर्ण जीवन अंगुलि-चिह्न विज्ञान के संवर्द्धन को समर्पित कर दिया था इसलिए उन्हें 'भारतीय अंगुलि-चिह्न विज्ञान का जनक' कहा जाता है।

राय बहादुर हेमचन्द्र बोस

हेमचन्द्र बोस, खान बहादुर अज़ीजुल हक के सहायक के रूप में 'एन्थ्रोपोमैट्रिक ब्यूरो', कोलकाता में तैनात थे। जब रिचर्ड हेनरी लोअर बंगाल के पुलिस महानिदेशक थे तब हेमचन्द्र बोस ने अपने प्रभारी अधिकारी अज़ीजुल हक के साथ मिलकर रिचर्ड हेनरी को अंगुलि-चिह्न विज्ञान संबंधी शोध कार्यों में महत्त्वपूर्ण सहयोग दिया जिसके फलस्वरूप हेनरी की वर्गीकरण-पद्धति, उप-वर्गीकरण पद्धति और सूक्ष्म खंडों (पिजन होल्स) द्वारा रिकॉर्डिंग की पद्धतियां प्रकार में आईं। अंगुलि-चिह्न विज्ञान में अपने वर्षों के अनुभव के आधार पर हेमचन्द्र बोस ने अंगुलि-चिह्न विज्ञान पर एक महत्त्वपूर्ण पुस्तक की भी रचना की जो *'फिंगर प्रिंट कम्पैनियन'* के नाम से 1927 में प्रकाशित हुई। उनकी एक अन्य पुस्तक *'क्लासिफिकेशन ऑफ ए सिंगिल डिजिट इम्प्रेशन'* नामक शीर्षक से 1924 में प्रकाशित हुई। अंगुलि-चिह्न विज्ञान में अविस्मरणीय योगदान के लिए ब्रिटिश सरकार ने हेमचन्द्र बोस को ***'रायबहादुर'*** की उपाधि से भी सम्मानित किया।

सलिल कुमार चटर्जी

प्रसिद्ध अंगुलि-चिह्न विज्ञानी सलिल कुमार चटर्जी का नाम अंगुलि-चिह्न विज्ञान के इतिहास में बेहद सम्मान के साथ लिया जाता है। अंगुलि-चिह्न विशेषज्ञ के रूप में सलिल कुमार चटर्जी ने अनुभव किया कि किसी व्यक्ति की दसों अंगुलियों के चिह्नों (निशानों) का रिकॉर्ड रखना काफी मुश्किल और श्रमसाध्य कार्य है इसलिए वे किसी अपेक्षाकृत सरल वर्गीकरण पद्धति की खोज में लग गए। चटर्जी की मेहनत 1960 में रंग लाई जब उन्होंने 'मध्यमा अंगुलि-चिह्न' के आधार पर एक नयी पद्धति का आविष्कार किया। मध्यमा अंगुलि-चिह्न वर्गीकरण पद्धति से संबंधित उनके शोध-पत्र पर, मैड्रिड में आयोजित इंटरपोल की बैठक में चर्चा की गई और विश्वभर के पुलिस अधिकारियों ने चटर्जी के शोध-कार्य की प्रशंसा की। बाद में सलिल कुमार चटर्जी ने रिकॉर्डिंग के उद्देश्य से आर्च पैटर्न को दस समूहों में वर्गीकृत करने की विधि विकसित की।

केंद्रिय अंगुलि-चिह्न ब्यूरो, कोलकता के निदेशक के रूप में सलिल कुमार चटर्जी ने एक और महत्त्वपूर्ण तथ्य उद्घाटित किया। एक शोध-पत्र में चटर्जी ने बताया कि अंगुलियों की रिजों के किनारों के अपने अलग विशिष्ट लक्षण होते हैं जो जीवनपर्यंत अपरिवर्तित रहते हैं। उन्होंने कहा कि रिजों के इन किनारों के आधार पर भी किसी व्यक्ति की पहचान स्थापित की जा सकती है। सलिल कुमार चटर्जी ने इस नये विज्ञान को 'ऐजोस्कोपी' (Edgeoscopy) नाम दिया। उनका यह महत्त्वपूर्ण शोध-पत्र, शिकागो (अमेरिका) की *'फिंगरप्रिंट एंड आइडेंटिफिकेशन मैगजीन'* में सितंबर, 1962 को प्रकाशित हुआ था।

अंगुलि चिह्न का अर्थ

अपनी हथेली को देखिए। इस पर बहुत सी रेखाएं उभरी हुई दिखाई देती हैं जो एक विशेष पैटर्न में सजी होती हैं। इन रेखाओं को पैपीलरी रिज कहते हैं। दो रेखाओं के बीच में एक गहरी रेखा होती है जिसे खांच (फुरो) कहते हैं। इसे समझने के लिए आलू के खेत को प्रतीकात्मक उदाहरण के रूप में ले सकते हैं। आलू के खेत में पास-पास मिट्टी की मेढ़ें बनाई जाती हैं। जिस प्रकार आलू के खेत में उभरी हुई मेढें होती हैं ठीक उसी प्रकार हमारी हथेली और तलवे की त्वचा पर उभरी हुई रेखाएं, पैपीलरी रिज कहलाती हैं।

मानव-भ्रूण का बारीकी से अध्ययन करने पर पता चलता है कि गर्भ के चौथे महीने से ही इन रघीनों या रिजों के बनने की प्रक्रिया प्रारंभ हो जाती है और गर्भ के छठवें माह में ये रिजें पूर्णतया विकसित हो जाती हैं और ये अपना एक विशिष्ट विन्यास ग्रहण कर लेती हैं। इस प्रकार स्पष्ट है कि किसी व्यक्ति के अंगुलि चिह्न, उसके जन्म से पहले ही निर्धारित हो जाते हैं, विकसित हो जाते हैं। गर्भ के छठे महीने में ही बन चुकी ये रिजें, जीवन-पर्यंत व्यक्ति का साथ नहीं छोड़ती हैं और इन्हें किसी भी रासायनिक, भौतिक, चिकित्सीय या किसी अन्य विधि द्वारा न तो परिवर्तित किया जा सकता है और न ही इनके विन्यास को बदला जा सकता है। इन रिजों के विन्यास की एक अनोखी विशेषता, इनका अनन्य और अद्वितीय होना है अर्थात किसी व्यक्ति की रिजों का विन्यास अपने आप में अनूठा होता है और पूरी पृथ्वी

चित्र : सीधे (प्लेन) अंगुलि चिह्न

चित्र : घुमावदार (रोल्ड) अंगुलि चिह्न

के व्यक्तियों में से किसी का भी रिज-विन्यास ऐसा नहीं होता है। रिज-विन्यास की इसी विशिष्टता के कारण अंगुलि चिह्न विज्ञान, व्यक्तिगत पहचान का सबसे प्रभावी और कारगर माध्यम माना जाता है।

आम बोलचाल की भाषा में अंगुलियों की रिजों के चिह्न को ही 'अंगुलि चिह्न' कहा जाता है लेकिन अंगुलि चिह्न विज्ञान और न्यायालयिक विज्ञान (फॉरेंसिक साइंस) की दृष्टि से यह परिभाषा अपूर्ण है। न्यायालयिक विज्ञान की आदर्श परिभाषा के अनुसार कोई भी अंगुलि चिह्न तब तक अनुपयोगी और अपूर्ण ही माना जाएगा जब तक उसमें अंगुलि चिह्न वर्गीकरण और तुलना (मिलान) के लिए आवश्यक दो निश्चित बिंदु, ***'डेल्टा'*** और ***'कोर'*** न हों। उपरोक्त चर्चा से स्पष्ट है कि अंगुलि चिह्न वास्तव में अंगुलियों की रिजों (रघीने या उभरी हुई रेखाएं) की चिह्न ही होते हैं। इसलिए अंगुलि चिह्नों को अच्छी तरह से समझने के लिए इन रिजों को समझना अत्यंत आवश्यक है।

रिजों की उत्पत्ति और विकास के संबंध में प्रो. हेरिस वेल्डर, डा. ए. कोलमन, डा. हेराल्ड कुम्मनिस और वर्ट वेन्टवर्थ द्वारा किए गए शोध, अध्ययन और वैज्ञानिक परीक्षण काफी महत्त्वपूर्ण सिद्ध हुए हैं और इन वैज्ञानिक शोधों के कारण अंगुलि चिह्न विज्ञान को नई दिशा मिली है और इनके कारण इस महत्त्वपूर्ण विज्ञान के कई नये आयाम उद्घाटित हुए हैं। प्रो. हेरिस वेल्डर के अनुसार प्रत्येक व्यक्ति के रिज लक्षण, अपने आप में विशिष्ट और अनूठे होते हैं। मानव-भ्रूण का अत्यंत सूक्ष्मता से अध्ययन करने पर प्रो. हेरिस वेल्डर ने बताया कि गर्भ के चौथे महीने से ही इन रिजों के निर्माण की प्रक्रिया प्रारंभ हो जाती है जो गर्भ के छठे महीने तक चलती रहती है। इस प्रकार व्यक्ति के जन्म से लगभग तीन माह पूर्व ही उसकी अंगुलियों की रिजों का विन्यास एक विशिष्ट स्वरूप ग्रहण कर लेता है। इसी क्रम में जीव-विज्ञानी वर्ट वेन्टवर्थ ने बताया कि भ्रूण के विभिन्न अंगों में ये रिजें धीरे-धीरे, अलग-अलग समय में बनती हैं। सबसे पहले हथेली पर रिजें बनती हैं और फिर पैर के तलवों पर इनका निर्माण होता है। हथेली के विभिन्न भागों पर भी रिजों का निर्माण अलग-अलग किन्तु निश्चित समय पर होता है। सबसे पहले अंगुलियों की पोरों पर ये रिजें बननी प्रारंभ होती हैं जो धीरे-धीरे पूरी हथेली पर फैल जाती हैं। ठीक इसी प्रकार

पैरों में भी पहले अंगुलियों की पोरों पर पैपीलरी रिजें बनती हैं, तत्पश्चात समूचे तलवे पर ये रिजें एक विशिष्ट विन्यास में विन्यासित हो जाती हैं।

भ्रूण के छठे महीने में ही रिजों का विन्यास निश्चित हो जाता है जो जीवन-पर्यंत अपरिवर्तित रहता है। जैसे-जैसे भ्रूण का और फिर शिशु का विकास होता है, इन रिजों का क्षेत्रफल और आकार भी बढ़ता जाता है लेकिन आश्चर्यजनक तथ्य यह है कि रिजों की आकृति, संख्या और विन्यास में कोई परिवर्तन नहीं होता है। हम जानते हैं कि प्रकृति में प्रत्येक वस्तु और प्रत्येक घटना का अपना महत्त्व और कुछ न कुछ उपयोग होता है। मानव शरीर का प्रत्येक अंग और सभी अंगों का प्रत्येक अंश, किसी न किसी विशेष कार्य के लिए ही निर्मित हुआ होता है। हमारे नाखूनों, बालों और यहां तक कि अत्यंत सूक्ष्म रोयों का भी कुछ न कुछ अर्थ होता है, कुछ न कुछ उपयोग होता है। अब सवाल उठता है कि अंगुलियों आदि पर पाए जाने वाली रिजों या रघीनों का क्या कार्य, क्या उपयोगिता है? शरीर-क्रिया-विज्ञान के अनुसार इन रिजों का प्रमुख और महत्त्वपूर्ण कार्य शरीर में उत्पन्न हुए पसीने को बाहर निकालना होता है। इनकी उपस्थिति के कारण अंगुलियों में एक विशेष प्रकार का खुरदरापन आ जाता है जिस कारण ये किसी वस्तु को मजबूती से पकड़ने और उसे फिसलने से रोकने में कारगर भूमिका अदा करते हैं।

अंगुलियों में उपस्थित इन रिजों के कारण ही अंगुलि चिह्न विज्ञान आज अस्तित्व में है क्योंकि इन्हीं के चिह्न को 'अंगुलि चिह्न' कहते हैं जिनकी सहायता से अपराधियों की पहचान संभव हो पाती है। न्यायालयिक-विज्ञान की परिभाषा के अनुसार रक्त, स्याही, रंग, पसीने, गंदगी या किसी अन्य पदार्थ की उपस्थिति के कारण किसी वस्तु पर रिजों के चिह्न ही 'अंगुलि चिह्न' कहलाते हैं।

प्रत्येक व्यक्ति के अंगुलि चिह्नों की अपनी विशिष्टता, अद्वितीयता, बेजोड़ बनावट और अनूठे विन्यास के कारण अंगुलि चिह्नों का अपराध-विज्ञान में एक महत्त्वपूर्ण स्थान है। किसी व्यक्ति की पहचान निर्धारित करने के लिए ये सबसे विश्वसनीय, प्रभावी, कारगर और अत्यंत सरल माध्यम हैं। अंगुलि चिह्न विज्ञान की दिनोंदिन बढ़ती लोकप्रियता का एक कारण इसका अन्य उपलब्ध विधियों की अपेक्षा सस्ता और सुविधाजनक होना भी है।

जीव विज्ञान की निगाह में अंगुलि चिह्न

व्यक्ति के अंगुलि चिह्नों की प्रकृति विशिष्ट होती है और जीवनपयंत इनके विन्यास में कोई अंतर नहीं आता है। इन अंगुलि चिह्नों का निर्माण व्यक्ति के जन्म से पूर्व ही हो जाता है। प्रो. हेरिस वेल्डर और वर्ट वेन्टवर्थ के अनुसार अंगुलियों की रिजें, गर्भ के चौथे महीने से ही बनने लगती हैं और गर्भावस्था के छठे महीने तक इन रिजों का निर्माण पूरा हो जाता है। इसी दौरान ये रिजें एक विशिष्ट विन्यास में विन्यासित हो जाती हैं जो विन्यास जीवनपर्यंत अपरिवर्तित रहता है।

यदि सूक्ष्मता से निरीक्षण किया जाए तो पता चलता है कि मानव की अंगुलियों पर दो प्रकार की रचनाएं पाई जाती हैं रेखाएं और रन्ध्र। इन रेखाओं और रन्ध्रों के आधार पर ही किसी व्यक्ति विशेष के विशिष्ट और अद्वितीय 'अंगुलि चिह्न' बनते हैं। ये रेखाएं (Ridge) और रन्ध्र (Pores), अंगुलि चिह्न विज्ञान की दृष्टि से अत्यंत महत्त्वपूर्ण हैं।

रिज अथवा रघीने

मनुष्य के हाथों की हथेली और अंगुलियों तथा पैरों के तलवे और अंगुलियों पर एक विशेष प्रकार की त्वचा पाई जाती है। यह त्वचा, अन्य भागों पर पाई जाने वाली त्वचा से सर्वथा भिन्न होती है। इस विशेष प्रकार की त्वचा पर रोम या बाल नहीं होते हैं लेकिन इसका रंग अपेक्षाकृत हल्का होता है।

मानव-विकास विज्ञान के अनुसार अंगुलियों की रिजें, भ्रूणावस्था में ही, गर्भ के चौथे माह से ही बननी प्रारंभ हो जाती हैं और गर्भ के छठे माह तक इनका विकास पूर्ण हो जाता है। एक बार इनका निर्माण पूरा हो जाए तो जीवनपर्यंत ये अपरिवर्तित रहती हैं। इन्हें किसी भी भौतिक, जैविक या रासायनिक विधि द्वारा बदला नहीं जा सकता है। भ्रूण में ये रिजें सभी स्थानों पर एक साथ न बनकर अलग-अलग समय में बनती हैं। पैरों की अपेक्षा हाथों में ये रिजें पहले बनती हैं। ठीक इसी प्रकार हथेली या तलवे की अपेक्षा अंगुलियों के पोरों पर ये रिजें पहले बनना शुरू होती हैं। इस प्रकार अंगुलियों

के पोरों से इन रिजों का विकास हथेली या तलवे की ओर होता है।

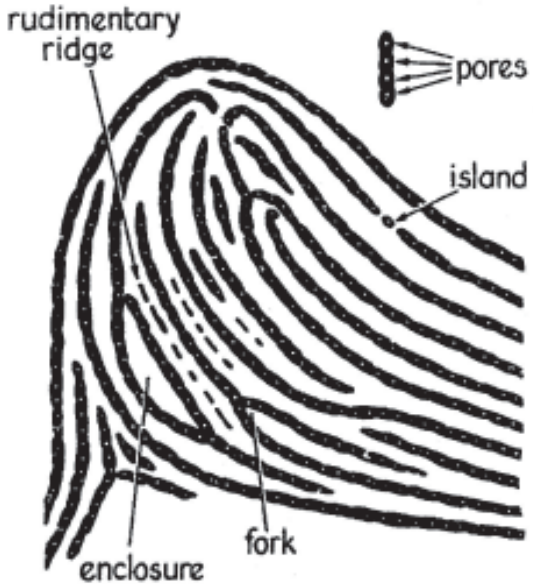
हथेली, तलवे और अंगुलियों की त्वचा पर दिखाई देने वाली लम्बी, आड़ी-तिरछी और गोलाकार रेखाएं ही रिज कहलाती हैं। 'रिज' एक अंग्रेजी शब्द है और इसका हिन्दी पर्याय 'रघीना' है (लेकिन हिन्दी भाषा में भी रिज शब्द ही अधिक लोकप्रिय है इसलिए भाषायी कट्टरता को छोड़ते हुए इस पुस्तक में सभी जगह रघीने के स्थान पर रिज शब्द का ही प्रयोग किया गया है ताकि पुस्तक को अधिक सुग्राह्य और सरल रूप दिया जा सके।) अंगुलियों से हथेली या तलवे की ओर बनने वाली ये रिजें, एक विशिष्ट विन्यास में विन्यासित हो जाती हैं। निर्माण और विकास शैली के कारण ही ये रिजें एक विशिष्ट विन्यास ग्रहण करती हैं। कभी-कभी ये रिजें दो भागों में बंट जाती हैं। जब रिज दो भागों में बंटती है तो सामान्यतः उसके दो रूप बन सकते हैं। पहले रूप में, दो भागों में विभाजित रिजें आगे चलकर पुनः परस्पर मिल जाती हैं जिससे एक 'द्वीप' जैसी रचना बन जाती है। इसी प्रकार दो भागों में बंटी रिजें जब परस्पर पुनः नहीं मिलती हैं और प्रत्येक रिज अपना स्वतंत्र रूप ग्रहण कर लेती है तो 'चिमटे' जैसी रचना बन जाती है। रिज विन्यास की इन विशेष बनावटों या विशेषताओं का ही उपयोग, अंगुलि-चिह्नों के मिलान करने में किया जाता है। रिजों की इन्हीं विशिष्टताओं के आधार पर ही दो अंगुलि चिह्नों में समरूपता या विरूपता स्थापित की जाती है।

प्राकृतिक नियम है कि कोई भी दो वस्तुएं पूर्णतया एक समान नहीं हो सकतीं, उनमें कुछ न कुछ अंतर अवश्य होता है। यहां तक कि घास के दो समान दिखने वाले तिनके, दो समान दिखने वाले फूल या दो समान दिखने वाले कुत्ते के पिल्ले भी कहीं न कहीं, कुछ न कुछ भिन्नता अवश्य रखते हैं। यह देखा गया है कि जैसे-जैसे एक नवजात शिशु धीरे-धीरे परिपक्व पुरुष या स्त्री में बदलता है, उसकी रिजों का क्षेत्रफल भी बढ़ता जाता है लेकिन रिजों के विन्यास व स्वरूप में कोई अंतर नहीं आता। यदि किसी नवजात शिशु के अंगुलि-चिह्नों को 60-70 वर्ष बाद वृद्धावस्था में प्राप्त अंगुलि-चिह्नों से मिलाकर देखा जाए तो कोई भी अंगुलि-चिह्न विशेषज्ञ, रिज-विशिष्टताओं के आधार पर तत्काल बता देगा कि वे एक ही व्यक्ति के अंगुलि-चिह्न हैं। इस संबंध में सर्वप्रथम विलियम हरशेल ने बताया था। विलियम हरशेल ने 30 वर्षों के अंतराल पर स्वयं अपनी

हथेली के दो चिह्न लिए और उनमें एक समान रिज-विशिष्टताएं पाईं।

अब प्रश्न यह है कि इन रिजों की उपयोगिता क्या है, प्रकृति ने इनकी रचना क्यों की? हम जानते हैं कि हमारे शरीर की आंतरिक गंदगी पसीने के रूप में बाहर निकलती है। शरीर का तापक्रम स्थिर बनाए रखने में भी पसीने की महत्त्वपूर्ण भूमिका होती है। हाथ तथा पैरों पर पाई जाने वाली रिजें, वास्तव में पसीना निकालने वाली नलिकाओं का मुख होती हैं। इस प्रकार इन रिजों का प्राकृतिक उद्देश्य शरीर की गंदगी को पसीने के माध्यम से बाहर उत्सर्जित करना होता है। इसके अतिरिक्त किसी वस्तु को मजबूती से पकड़ने में भी ये रिजें कारगर सिद्ध होती हैं। चूंकि रिजों की उपस्थिति के कारण हाथों में एक विशेष प्रकार का खुरदरापन आ जाता है इसलिए किसी चिकनी वस्तु को हाथों से फिसलने से रोकने में ये रिजें महत्त्वपूर्ण भूमिका निभाती हैं।

जब हम अपनी हथेली या अंगुलियों को किसी वस्तु से स्पर्श कराते हैं तो पसीने की उपस्थिति के कारण रिजों (रघीनों) के चिह्न उस वस्तु पर लग



चित्र : रिजों में पोरों की स्थिति

जाते हैं जो 'अंगुलि चिह्न' या 'हथेली चिह्न' कहलाते हैं। न्यायालयिक विज्ञान की परिभाषा के अनुसार अंगुलियों के छोरों पर उपस्थित रिजों की बनावट तथा विन्यास का स्याही, रक्त, रंग, गंदगी, नमी, चिकनाहट या पसीने आदि की सहायता से वस्तु पर अंकित होना ही 'अंगुलि चिह्न' कहलाता है। जब हम छपाई की स्याही से किसी व्यक्ति के अंगुलि चिह्न लेते हैं तो इस प्रक्रिया में स्याही, उभरी हुई रिजों से लग जाती है और दो रिजों के बीच में उपस्थित नलियां, स्याही से अछूती रह जाती हैं। इन स्याही युक्त अंगुलियों के चिह्न जब सफेद कागज आदि पर लिए जाते हैं तो अंगुलि चिह्न की काली रेखाएं इन रिजों को ही प्रदर्शित करती हैं जबकि सफेद रेखाएं (रिक्त रेखाएं), नलियों (Furrows) का प्रतिनिधित्व करती हैं। वास्तव में रिजों को प्रदर्शित करने वाली काली रेखाओं की विशिष्टताओं के आधार पर ही अंगुलि चिह्नों का वर्गीकरण या उनका मिलान किया जाता है।

हमारा पूरा शरीर त्वचा के द्वारा एक आवरण में बंद रहता है। हथेली, तलवे और सभी अंगुलियों की त्वचा अपने आप में विशिष्ट तथा अलग किस्म की होती है। यह विशिष्टता, रिजों की उपस्थिति के कारण होती है। चूंकि ये रिजें हथेली और वस्तु के बीच घर्षण पैदा करके वस्तु को हाथ से फिसलने से रोकती हैं इसलिए रिजों की उपस्थिति वाली हथेली और तलवे की त्वचा को 'घर्षण त्वचा' (Friction Skin) कहते हैं और ये रिजें, 'घर्षण रघीने' (Friction Ridge) कहलाती हैं। इन रिजों की बनावट और विन्यास अपने आप में अनूठा होता है। अक्सर ये रिजें दो या तीन भागों में विभाजित हो जाती हैं। विभाजन के बाद कभी तो ये रिजें पुनः परस्पर मिल जाती हैं तो कभी प्रत्येक नयी रिज अपना स्वतंत्र अस्तित्व ग्रहण कर लेती है। इस प्रकार चिमटाकार, द्वीपाकार या गोलाकार रचनाएं बन जाती हैं। ये विशिष्ट प्रकार की रचनाएं 'गाल्टन विवरण' (Galton details) कहलाती हैं।

अपराधों की रोकथाम में अंगुलि चिह्नों का प्रयोग

यह अंगुलि चिह्नों का महत्त्व ही है कि इनका उपयोग विभिन्न रूपों में सदियों से किया जा रहा है। न्यायिक प्रक्रिया में अपराधी की पहचान स्थापित करने के लिए तो हथेली और अंगुलि की रेखाओं का उपयोग किया ही जाता

है साथ ही इनके सहारे भविष्यवाणी भी की जाती है। ज्योतिष शास्त्र में अंगुलियों तथा हथेली की रेखाओं के आधार पर ही सटीक भविष्यवाणियां कर दी जाती हैं। विभिन्न वस्तुओं पर अंगुलि चिह्न अंकित करना एक अत्यंत प्राचीन प्रथा है। प्रागैतिहासिक काल के मिट्टी के बर्तनों और पक्की मिट्टी की मूर्तियों पर हाथ तथा अंगुलियों के चिह्न (चिह्न) पाए गए हैं। पुरातत्वविद कर्नल मैलारी ने नोवास्कोसिया पर्वत-श्रृंखला की चोटी पर इसी प्रकार की प्रागैतिहासिक काल की मिट्टी की मूर्तियां प्राप्त की हैं। इन मूर्तियों पर अंगुलि चिह्न किस उद्देश्य से लिए गए, इस बारे में कर्नल मैलोरी कुछ बता तो नहीं पाए लेकिन तय है कि इनका कुछ विशेष महत्त्व रहा होगा।

आधुनिकता के इस युग में व्यक्ति की इच्छाएं असीमित हो गई हैं और वह रातों-रात धनवान बनकर समस्त ऐशो-आराम पा लेना चाहता है। लोगों की मानसिकता में इस परिवर्तन के कारण भारत सहित समूचे विश्व में अपराधों की संख्या और उनकी गंभीरता में लगातार वृद्धि हो रही है। अपराधियों द्वारा अपराध करने और अपनी पहचान छिपाने के नये-नये आयाम दिन-प्रतिदिन उद्घाटित हो रहे हैं। इस कारण पुलिस तथा अन्य जांच-एजेंसियों के उत्तरदायित्वों के साथ-साथ उन पर काम का दबाव भी अत्याधिक बढ़ गया है। अंगुलि चिह्न एक ऐसा विज्ञान है जिसकी सहायता से पुलिस की मजबूरियों को उसकी शक्ति में बदला जा सकता है।

कई बार ऐसी घटनाएं घट जाती हैं कि सत्यता जानते हुए भी जांच एजेंसियां और न्यायालय अपनी विधिक मजबूरी के चलते न्याय नहीं दे पाते हैं। अंगुलि चिह्नों के अधिकाधिक प्रयोग से इस प्रकार की घटनाएं रोकी जा सकती हैं। पिछले दिनों उत्तर प्रदेश में कुछ लोगों को सरकारी दस्तावेजों में भूलवश मृतक दर्ज कर लिया गया जबकि वे जीवित थे। मृतक घोषित इन जीवित लोगों ने राज्य सरकार से अपने को जीवित घोषित करने और 'जीवन प्रमाण-पत्र' जारी करने का अनुरोध किया ताकि वे अपनी आर्थिक गतिविधियां जारी रखते हुए अपना सामाजिक जीवन बिना किसी व्यवधान के व्यतीत कर सकें। सरकारी दस्तावेजों में दर्ज रिकॉर्ड की मजबूरी के चलते सरकार, पीड़ितों को न्याय देने में असमर्थ रही फलस्वरूप पीड़ितों ने 'मृतक संघ' बनाकर दिल्ली के जंतर-मंतर और लखनऊ में विधानसभा के समक्ष धरना-प्रदर्शन

किया। स्थिति यह है कि जीवित लोग अपने को जीवित सिद्ध करने के लिए भटक रहे हैं। यदि सभी प्रकार के सरकारी दस्तावेजों में अंगुलि चिह्न लेने आवश्यक कर दिए जाते और किसी व्यक्ति के 'मृत्यु- प्रमाणपत्र' में उसके (मृत शरीर) अंगुलि चिह्न अंकित करने को अनिवार्य बना दिया जाए तो उपरोक्त प्रकार के मामलों पर रोक लग सकती है।

इसी तरह का एक दूसरा मामला सांसद फूलनदेवी हत्याकांड में देखने को मिला। हत्याकांड के मुख्य अभियुक्त शेरसिंह राणा और रवीन्द्र सिंह ने पूर्व नियोजित योजना के तहत सांसद हत्याकांड के समय अपने स्थान पर दो अन्य व्यक्तियों को जेल भिजवा दिया ताकि हत्या के आरोप से बचा जा सके और अपने पक्ष में मजबूत *'एलीबाई'* प्रस्तुत की जा सके।

इन दोनों अभियुक्तों पर अवैध रूप से शराब रखने के जुर्म में आबकारी अधिनियम के तहत मुकदमा पंजीकृत था और ये जमानत पर छूटे हुए थे। हत्या करने से ठीक पूर्व इन दोनों ने अपनी जमानत तुड़वा ली और न्यायालय में अपने दो साथियों को अपने नाम-पतों के साथ प्रस्तुत कर दिया जिन्हें जेल भेज दिया गया। 25 जुलाई 2001 को हत्या करने के बाद दोनों अभियुक्तों ने फिर अपनी जमानतें करवा लीं फलस्वरूप उनके दोनों साथी रिहा हो गए। हत्या की चश्मदीद गवाह, सांसद की बहन मुन्नी देवी का दावा है कि शेर सिंह राणा और रविन्द्र सिंह ने ही उनकी बहन पर गोलियों की बौछार की और स्वयं हत्याभियुक्तों ने स्वीकार कर लिया था कि हत्या उन्होंने ही की थी। लेकिन न्यायालय और जेल के रिकॉर्ड के मुताबिक हत्या के समय दोनों अभियुक्त जेल में बंद थे। इस शातिर षड्यंत्र के कारण अभियोजन-पक्ष को काफी मुश्किलों का सामना करना पड़ा। यदि गिरफ्तारी के समय और जमानत प्रदान करते समय ही अंगुलि चिह्न लेने आवश्यक कर दिए जाएं और इन अंगुलि चिह्नों का मिलान जेल के भीतर कैदी को प्रवेश देते समय उसके अंगुलि चिह्नों से किया जाने लगे तो अपने स्थान पर किसी और को जेल भिजवाने की घटनाओं पर रोक लगाई जा सकती है।

वर्षों पूर्व ही वैज्ञानिक रूप से सिद्ध किया जा चुका है कि किसी व्यक्ति की व्यक्तिगत पहचान स्थापित करने में अंगुलि चिह्न ही सबसे सशक्त और अकाट्य माध्यम हैं। अपने सामाजिक जीवन में व्यक्ति को कई बार अपनी 'पहचान' सिद्ध करनी पड़ती है इसलिए अंगुलि चिह्नों का प्रयोग मात्र पुलिस

विभाग तक ही सीमित नहीं है। बहुधा देखा गया है कि कोई व्यक्ति किसी अन्य व्यक्ति के नाम पर विभिन्न प्रकार के लाभ उठा लेता है। फर्जी रूप से न्यायालयों में गवाही देना, फर्जी पासपोर्टों पर विदेश यात्रा करना, पेंशनर की मृत्यु के बाद भी किसी अन्य व्यक्ति द्वारा पेंशन प्राप्त करते रहना, फर्जी रूप से किसी की जमानत देना और किसी अन्य व्यक्ति को किसी अन्य के रूप में जेल भिजवा देना, ऐसे अपराध हैं जिन्हें ***'अंगुलिचिन्हविज्ञान'*** के व्यापक प्रयोग से रोका जा सकता है। फिलहाल निम्नलिखित मामलों में अंगुलि चिह्नों का सफलतापूर्वक प्रयोग किया जा रहा है :

(1) ऐसे अपराधियों की पहचान स्थापित करने में जिन्हें पूर्व में न्यायालय द्वारा दण्डित किया जा चुका हो और जिनके अंगुलि चिह्न केंद्रीय अंगुलि चिह्न ब्यूरो या राज्यों के ब्यूरो में अभिलेखित हों।

(2) घटनास्थल से अपराधियों के अंगुलि-चिह्न विकसित कर न्यायालय में उन्हें 'साक्ष्य' के रूप में प्रस्तुत करने में।

(3) जेल से फरार कैदियों की गिरफ्तारी में।

(4) अनाधिकृत व्यक्ति को देश में प्रवेश देने से रोकने में।

(5) अनाधिकृत व्यक्ति द्वारा किसी की पेंशन आदि प्राप्त करने से रोकने में।

(6) किसी अन्य व्यक्ति के नाम से शासकीय सेवा में नियुक्ति पाने से रोकने में।

(7) बैंक तथा डाकघरों से फर्जी व्यक्ति द्वारा धन-निकासी को रोकने में।

(8) किसी मामले में गिरफ्तार व्यक्ति के पुराने आपराधिक कुकृत्यों का पता लगाकर उसे सजा दिलवाने में।

(9) लावारिस शव की पहचान (यदि वह अपराधी रहा हो) स्थापित करने में।

उपरोक्त मामलों में पुलिस तथा अन्य जांच एजेंसियां, अंगुलि-चिह्न विज्ञान का उपयोग सफलतापूर्वक कर रही हैं और इसके कारण पुलिस की समस्याएं काफी कम हो गई हैं। इस महत्त्वपूर्ण और सर्वमान्य विज्ञान के उपयोग

और अनुप्रयोग असीमित हैं इसलिए जीवन के अन्य क्षेत्रों में भी इस विज्ञान के अनुप्रयोगों को लागू किया जा सकता है। निम्नलिखित क्षेत्र ऐसे हैं जिनमें अंगुलि-चिह्न द्वारा पहचान स्थापित करने को कानूनन अनिवार्य बना दिए जाने से उत्साहवर्द्धक नतीजे प्राप्त किए जा सकते हैं :

(1) कई मामलों में किसी व्यक्ति के स्थान पर कोई दूसरा व्यक्ति परीक्षा देते हुए पकड़ा जाता है। लाख कोशिशों के बावजूद ऐसे मामले होते रहते हैं और फर्जी व्यक्ति परीक्षा उत्तीर्ण भी कर लेता है। बिहार के सांसद शहाबुद्दीन के स्थान पर किसी और व्यक्ति ने एल.एल.बी. की परीक्षा दी और सांसद महोदय को उत्तीर्ण घोषित कर दिया गया। यदि शैक्षणिक तथा प्रतियोगी परीक्षाओं के आवेदन-पत्रों में अभ्यर्थी के हस्ताक्षरों के साथ-साथ उसके अंगूठे का निशान भी ले लिया जाएं तो इस तरह के फर्जी मामलों को पूर्णतया रोका जा सकता है।

(2) लोकतांत्रिक प्रक्रिया में चुनाव अत्यंत महत्त्वपूर्ण होते हैं लेकिन हमारे देश में फर्जी मतदान के कारण चुनावों की वैधता पर प्रश्नचिह्न लग गया है और जनता की लोकतांत्रिक प्रक्रिया में आस्था दिन-प्रतिदिन कम होती जा रही है। यदि 'मतदाता पहचान-पत्र' में धारक के अंगुलि-चिह्न भी अंकित कर दिए जाएं तो फर्जी मतदान पर नियंत्रण किया जा सकता है। लोकतंत्र में जनता का विश्वास बनाए रखने के लिए ऐसा किया जाना अति आवश्यक है। लोकतांत्रिक व्यवस्था को और अधिक निष्पक्ष बनाने के लिए अब प्रत्येक भारतीय नागरिक को 'राष्ट्रीय पहचान पत्र' दिए जाने की योजना प्रारंभ हो चुकी है। इस राष्ट्रीय पहचान पत्र पर अन्य विवरण के अतिरिक्त, धारक के अंगुलि चिह्न भी अंकित रहेंगे।

(3) विभिन्न जीवन बीमा कंपनियां (जैसे भारतीय जीवन बीमा निगम) यदि पॉलिसी-धारक के अंगुलि-चिह्न भी अपने रिकॉर्ड में रखें तो झूठी मृत्यु के आधार पर फर्जी दावों से मुआवजे की रकम प्राप्त करने को रोका जा सकता है।

(4) चिकित्सा प्रमाण-पत्र, मृत्यु प्रमाण-पत्र और जन्म प्रमाण-पत्रों में यदि अंगुलि-चिह्न लेने वैधानिक रूप से अनिवार्य कर दिए जाएं तो फर्जी दावों और फर्जी पेंशन प्राप्त करने के मामलों को रोका जा सकता है।

(5) पासपोर्टों (पारगमन-पत्र) पर भी अन्य विवरण के साथ-साथ धारक के अंगुलि-चिह्न भी अंकित किए जाने चाहिएं। इससे चित्र बदलकर गैर-कानूनी रूप से विदेश यात्रा करने वालों को नियंत्रित और दण्डित किया जा सकता है। कुछ देशों में ऐसा किया भी जा रहा है जिसके उत्साहवर्द्धक नतीजे मिल रहे हैं।

(6) यदि अस्पतालों और प्रसूतिगृहों में जन्म के तुरंत बाद ही शिशु के अंगुलि-चिह्न ले लिए जाएं तो अवैध संबंधों के चलते पैदा हुए अनचाहे शिशुओं को इधर-उधर कूड़ेदानों में फेंक देने की घटनाओं को रोका जा सकता है।

राष्ट्रीयपहचान-पत्रः भारत सरकार द्वारा एक अत्यंत महत्त्वाकांक्षी परियोजना पर कार्य किया जा रहा है जिसके अंतर्गत प्रत्येक भारतीय नागरिक को एक 'राष्ट्रीय पहचान पत्र' दिए जाने की योजना है। यह राष्ट्रीय पहचान-पत्र, एक 'स्मार्ट कार्ड' के रूप में होगा जिस पर धारक के अंगुलि चिह्न भी होंगे। इस योजना के क्रियान्वयन के बाद विभिन्न प्रकार के अपराधों की रोकथाम करना बेहद आसान हो जाएगा क्योंकि ऐसा होने पर कोई भी व्यक्ति अपनी वास्तविक पहचान नहीं छिपा सकेगा। भारत सरकार द्वारा प्रायोगिक आधार पर इस योजना का क्रियान्वयन प्रारंभ भी कर दिया गया है और देश का पहला 'राष्ट्रीय पहचान-पत्र', महामहिम राष्ट्रपति महोदया श्रीमती प्रतिभा देवीसिंह पाटिल को सौंपा भी जा चुका है।

प्रत्येक भारतीय नागरिक को जो राष्ट्रीय पहचान-पत्र दिया जाना है, उसमें एक 'माइक्रो प्रोसेसर चिप' लगा होगा, जिसकी क्षमता 16 के.बी. मेमोरी की होगी। इस पहचान-पत्र के न तो नकली पहचान-पत्र बनाए जा सकेंगे और न ही इनका प्रतिरूप (क्लोन) बनाना संभव होगा क्योंकि इस कार्ड को बनाने में अत्याधुनिक 'की-क्रिप्टोग्राफी' तकनीक का इस्तेमाल किया जाएगा। प्लास्टिक से निर्मित इस स्मार्ट कार्ड में धारक के निम्नलिखित विवरण दर्ज होंगे :

- ☆ राष्ट्रीय पहचान-पत्र संख्या (NIN)
- ☆ धारक का नाम व उपनाम
- ☆ लिंग
- ☆ पिता का नाम
- ☆ माता का नाम
- ☆ जन्म तिथि
- ☆ जन्म स्थान
- ☆ वैवाहिक स्थिति
- ☆ जीवन साथी (पति/पत्नी) का नाम
- ☆ निवास का वर्तमान पता
- ☆ स्थायी निवास का पता
- ☆ दिखाई देने योग्य पहचान का चिह्न
- ☆ धारक का डिजिटल चित्र
- ☆ अंगुलियों का बायोमैट्रिक विवरण
- ☆ पंजीकरण की तिथि
- ☆ जारी करने की तिथि

स्पष्ट है कि पहले अंगुलि चिह्नों का प्रयोग मात्र अपराध व अपराधी की पहचान तक ही सीमित था लेकिन आधुनिक युग में अंगुलि चिह्नों का इस्तेमाल, अपराधों की रोकथाम में भी किया जाने लगा है। अब बहुत से ऐसे उपकरण अस्तित्व में आ चुके हैं जिनमें अंगुलि चिह्नों का प्रयोग करके, अपराध को घटित होने से पहले ही रोका जा सकता है। वर्तमान समय में, अपराधों की रोकथाम में सबसे अधिक प्रयोग, विभिन्न बायोमैट्रिक उपकरणों व विधियों का किया जाता है। बायोमैट्रिक उपकरणों व विधियों में सबसे अधिक प्रयोग, अंगुलि चिह्नों का ही दुनियाभर में किया जाता है।

●

5

साइबर अपराध और प्रौद्योगिकी

साइबर का संबंध कंप्यूटर से जोड़ा जाता है लेकिन अपराध के संदर्भ में साइबर का संबंध सूचना प्रौद्योगिकी से है। इस प्रकार सूचना प्रौद्योगिकी से संबंधित सभी प्रकार के अपराध, साइबर-अपराध की श्रेणी में आते हैं। आज कंप्यूटर और सूचना प्रौद्योगिकी ने हमारे जीवन के प्रत्येक क्षेत्र में अपनी जगह बना ली है। कंप्यूटर, मोबाइल फोन, इंटरनेट, कंप्यूटरीकृत बैंकिंग, क्रेडिट व डेबिट कार्ड आदि का प्रयोग आज काफी बढ़ गया है। इन सूचना प्रौद्योगिकी संबंधित चीजों का प्रचलन बढ़ा है तो इनसे संबंधित अपराध भी अब प्रकाश में आने लगे हैं। सूचना प्रौद्योगिकी के अधिकाधिक प्रयोग के कारण यदि आज साइबर-अपराध के मामले बढ़े हैं तो सूचना प्रौद्योगिकी ने ही हमें वे उपकरण व तकनीक भी उपलब्ध कराई हैं, जिनकी सहायता से साइबर अपराधों की रोकथाम की जा सकती है।

बढ़तेसाइबरअपराध: भारत के आपराधिक परिदृश्य के लिए साइबर अपराध भले ही एक नई चीज हो परंतु विकसित देश पिछले काफी समय से साइबर अपराधों का दंश झेलने को अभिशप्त हैं। भारत में सूचना प्रौद्योगिकी का उपयोग बढ़ा है तो साइबर अपराधों के मामले भी अब प्रकाश में आने लगे हैं।

भारत में साइबर अपराध से संबंधित मामले सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत दर्ज किए जाते हैं। इसके अतिरिक्त भारतीय दंड संहिता की विभिन्न धाराओं के अंतर्गत भी साइबर-अपराध के मामले दर्ज किए जाते हैं। साइबर अपराध वर्ग के अंतर्गत अग्रलिखित प्रकार के अपराध आते हैं :

1. कंप्यूटर स्रोत से छेड़छाड़
2. कंप्यूटर तंत्र की हैकिंग
3. इलैक्ट्रॉनिक माध्यमों पर अश्लील प्रसारण/प्रकाशन
4. किसी कंप्यूटर तंत्र के डाटाबेस तक अनाधिकृत रूप से पहुंचना
5. संरक्षित कंप्यूटर तंत्र तक पहुंचने का प्रयास
6. गलत इलैक्ट्रॉनिक-हस्ताक्षरों का प्रकाशन
7. इलैक्ट्रॉनिक गोपनीयता भंग करना
8. इलैक्ट्रॉनिक निजता (प्राइवेसी) भंग करना
9. वेबसाइट हैकिंग
10. ई-मेल हैकिंग

क्र. सं.	*अपराध*	*दर्ज मामले*		
		2004	**2005**	**2006**
1.	कंप्यूटर से छेड़छाड़	2	10	10
2.	हैकिंग	26	74	59
3.	अश्लील प्रसारण	34	88	69
4.	कंप्यूटर तक अनाधिकृत पहुंच	0	0	0
5.	अनाधिकृत रूप से डिटिजल हस्ताक्षर प्राप्त करना	0	0	0
6.	गलत डिजिटल हस्ताक्षरों का प्रकाशन	0	1	1
7.	डिजिटल धोखाधड़ी	0	1	1
8.	निजता का उल्लंघन	6	3	3
	कुल	**68**	**179**	**142**

तालिका : विभिन्न साइबर अपराधों के कुल मामले

11. सामाजिक-वेबसाइटों पर किसी अन्य के विवरण से छेड़छाड़
12. इंटरनेट के जरिए किसी को धमकी देना
13. इंटरनेट के जरिए किसी की मानहानि करना
14. किसी अन्य के ई-मेल खाते का अनाधिकृत रूप से प्रयोग

15. वेबसाइट के जरिए बैंकिंग धोखाधड़ी

16. अश्लील *एस.एम.एस.* का प्रसारण

'क्राइम इन इंडिया' (राष्ट्रीय अपराध रिकार्ड ब्यूरो, गृह मंत्रालय) के आंकड़ों के मुताबिक सन् 2005 के दौरान सूचना प्रौद्योगिकी अधिनियम के अंतर्गत कुल 176 मामले दर्ज किए गए थे। सन् 2006 के दौरान साइबर अपराध से संबंधित इस अधिनियम के अंतर्गत कुल 142 मुकदमे, देशभर के थानों में दर्ज किए गए थे। सन् 2006 के दौरान दर्ज कुल 142 मामलों में से 35 मामले (कुल के 24.6 फीसदी) अकेले महाराष्ट्र राज्य में दर्ज किए गए थे। 27 मामलों के साथ कर्नाटक द्वितीय स्थान पर और 14 मामलों के साथ आंध्र प्रदेश, तीसरे स्थान पर रहा। केरल और पंजाब में सूचना प्रौद्योगिकी अधिनियम के अंतर्गत कुल 12-12 मामले दर्ज किए गए।

सूचना प्रौद्योगिकी अधिनियम के अंतर्गत दर्ज कुल मामलों में लगभग 47 फीसदी मामले (69 मामले) अकेले अश्लील प्रसारण/प्रकाशन (इलैक्ट्रॉनिक माध्यमों द्वारा) से संबंधित थे। इस तरह के मामलों को आमतौर पर *'साइबर पोर्नोग्राफी'* की संज्ञा दी जाती है। साइबर पोर्नोग्राफी से संबंधित अपराधों के सिलसिले में कुल 812 व्यक्तियों को वर्ष 2006 के दौरान गिरफ्तार किया गया। इस दौरान हैकिंग के कुल 59 मामले दर्ज किए गए और इस अपराध के लिए कुल 63 व्यक्तियों को गिरफ्तार किया गया। हैकिंग के अधिकतर मामले कर्नाटक, आंध्र प्रदेश और महाराष्ट्र में प्रकाश में आए। साइबर अपराधों के लिए सबसे अधिक आरोपी भी महाराष्ट्र राज्य में ही गिरफ्तार किए गए।

सूचना प्रौद्योगिकी अधिनियम के अतिरिक्त भारतीय दंड संहिता के अंतर्गत भी साइबर अपराध दर्ज किए जाते हैं। सन् 2005 के दौरान भारतीय दंड संहिता की विभिन्न धाराओं के अंतर्गत कुल 302 मामले दर्ज किए गए जबकि सन् 2006 के दौरान इस प्रकार के 311 मामले प्रकाश में आए। इस प्रकार सन् 2005 के मुकाबले सन् 2006 में भारतीय दंड संहिता के अंतर्गत दर्ज साइबर अपराधों में लगभग 3 प्रतिशत बढ़ोत्तरी दर्ज की गई। भारतीय दंड संहिता के अंतर्गत साइबर फर्जीवाड़े के कुल 160 मामले दर्ज किए गए। साइबर अपराधों के लिए भारतीय दंड संहिता की विभिन्न धाराओं के अंतर्गत सन् 2006 में कुल 411 व्यक्तियों को गिरफ्तार किया गया। हमारे देश में कुल 35 महानगर

हैं और इन 35 महानगरों में से 19 महानगरों में साइबर अपराध का एक भी मामला प्रकाश में नहीं आया था। महानगरों में सबसे अधिक साइबर अपराध के मामले बंगलुरु (27), राजकोट (10) और मुम्बई (9) में दर्ज किए गए।

इंटरनेटकाबढ़ताप्रयोग: आज अगर साइबर अपराध के मामलों में बढ़ोत्तरी दर्ज की जा रही है तो इसका बड़ा कारण इंटरनेट का लगातार बढ़ता इस्तेमाल भी है। अधिकतर साइबर अपराध इंटरनेट के जरिए ही होते हैं। इंटरनेट ने आज आम आदमी के जीवन में भी अपनी एक जगह बना ली है। इंटरनेट आज किसी वरदान से कम नहीं है। *'जस्ट कंसल्ट'* नामक एक शोध एजेंसी के मुताबिक भारत में कुल आबादी का लगभग 4.5 फीसदी भाग आज इंटरनेट का इस्तेमाल करता है। इस एजेंसी की एक रिपोर्ट के मुताबिक भारत में लगभग 25 मिलियन लोग ऐसे हैं जो प्रतिदिन इंटरनेट का इस्तेमाल करते हैं जबकि महीने में न्यूनतम एक बार इंटरनेट का इस्तेमाल करने वाले लोगों की संख्या लगभग 35 मिलियन है।

क्र. सं.	*इंटरनेट कार्य*	*प्रयोगकर्ता (% में)*
1.	ई-मेल भेजने के लिए	91%
2.	नौकरी तलाशने के लिए	72%
3.	चैटिंग हेतु	70%
4.	समाचार जानने के लिए	63%
5.	खेल कार्यक्रमों के लिए	57%
6.	संगीत/फिल्म डाउनलोड करने के लिए	54%
7.	विवाह/मित्रता हेतु	50%

तालिका : विभिन्न कार्यों हेतु भारत में इंटरनेट का प्रयोग

इंटरनेट के बढ़ते इस्तेमाल के कारण धोखाधड़ी के भी बहुत से मामले अब सामने आने लगे हैं। युवाओं में 'चैटिंग' की भी काफी लोकप्रियता है लेकिन अक्सर ऐसे मामले सामने आते रहते हैं जब 'चैटिंग' के जरिए किसी युवती से मित्रता की गई और फिर उसका शारीरिक शोषण किया गया। इसी प्रकार की धोखाधड़ी, वैवाहिक वेबसाइटों के जरिए विवाह करने के कुछ मामलों में भी

देखी गई है। आने वाले समय में इंटरनेट का इस्तेमाल गांव-गांव तक फैल जाएगा क्योंकि भारतीय प्रौद्योगिकी संस्थान, खड़गपुर के दो छात्रों ने 'क्रांति' *(कियोस्क इन रूरल एरियाज नेटवर्क एण्ड टेलीकम्यूनिकेशन्स इंफ्रास्ट्रक्चर)* नामक एक परियोजना प्रारंभ की है जिसके जरिए सुदूर हिस्सों तक को बेहद कम लागत में प्रभावशाली तरीके से आपस में जोड़ा जा सकेगा। इंटरनेट का इस्तेमाल बढ़ेगा तो निश्चित रूप से साइबर-अपराध के मामले भी बढ़ेंगे।

तकनीकएवंप्रौद्योगिकीतथाहैकिंगसेबचाव: हैकिंग को एक सबसे खतरनाक साइबर अपराध माना जाता है क्योंकि इसके जरिए किसी भी वेबसाइट से महत्त्वपूर्ण सूचनाएं व डाटा चुरा कर उनका इस्तेमाल विभिन्न प्रकार की आतंकवादी गतिविधियों और आपराधिक कृत्यों के लिए किया जा सकता है। हैकिंग का अर्थ है अनाधिकृत रूप से किसी भी वेबसाइट या ई-मेल खाते तक पहुंच कर उससे डाटा आदि चुरा लेना। हाल ही में राष्ट्रीय रक्षा अकादमी और रक्षा अनुसंधान एवं विकास संगठन के अनेक उच्चाधिकारियों के ई-मेल के पते विभिन्न देशों को पोस्ट कर दिए गए थे।

दरअसल इन अधिकारियों के ई-मेल खातों को हैक करके ही इस प्रकार का कृत्य किया गया था। दरअसल हैकर ने पी.ओ.पी. *(पोस्ट ऑफिस प्रोटोकाल)* के मेल-सर्वर की कुछ कमियों का लाभ उठाकर ऐसा किया था। यह एक बेहद संवेदनशील मामला है क्योंकि हैकिंग के जरिए किन्हीं दो अधिकारियों द्वारा ई-मेल द्वारा की जाने वाली बातचीत को भी जाना या सुना जा सकता है। सोचिए कि राष्ट्रपति और प्रधानमंत्री किसी महत्त्वपूर्ण मसले पर ई-मेल के जरिए सूचनाओं और आंकड़ों का आदान-प्रदान कर रहे हों और कोई हैकर इस सूचना को प्राप्त कर ले तो कितना बड़ा अनर्थ हो सकता है। इसी प्रकार राष्ट्रीय सुरक्षा से संबंधित दस्तावेजों को भी हैक किया जा सकता है।

वास्तव में हैकिंग आज के साइबर-युग की सबसे बड़ी समस्या है। हैकिंग के कारण पूरे सूचना-तंत्र को ध्वस्त किया जा सकता है, किसी कंप्यूटर तंत्र में उपस्थित डाटा को नष्ट किया जा सकता है अथवा इस डाटा को चुराया जा सकता है। हैकिंग के कारण किसी देश की सुरक्षा व्यवस्था भी खतरे में पड़ सकती है। किसी सॉफ्टवेयर में सेंध लगाने को भी हम हैकिंग का नाम दे सकते हैं। इस प्रकार मात्र हैकिंग द्वारा ही किसी बड़ी से बड़ी आतंकी घटना को

अंजाम दिया जा सकता है। उदाहरण के लिए, दिल्ली मेट्रो रेल कार्पोरेशन, मेट्रो रेल का परिचालन पूरी तरह से कंप्यूटरों के द्वारा ही करता है। यदि कोई दिल्ली मेट्रो रेल कार्पोरेशन के कंप्यूटर तंत्र को हैक कर ले तो पूरी व्यवस्था को ध्वस्त किया जा सकता है, दो मेट्रो रेलों को आपस में टकराया जा सकता है। इस प्रकार हैकर किसी भी अनहोनी को अंजाम दे सकते हैं।

हैकिंग एक बड़ी समस्या है तो तकनीक व प्रौद्योगिकी ने हमें इससे बचने के साधन भी उपलब्ध कराए हैं। कंप्यूटर तंत्र के सॉफ्टवेयर को फुलप्रूफ बनाकर उसे हैक होने से बचाया जा सकता है। हैकिंग से सुरक्षा प्राप्त करने के लिए आजकल काफी शोध व अनुसंधान कार्य चल रहे हैं। भारत की एक प्रमुख सूचना-प्रौद्योगिकी प्रमाणन कम्पनी, *'अप्पीन'* ने हैकिंग की रोकथाम करने के लिए एक बहुराष्ट्रीय कम्पनी *'इंटरटेक'* से समझौता किया है। समझौते के मुताबिक *'अप्पीन'* और *'इंटरटेक'* परस्पर मिलकर एक सॉफ्टवेयर बनाएंगे जो हैकिंग से कंप्यूटर-तंत्र की सुरक्षा करेगा। इस सुरक्षा-सॉफ्टवेयर को *'एपीपीएसईसी'* नाम दिया गया है। यह वास्तव में *'सॉफ्टवेयर एप्लीकेशन सिक्युरिटी सर्टिफिकेट'* होगा। यह सुरक्षा प्रमाण-पत्र प्रदान करने से पहले *'अप्पीन'* और *'इंटरटेक'* मिलकर सॉफ्टवेयर का 20 मानदंडों पर परीक्षण करेंगी। *'एपीपीएसईसी'* नामक इस सॉफ्टवेयर को संयुक्त राज्य अमेरिका, इंग्लैंड सहित लगभग सभी यूरोपियन देशों में मान्यता प्राप्त हैं।

सामाजिकसाइट्सकेअपराधऔरउनकीरोकथाम: सामाजिक साइट्स अर्थात् 'सोशल साइट्स' आज के युवाओं का सबसे प्रिय शगल है। इन्हें डेटिंग-साइट्स और मित्रता-साइट्स भी कहते हैं। दरअसल ये ऐसी वेबसाइट्स होती हैं जहां पर आप अपना व्यक्तिगत विवरण (नाम, पता, दूरभाष संख्या, शौक आदि) डाल कर लोगों से मित्रता कर सकते हैं, उनसे मेलजोल कर सकते हैं। ऐसी कुछ प्रमुख साइट्स निम्नलिखित हैं :

- ☆ ऑरकुट
- ☆ फेस बुक
- ☆ फ्रॉयर
- ☆ हाय 5
- ☆ बेबो

☆ माई स्पेस

☆ भारत स्टूडेंट

उपरोक्त सामाजिक साइटों के अलावा और भी सैकड़ों सामाजिक साइट्स आज इंटरनेट पर मौजूद हैं। इन साइटों पर मात्र एक विकल्प क्लिक करते ही आप जानकारियों और विचारों का आदान-प्रदान कर सकते हैं। इन साइटों पर किसी व्यक्ति विशेष के विवरण को *'प्रोफाइल'* कहा जाता है। सामाजिक साइटों के संदर्भ में आज की सबसे बड़ी दिक्कत यह है कि यहां वास्तविक प्रोफाइलों के मुकाबले फर्जी प्रोफाइलों की अधिकता है। विभिन्न सामाजिक साइटों का इस्तेमाल आज साइबर अपराधों के लिए भी हो रहा है। कुछ लोग अपने किसी परिचित या परिचिता से तथाकथित बदला लेने के लिए उसका अश्लील प्रोफाइल या उसका व्यक्तिगत विवरण इन साइटों पर डाल देते हैं जिस कारण उन लोगों का जीवन बुरी तरह से असामान्य हो जाता है जिनके बारे में अश्लील बातें, सामाजिक साइटों पर डाली जाती हैं।

हाल ही में आई एक रिपोर्ट के मुताबिक यदि आप किसी सामाजिक नेटवर्किंग साइट पर सक्रिय हैं तो अपने प्रोफाइल को जरा संभालकर रखें। जरूरत इस बात की है कि अपनी व्यक्तिगत और गोपनीय बातों को इस प्रकार की साइटों पर कदापि नहीं डालें। युवतियों को तो अपने संपर्क पते और दूरभाष संख्या इन साइटों पर बिल्कुल नहीं डालने चाहिएं। अपने प्रोफाइल का दुरुपयोग होने से बचाने के लिए आवश्यक है कि :

1. किसी अजनबी को अपने संपर्क का विवरण न दें।
2. अपना चित्र, प्रोफाइल में न डालें।
3. यदि आवश्यक हो तो समूह-चित्र ही डाउनलोड करें।
4. अपना पूरा नाम लिखने के स्थान पर संक्षिप्त अक्षरों का प्रयोग करें।
5. यदि स्क्रैप में कोई किसी लिंक पर क्लिक करने को कहे तो ऐसा न करें क्योंकि इससे आपका पासवर्ड हैक हो सकता है।
6. यदि किसी साइबर कैफे का इस्तेमाल कर रहे हैं तो ध्यान रखें कि कहीं उस कंप्यूटर पर *'हैकिंग सॉफ्टवेयर'* तो डाउनलोड नहीं है।

सामाजिक साइट्स की दुनिया में बेहद सावधान रहने की आवश्यकता है।

थोड़ी सी तकनीक का इस्तेमाल करते हुए आप अपने पासवर्ड को हैक होने से बचा सकते हैं। यदि आपका पासवर्ड 'Swapn@123' है तो पासवर्ड टाइप करते समय पहले 'Swapn@' टाइप करें और फिर @ को मिटा दें। ऐसा दो-तीन बार करें। किसी केरेक्टेर को दो-तीन बार मिटाने के बाद पूरा पासवर्ड टाइप करें। अब यदि कोई आपका पासवर्ड हैक करेगा तो उसे 'Swapn@@123' या 'Swapn@@@123' दिखायी देगा। इसके अलावा अपनी जन्मतिथि वाहन संख्या आदि के आधार पर कभी भी अपना पासवर्ड न बनाएं।

ऑनलाइनखरीदारीऔरअपराधकीरोकथाम: भागदौड़ वाली इस जिंदगी में आज लोगों के पास समय की भारी कमी है और शायद इसीलिए ऑनलाइन खरीदारी का प्रचलन लगातार बढ़ता जा रहा है। ऑनलाइन खरीदारी का अर्थ है इंटरनेट के जरिए होने वाली खरीदारी। इसमें हम इंटरनेट पर किसी उत्पाद या वस्तु को देखते हैं और फिर इंटरनेट पर ही उसे खरीदने के निर्देश जारी कर देते हैं। ऑनलाइन खरीददारी में उत्पाद का मूल्य, प्लास्टिक कार्ड (डेबिट या क्रेडिट कार्ड) के जरिए चुकाया जाता है। वैसे आजकल चेक के जरिए भी भुगतान होने लगा है लेकिन इस मामले में उत्पाद की आपूर्ति तभी होती है जब चेक द्वारा कम्पनी को भुगतान प्राप्त हो जाता है।

ऑनलाइन खरीदारी को आजकल कई उपभोक्ता काफी लाभदायक व सुविधाजनक मानते हैं तो इसके कई कारण हैं। सबसे बड़ा कारण तो यह है कि ऑनलाइन खरीदारी करने से मध्यस्थ या दलाल की भूमिका समाप्त हो जाती है और उपभोक्ता को वस्तु अपेक्षाकृत सस्ते दामों पर मिल जाती है। दूसरा कारण यह है कि इंटरनेट पर उपभोक्ताओं को किसी उत्पाद के कई विकल्प मिल जाते हैं फलस्वरूप वह उत्पाद का तुलनात्मक अध्ययन कर सकता है। ऑनलाइन खरीदारी के बढ़ते प्रचलन का एक प्रमुख कारण यह भी है कि यह उधारी के जरिए (क्रेडिट कार्ड के द्वारा) भी हो सकती है। इसके अलावा इंटरनेट पर चौबीस घंटे खरीदारी संभव है जो किसी बाजार में संभव नहीं है। ऑनलाइन खरीदारी के लिए निम्नलिखित साइटें काफी लोकप्रिय हैं :

- ☆ अमेजन डॉट कॉम
- ☆ रेडिफ डॉट कॉम
- ☆ इंडियाटाइम्स डॉट कॉम

☆ फेमार्ट डॉट कॉम

☆ सिफी डॉट कॉम

ऑनलाइन खरीदारी करना सुविधाजनक तो है लेकिन इससे कुछ खतरे भी जुड़े हैं। किसी उत्पाद को खरीदते समय उपभोक्ता से कुछ जानकारियां मांगी जाती हैं जैसे नाम, पता, ई-मेल का पता, क्रेडिट कार्ड की वैधता तिथि और उसकी संख्या आदि। उपभोक्ता द्वारा दी गई इन जानकारियों का दुरुपयोग भी हो सकता है इसलिए कुछ सावधानियां बरतने की जरूरत है। सबसे पहले इस बात की पुष्टि कर लें कि जिस साइट पर आप अपनी क्रेडिट कार्ड या डेबिट कार्ड संख्या दे रहे हैं, वह पूरी तरह से सुरक्षित हो। इसके लिए आपकी स्क्रीन के निचले हिस्से में 'पेडलॉक' अर्थात् ताले के आकार का चिह्न बना होगा, जिसे देखकर आप साइट की सुरक्षा की जांच कर सकते हैं। उपभोक्ताओं को किसी भी धोखाधड़ी से बचाने के लिए कुछ बैंकिंग संस्थानों ने काफी तकनीकी इंतजाम किए हैं। सिटी बैंक, एच.डी.एफ.सी. और आईसीआईसीआई भुगतान गेटवे का प्रयोग करके आप भविष्य में होने वाली किसी भी धोखाधड़ी से बच सकते हैं।

ऑनलाइन खरीददारी के साथ-साथ आजकल ऑनलाइन टिकटिंग या ई-टिकटिंग भी काफी लोकप्रिय हो रही है। इसमें इंटरनेट के द्वारा रेलवे, हवाई सेवा आदि के टिकट आरक्षित किए जाते हैं। यह भी काफी सुविधाजनक है लेकिन साइबर अपराधी, ई-टिकटिंग के जरिए भी लोगों को चूना लगाने से बाज नहीं आते हैं। अधिकतर अपराधी किसी और के क्रेडिट कार्ड से टिकट बुक करा देते हैं और फिर उन टिकटों को बेच देते हैं। हाल ही में दिल्ली पुलिस ने एक ऐसे गिरोह को पकड़ा जो थाइलैंड, सिंगापुर आदि देशों के निवासियों के क्रेडिट कार्ड का डाटा चुराकर उससे स्पाइसजेट, गो इयर, इंडिगो एयरलाइंस, किंग फिशर और एयर इंडिया एक्सप्रेस आदि के टिकट आरक्षित करा लेते थे और फिर सस्ते दामों में लोगों को बेच देते थे। इस तरह यह गिरोह, उपरोक्त एयरलाइंसों को करोड़ों का चूना लगा चुका था। इस तरह की धोखाधड़ी से उपभोक्ताओं को बचाने के लिए क्रेडिट कार्ड कम्पनियों ने कई तकनीकी प्रबंध किए हैं। प्रत्येक कार्ड के पीछे एक तीन अंकों की *'सीवीवी'* संख्या होती है जिसका पता केवल कार्ड धारक को ही होता है। अब ई-टिकटिंग के समय

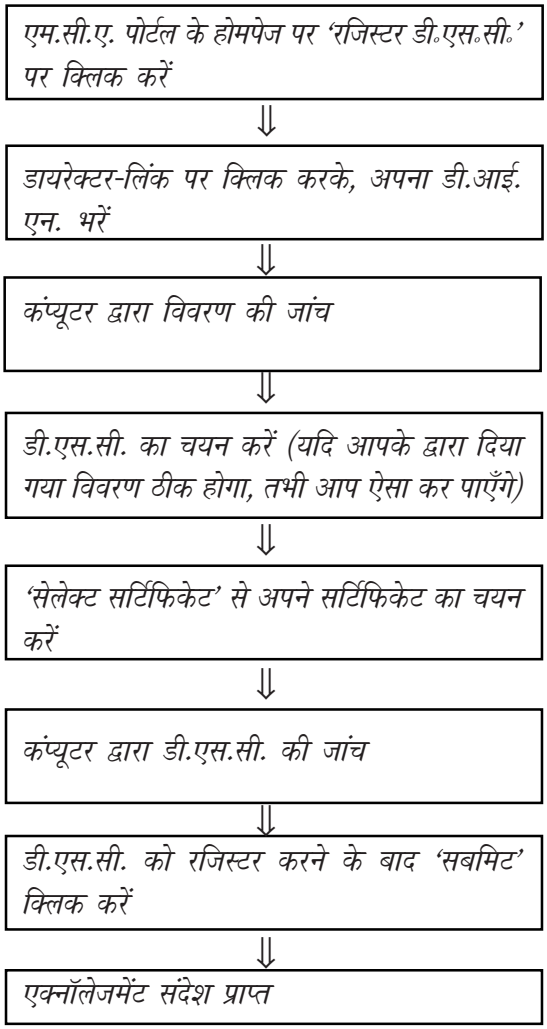
सीवीवी संख्या भी पूछी जाती है। इस प्रकार किसी के क्रेडिट कार्ड का डाटा चुरा कर उसका दुरुपयोग करना काफी कठिन हो गया है।

डिजिटल हस्ताक्षर और अपराधों की रोकथाम: आम जनजीवन में हस्ताक्षरों का अत्याधिक महत्त्व है। किसी अधिकृत व्यक्ति के हस्ताक्षर होने मात्र से किसी कागजात को प्रमाणिक मान लिया जाता है। साइबर विश्व में इस प्रकार की कोई सुविधा नहीं थी लेकिन तकनीक एवं प्रौद्योगिकी ने इतना विकास कर लिया है कि इंटरनेट द्वारा भेजे गए कागजातों पर भी हस्ताक्षर किए जाने संभव हो गए हैं। इन्हें डिजिटल हस्ताक्षर कहा जाता है।

जब हम किसी को कोई पत्र लिखते हैं तो पत्र के अंत में हम अपने हस्ताक्षर भी करते हैं। हस्ताक्षर देख कर ही पत्र प्राप्तकर्ता को भरोसा हो जाता है कि पत्र हमने ही भेजा है। इसके विपरीत यदि हम किसी परिचित को ई-मेल करते हैं तो उसमें हस्ताक्षर जैसी कोई सुविधा नहीं होती है। ई-मेल प्राप्तकर्ता हमारे ई-मेल खाते से पत्र प्राप्त करके ही यह भरोसा करने को मजबूर होता है कि पत्र (ई-मेल) हमने ही भेजा है। यदि कोई हमारे ई-मेल खाते को हैक करके किसी को ई-मेल भेज दे अथवा यदि कोई हमारा पासवर्ड जानकर हमारा ई-मेल खाता खोल ले तो किसी को पता तक नहीं चलेगा कि ई-मेल हम भेज रहे हैं या हमारे नाम पर कोई और। तकनीक एवं प्रौद्योगिकी ने इस समस्या का भी हल निकाल लिया है और हमें 'डिजिटल हस्ताक्षर' जैसी एक सुविधा प्रदान कर दी है। अब इंटरनेट द्वारा कोई दस्तावेज भेजने के लिए डिजिटल हस्ताक्षरों का इस्तेमाल किया जा सकता है।

डिजिटल हस्ताक्षरों की विशेषता यह होती है कि इनमें हस्तलिखित हस्ताक्षरों की भांति कोई परिवर्तन नहीं किया जा सकता है। डिजिटल हस्ताक्षरों के दुरुपयोग की आशंका लगभग नगण्य है क्योंकि इसमें एक नियंत्रक की कड़ी निगरानी में ही प्रमाणन एजेंसियों को लायसेंस दिए जाते हैं। डिजिटल हस्ताक्षर के अंतर्गत सब्सक्राइबर के पास दो कोड होते हैं पहला निजी कोड और दूसरा सार्वजनिक कोड। निजी कोड केवल सब्सक्राइबर को अथवा उसके द्वारा अधिकृत किसी व्यक्ति को ही पता होता है। इस निजी कोड के जरिए ही किसी दस्तावेज पर डिजिटल हस्ताक्षर हो सकते हैं। सार्वजनिक कोड के जरिए इन दस्तावेजों को कोई भी व्यक्ति देख सकता है। डिजिटल हस्ताक्षरों की उपस्थिति के कारण कोई

दूसरा व्यक्ति इन दस्तावेजों को देख तो सकता है लेकिन वह इनका दुरुपयोग नहीं कर सकता है। सूचना प्रौद्योगिकी अधिनियम की धारा-5 के अंतर्गत डिजिटल हस्ताक्षरों को विधिक मान्यता दी गई है। निम्नलिखित प्रक्रिया का पालन करके किसी दस्तावेज पर डिजिटल हस्ताक्षर किए जा सकते हैं :



डिजिटल-हस्ताक्षरों के कारण साइबर धोखाधड़ी के मामलों में काफी कमी आई है। डिजिटल-हस्ताक्षर एक ऐसी तकनीक है जो संदेश या दस्तावेज भेजने वाले स्रोत को प्रमाणित करते हैं। उदाहरण के लिए, यदि किसी बैंक की एक शाखा अपने मुख्यालय से किसी बैंक खाते में किसी परिवर्तन का अनुरोध करती है, तो ऐसे में अनुरोध की प्रमाणिकता को डिजिटल हस्ताक्षर के जरिए जांचा जा सकता है। अक्सर संदेश भेजते समय, संदेश भेजने वाले और संदेश प्राप्त करने वाले के मन में आशंका बनी रहती है कि कहीं संदेश में रास्ते में कोई परिवर्तन न कर दे। डिजिटल हस्ताक्षर युक्त संदेश या दस्तावेज में बीच में कोई परिवर्तन करने पर कंप्यूटर-तंत्र, संदेश (दस्तावेज) को अवैध घोषित कर देता है। किसी दस्तावेज पर डिजिटल हस्ताक्षर करते समय ध्यान रखें कि ऐसा अपने कंप्यूटर पर ही किया जाए। इसके अलावा डिजिटल हस्ताक्षरों का इस्तेमाल ऐसे एप्लीकेशंस में ही करें, जिसमें हैकिंग की आशंका न्यूनतम हो।

कंप्यूटर वाइरस की रोकथाम में प्रौद्योगिकी : कंप्यूटर इस्तेमाल करने वालों के लिए वायरस एक बड़ी समस्या है। इन वायरसों के कारण कंप्यूटर का समूचा डाटा नष्ट हो सकता है इसलिए कुछ कंपनियां या देश अक्सर दुश्मन कंपनियों या देशों के कंप्यूटर डाटा को नष्ट करने के लिए वायरस-हमला करते रहते हैं। कंप्यूटर वायरस से किस प्रकार किसी साइबर अपराध को कारित किया जाता है और प्रौद्योगिकी के इस्तेमाल से किस प्रकार वायरसों से बचा जा सकता है, यह जानने से पहले यह समझना प्रासंगिक रहेगा कि कंप्यूटर वायरस होते क्या हैं, और ये किस प्रकार कार्य करते हैं?

जैसे-जैसे कंप्यूटर तकनीक का विकास हो रहा है, वैसे-वैसे कंप्यूटर से संबंधित कई समस्याएं भी सिर उठाती जा रही हैं। ऐसी ही एक समस्या है, कंप्यूटर वायरस। इंटरनेट के कारण तो यह समस्या और अधिक विकराल होती जा रही है। सबसे पहला कंप्यूटर वायरस, ब्रेन (BRAIN) था जिसकी खोज डेलवेयर यूनिवर्सिटी के वैज्ञानिकों ने की थी। विशेषज्ञों का मानना है कि वर्तमान में लगभग 30 हजार वायरस सक्रिय हैं जिस कारण हमारे कंप्यूटर डेटा पर खतरे की तलवार लटकी हुई है।

शुरुआत में किसी वायरस को फैलने में महीनों लग जाते थे लेकिन जब से इंटरनेट को लोकप्रियता मिली है, तब से वायरस, रातों रात दुनियाभर के

कंप्यूटरों पर हमला कर देते हैं। ये कंप्यूटर वायरस वास्तव में मानवनिर्मित डिजिटल परजीवी हैं जो किसी दूसरे कंप्यूटर के डेटा को संक्रमित कर देते हैं। यदि कोई जाना-पहचाना वायरस किसी प्रोग्राम में छिपा हो तो उसे मात्र 10 मिनट में खोज कर नष्ट किया जा सकता है लेकिन किसी अपरिचित व नए वायरस को ढूंढना कभी-कभी काफी कठिन हो जाता है।

जैसे-जैसे कंप्यूटर वायरसों का खतरा बढ़ता जा रहा है, वैसे-वैसे वायरस विरोधी उद्योग (एंटी वायरस इंडस्ट्री) भी फैलता जा रहा है। इस व्यवसाय में तेजी का आलम यह है कि जैसे ही हम कोई एंटी वायरस फ्लॉपी या सीडी खरीदते हैं, वैसे ही वह पुरानी हो जाती है और हमें नए एंटी-वायरस की जरूरत महसूस होने लगती है।

जितनी तेजी से कंप्यूटर तकनीक बदल रही है उतनी ही तेजी से कंप्यूटर वायरसों में तकनीकों का प्रयोग बढ़ रहा है और वायरस लगातार अधिक आक्रामक व अधिक घातक होते जा रहे हैं। सबसे पहला कंप्यूटर-वायरस सी-ब्रेन (C Brain) को माना जाता है जो 1980 के दशक में प्रकाश में आया था। 1992-93 के आसपास कंप्यूटर वायरसों ने मीडिया का ध्यान आकर्षित किया तो लोग इसके बारे में सचेत हुए।

जैसे-जैसे वायरसों का खतरा बढ़ रहा है, वैसे-वैसे ही वायरस विरोधी उद्योग भी विकसित हो रहा है। यह उद्योग कुछ विशेष प्रोग्रामों पर आधारित होता है। कुछ प्रमुख वायरस विनाशक उत्पाद निम्नलिखित हैं :

CERTUS

NOVI

Untouchable Network

Central Point

WAN

HEURISTIC SCANNING

NLMS

VXDS

SELF Containd Disk

जैसे-जैसे इंटरनेट का प्रयोग बढ़ा, वैसे-वैसे वायरसों का खतरा भी बढ़ता जा रहा है। इंटरनेट के कारण सबसे ज्यादा 'मेकर' वायरस फैला जो डेटा फाइलों को अपना निशाना बनाता है। HEURISTIC SCANNING नामक वायरस विरोधी उत्पादन, नए वायरसों को खोजने के काम में बेहद उपयोगी है।

वायरसों की संख्या

वर्तमान में दुनियाभर के कंप्यूटरों में 20 हजार से 40 हजार तक वायरस हैं और रोजाना 15 से भी अधिक नए वायरसों का जन्म हो जाता है। यहां यह उल्लेखनीय है कि पुराने वायरस धीरे-धीरे चलन से बाहर हो जाते हैं और रिसर्च लैब में केवल नए वायरस ही रह जाते हैं। विशेषज्ञ मानते हैं कि एक माह में लगभग 200 से 300 वायरस ही सक्रिय रहते हैं।

समय के साथ-साथ वायरसों के प्रकार में तो बदलाव आता ही है साथ ही उनकी तीव्रता भी बढ़ जाती है। पहले जिस प्रोग्राम को हम कंप्यूटर वायरस कहते थे उसे अब *'कंप्यूटर इंफेक्शन'* कहा जाता है।

कैसे काम करता है वायरस

हम पढ़ चुके हैं कि वायरस एक छोटा सा प्रोग्राम होता है जिसमें कॉपी करने की क्षमता होती है। पहले यह हार्ड ड्राइव, फ्लॉपी की प्रोग्राम फाइलों और बूट सेक्टर में स्वयं प्रवेश कर जाता है। बूट सेक्टर वायरस आमतौर पर ऑपरेटिंग सिस्टम और हार्ड ड्राइव की फाइलों को संक्रमित (प्रभावित) करता है।

फाइल और प्रोग्राम वायरस .EXE और .COM फाइलों को प्रभावित करता है। एक संक्रमित (प्रभावित) प्रोग्राम द्वारा वायरस उत्प्रेरित होता है। संशोधित प्रोग्रामों की तुलना करके नए वायरसों की पहचान आसानी से की जा सकती है। ऐसा करके किसी बड़े नुकसान से बचा जा सकता है। मैक्रो वायरस की खोज अगस्त, 1995 में हुई थी। ये मैक्रो वायरस, टेक्सट वाले डाक्यूमेंटों और एक्सेल स्प्रेडशीटों को संक्रमित करते हैं।

आजकल कंप्यूटरों पर वायरसों का हमला बहुत अधिक बढ़ गया है। 'कंप्यूटर प्रोटेक्शन एसोशिएसन' के मुताबिक कंप्यूटर इस्तेमाल करने वाला हर

तीसवां व्यक्ति आज कंप्यूटर वायरस से परेशान है। वायरसों के कारण हमारे कंप्यूटर का डेटा नष्ट हो जाता है। कई बार तो यह डेटा पुनः प्राप्त किया जा सकता है तो अक्सर इसे दुबारा प्राप्त करना संभव ही नहीं रहता। यदि खराब हुए डेटा को पुनः प्राप्त कर भी लिया जाए तो भी इसमें समय और पैसे की भारी हानि होती है।

ऐसे बचें वायरसों से

वायरसों के कारण हमें काफी असुविधा होती है लेकिन थोड़ी सी सावधानी बरत कर हम वायरसों के हमले से अपने कंप्यूटरों को आसानी से बचा सकते हैं। निम्नलिखित उपाय अपना कर वायरसों के संक्रमण से बचा जा सकता है :

(1) वायरस विरोधी रणनीति बनाएं।
(2) वायरस विरोधी प्रोग्रामों (एंटी वायरस प्रोग्राम) का प्रयोग करें।
(3) नेटवर्क और वेब के माध्यम से सूचनाओं का आदान-प्रदान करते समय पर्याप्त सावधानी बरतें।
(4) अनजाना ई-मेल न खोलें।
(5) नेटवर्क पर कार्यक्रमों की साझेदारी कम से कम करें।

वायरस इंफेक्शन से बचने का सबसे सरल उपाय, एंटी वायरस सॉफ्टवेयर का उपयोग ही है। जब भी आप पर्सनल कंप्यूटर पर काम करना शुरू करते हैं तो एंटी-वायरस सॉफ्टवेयर, क्षणभर में वायरस की खोज कर उसे नष्ट कर देता है। आजकल उपलब्ध माइक्रोसॉफ्ट वर्ड और एक्सेल के नवीनतम संस्करणों में तो मैक्रा वायरस सुरक्षा पहले से ही लगी आती है। वायरसों से बचने के लिए जरूरी है कि आप जब भी कोई अटैचमेंट फाइल प्राप्त करें तो सबसे पहले उसे स्कैन कर लें ताकि यदि कोई वायरस हो तो उसे नष्ट किया जा सके। यह भी जरूरी है कि सदैव ई-मेल प्रोग्राम के नवीनतम संस्करणों का ही प्रयोग किया जाए।

मैक्रो वायरस

शुरुआत में हम सामान्य वायरसों से ही परेशान थे लेकिन फिर धीरे-धीरे मैक्रो वायरसों ने हमारे कंप्यूटरों पर हमला बोल दिया। हाल ही में भारत में

निम्नलिखित मैक्रो-वायरस देखे गए थे :

एनपैड (N PAD)
एलाइन (Alien)
नेमेसिस (Nemesis)
कलर (Colour)
वाजू (Wazzu)
न्यूक्लियर (Nuclear)

हजारों की संख्या में आज कंप्यूटर वायरस सक्रिय हैं। इनमें से कुछ तो इतने खतरनाक हैं कि कंप्यूटर क्षेत्र से संबंधित प्रत्येक व्यक्ति इनके बारे में जानता है। यहां हम कुछ प्रचलित वायरसों के नाम के साथ-साथ उनके अन्य नामों, खोज के वर्ष व स्थान तथा लक्षणों का उल्लेख करेंगे।

कुछ प्रचलित वायरस

सं. नाम	*अन्य नाम*	*खोज*	*लक्षण*
1. 1008	सुओमी ओउलू	जून 1990, फिनलैंड	बूट करने पर सिस्टम बंद
2. 1704	रेन ड्रॉप	जनवरी 1989	आ.प., अक्षर गिर जाते हैं
3. मिनिट्स	इंडियन वाइरस	1991, भारत	आ.प., अनर्गल अक्षर दिखना
4. ऐम्बुलेंस-कार	रेड एक्स		जून 1990, प. जर्मनी आ.प. ग्राफिक्स, सायरन की आवाज
5. आर्मागेडॉन	आर्मागेडॉन द फर्स्ट आर्मागेडॉन द ग्रीक	जून 1990, ग्रीस	आ.प.
6. बर्जर	सी.आई.ए.	1986, प. जर्मनी	आ.प.हो., प्रोग्राम शुरू नहीं होता
7. ब्लडी	जून 4, स्टोन	12/90, ताइवान	बूट के समय संदेश
8. ब्रेन	पाकिस्तानी ब्रेन	1986, पाकिस्तान	अक्षर गायब हो जाना
9. चाइनीज फिश	फिश बूट		संदेश

10. क्रिसमस	टानेन बॉम,XAI	3/90, जर्मनी	आ. प. क्रिसमस ट्री का चित्र
11. कॉफी शॉप			आ.प. धतूरे की पत्ती का चित्र
12. डार्क एवेंजर,	डायना, एड्डी	9/89, बुल्गेरिया	आ.प. बूट सेक्टर बदलता है
13. डी बेस	डी बी एफ	9/88, अमेरिका	आ.प. फैट डायरेक्टरी करप्टेड
14. डू नथिंग	स्टुपिड	10/89, इजराइल	आ.प.
15. फेलोशिप	1022	7/90, ऑस्ट्रेलिया	आ.प., संदेश
16. फ्राइडे, द'13	म्यूनिख	11/87, द. अफ्रीका	आ.प., फाइल गायब
17. घोस्ट बॉल	घोस्ट, कॉम	10/89, आइसलैंड	स्क्रीन पर चलित ग्राफिक
18. होलोकास्ट	स्टेल्थ	12/90, स्पेन	आ.प., फाइल में त्रुटि
19. जोशी		1989, भारत	संदेश
20. प्लास्टिक	प्लास्टिक बम	7/90, ताइवान	आ.प., शोर
21. मर्फी	मर्फी	14/90, बुल्गेरिया	आ.प., संदेश, शोर
22. पैरालिसिस		6/90, भारत	की-बोर्ड की अनेक की
24. पेन्टागन			काम नहीं करती
25. प्रीडेटर	प्रीडेटर-1 प्रीडेटर-2		सिस्टम फेल
26. स्लो		5/90, आस्ट्रेलिया	आ.प.
27. सॉरी	जी वाइरस	6/90	आ.प., मेमोरी में कमी
28. संडे		11/89, अमेरिका	आ.प., संदेश
29. स्वैप	फालिंग लेटर्स	8/89, इजराइल	अक्षर गिर जाते हैं
30. टर्बो 448	पोलिश-2	11/90, हंगरी	आ.प.
31. यूएस एसआर		12/90, यूएसएसआर	आ.प.
32. विक्टर		5/90, यूएसएसआर	आ.प. फाइल दोष
33. विएना	यूनेस्को	4/88, आस्ट्रिया	आ.प.
34. हवेल	मदर फिश	8/90, प. जर्मनी	आ.प.
35. विस्कांसिन	पास्कल की मृत्यु	10/90, अमेरिका	आ.प.
36. जीरो बग	पैलेट, 1536	9/89, हॉलैंड	आ.प. ग्राफिक, हंसता चेहरा सभी अक्षरों को खा जाता है।

37. आईलवयू	वेरी फनी	5/2000, फिलीपीन	संदेश, आ.प.
38. मेलिसा		98, ताइवान	प्रेम संदेश
39. चेर्नोबिल		4/98, ताइवान	आ.प.
40. डिस्क किलर		10/89	संदेश
41. येरुशेलम	न्यू येरुशेलम, फ्राइडे में	13/88	येरूशेलम संदेश

आ.प. आकार में परिवर्तन, आ.प. हो. आकार परिवर्तन हो सकता है।

कंप्यूटर वाइरस : तथ्य और आंकड़े

- ★ मूलतः वाइरस प्रोग्रामर द्वारा निर्मित एक प्रोग्राम है। एक बार सक्रिय हो जाने के बाद यह स्वयं को स्वतः ही दुहराता रहता है और फैलता रहता है।
- ★ जिस डिस्क को सुरक्षित कर दिया जाता है उसमें न तो वाइरस संक्रमण फैला सकता है न उसको हानि पहुँचा सकता है।
- ★ किसी फाइल का आकार बढ़ाए बिना ही वाइरस उस फाइल को दूषित कर सकता है।
- ★ फाइल की तारीख तथा समय का संशोधन किए बिना ही वाइरस फाइल को संक्रमित कर सकता है।
- ★ DOS फाइल के 1/0 functions का प्रयोग किए बगैर ही फाइल को संक्रमित कर सकता है।
- ★ डाटा फाइल में वाइरस संक्रमण नहीं फैलाता है बल्कि उसको नष्ट कर देता है।
- ★ प्राथमिक रूप से बूट सेक्टर वाइरस (BSV) सिस्टम का नियंत्रण तभी कर पाता है जब सिस्टम को किसी बूट सेक्टर वाइरस से संक्रमित डिस्क से बूट किया जाता है।
- ★ बूट सेक्टर वाइरस फाइल को संक्रमित कर सकता है।
- ★ बूट सेक्टर वाइरस हर प्रकार की डिस्क को संक्रमित कर सकता है।

- ★ डिस्क के संक्रमित होने पर डिस्क स्पेस कम नहीं होता है।
- ★ स्मृति (मैमोरी) में वाइरस के घर बना लेने के बाद भी सिस्टम की स्मृति कम नहीं होती है।
- ★ अपने को फैलाने के लिए स्मृति में बसे हुए वाइरस को डिस्क 1/0 इंटरप्ट को पुनर्निर्देश देना आवश्यक नहीं है।
- ★ बिना डायरेक्टरी संरचना तथा फाइल एलोकेशन टेबुल (फैट) को बदले हुए फाइल स्वयं को बढ़ा सकते हैं। इसके लिए वाइरसों को डायरेक्टरी संरचना का क्रमवीक्षण (स्कैनिंग) करना पड़ सकता है।
- ★ सिस्टम को 'ऑफ' कर देने पर कोई भी वाइरस स्मृति में सक्रिय नहीं रह सकता है।
- ★ डिस्क पर संक्रमित कोई भी वाइरस सिस्टम को नियंत्रण में लेने के लिए स्वतः सक्रिय नहीं हो सकते हैं।
- ★ प्रोग्राम कोड होने के कारण वाइरस अधिक से अधिक उतना ही कर सकते हैं जो एप्लीकेशन प्रोग्राम कर सकते हैं। अंतर केवल यह है कि वाइरस उपयोक्ता की जानकारी के बगैर ही सक्रिय हो जाते हैं।

जैविक वायरस बनाम कंप्यूटर वायरस

समानताएं

- ★ दोनों वाइरसों के कार्य करने की प्रणाली एक-सी है।
- ★ दोनों वाइरस कूट निर्देशों के आधार पर कार्य करते हैं।
- ★ जिस प्रकार जैविक वाइरस शरीर की सूक्ष्मतम इकाई, कोशिकाओं में स्वतः प्रगुणित होते हैं और पर्याप्त संख्या तक पहुंच जाने पर कोशिकाओं को नष्ट कर देते हैं, उसी प्रकार कंप्यूटर वाइरस ऑपरेटिंग सिस्टम के सूक्ष्मतम भाग, कमांड-कॉम पर आक्रमण कर उन्हें अपने और अनेक प्रतिरूप बनाने को बाध्य करते हैं। पर्याप्त संख्या में प्रतियां बन जाने पर ये वाइरस कमांड-कॉम को ही संक्रमित कर देते हैं।

- ★ संक्रमित करने के बाद जैविक वाइरस कोशिकाओं से बाहर निकल आते हैं और अन्य कोशिकाओं को संक्रमित करने लगते हैं। इसी प्रकार, कंप्यूटर वाइरस स्क्रीन पर कुछ संदेश देने अथवा चित्र छापने लगते हैं और फिर कंप्यूटर के प्रोग्राम को इस तरह से परिवर्तित कर देते हैं कि अन्य प्रोग्रामों को क्षति पहुंचती है।
- ★ जिस प्रकार जैविक वाइरसों का अपना एक कोड होता है वैसे ही कंप्यूटर वाइरस का अपना एक सिगनेचर होता है।
- ★ दोनों प्रकार के वाइरसों को प्रगुणित होने के लिए अनुकूल परिस्थितियों की आवश्यकता होती है।
- ★ दोनों प्रकार के वाइरसों के शिकार संक्रमित होने के पश्चात् निश्चित लक्षण दिखलाने लगते हैं।

असमानताएं

- ★ जैविक वाइरस नैसर्गिक है जबकि कंप्यूटर वाइरस कृत्रिम होता है।
- ★ जैविक वाइरस में प्रतिबाधक (प्रिवेंटिव) उपाय होते हैं इसलिए इनका उपयोग करके उस वाइरस द्वारा फैलाई बीमारी के टीके (वैक्सीन) बनाए जाते हैं जिनसे उस बीमारी का निदान होता है। कंप्यूटर वाइरस में ऐसा कोई प्रतिबाधक उपाय नहीं होता है।
- ★ नैसर्गिक होने के कारण जैविक वाइरस का निदान तब तक स्थाई रहेगा जब तक वाइरस की कोड रचना में कोई परिवर्तन न आए।

किसी भी बीमारी से निजात पाने के लिए जरूरी है कि पहले उस बीमारी की पहचान की जाए। इसीलिए बीमार होने पर डॉक्टर पहले हमारी जांच करता है, रोग की पहचान करता है और फिर उस रोग का ईलाज करता है। कंप्यूटर संक्रमण (वायरस) से बचने के लिए भी जरूरी है कि पहले वायरसों की पहचान की जाए। इसीलिए हमने यहां वायरसों की चर्चा की है ताकि वायरसों की जानकारी प्राप्त करके उनसे बचा जा सके।

कंप्यूटर को खराब करने वाले वायरस, वर्म्स और ट्रोजन्स की संख्या आज दस लाख को भी पार कर गई है। 'सिमैंटेक' द्वारा सन् 2008 में जारी अपनी द्विवार्षिक रिपोर्ट 'इंटरनेट सुरक्षा को खतरे' में कहा गया है कि अधिकतर

वायरस (प्रोग्राम) पिछले 12 महीनों के भीतर ही तैयार किए गए हैं। रिपोर्ट के मुताबिक, साइबर अपराधी, एंटी-वायरस प्रोग्राम को निष्क्रिय करने और अपने आपराधिक इरादों को अंजाम देने के लिए लगातार प्रयास कर रहे हैं। अधिकांश वायरस, उन कंप्यूटरों को निशाना बना रहे हैं जिनमें 'विन्डोज' सॉफ्टवेयर लगे हैं। ये वायरस, मौजूदा वायरसों के ही संशोधित रूप हैं और ये हाईटेक अपराधियों के लिए काफी लाभदायक सिद्ध हो रहे हैं। अब अपराधी किसी कंप्यूटर-तंत्र तक पहुंचने के लिए 'ट्रोजन्स' का भी इस्तेमाल कर रहे हैं और ट्रोजन्स के माध्यम से ही वे कई प्रोग्राम डाउनलोड कर रहे हैं अथवा उन्हें इंस्टाल कर रहे हैं।

वायरसों के हमले से बचने के लिए 'एंटी-वायरस' काफी लाभदायक होते हैं। एंटी-वायरस, एक कंप्यूटर प्रोग्राम होता है जो कंप्यूटर को वायरस से ग्रसित होने से रोकता है। ये एंटी-वायरस न केवल वायरस अपितु वार्म्स, ट्रोजन होर्सेज और रूटकिट्स आदि से भी कंप्यूटर का बचाव करते हैं। एंटी-वायरस सबसे पहले कंप्यूटर फाइल्स को स्कैन करता है ताकि किसी वायरस की उपस्थिति का पता लगाया जा सके। याद रखें कि जब भी आप कोई मेजर सॉफ्टवेयर, इंस्टाल कर रहे हों तो वायरस-सुरक्षा को निष्क्रिय कर दें। ऐसा न करने पर हो सकता है कि आपके द्वारा इंस्टाल किया जाने वाला सॉफ्टवेयर ठीक से इंस्टाल ही न हो। तकनीक और प्रौद्योगिकी ने एंटी-वायरसों में कई उपयोगी विशेषताएं दे दी हैं जैसे मल्टीपल वायरस स्कैन, एडवांस स्कैन शैडयूलिंग स्पेसिफिक लोकेशन और रीयल-टाइम स्कैनिंग। एंटी वायरस में उपस्थित रीयल-टाइल स्कैनिंग, नामक विशेषता के कारण ये एंटी-वायरस, एक निश्चित समयान्तराल के बाद कंप्यूटर को स्कैन करते रहते हैं ताकि किसी वायरस के कंप्यूटर में प्रवेश करते ही उसका पता लगा कर उसे नष्ट किया जा सके। एंटी-वायरस के संदर्भ में निम्नलिखित सावधानियां बरतने की जरूरत होती है :

1. एंटी-वायरस को समय-समय पर अपडेट करते रहें।
2. स्वचालित अपडेट के विकल्प को सदैव सक्रिय रखें ताकि इंटरनेट के माध्यम से एंटी-वायरस हमेशा अपने आप ही अपडेट होता रहे।
3. स्वचालित रिपेयर के विकल्प को भी सदैव सक्रिय रखें।
4. समय-समय पर *'फुल सिस्टम स्कैन'* करते रहें। इसके लिए 'ऑटोमैटिक

फुल सिस्टम स्कैन' के विकल्प को भी शैडयूल्ड किया जा सकता है।

अपने कंप्यूटर तंत्र को सप्ताह में कम से कम एक बार अवश्य स्कैन करें। एंटी-वायरस सॉफ्टवेयर को 'गूगल-सर्च' ही सहायता से भी डाउनलोड किया जा सकता है। कुछ प्रमुख एंटी-वायरस प्रोग्राम निम्नलिखित हैं :

–AVG एंटी वायरस

–Norton एंटी वायरस

–MCA Fee एंटी वायरस

–EAV एंटी वायरस

–avast एंटी वायरस

–PC tools एंटी वायरस

–PC clinn एंटी वायरस

वायरस के अलावा कंप्यूटर प्रयोगकर्ता 'स्पैम मेल' से भी काफी परेशान रहते हैं। आपके कंप्यूटर पर आने वाले हजारों की संख्या में अवांछनीय ई-मेल ही स्पैम कहलाते हैं। वेबसाइट्स पर पोस्ट किए गए ई-मेल के पते और 'न्यूज ग्रुप्स', स्पैम को आकर्षित करते हैं। इंटरनेट के लिए मुसीबत बन चुके स्पैम को फिल्टर करने के लिए कंप्यूटर विशेषज्ञ लगातार शोध कर रहे हैं। स्पैम से बचने के लिए जरूरी है कि कभी भी किसी स्पैम-मेल का जवाब न दें अन्यथा आपके ई-मेल खाते में स्पैम-मेल की बमबारी प्रारंभ हो जाएगी। यही नहीं वे दूसरे स्पैमर्स को भी आपका ई-मेल पता बांट देंगे। स्पैम-मेल से बचने के लिए जरूरी है कि अपने ब्राउजर में सिक्योरिटी-सेटिंग ठीक प्रकार से करें। स्पैम-मेल के साथ वायरस भी हो सकते हैं इसलिए इन्हें हटा देना (डिलीट कर देना) ही सबसे अच्छा उपाय है।

प्रौद्योगिकीद्वाराचोरीसेबचाव: चोरी एक ऐसा अपराध है जो सदियों से हर सभ्यता और हर समाज में पाया जाता है। प्रौद्योगिकी ने आज हमें ऐसे उपकरण उपलब्ध करा दिए हैं जिनकी सहायता से हम बहुतायत से होने वाली चोरियों को भी रोक सकते हैं। चोरी की वारदातों को रोकने के लिए जो अत्याधुनिक उपकरण उपलब्ध हैं वे कुल तीन प्रकार के हो सकते हैं : रीडर, नियंत्रक और ताले। रीडर, आपके विवरण को प्राप्त कर उसका मिलान उसमें पहले से दर्ज आपके विवरण से करता है। नियंत्रक से मिलने वाले आदेश/निर्देश

के बाद स्वचालित ताले सक्रिय होते हैं। ऐसे बायोमैट्रिक उपकरण भी अब उपलब्ध हैं जो व्यक्ति के हाथ या उसकी आंखों को पढ़ कर उसकी पहचान स्थापित करते हैं।

घर, आवास, दुकान या कार्यालय आदि में होने वाली चोरियों को रोकने के लिए सबसे अधिक प्रयोग, सीसीटीवी कैमरों का किया जाता है। पहले के सीसीटीवी कैमरे आकार में बड़े होते थे जिन्हें चोरों द्वारा आसानी से देख लिया जाता था लेकिन अब ऐसे छोटे सीसीटीवी कैमरे भी अस्तित्व में आ चुके हैं, जिन्हें ढूंढ़ना आसान नहीं है। सीसीटीवी कैमरे से एक पतला तार निकला होता है जिसे आप अपने टेलीविजन या कंप्यूटर से जोड़ सकते हैं और फिर आसानी से किसी स्थान विशेष की निगरानी कर सकते हैं। इसके अलावा आजकल वायरलैस सीसीटीवी कैमरे भी बाजार में आ चुके हैं, जिन्हें टेलीविजन या कंप्यूटर से जोड़ने के लिए तार की आवश्यकता भी नहीं पड़ती है। कुछ वायरलैस सीसीटीवी कैमरों के साथ एक छोटा सा एल.सी.डी. उपकरण भी आता है जिसकी सहायता से क्षेत्र विशेष पर पूरी नजर रखी जा सकती है। इस एल.सी.डी. उपकरण की सहायता से सी.सी.टी.वी. कैमरे के कोण को भी दूर से ही बदला जा सकता है।

चोरी की घटनाओं की रोकथाम में 'पाम रीडर' भी बेहद महत्त्वपूर्ण भूमिका अदा करते हैं। पाम रीडर में अधिकृत व्यक्ति की हथेली के चित्र को अंकित कर लिया जाता है और बाद में दरवाजे के भीतर प्रवेश देने से पूर्व यह पाम-रीडर, प्रवेश करने वाले व्यक्ति की हथेली के चित्र का मिलान, पहले से ही अभिलेखित किए गए हथेली के चित्र से करता है। यदि कोई अनाधिकृत व्यक्ति पाम-रीडर से छेड़छाड़ का प्रयास करता है तो यह उपकरण, अलार्म बजाकर आसपास के लोगों को सावधान कर देता है। आजकल इलैक्ट्रोमैग्नेटिक ताले भी अस्तित्व में आ चुके हैं, जिनकी नकली चाबियां बनवाना असंभव है। इस अत्याधुनिक ताले के भीतर एक रीडर होता है जो पहले अपनी चाबी की पहचान करता है और फिर ताले को खुलने का संकेत करता है। हाल ही में न्यूमैरिक ताले भी बाजार में उपलब्ध हो चुके हैं जिन्हें आमतौर पर घर के दरवाजों और अलमारियों में लगाया जाता है। इस प्रकार के ताले एक विशेष कोडवर्ड का प्रयोग करने पर ही खुलते हैं।

इलैक्ट्रॉनिक-प्रमाणकीप्रमाणिकता: अभी तक किसी इलैक्ट्रॉनिक प्रमाण (एवीडेंस) को प्रमाणिक ही माना जाता था लेकिन तकनीक के प्रयोग से अब इन इलैक्ट्रॉनिक प्रमाणों से भी छेड़छाड़ संभव हो गई है। भाजपा नेता श्री प्रमोद महाजन की हत्या के मामले की न्यायालय में सुनवाई के दौरान न्यायालय के सम्मुख एक अभियंता ने सिद्ध किया कि 'एसएमएस' भी जाली और बनावटी हो सकते हैं। इसके बाद 'एसएमएस' की गवाही के रूप में स्वीकार्यता पर प्रश्नचिह्न लग गया।

आजकल 'एसएमएस' और ई-मेल जैसे टेक्स्ट संदेश का उपयोग, न्यायालय में किसी मामले को कमजोर या मजबूत करने के लिए खूब किया जा रहा है लेकिन जबसे इनके भी फर्जी होने की आशंका बढ़ी है, तभी से यह विवाद का विषय हो गया है कि क्या इन्हें भी इलैक्ट्रॉनिक प्रमाण माना जाना चाहिए। हालांकि एस.एम.एस. या ई-मेल संदेश के आधार पर न तो किसी को दोषी ठहराया जा सकता है और न ही इनके आधार पर किसी को बरी किया जा सकता है लेकिन इनके आधार पर अभियोजन-पक्ष को घटना की कड़ी जोड़ने में तो सहायता मिलती ही है। कोलकाता के हाईप्रोफाइल रिजवानुर मामले में भी सिद्ध किया जा चुका है कि भेजे गए या प्राप्त किए गए इलैक्ट्रॉनिक संदेशों में परिवर्तन किया जा सकता है। आजकल कुछ मामलों में न्यायालय के नोटिस तक एस.एम.एस. या ई-मेल के जरिए भेजे जाने लगे हैं और इनकी पूरी स्वीकार्यता होती है लेकिन इनके साथ छेड़खानी की आशंका के बाद अब सेवा-प्रदाता का उत्तरदायित्व कुछ और बढ़ गया है। तकनीक व प्रौद्योगिकी की सहायता से सेवा-प्रदाता को भेजे गए या प्राप्त किए गए एस.एम.एस. का रिकॉर्ड कुछ और लंबे समय तक रखना होगा ताकि इन इलैक्ट्रॉनिक संदेशों की वास्तविकता का पता आवश्यकता पड़ने पर लगाया जा सके।

वास्तव में आजकल ऐसे सॉफ्टवेयर बाजार में उपलब्ध हैं जिनकी सहायता से इलैक्ट्रॉनिक संदेशों से छेड़छाड़ की जा सकती है। इस प्रकार के सॉफ्टवेयर, इंटरनेट पर भी आसानी से उपलब्ध हैं। इस प्रकार के और भी अनेको 'टूल्स' को इंटरनेट पर आसानी से खोजा जा सकता है। कोई भी *'टैक सैवी'* व्यक्ति, इन्हें डाउनलोड करके उनका आसानी से प्रयोग कर सकता है। इनके द्वारा न केवल किसी इलैक्ट्रॉनिक संदेश को परिवर्तित किया जा सकता है अपितु किसी

नंबर विशेष से भी किसी संदेश को भेजा जा सकता है। भारतीय साक्ष्य अधिनियम, 2000 की धारा 65-बी के अनुसार इलैक्ट्रॉनिक-प्रमाण न्यायालय में स्वीकार्य हैं। यहां एक बात का उल्लेख प्रासंगिक रहेगा कि ई-मेल संदेश के साथ छेड़छाड़ करना बेहद आसान है जबकि 'एस.एम.एस.' के साथ छेड़छाड़, इस बात पर निर्भर करती है कि आप कौन से मोबाइल फोन का इस्तेमाल कर रहे हैं। कुछ मोबाइल फोनों में इस प्रकार की प्रौद्योगिकी का इस्तेमाल किया जाता है कि उनसे भेजे गए एस.एम.एस. संदेशों के साथ किसी प्रकार की कोई छेड़छाड़ संभव नहीं है।

सूचना-प्रौद्योगिकी अधिनियम, 2000

सन् 2000 में पारित सूचना प्रौद्योगिकी अधिनियम, विभिन्न प्रकार के साइबर अपराधों को सुलझाने में तो सहायता करता ही है साथ ही यह उन प्रावधानों का जिक्र भी करता है जिनके आधार पर, तकनीक व प्रौद्योगिकी का इस्तेमाल करके अपराधों की रोकथाम की जा सकती है। उदाहरण के लिए, इस अधिनियम में चर्चा की गई है कि किन परिस्थितियों में और किन मानदंडों के आधार पर इलैक्ट्रॉनिक सर्विलांस की जा सकती है। इस प्रकार तकनीक व प्रौद्योगिकी का इस्तेमाल करते हुए अपराधों की रोकथाम में 'सूचना प्रौद्योगिकी अधिनियम', बेहद आवश्यक है अतः यहां इस अधिनियम की चर्चा प्रासंगिक होगी।

पृष्ठभूमि तथा उद्देश्य

(1) नई संचार प्रणाली तथा आंकिक तकनीक ने हमारी जिन्दगी जीने के तरीके को नाटकीय रूप में परिवर्तित कर दिया है। लोगों के व्यापारिक व्यवहारों में एक क्रांति हो रही है। व्यापारी एवं उपभोक्ताओं में रूढ़िगत कागजी दस्तावेजों के स्थान पर सूचनाओं को बनाने, उन्हें प्रेषित करने एवं उनका संग्रहण करने हेतु कंप्यूटरों का उपयोग बढ़ता जा रहा है। वैद्युतिक रूप में संग्रहीत की गई सूचना के काफी फायदे होते हैं। ये सस्ती होती है, संग्रहीत करने में आसान होती है एवं इसकी पुनः प्राप्ति एवं प्रेषण अधिक गतिशील होता है, यद्यपि लोगों को इन फायदों का पता था परंतु फिर भी वे उपयुक्त वैधानिक

ढांचे की कमी के कारण वैद्युतिक रूप में व्यवहार करने अथवा व्यापार करने में हिचकिचाते थे। वैधानिक मान्यता हेतु दस्तावेज का लेखन एवं हस्ताक्षर दो ऐसी आवश्यकताएं हैं जो कि वैद्युतिक वाणिज्य तथा वैद्युतिक शासन के रास्ते की सबसे बड़ी रुकावटें हैं। वर्तमान समय में प्रचलित विभिन्न वैधानिक प्रावधान कागजी प्रलेखों एवं दस्तावेजों तथा ऐसे प्रलेखों को मान्यता देते हैं जो कि हस्ताक्षरयुक्त होते हैं। साक्ष्य अधिनियम परम्परागत तौर पर कागजी प्रलेखों तथा मौखिक गवाही पर आधारित हैं। चूंकि वैद्युतिक वाणिज्य में कागजी सौदों की आवश्यकता को हटा दिया गया है इसलिए ई-कॉमर्स को सहायता देने हेतु समुचित वैधानिक परिवर्तन किया जाना अत्यंत आवश्यक हो गया है। अंतर्राष्ट्रीय व्यापार पिछले कुछ वर्षों में ई-कॉमर्स के माध्यम से तेजी से बढ़ रहा है एवं बहुत से देशों ने कागज आधारित वाणिज्य को ई-कॉमर्स में बदल दिया है।

(2) संयुक्त राष्ट्रों की सामान्य सभा ने अपने प्रस्ताव क्रमांक 51/162 दिनांक 30 जनवरी, 1997 के द्वारा अनुमोदन किया था कि सभी राज्य अपने यहां विधान बनाते समय या उन्हें परिवर्तित करते समय प्रादर्श विधान को ध्यान में रखें। वैद्युतिक वाणिज्य हेतु इस प्रादर्श विधान को सन् 1996 में संयुक्त राष्ट्र की अंतर्राष्ट्रीय व्यापार विधान कमीशन ने पारित किया था। इस आदर्श विधान में कागजी संचार तथा वैद्युतिक संचार उपभोक्ताओं के लिए समान वैद्युतिक व्यवहार हेतु प्रावधान निहित हैं। विश्व व्यापार संगठन के विभिन्न सदस्य देशों ने भी हाल ही में घोषणा की है कि वे भी वैद्युतिक वाणिज्य के माध्यम से विभिन्न व्यापारिक सौदों के परिचालन हेतु संभावनाओं को ढूंढने तथा एक रूप बनाने के लिए एक सम्मिलित कार्यक्रम बनाएंगे।

(3) हमारे देश में ई-कॉमर्स को सहायता देने हेतु वर्तमान कानूनों में समुचित परिवर्तनों की आवश्यकता है। इसलिए यह प्रस्तावित किया गया कि वैद्युतिक प्रलेखों तथा आंकिक हस्ताक्षरों को वैद्युतिक मान्यता देने हेतु प्रावधान बनाए जाएं जिससे कि वैद्युतिक माध्यमों द्वारा किए गए अनुबंधों के अनुमोदन द्वारा अधिकारों तथा दायित्वों की रचना की जा सके। यह भी प्रस्तावित किया गया है कि आंकिक हस्ताक्षर प्रमाणपत्र जारी करने वाले प्रमाणीकरण प्राधिकारों को नियंत्रित करने हेतु नियमित शासन पद्धति हेतु प्रावधान बनाए जाएं। वैद्युतिक माध्यमों द्वारा दिए गए सौदों एवं व्यवहारों के द्वारा होने वाले सम्मिलित दुरुपयोगों

को रोकने के लिए प्रस्तावित कानूनों के उल्लंघन हेतु दीवानी तथा फौजदारी दायित्व भी प्रस्तावित हैं।

(4) वैद्युतिक शासन को सहायता देने के उद्देश्य से यह भी प्रस्तावित किया गया है कि शासकीय एवं इनके अभिकर्ताओं के कार्यालयों में वैद्युतिक प्रलेखों तथा आंकिक हस्ताक्षरों के उपयोग को मान्यता प्रदान करने हेतु प्रावधान बनाए जाएं। इससे नागरिकों तथा शासकीय कार्यालयों के मध्य स्वतंत्र व्यवहार होंगे।

(5) भारतीय दंड संहिता तथा भारतीय साक्ष्य अधिनियम, 1872 में समुचित परिवर्तन भी प्रस्तावित हैं जिनके द्वारा दस्तावेजों तथा कागज रहित सौदों संबंधी अपराधी हेतु प्रावधानों में आवश्यक परिवर्तन लाने के लिए प्रस्तावित हैं। वित्तीय संस्थानों तथा बैंक के मध्य वैद्युतिक कोष स्थानांतरण को सहायता देने हेतु रिजर्व बैंक ऑफ इण्डिया अधिनियम 1934 में भी परिवर्तन प्रस्तावित किए गए हैं। बैंकों द्वारा वैद्युतिक प्रारूप में लेखा पुस्तकों के पालन को वैधानिक मान्यता देने हेतु ''बैंकर्स ब्रुक्स'' साक्ष्य अधिनियम, 1891 में भी आवश्यक परिवर्तन प्रस्तावित हैं।

(6) प्रस्तावों को राज्य सरकारों के मध्य भी संचारित किया गया था, उन्होंने प्रस्तावित कानूनों का अनुमोदन किया है एवं इस कानून को अत्यधिक आवश्यक भी माना है।

अध्याय–I

संक्षिप्त नाम, प्रारंभ एवं अनुप्रयोग : यह अधिनियम 'सूचना तकनीक अधिनियम 2000' के नाम से पुकारा जाएगा। यह पूरे भारतवर्ष में प्रभावी होगा तथा इस अधिनियम के विपरीत प्रावधानों को सुरक्षित रखते हुए यह किसी व्यक्ति द्वारा भारत के बाहर भी किए गए किसी अपराध अथवा उल्लंघन पर भी लागू होगा। इसमें यह प्रावधानित किया गया है कि केंद्र सरकार इस अधिनियम के प्रावधानों को प्रभावशाली करने हेतु दिनांक अथवा कई अलग-अलग विधियों को अधिसूचित करेगी एवं जिस तिथि से यह विभिन्न प्रावधान अधिसूचित होंगे उसी तिथि से इस अधिनियम के तहत यह प्रभावशाली हो जाएंगे।

निम्नलिखित दस्तावेजों इत्यादि पर यह अधिनियम लागू नहीं होगा :

(क) एक 'विनिमय विपत्र' जिसे विनिमय विपत्र अधिनियम 1881 की धारा 13 के अंतर्गत परिभाषित किया गया हो।

(ख) एक 'अभिकर्ता पत्र' जिसे कि पावर ऑफ अटॉर्नी एक्ट 1882 की धारा 1 (ए) के तहत परिभाषित किया गया हो।

(ग) एक 'ट्रस्ट' जिसे कि भारतीय ट्रस्ट अधिनियम 1882 की धारा 3 के तहत परिभाषित किया गया हो।

(घ) एक 'इच्छापत्र' जिसे कि भारतीय उत्तराधिकार अधिनियम 1925 की धारा 2 (एच) के तहत परिभाषित किया हो।

(ड.) किसी अचल संपत्ति या उसमें निहित किसी अधिकार को विक्रय अथवा अंतरण करने हेतु किए गए अनुबंध।

(च) दस्तावेजों अथवा सौदों की कोई ऐसी श्रेणी जिसे कि केंद्र सरकार शासकीय गजट में अधिसूचित करें।

परिभाषाएं : इस अधिनियम की धारा 2 के तहत विभिन्न तकनीकी शब्दों को निम्नलिखित रूप में परिभाषित किया गया हैं :

(1) पहुंच : इसे शाब्दिक तथा प्रासंगिक रूप में इस तरह परिभाषित किया गया है कि एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र के तार्किक, गणितीय अथवा स्मृति कार्य स्रोतों में प्रवेश करना, निर्देश देना अथवा इनसे वार्तालाप करना।

(2) संबोधित : से तात्पर्य एक ऐसे व्यक्ति से होता है जिसे कि मूल प्रेषक कोई वैद्युतिक प्रलेख भेजना चाहता है परंतु इसमें मध्यस्थों को शामिल नहीं किया जाता है।

(3) न्यायिक अधिकारी : से आशय उस न्यायिक अधिकारी से होता है जिसे कि धारा 46 की उपधारा (1) के अधीन नियुक्त किया जाता है।

(4) आंकिक हस्ताक्षर नत्थी करने : से आशय एक व्यक्ति द्वारा उस प्रणाली अथवा प्रक्रिया को बनाना होता है जिसके द्वारा एक वैद्युतिक प्रलेख को आंकिक हस्ताक्षरों के माध्यम से प्रमाणीकृत किया जाता है।

(5) उपयुक्त सरकार : किसी मामले में उपयुक्त सरकार से आशय :

(i) जिसका वर्णन संविधान की सातवीं अनुसूची की दूसरी

तालिका में किया गया हो।

(ii) संविधान की सातवीं अनुसूची की तृतीय तालिका के अंतर्गत किसी राज्य कानून को पारित करने संबंधित राज्य सरकार एवं अन्य प्रकरणों में केन्द्र सरकार।

(6) असमान गुप्त लेखन प्रणाली : से आशय एक ऐसी प्रणाली से होता है जिसमें कि एक सुरक्षित कुंजी के जोड़े का प्रयोग किया जाता है। इसमें एक निजी कुंजी आंकिक हस्ताक्षरों की रचना हेतु प्रयोग की जाती है तथा दूसरी व्यावसायिक कुंजी आंकिक हस्ताक्षरों को प्रमाणित करती है।

(7) प्रमाणीकरण प्राधिकारी : से आशय एक ऐसे व्यक्ति से होता है जिसे कि धारा 24 के अंतर्गत आंकिक हस्ताक्षर प्रमाणपत्र जारी करने हेतु अनुज्ञापत्र जारी किया गया हो।

(8) प्रमाणीकरण नियम कथन : एक विवरणी को कहते हैं जिसे कि एक प्रमाणीकरण प्राधिकारी द्वारा जारी किया जाता है जिसमें कि उन नियमों का उल्लेख होता है जिसे प्रमाणीकरण प्राधिकरण आंकिक हस्ताक्षर प्रमाणपत्र जारी करने हेतु लागू करते हैं।

(9) कंप्यूटर : से आशय वैद्युतिक, चुम्बकीय, प्रकाश अथवा तीव्र समंक प्रक्रियाकरण उपकरण अथवा प्रणाली से होता है जो कि वैद्युतिक, चुम्बकीय अथवा प्रकाश तरंगों के कुशलतापूर्वक प्रबंधन द्वारा तार्किक, गणितीय एवं स्मृति क्रियाओं को संपन्न करते हैं एवं इसमें सभी आगम, निर्गम, प्रक्रियाकरण, भण्डारण कंप्यूटर सॉफ्टवेयर तथा संचार सुविधाओं को शामिल किया जाता है जो कि एक कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में संगणक यंत्रों से जुड़े होते हैं अथवा संबंधित होते हैं।

(10) कंप्यूटर तंत्र : से आशय एक या अधिक संगणक यंत्रों के अंतर संबंध से होता है जो कि निम्नलिखित माध्यमों द्वारा हो सकता है :

(i) उपग्रह, सूक्ष्म तरंग अथवा भूमिगत लाइनों अथवा अन्य संचार माध्यमों के उपयोग द्वारा, अथवा

(ii) दो या अधिक अंतर्संबंधित संगणक यंत्रों का एक सामूहिक मिश्रण अथवा शीर्ष जहां चाहे अंतर्संबंध लगातार चालू रखा जाता हो अथवा नहीं।

(11) कंप्यूटर स्रोत : का आशय संगणक यंत्र प्रणाली, कंप्यूटर तंत्र, समंक, कंप्यूटर समंक आधार अथवा सॉफ्टवेयर से होता है।

(12) कंप्यूटर प्रणाली : से आशय एक उपकरण अथवा उपकरणों के समूह से होता है जिसमें कि कार्यक्रम के अयोग्य गणक यंत्रों को छोड़कर, उन आगम एवं निर्गम तथा सहायक यंत्रों को शामिल किया जाता है जो कि बाहरी फाइलों जिसमें कि कंप्यूटर कार्यक्रम, वैद्युतिक निर्देश, आगम समंक तथा निर्गम समंक निहित होते हैं, के साथ उपयोग करने योग्य होते हैं एवं जो कि तार्किक, अंकगणितीय, समंक भण्डारण एवं पुनर्प्राप्ति, संचार नियंत्रण तथा अन्य कार्यों को संपन्न करते हैं।

(13) नियंत्रक : से आशय धारा 17 की उपधारा (1) के अधीन नियुक्त किए गए प्रमाणीकरण प्राधिकारियों के नियंत्रक से होता है।

(14) साइबर अपीलीय न्यायाधिकरण : से आशय धारा 48 की उपधारा (1) के तहत स्थापित साइबर नियमन अपीलीय न्यायाधिकरण से होता है।

(15) समंक : से आशय सूचना, ज्ञान, तथ्य, धारणा अथवा निर्देशों के एक प्रतिनिधित्व से होता है जिसे एक औपचारिक रीति से निर्मित किया गया है, अथवा निर्मित किया जा सकता हो जोकि एक कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में प्रक्रियागत किए जा रहे हों, अथवा जिसका उद्देश्य प्रक्रियागत किया जाना हो एवं जो किसी भी प्रारूप में हो सकते हैं, (जिसमें कंप्यूटर मुद्रित पत्र, चुम्बकीय अथवा प्रकाश भण्डारण माध्यम, छिद्रित पत्रक, छिद्रित फीते सम्मिलित हैं) अथवा कंप्यूटर की स्मृति में आंतरिक रूप भण्डारित हों।

(16) आंकिक हस्ताक्षर : से आशय एक अंशदाता द्वारा किसी वैद्युतिक अभिलेख के सत्यापन करने से होता है। जो कि धारा 3 के प्रावधानों के अनुसार एक वैद्युतिक रीति अथवा प्रणाली द्वारा किया जाता है।

(17) आंकिक हस्ताक्षर प्रमाण पत्र : से आशय धारा 35 की उपधारा (4) के तहत जारी किए गए एक आंकिक हस्ताक्षर प्रमाणपत्र से होता है।

(18) वैद्युतिक प्रारूप : सूचना के संबंध में वैद्युतिक प्रारूप से आशय किसी ऐसी सूचना से होता है जिसका उत्पादन, प्रेषण, प्राप्ति अथवा भण्डारण

चुम्बकीय, प्रकाश, कंप्यूटर स्मृति, माइक्रोफिल्म, कंप्यूटर उत्पादित माइक्रोफिश अथवा समान उपकरणों के माध्यम से किया जाता हो।

(19) वैद्युतिक गजट : से आशय ऐसे अधिकारिक गजट से होता है जिसे कि वैद्युतिक प्रारूप में प्रकाशित किया जाता है।

(20) वैद्युतिक अभिलेख : से आशय समंकों, अभिलेखों, दृश्य अथवा ध्वनि से होता है जिसे कि एक वैद्युतिक प्रारूप अथवा माइक्रोफिल्म अथवा कंप्यूटर उत्पादित माइक्रोफिश में भण्डारित किया, प्राप्त किया अथवा भेजा जाता हो।

(21) क्रियाएं : एक कंप्यूटर के संबंध में क्रियाओं के अंतर्गत तार्किक, नियंत्रण, गणितीय प्रक्रिया, मिटाना, भण्डारण एवं पुनः प्राप्ति एवं एक कंप्यूटर से अथवा उसके अंतर्गत संचार अथवा दूरसंचार क्रियाओं को सम्मिलित किया जाता है।

(22) सूचना : में समंक लेख, दृश्य, ध्वनि, आवाज, कूट संकेत, कंप्यूटर कार्यक्रम, सॉफ्टवेयर एवं समंक आधारों अथवा माइक्रोफिल्म अथवा कंप्यूटर उत्पादित माइक्रोफिश को सम्मिलित किया जाता है।

(23) मध्यस्थ : से आशय एक ऐसे व्यक्ति से होता है जो किसी अन्य व्यक्ति की ओर से किसी संदेश को प्राप्त करता है, भण्डारित अथवा प्रेषण करता है अथवा उस संदेश के संबंध में अन्य सेवाएं प्रदान करता है।

(24) कुंजी युग्म : एक असमान गुप्त प्रणाली में कुंजी युग्म से आशय एक निजी कुंजी तथा इससे गणितीय रूप से जुड़ी सार्वजनिक कुंजी से होता है जो कि परस्पर एक दूसरे से इस प्रकार संबंधित होती है कि निजी कुंजी द्वारा बनाए गए एक आंकिक हस्ताक्षरों को सार्वजनिक कुंजी प्रमाणित कर सकती है।

(25) विधि : में लोकसभा अथवा किसी राज्य कानून व अधिनियम, राष्ट्रपति अथवा राज्यपाल द्वारा जारी अध्यादेश, अनुच्छेद 240 के, अधीन राष्ट्रपति द्वारा बनाए गए अधिनियम, संविधान के अनुच्छेद 357 के वाक्य-1 के उपवाक्य (ए) के अधीन राष्ट्रपति के अधिनियम के समान पारित किए गए बिलों को शामिल किया जाता है तथा इनके अधीन जारी किए गए नियमों, अधिनियमों, उप नियमों एवं आदेशों को भी सम्मिलित किया जाता है।

(26) अनुज्ञप्ति : से आशय धारा 24 के अंतर्गत एक प्रमाणीकरण प्राधिकारी को प्रदान की गई अनुज्ञप्ति से होता है।

(27) मूल व्यक्ति : से आशय एक ऐसे व्यक्ति से होता है जो कि वैद्युतिक संदेश प्रेषित, उत्पादित, भण्डारित अथवा भेजता है अथवा किसी अन्य व्यक्ति को कोई वैद्युतिक संदेश भेजे जाने, उत्पादित करने, भण्डारित करने अथवा प्रेषित करने की व्यवस्था करता है परंतु इसमें एक मध्यस्थ को शामिल नहीं किया जाता है।

(28) निर्धारित : से आशय इस अधिनियम के तहत बनाए गए विभिन्न नियमों से होता है।

(29) निजी कुंजी : से आशय एक कुंजियों की जोड़े की उस कुंजी से होता है जो एक आंकिक हस्ताक्षरों की रचना हेतु प्रयोग की जाती है।

(30) सार्वजनिक कुंजी : से आशय एक कुंजियों के जोड़े की उस कुंजी से होता है जो कि आंकिक हस्ताक्षर को सत्यापित करने हेतु प्रयोग की जाती है एवं जो कि आंकिक हस्ताक्षर प्रमाणपत्र में सूचीबद्ध होती है।

(31) सुरक्षित प्रणाली : से आशय उन कंप्यूटर हार्डवेयर, सॉफ्टवेयर एवं प्रक्रियाओं से होता है जो कि :

(i) अनाधिकृत पहुंच एवं दुरुपयोग से समुचित तौर पर सुरक्षित होते हैं।

(ii) जो एक समुचित विश्वसनीयता का स्तर एवं सही क्रियाविधि प्रदान करते हैं।

(iii) जो कि दी गई क्रियाओं को संपन्न करने हेतु उचित रूप से उपयुक्त हों एवं

(iv) जो कि सामान्य रूप से स्वीकार्य सुरक्षा प्रक्रियाओं का पालन करते हों।

(32) सुरक्षा कार्य प्रणाली : से आशय उन सुरक्षा क्रिया सुविधाओं से है जिन्हें कि धारा 16 के तहत केन्द्र सरकार ने प्रस्तावित किया हो।

(33) अंशदाता : से आशय एक ऐसे व्यक्ति से होता है जिसके नाम में आंकिक हस्ताक्षर प्रमाणपत्र जारी किया गया हो।

(34) प्रमाणीकरण : से आशय एक आंकिक हस्ताक्षर, आंकिक प्रलेख अथवा सार्वजनिक कुंजी के संबंध में इसके सभी व्याकरण अर्थ एवं समान अर्थों के साथ यह जांच करना होता है कि :

(i) ग्राहक के प्रारंभिक वैद्युतिक प्रलेख को सार्वजनिक कुंजी से संबंधित निजी कुंजी का प्रयोग करते हुए आंकिक हस्ताक्षरों से मुहरबंद किया गया था। एवं

(ii) कि प्रारंभिक वैद्युतिक प्रलेख आंकिक हस्ताक्षरों से मुहरबंद करने से लेकर अभी तक ज्यों का त्यों रखा गया है अथवा परिवर्तित किया गया है।

अध्याय–II
आंकिक हस्ताक्षर

वैद्युतिक प्रलेखों का प्रमाणीकरण

1. इस धारा के प्रावधानों के अनुसार कोई अंशदाता अपने आंकिक हस्ताक्षरों से युक्त करके एक वैद्युतिक अभिलेख को प्रमाणीकृत कर सकता है।

2. वैद्युतिक अभिलेखों का प्रमाणीकरण असमान गुप्त लेखन प्रणाली एवं हैश क्रिया द्वारा किया जाएगा जो कि प्रारंभिक वैद्युतिक अभिलेख को दूसरे वैद्युतिक अभिलेख में परिवर्तित करते हुए मुहर बंद कर देती है।

स्पष्टीकरणः इस उपधारा के अंतर्गत हैश क्रियाओं से तात्पर्य बिटों की एक श्रेणी को सामान्यतः छोटी दूसरी अन्य श्रेणी में जिसे कि हैश परिणाम के नाम से जानते हैं, में अनुवाद करने अथवा खाके की रचना हेतु उपयोगी प्रतीक गणित से होता है। यह हैश परिणाम किसी वैद्युतिक अभिलेख में जब उस प्रतीक गणित को उपयोग किया जाता है तो प्रत्येक बार एक समान प्राप्त होते हैं। एवं इन्हें इस प्रकार से तैयार किया जाता है कि जब इन्हें गणना में प्रयोग किया जाए तो मूल वैद्युतिक प्रलेख के हैश परिणाम तथा इससे पुनः बनाए गए अभिलेख के हैश परिणाम समान नहीं हों तथा दो अलग-अलग वैद्युतिक प्रलेख उस प्रतीक गणित के उपयोग द्वारा एक समान परिणाम उत्पन्न नहीं कर सकें।

3. कोई भी व्यक्ति अंशदाता द्वारा उपयोग की गई एक सार्वजनिक कुंजी

का प्रयोग करके वैद्युतिक अभिलेख की जांच कर सकता है।

4. निजी कुंजी एवं सार्वजनिक कुंजी प्रत्येक अंशदाता हेतु अनूठी होती है एवं ये कार्यकारी कुंजी जोड़े निर्मित करती हैं।

अध्याय–III
वैद्युतिक शासन

वैद्युतिकअभिलेखोंकोवैधानिकमान्यता **:** धारा 4 के अनुसार जहां किसी विधि में यह प्रावधान है कि सूचना या अन्य कोई सामग्री लिखित रूप में अथवा टंकित रूप में अथवा मुद्रित प्रारूप में रखी जाती है। वहां यह आवश्यकता संतुष्ट मानी जाएगी यदि वह सूचना अथवा सामग्री :

(a) एक वैद्युतिक प्रारूप में प्रदान की जाए अथवा उपलब्ध करा दी जाए एवं

(b) जो कि भविष्य की आवश्यकताओं हेतु पुनः प्राप्त की जा सके एवं उपयोगी हो सके।

आंकिकहस्ताक्षरोंकोवैधानिकमान्यता **:** धारा 5 के अनुसार जहां किसी कानून में यह प्रावधानित है कि कोई सूचना व अन्य सामग्री हस्ताक्षर करके प्रमाणित की जाएगी अथवा किसी दस्तावेज को किसी व्यक्ति द्वारा हस्ताक्षर किया जाएगा तो यदि इस सूचना या सामग्री अथवा दस्तावेज को केन्द्र सरकार द्वारा अनुमोदित तरीकों से आंकिक हस्ताक्षर द्वारा प्रमाणीकृत कर दिया जाता है तो यह आवश्यकता संतुष्ट मानी जाएगी।

सरकार एवं उसके अभिकर्ताओं में वैद्युतिक अभिलेख एवं आंकिकहस्ताक्षरोंकाउपयोग **:** धारा-6 जहां किसी कानून में प्रावधान है कि :

(अ) कोई प्रारूप, आवेदन अथवा कोई अन्य दस्तावेज किसी दफ्तर, प्राधिकारी, अंग अथवा अभिकर्ता जो कि किसी उपयुक्त सरकार के अधीन हों अथवा नियंत्रण में हों के पास दाखिल किए जाने हों;

(ब) कोई अनुज्ञप्ति, परमिट, अनुशंसा, अथवा अनुमोदन किसी भी नाम से पुकारा जाए एक विशिष्ट तरीके या प्रकार से जारी अथवा प्रदान किए जाने हों।

(स) एक विशिष्ट प्रकार या तरीके से धन की प्राप्ति अथवा भुगतान किया जाना हो।

तब किसी अन्य विधि में जो कि उस समय प्रभावशाली हों, में निहित किसी अन्य प्रावधान के अलावा उपरोक्त आवश्यकताएं संतुष्ट हुई मानी जाएंगी यदि यह जमा कराना, जारी करना, प्राप्त करना अथवा भुगतान करना जैसा भी कार्य हो किसी उपयुक्त सरकार द्वारा अनुमोदित वैद्युतिक प्रारूप के जरिए संपन्न किए जाएं।

उपयुक्त सरकार उपरोक्त हेतु आवश्यक नियम बनाती हुई अनुमोदित कर सकती है कि :

(अ) किस प्रारूप अथवा तरीके से इन वैद्युतिक प्रलेखों की रचना की जाएगी, जारी किए जाएंगे अथवा जमा किए जाएंगे।

(ब) वाक्य (अ) में वर्णित किसी वैद्युतिक अभिलेख के जमा कराने, रचना करने अथवा जारी करने हेतु किसी शुल्क अथवा प्रभार के भुगतान की विधि अथवा तरीका।

***वैद्युतिकप्रलेखोंकाधारण* :** धारा 7 में प्रावधान है कि किसी कानून के प्रावधान के अनुसार कोई दस्तावेज, अभिलेख अथवा सूचना, को किसी विशिष्ट अवधि हेतु संभाल कर रखना हो तब यह आवश्यकता पूरी की हुई समझी जाएगी यदि ये दस्तावेज अभिलेख अथवा सूचना वैद्युतिक प्रारूप में सुरक्षित रखी जाएं तथा :

(अ) इनमें निहित सूचनाएं आगामी संबोधन हेतु पहुंचने योग्य तथा उपयोगी रहें।

(ब) वैद्युतिक अभिलेख उस प्रारूप में रखे जाएं जिनमें कि ये मूल रूप से उत्पादित, प्रेषित अथवा प्राप्त किए गए थे अथवा एक ऐसे प्रारूप में हों जो कि मूल उत्पादित, प्रेषित अथवा प्राप्त सूचना को यथार्थ रूप में प्रदर्शित करता हो।

(स) ऐसे विवरण जो कि उस वैद्युतिक अभिलेख के उद्गम तथा गंतव्य स्थान, भेजे जाने अथवा प्राप्त करने का समय तथा स्थान इत्यादि सूचनाओं की पहचान उपलब्ध कराने में सहायक हों, संबंधित वैद्युतिक अभिलेख में उपलब्ध रहे।

इस धारा के प्रावधान कोई ऐसी सूचना पर लागू नहीं होते जो कि एक वैद्युतिक अभिलेख के भेजने अथवा प्राप्त करने के दौरान स्वतः स्वचालित रूप से उत्पादित होती है। इस धारा के प्रावधान वहां भी लागू नहीं होते जहां कि किसी कानून में वैद्युतिक अभिलेखों के प्रारूप में दस्तावेजों, अभिलेखों अथवा सूचनाओं को रखा जाना स्पष्ट रूप से प्रावधानित किया गया हो।

वैद्युतिक गजट में प्रकाशन: धारा 8 के प्रावधानों के अनुसार जहां कि किसी विधि में प्रावधान है कि कोई नियम, विनियम, आदेश, उप नियम, अधिसूचना अथवा अन्य सामग्री अधिकारिक गजट में प्रकाशित की जाएगी तब यह आवश्यकता संतुष्ट मानी जाती है यदि ये नियम, विनियम इत्यादि अधिकारिक गजट या वैद्युतिक गजट में प्रकाशित कर दिए जाते हैं। उपरोक्त प्रकाशन हेतु प्रभावशाली दिनांक वह मानी जाती है जिस तिथि पर उपरोक्त नियम इत्यादि का प्रकाशन प्रथम बार किसी भी प्रारूप में प्रकाशित किया गया हो।

धारा 6, 7 एवं 8 द्वारा कोई अधिकार नहीं: धारा 9 के अनुसार धारा 6, 7, 8 में वर्णित प्रावधान किसी व्यक्ति को यह अधिकार प्रदान नहीं करते कि वह केन्द्र सरकार अथवा राज्य सरकार के किसी मंत्रालय अथवा विभाग अथवा किसी विधि के अंतर्गत स्थापित कोई व्यक्ति अथवा केन्द्र अथवा राज्य शासन द्वारा पोषित अथवा नियंत्रित संस्था को कोई दस्तावेज वैद्युतिक अभिलेख के प्रारूप में स्वीकार, जारी, निर्मित करने, रखने अथवा सुरक्षित रखने के लिए आग्रह करें अथवा कोई मौद्रिक व्यवहार वैद्युतिक प्रारूप में करने हेतु आग्रह करें।

केन्द्र सरकार को नियम बनाने की शक्ति: इस अध्याय की धारा 10 के अनुसार केन्द्र सरकार को यह शक्ति प्रदान की गई है कि वह इस अधिनियम के उद्देश्यों को प्राप्त करने हेतु नियम बनाकर प्रस्तावित कर सकती है :

(अ) आंकिक हस्ताक्षरों के प्रकार।

(ब) आंकिक हस्ताक्षर किस तरीके एवं प्रारूप में मुहरबंद किए जाएंगे।

(स) वह प्रक्रिया तथा विधि जोकि आंकिक हस्ताक्षर को करने वाले व्यक्ति की पहचान करने में सहायक हो।

(द) वैद्युतिक अभिलेखों तथा भुगतानों की समुचित सत्य निष्ठा, सुरक्षा एवं विश्वसनीयता को निश्चित करने वाली नियंत्रण प्रक्रियाएं एवं

विधियां तथा।

(इ) आंकिक हस्ताक्षरों को वैधानिक प्रभाव देने हेतु अन्य आवश्यक विषय वस्तुएं।

अध्याय–IV

वैद्युतिक अभिलेखों की सम्बद्धता, स्वीकृति एवं प्रेषण

वैद्युतिकअभिलेखोंकीसंबद्धता **:** एक वैद्युतिक अभिलेख इसके मूल लेखक से संबद्ध माना जाएगा यदि :

(अ) यह स्वयं मूल लेखक द्वारा भेजा गया हो।

(ब) यदि यह मूल लेखक की ओर से उस वैद्युतिक अभिलेख के संबंध में अधिकृत व्यक्ति द्वारा भेजा गया हो अथवा

(स) यदि यह सूचना एक सूचना प्रणाली द्वारा भेजी गई हो जिसे कि मूल लेखक अथवा उसकी ओर स्वचालित रूप से कार्य करने हेतु कार्यक्रमित किया गया हो (धारा 11)

प्राप्ति की स्वीकृति

1. धारा 12 के प्रावधानों के अनुसार यदि मूल लेखक एवं संबोधित व्यक्ति के मध्य एक विशिष्ट प्रारूप अथवा विशिष्ट विधि से वैद्युतिक अभिलेखों की प्राप्ति की स्वीकृति प्रदान किए जाने के संबंध में सहमति नहीं है तो एक प्राप्ति सूचना निम्नलिखित तरीके से दी जा सकती है :

(अ) संबोधनकर्ता द्वारा स्वचालित अथवा अन्य तरीके से किया गया कोई संवाद, अथवा

(ब) संबोधित व्यक्ति द्वारा किया गया कोई व्यवहार जो कि मूल लेखक को यह इंगित करने हेतु पर्याप्त हो कि वैद्युतिक अभिलेख प्राप्त हो चुका है।

2. यदि मूल लेखक ने यह निर्देशित किया है कि वैद्युतिक प्रलेख उस पर तभी बध्य होंगे जबकि उसे उन वैद्युतिक प्रलेखों की प्राप्ति की स्वीकृति मिल जाएगी। तो जब तक कि प्राप्ति स्वीकृति प्राप्त न हो जाए यह माना जाएगा कि मूल लेखक ने वह वैद्युतिक अभिलेख कभी भेजा ही नहीं था।

3. जहां पर कि मूल लेखक ने यह निर्देशित नहीं किया है कि वह वैद्युतिक

अभिलेख केवल प्राप्ति की स्वीकृति प्राप्त हो जाने के बाद ही उस पर बाध्य होंगे एवं मूल लेखक को दी गई अथवा सहमति समय सीमा में प्राप्ति सूचना नहीं मिलती है अथवा यदि कोई सीमा निर्धारित नहीं है तो उचित समय में यह प्राप्त नहीं होती है तो मूल लेखक संबोधित व्यक्ति को सूचित कर सकता है कि उसे सूचना प्राप्ति की स्वीकृति अब तक नहीं प्राप्त हुई है एवं वह एक उचित समय इसमें निर्धारित कर सकता है जिसमें कि प्राप्ति सूचना उसे अवश्य प्राप्त हो सके चाहे यदि सूचना देने के उपरांत ऊपर उल्लेखित समय सीमा में उसे प्राप्ति स्वीकृति संबोधित व्यक्ति द्वारा प्राप्त नहीं होती है तो वह उस वैद्युतिक अभिलेख को कभी भी नहीं भेजा गया यह मान लेगा।

वैद्युतिक अभिलेख के भेजने एवं इसकी प्राप्ति का समय एवं स्थान(धारा13)

1. मूल लेखक तथा संबोधित व्यक्ति के बीच कोई विपरीत सहमति होने के अतिरिक्त, एक वैद्युतिक प्रलेख का प्रेषण तब माना जाता है जबकि यह मूल लेखक के नियंत्रण से बाहर एक कंप्यूटर स्रोत में प्रवेश करता है।

2. मूल लेखक एवं संबोधित व्यक्ति के मध्य हुई पारस्परिक सहमति के अतिरिक्त, एक वैद्युतिक अभिलेख की प्राप्ति निम्नलिखित रूप में तय की जाएगी :

(अ) यदि संबोधित व्यक्ति द्वारा वैद्युतिक अभिलेखों की प्राप्ति हेतु एक कंप्यूटर स्रोत तय किया हुआ है तो प्राप्ति उस समय मानी जाती है जबकि यह वैद्युतिक अभिलेख तय कंप्यूटर स्रोत में प्रवेश करता है अथवा यदि वैद्युतिक अभिलेख संबोधित व्यक्ति के ऐसे कंप्यूटर स्रोत को भेजा गया है जो कि तय कंप्यूटर साधन नहीं है तो इसका प्राप्ति समय वह माना जाता है जबकि संबोधित व्यक्ति उस वैद्युतिक अभिलेख को प्राप्त करता है।

(ब) यदि संबोधित व्यक्ति ने कोई कंप्यूटर साधन, किसी समय अवधि के साथ निर्धारित नहीं किया हुआ है तो प्राप्ति तब मानी जाएगी जबकि वैद्युतिक प्रलेख संबोधित व्यक्ति के कंप्यूटर साधन में प्रवेश करता है।

3. मूल लेखक एवं संबोधित के मध्य परस्पर सहमति के अतिरिक्त एक वैद्युतिक अभिलेख का प्रेषण स्थान वह माना जाता है जहां कि मूल लेखक अपना व्यवसाय करता है एवं प्राप्ति स्थान वह माना जाता है जहां कि संबोधित

व्यक्ति अपना व्यवसाय करता है।

4. उपधारा 2 के तहत वर्णित समय सीमा संबंधी प्रावधानों के लागू होने पर कोई प्रभाव नहीं पड़ेगा चाहे उपधारा 2 में तय किया गया कंप्यूटर साधन का स्थान जहां कि वैद्युतिक अभिलेखों की प्राप्ति होनी है, उपधारा 3 में वर्णित प्राप्ति स्थान से भिन्न है।

5. इस धारा के प्रावधानों हेतु :

(अ) यदि मूल लेखक एवं संबोधित व्यक्ति के एक से अधिक व्यवसाय स्थान हैं तो इस स्थिति में उनके व्यवसाय का मुख्य स्थान, व्यवसाय का स्थान होगा।

(ब) यदि मूल लेखक अथवा संबोधित व्यक्ति के पास कोई व्यवसाय का स्थान नहीं है तो उनके सामान्य निवास का स्थान उनका व्यवसाय का स्थान माना जाएगा।

(स) एक निगमित व्यक्ति के संबंध में सामान्य निवास स्थान से आशय उस स्थान से होता है जहां कि ये पंजीकृत हैं।

अध्याय–V

सुरक्षित वैद्युतिक अभिलेख एवं सुरक्षित आंकिक हस्ताक्षर

सुरक्षितवैद्युतिकअभिलेख **:** जब एक वैद्युतिक अभिलेख पर कोई सुरक्षा प्रक्रिया प्रयुक्त की जाती है तब उस समय से लेकर सत्यापित किए जाने के समय तक वह अभिलेख एक सुरक्षित वैद्युतिक अभिलेख माना जाएगा (धारा 14)।

सुरक्षितआंकिकहस्ताक्षर **:** यदि संबंधित पक्षों की परस्पर सहमति से एक सुरक्षा प्रक्रिया अपनाए जाने पर यह सत्यापित किया जा सके कि एक आंकिक हस्ताक्षर जिस समय इसे मुहरबंद किया गया था :

(अ) ग्राहक जिसने इसे लगाया उसके लिए अनूठा था।

(ब) उस ग्राहक की पहचान करने में सक्षम है।

(स) अंशदाता के एक मात्र नियंत्रण में एक विधि या एक तरीके से इसे तैयार किया गया हो एवं ये वैद्युतिक अभिलेख से इस प्रकार संबंधित हों कि यदि वैद्युतिक अभिलेख को परिवर्तित किया जाए

तो आंकिक हस्ताक्षर अवैध हो जाए।

तब ये आंकिक हस्ताक्षर एक सुरक्षित आंकिक हस्ताक्षर माने जाएंगे (धारा 15)।

सुरक्षाप्रक्रिया: जिस समय यह प्रणाली उपयोग की जाए उस समय की वाणिज्यिक परिस्थितियों को ध्यान में रखते हुए केन्द्र सरकार इस अधिनियम के उद्देश्यों हेतु एक सुरक्षा प्रणाली प्रस्तावित करेगी जिसमें कि निम्नलिखित शामिल होंगे :

(अ) सौदे की प्रकृति
(ब) तकनीकी क्षमता के संबंध में पक्षों की कुशलता का स्तर
(स) अन्य पक्षकारों की समान सौदों की मात्रा
(द) प्रस्तावित विकल्पों की उपलब्धता, परंतु जिसे किसी पक्ष ने रद्द कर दिया हो
(इ) विकल्प प्रक्रियाओं की लागत एवं
(फ) समान प्रकार के सौदों अथवा संचार हेतु सामान्य उपयोगों में लाई जाने वाली प्रक्रियाएं (धारा 16)

अध्याय--VI
प्रमाणीकरण प्राधिकारियों का नियमन

सामान्य प्रावधान

1. इस अधिनियम की धारा 17 के विभिन्न प्रावधानों में प्रमाणीकरण प्राधिकारियों के नियंत्रण एवं इस अधिनियम के उद्देश्यों की प्राप्ति हेतु एक नियंत्रक, उपनियंत्रकों तथा सहायक नियंत्रकों की नियुक्ति केन्द्र सरकार द्वारा अधिसूचना जारी करके की जा सकती है। इसके अतिरिक्त इन पदाधिकारियों के क्या कर्तव्य एवं दायित्व होंगे इनकी सेवाओं हेतु योग्यता, अनुभव तथा अन्य शर्तें भी केन्द्र सरकार द्वारा प्रस्तावित की जाएंगी। इनके मुख्य कार्यालय तथा शाखा कार्यालयों के स्थान भी केन्द्र सरकार द्वारा तय किए जाएंगे।

2. धारा 18 में उन विविध कार्यों का वर्णन किया गया है जो कि एक प्रमाणीकरण प्राधिकारियों के नियंत्रक द्वारा संपन्न किए जाएंगे।

3. इस अधिनियम की धारा 19 के तहत उन विभिन्न नियमों, परिस्थितियों

तथा प्रतिबंधों का उल्लेख किया गया है जिसे कि नियंत्रक केन्द्र सरकार की पूर्व अनुमति प्राप्त करके विदेशी प्रमाणीकरण प्राधिकारियों को मान्यता देने हेतु लागू कर सकता है एवं शासकीय गजट में अधिसूचना जारी करते हुए इनके नियंत्रण एवं नियमन हेतु अन्य प्रतिबंध एवं नियम भी प्रस्तावित किए जा सकते हैं।

4. धारा 20 के प्रावधानों के अनुसार नियंत्रक सभी आंकिक हस्ताक्षर प्रमाणपत्र जो कि इस अधिनियम के तहत जारी किए गए हों, हेतु सुरक्षित कोष का कार्य करेंगे। इस संबंध में विभिन्न हार्डवेयर, सॉफ्टवेयर, मानक तथा विभिन्न सुरक्षा प्रक्रियाएं इत्यादि का उल्लेख है जिनके द्वारा नियंत्रक सभी सार्वजनिक कुंजियों को इस प्रकार सुरक्षित रखेंगे कि वह जनता के किसी भी सदस्य को उपलब्ध हो सकें।

5. धारा 21 के तहत यह प्रावधान है कि नियंत्रक किसी भी आवेदनकर्ता को आंकिक हस्ताक्षर प्रमाणपत्र जारी करने हेतु अनुज्ञप्ति प्रदान कर सकता है, उन विभिन्न योग्यता, कुशलता, आर्थिक स्रोतों एवं अन्य आधारभूत सुविधाओं इत्यादि आवश्यकताओं का उल्लेख है जो कि आंकिक हस्ताक्षर प्रमाणपत्र जारी करने वाले अनुज्ञप्ति धारक के पास होना चाहिए। इस अनुज्ञप्ति का कार्यकाल तथा अन्य शर्तें एवं नियम केन्द्र सरकार द्वारा निर्दिष्ट किए जाएंगे।

6. इस अधिनियम की धारा 22 के अंतर्गत उपरोक्त अनुज्ञप्ति को प्राप्त करने हेतु किए जाने वाले आवेदनपत्र की विभिन्न आवश्यकताएं जैसे कि प्रारूप, शुल्क (25,000 रुपये से अधिक नहीं) एवं प्रक्रिया इत्यादि का वर्णन किया गया है।

7. धारा 23 में उपरोक्त अनुज्ञप्ति के नवीनीकरण हेतु नियमों का वर्णन किया गया है। नवीनीकरण शुल्क 5,000 रुपये से अधिक नहीं होगा तथा नवीनीकरण आवेदन अनुज्ञप्ति समाप्ति की तिथि के कम से कम 45 दिन पूर्व देना होगा।

8. धारा 24 में प्रावधान किया गया है कि धारा 21 में वर्णित एक आवेदन के प्राप्त हो जाने पर नियंत्रक आवेदन के साथ प्रस्तुत दस्तावेजों एवं अन्य बिंदुओं पर विचार करते हुए आवेदक को अनुज्ञप्ति प्रदान कर सकता है अथवा आवेदन को खारिज कर सकता है। यह भी प्रावधान है कि किसी आवेदन को

खारिज करने से पूर्व आवेदक को अपना पक्ष प्रस्तुत करने हेतु एक समुचित अवसर अवश्य प्रदान किया जाए।

अनुज्ञप्ति का निलंबन

1. धारा 25 के अनुसार नियंत्रक आवश्यक जांच करने के उपरांत यदि वह संतुष्ट है कि :

(अ) अनुज्ञप्ति के जारी करने अथवा नवीनीकरण हेतु प्रस्तुत आवेदन में कई महत्त्वपूर्ण विवरण असत्य अथवा गलत है।

(ब) अनुज्ञप्ति प्रदान करने की शर्तों एवं नियमों का पालन नहीं किया गया है।

(स) धारा 20 की उपधारा (2) के कथन (ब) में वर्णित मानकों को निर्वाह नहीं किया गया है।

(द) इस अधिनियम के प्रावधानों अथवा इसके अधीन बने नियमों, विनियमों अथवा आदेशों का उल्लंघन किया गया है।

तो यह अनुज्ञप्ति निलंबित की जा सकती है। यह भी प्रावधानित है कि कोई भी अनुज्ञप्ति तब तक निलंबित नहीं होगी जब तक कि प्रमाणीकरण प्राधिकारी को प्रस्तावित निलंबन के विरुद्ध अपना पक्ष प्रस्तुत करने हेतु एक समुचित अवसर प्रदान नहीं किया जाता।

यदि नियंत्रक को समुचित कारणों के साथ विश्वास है तो अनुज्ञप्ति को, जांच कार्य हेतु आदेश जारी करते हुए उस जांच के समापन तक निलंबित कर सकता है। परन्तु प्रमाणीकरण प्राधिकारी को सुनवाई का बिना समुचित अवसर दिए इस निलंबन की अवधि को 10 दिन से अधिक नहीं बढ़ाया जा सकता है।

2. धारा 26 के प्रावधानों के अनुसार किसी प्रमाणीकरण प्राधिकारी के अनुज्ञप्ति के निलंबन अथवा रद्दीकरण की सूचना नियंत्रक द्वारा नियमित समंक आधार अथवा आधारों में एवं एक पूरे समय क्रियाशील वेबसाइट में तथा किसी वैद्युतिक अथवा अन्य माध्यमों में प्रकाशित की जाएगी।

3. धारा 27 के तहत नियंत्रक इस अध्याय में वर्णित अपनी विभिन्न शक्तियों के प्रयोग हेतु उपनियंत्रक अथवा सहायक नियंत्रक को अधिकृत कर सकता है।

इस अधिनियम के प्रावधानों, नियमों इत्यादि के उल्लंघन की जांच नियंत्रक

अथवा उसके द्वारा अधिकृत किसी भी अधिकारी द्वारा जांच की जा सकती है एवं इस अन्वेषण हेतु नियंत्रक अथवा उसके अधिकारी उन्हीं समान शक्तियों का प्रयोग कर सकते हैं जो कि आयकर अधिनियम, 1961 के अध्याय 13 के अंतर्गत आयकर अधिकारियों को प्रदान की गई है।

नियंत्रक अथवा उसके द्वारा अधिकृत किसी व्यक्ति को किसी कंप्यूटर प्रणाली, उपकरण अथवा उस प्रणाली से संबंधित अन्य सामग्री तक पहुंचने का अधिकार होगा, यदि उसे यह समुचित विश्वास है कि इस अधिनियम के प्रावधानों अथवा नियमों का उल्लंघन किया गया है। जांच कार्य हेतु नियंत्रक अथवा अन्य अधिकृत व्यक्ति द्वारा उस कंप्यूटर प्रणाली के प्रभारी व्यक्ति को समुचित तकनीकी एवं अन्य सहायता प्रदान करने हेतु भी आदेशित किया जा सकता है।

प्रमाणीकरणप्राधिकारीकेदायित्व: धारा 30 के अनुसार प्रत्येक प्रमाणीकरण प्राधिकारी :

(अ) ऐसे हार्डवेयर, सॉफ्टवेयर एवं प्रक्रियाओं का उपयोग करेंगे जो कि दुरुपयोग एवं अनाधिकृत प्रवेश से सुरक्षित हों।

(ब) अपनी सेवाओं में समुचित विश्वसनीयता प्रदान करेंगे जो कि वांछित क्रियाओं को संपन्न करने हेतु स्वीकार्य हों।

(स) ऐसी सुरक्षा प्रणाली अपनाएंगे जिससे कि आंकिक हस्ताक्षर की गोपनीयता सदैव निश्चित रहे एवं,

(द) उन अन्य मानकों को अपनाएंगे जो कि विनियमों में निर्देशित हों।

धारा 31 में वर्णित किया गया है कि प्रमाणीकरण प्राधिकारी तथा उसके कर्मचारीगण अपने क्रियाकलापों के दौरान इस अधिनियम के विभिन्न प्रावधानों तथा नियमों का पालन किया जाना सुनिश्चित करेंगे।

प्रत्येक प्रमाणीकरण प्राधिकारी अपने व्यवसाय भवन में समुचित स्थान पर प्राप्त अनुज्ञप्ति का प्रदर्शन करेंगे। (धारा 32)

प्रत्येक प्रमाणीकरण प्राधिकारी निलंबन के तुरंत बाद अपनी अनुज्ञप्ति को नियंत्रक के समक्ष समर्पित करेंगे। ऐसा न किए जाने की दशा में वे 10,000 रुपये का जुर्माना अथवा 6 महीने तक का कारावास अथवा दोनों से ही दण्डित किए जा सकते हैं। (धारा 33)

इस अध्याय की धारा 34 के तहत प्रत्येक प्रमाणीकरण प्राधिकारी हेतु उन नियमों को वर्णित किया गया है जो कि उसके द्वारा जारी आंकिक हस्ताक्षर प्रमाण पत्र एवं अन्य व्यवहारों में विभिन्न प्रकार की घोषणाओं से संबंधित हैं।

अध्याय–VII
आंकिक हस्ताक्षर प्रमाणपत्र

आंकिकहस्ताक्षरप्रमाणपत्रजारीकरना : अधिनियम की धारा 35 से लेकर 39 तक में आंकिक हस्ताक्षर प्रमाणपत्रों के जारी किए जाने हेतु विभिन्न नियमों तथा प्रावधानों को उल्लेखित किया गया है।

धारा 35 में एक आंकिक हस्ताक्षर प्रमाणपत्र के जारी किए जाने की प्रक्रिया का वर्णन किया गया है। इसमें प्रावधान है कि इस प्रमाणपत्र को प्राप्त करने हेतु एक आवेदन निर्धारित प्रारूप में, तथा शुल्क जो कि 25,000 रुपये से अधिक नहीं होगा के साथ जमा किया जाएगा। इस शुल्क की राशि केन्द्र सरकार द्वारा निर्धारित की जाएगी। विभिन्न श्रेणी के आवेदनों हेतु अलग-अलग फीस भी प्रस्तावित की जा सकती है।

इस धारा में यह भी प्रावधान है कि कोई आंकिक हस्ताक्षर प्रमाणपत्र प्रदान नहीं किया जाएगा जब तक कि प्रमाणीकरण प्राधिकारी संतुष्ट नहीं हो जाते हैं कि :

(अ) आवेदक के पास आंकिक हस्ताक्षर प्रमाणपत्र में सूचीबद्ध करने हेतु एक सार्वजनिक कुंजी से संबंधित निजी कुंजी है।

(ब) आवेदक के पास एक ऐसी निजी कुंजी है जो कि एक आंकिक हस्ताक्षर की रचना करने में सक्षम है।

(स) प्रमाणपत्र में सूचीबद्ध की जानेवाली सार्वजनिक कुंजी एक आंकिक हस्ताक्षर जिसे कि आवेदक ने अपनी निजी कुंजी के द्वारा निर्मित किया है, को प्रमाणीकृत अथवा सत्यापित कर सकती है।

कोई भी आवेदन बिना आवेदक को सुनवाई का उचित अवसर प्रदान किए निरस्त नहीं किया जाएगा।

आंकिक हस्ताक्षर प्रमाणपत्र जारी करते समय प्रमाणीकरण प्राधिकारी यह सत्यापित करेंगे कि उन्होंने इस अधिनियम के प्रावधानों, इसके तहत बनाए

गए नियमों एवं विनियमों में आंकिक हस्ताक्षर प्रमाणपत्र में वर्णित अन्य शर्तों का पालन किया है।

आंकिकहस्ताक्षरप्रमाणपत्रकानिलंबन : प्रमाणीकरण प्राधिकारी, किसी आंकिक हस्ताक्षर प्रमाणपत्र को निलंबित कर सकते हैं यदि उन्हें यह विश्वास हो कि ऐसा कदम उठाना सार्वजनिक हित में होगा। (धारा 37)

कोई प्रमाणपत्र 15 दिवस की अवधि से अधिक समय के लिए निलंबित नहीं किया जा सकता जब तक कि अंशदाता को एक उचित सुनवाई का अवसर प्रदान नहीं किया जाता।

धारा 38 में उन विभिन्न परिस्थितियों का उल्लेख किया गया है जिनके अंतर्गत किसी आंकिक हस्ताक्षर प्रमाणपत्र को खारिज किया जा सकता है। यह खंडन तब तक नहीं किया जा सकेगा जब तक कि अंशदाता को उस विषय में सुनवाई का एक समुचित अवसर प्रदान नहीं किया जाता।

एक आंकिक हस्ताक्षर प्रमाणपत्र के उपरोक्त निलंबन अथवा खंडन की अधिसूचना प्रमाणीकरण प्राधिकारी के द्वारा प्रकाशित की जाएगी।

अध्याय–VIII
अंशदाताओं के कर्तव्य

कुंजियोंकेजोड़ेकाउत्पादन : धारा 40 के प्रावधानों के अनुसार जब कोई आंकिक हस्ताक्षर प्रमाणपत्र किसी अंशदाता द्वारा उन परिस्थितियों में लिया जाता है कि उसके पास आंकिक प्रमाणपत्र में सूचीबद्ध होने वाली सार्वजनिक कुंजी के अनुरूप निजी कुंजी उपलब्ध है तो वह अंशदाता सुरक्षा प्रणाली को लागू करते समय कुंजी के जोड़े को उत्पादित करेगा।

आंकिकहस्ताक्षरप्रमाणपत्रकीस्वीकृति (धारा41) :

1. एक अंशदाता द्वारा एक आंकिक हस्ताक्षर प्रमाणपत्र स्वीकृत माना जाता है यदि वह इस आंकिक हस्ताक्षर प्रमाणपत्र को प्रकाशित करता है अथवा इसके प्रकाशन हेतु किसी एक या अधिक व्यक्तियों को अथवा एक कोष को प्रकाशन की अनुमति प्रदान करता है। अथवा किसी अन्य तरीके से आंकिक हस्ताक्षर प्रमाणपत्र को अपनी स्वीकृति का प्रदर्शन करता है।

2. एक आंकिक हस्ताक्षर प्रमाणपत्र को स्वीकृत करते हुए अंशदाता उन

सभी को जो कि उचित रूप से आंकिक हस्ताक्षर प्रमाणपत्र में निहित सूचनाओं पर विश्वास करते हैं, को प्रमाणित करता है कि :

(अ) अंशदाता के पास आंकिक हस्ताक्षर प्रमाणपत्र में सूचित सार्वजनिक कुंजी से संबंधित निजी कुंजी है तथा वह इसे रखने हेतु अधिकृत है।

(ब) अंशदाता द्वारा प्रमाणीकरण प्राधिकारी के समक्ष प्रस्तुत सभी प्रतिवेदन एवं आंकिक हस्ताक्षर प्रमाणपत्र में निहित सूचनाओं से संबंधित सभी तथ्य सत्य हैं।

(स) अंशदाता की जानकारी के अनुसार आंकिक हस्ताक्षर प्रमाणपत्र में निहित सभी सूचनाएं सत्य हैं।

निजीकुंजीकानियंत्रण(धारा42)

1. प्रत्येक अंशदाता निजी कुंजी जो कि आंकिक हस्ताक्षर प्रमाणपत्र में सूचित सार्वजनिक कुंजी के अनुरूप है, पर नियंत्रण रखने हेतु समुचित कार्रवाई करेगा, एवं वह सभी आवश्यक कदम उठाएगा जो कि इसके किसी ऐसे व्यक्ति जिसे कि अंशदाता ने आंकिक हस्ताक्षर हेतु अधिकृत नहीं किया हो, के समक्ष प्रकट होने से रोकने के लिए आवश्यक हैं।

2. यदि कोई निजी कुंजी जो कि आंकिक हस्ताक्षर प्रमाणपत्र में सूचीबद्ध सार्वजनिक कुंजी से संबंधित है, जब विवादित हो जाती है तो अंशदाता इसे बिना कोई समय गंवाए विनियमों में निहित तरीके से प्रमाणीकरण प्राधिकारी को सूचित करेंगे।

3. भ्रांतियों को दूर करने हेतु यहां यह स्पष्ट किया जाता है कि उस समय तक जब तक कि निजी कुंजी के विवादित होने की सूचना प्रमाणीकरण प्राधिकारी तक नहीं पहुंच जाती अंशदाता उत्तरदायी रहेगा।

अध्याय–IX
दंड एवं न्यायिक निर्णय

कंप्यूटर,कंप्यूटरप्रणालीइत्यादिकोनुकसानहेतुशास्ति : (धारा 43) के प्रावधानों के अनुसार यदि कोई व्यक्ति एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र के मालिक अथवा कोई अन्य प्रभारी व्यक्ति की आज्ञा के बिना :

(अ) उसे कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में प्रवेश करता है।

(ब) उस कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र जिसमें कि किसी प्रतिस्थापन योग्य भण्डारण माध्यम में निहित समंक अथवा सूचना भी सम्मिलित हैं, से कोई समंक, कंप्यूटर समंक आधार अथवा सूचना को नकल करता है, डाउन लोड करता है, अथवा निकालता है।

(स) किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में कोई कंप्यूटर प्रदूषण अथवा कंप्यूटर वायरस को प्रविष्ट करता है अथवा कराता है।

(द) कोई कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र एवं इनमें निहित समंक, समंक आधार अथवा अन्य कार्यक्रमों को क्षति पहुंचाता है अथवा क्षति पहुंचाने का भागीदार बनता है।

(इ) कोई कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में विघ्न पैदा करता है अथवा विघ्न पैदा कराता है।

(फ) किसी व्यक्ति को जो कि किसी कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में पहुंचने के लिए अधिकृत है, को किसी भी तरीके द्वारा प्रवेश की मनाही करता है अथवा मनाही कराता है।

(ज) इस अधिनियम के प्रावधानों तथा इसके तहत बनाए गए नियमों अथवा विनियमों का उल्लंघन करते हुए किसी व्यक्ति को एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में प्रवेश करने की कोई सुविधा उपलब्ध कराता है।

(च) किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र से छेड़-छाड़ अथवा हेराफेरी करते हुए किसी व्यक्ति के द्वारा उपयोग की गई सेवाओं का शुल्क किसी दूसरे व्यक्ति के खाते में लगाता है।

वह व्यक्ति इस प्रकार से प्रभावित व्यक्ति को क्षतिपूर्ति जो कि 1,00,00,000 रुपये (एक करोड़ रुपये) से अधिक न हो, का भुगतान करने हेतु उत्तरदायी होगा।

स्पष्टीकरण : इस धारा के उद्देश्यों हेतु :

(i) 'कंप्यूटर प्रदूषण' से आशय कंप्यूटर निर्देशों की एक श्रेणी से होता है जो कि एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में विद्यमान किसी अभिलेख, प्रेषण समंक अथवा कार्यक्रम को परिवर्तित अथवा नष्ट करने हेतु बनाए जाते हैं अथवा कंप्यूटर अथवा कंप्यूटर तंत्र के सामान्य क्रियाकलापों पर किसी भी साधन द्वारा अनधिकृत कब्जा कर लेने से होता है।

(ii) 'कंप्यूटर समंक आधार' से आशय सूचना, ज्ञान, तथ्य, विचार अथवा निर्देशों के प्रतिनिधित्व हेतु बनाए गए दस्तावेज, आकृति, ध्वनि एवं दृश्यों से है जो कि औपचारिक तौर पर बनाए गए हैं अथवा एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र द्वारा उत्पादित किए गए हैं एवं जिनका उद्देश्य एक कंप्यूटर अथवा कंप्यूटर प्रणाली में प्रयोग किया जाना है।

(iii) 'कंप्यूटर वायरस' से आशय किसी कंप्यूटर निर्देश, सूचना, समंक अथवा कार्यक्रम से होता है जो कि एक कंप्यूटर स्रोत को नष्ट कर देता है, हानि पहुंचाता है अथवा उसकी कार्यक्षमता को कम करता है अथवा उसे विपरीत रूप से प्रभावित करता है। अथवा यह अपने आपको किसी दूसरे कंप्यूटर स्रोत से जोड़ लेता है एवं उस दूसरे कंप्यूटर में जैसे ही कार्यक्रम, समंक अथवा निर्देश क्रियान्वित किए जाते हैं अथवा कोई अन्य घटना घटती है तब यह क्रियाशील हो जाते हैं एवं उसे भी नुकसान पहुंचाते हैं।

(iv) ''क्षति'' से आशय किसी कंप्यूटर स्रोत को किसी भी प्रकार से नष्ट करना, परिवर्तित करना, मिटाना, चुराना, बदलना अथवा पुनः व्यवस्थित करने से होता है।

अन्यजुर्माने : धारा 44 एवं 45 में कुछ अन्य अपराध अथवा भूलों हेतु शास्ति अथवा जुर्माना लगाए जाने के प्रावधानों को वर्णित किया गया है। ये अपराध अथवा चूकें समय पर सूचना, विवरण अथवा दस्तावेज अथवा प्रतिवेदन, इत्यादि जमा नहीं करने से संबंधित हैं तथा ऐसे उल्लंघन भी इनमें शामिल हैं जिनका उल्लेख स्पष्ट रूप से इस अधिनियम में कहीं नहीं किया गया है। इन धाराओं में 5,000 रुपये प्रतिदिन से लेकर प्रत्येक गलती के लिए

1,50,000 रुपये तक की शास्ति वसूलने का प्रावधान है।

न्यायिकजांच(धारा46) : धारा 46 के द्वारा यह अधिकार दिया गया है कि एक अधिकारी जो कि भारत सरकार के एक डायरेक्टर के नीचे के पद का न हो अथवा एक राज्य सरकार का समरूप अधिकारी हो, इस अधिनियम के उल्लंघन की न्यायिक जांच कर सकता है। यह नियुक्ति केन्द्र सरकार द्वारा की जाएगी। एक न्यायिक जांच अधिकारी के पद पर नियुक्ति हेतु योग्यताओं में उस व्यक्ति को केन्द्र सरकार द्वारा प्रस्तावित सूचना तकनीक क्षेत्र का समुचित अनुभव होना चाहिए एवं विधि अथवा न्यायिक कार्यों का अनुभव भी होना चाहिए। इस प्रकार से नियुक्त न्यायिक जांच अधिकारी दूसरे पक्ष को सुनवाई का समुचित अवसर देते हुए निर्दिष्ट तरीके से जांच करने हेतु जिम्मेदार होगा एवं इसके पश्चात् जहां आवश्यकता हो वहां जुर्माना या शास्ति भी लगाएगा।

धारा 47 में प्रावधानित किया गया है कि क्षतिपूर्ति की राशि निर्धारित करते समय न्यायिक जांच अधिकारी को दोषी व्यक्ति द्वारा प्राप्त किए गए अनुचित फायदों एवं किसी व्यक्ति को हुई क्षति एवं साथ ही साथ हुई त्रुटि की प्रकृति को समुचित ध्यान में रखना होगा।

अध्याय–X
साइबर नियमन अपीलीय न्यायाधिकरण

साइबरनियमनअपीलीयन्यायाधिकरणकीस्थापना : केन्द्र सरकार अधिसूचना जारी करके एक या अधिक अपीलीय न्यायाधिकरणों की स्थापना कर सकती है। जहां कि साइबर नियमन अपीलीय न्यायाधिकरण के नाम से जाना जाएगा। (धारा 48)

केन्द्र सरकार उपरोक्त अधिसूचना में उन विषयों तथा स्थानों का भी उल्लेख करेगी जो कि इस साइबर अपीलीय न्यायाधिकरण के न्याय क्षेत्र में आएंगे।

धारा 49 के प्रावधानों के अनुसार एक साइबर अपीलीय न्यायाधिकरण में केवल एक ही सदस्य होगा जिसकी नियुक्ति केन्द्र सरकार द्वारा अधिसूचना जारी करके की जाएगी। (बाद में इस व्यक्ति को साइबर अपीलीय न्यायाधिकरण के पीठासीन अधिकारी के नाम से संबोधित किया गया है।)

पीठासीनअधिकारी : धारा 50 के अनुसार किसी साइबर अपीलीय न्यायाधिकरण के पीठासीन अधिकारी के पद पर नियुक्ति हेतु निम्नलिखित योग्यताएं होना आवश्यक है :

(अ) वह एक उच्च न्यायालय का न्यायाधीश हो अथवा रहा हो अथवा होने के योग्य हो अथवा

(ब) भारतीय न्यायिक सेवाओं का एक सदस्य हो अथवा सदस्य रहा हो एवं इन सेवाओं में ग्रेड-1 के पद पर कम से कम 3 वर्षों तक रहा हो।

एक साइबर अपीलीय न्यायाधिकरण के पीठासीन अधिकारी का कार्यकाल उसके दफ्तर में प्रवेश से 5 वर्षों तक अथवा उसकी 65 वर्ष की आयु पूरी होने तक दोनों में से जो भी कम हो, का होगा। (धारा 51)

धारा 52 में पीठासीन अधिकारी को दिए जाने वाले वेतन, भत्तों तथा उनकी सेवा की अन्य शर्तें जिनमें सेवा निवृत्ति लाभ इत्यादि सम्मिलित हैं, का वर्णन किया गया है।

धारा 53 के प्रावधानों के अनुसार अस्थायी छुट्टी को छोड़कर पीठासीन अधिकारी के दफ्तर में हुई रिक्त की पदस्थापना केन्द्र सरकार द्वारा की जाएगी।

एक पीठासीन अधिकारी अपने हस्ताक्षरों द्वारा केन्द्र सरकार को अपने पद से त्यागपत्र भेज सकता है परंतु वह उक्त सूचना देने के पश्चात् तीन माह तक अथवा उसके स्थान पर किसी दूसरे व्यक्ति की नियुक्ति तक दोनों में से जो भी पहले हो अपना पद नहीं छोड़ सकता।

दुर्व्यवहार अथवा अक्षमता का दोषी पाए जाने पर एक सर्वोच्च न्यायालय के न्यायाधीश द्वारा जांच किए जाने एवं दोष सिद्ध पाए जाने पर केन्द्र सरकार पीठासीन अधिकारी को उसके पद से हटा सकती है।

अपीलीय न्यायाधिकरण के पीठासीन अधिकारी की नियुक्ति हेतु केन्द्र सरकार द्वारा पारित किए गए आदेश अंतिम माने जाएंगे एवं इनमें कोई खामी है तो भी यह इसकी जांच कार्यों को अवैध नहीं करेगी। (धारा 55)

केन्द्र सरकार साइबर अपीलीय न्यायाधिकरण हेतु अन्य अधिकारियों एवं कर्मचारियों की नियुक्ति भी करेगी, इनके वेतन भत्ते इत्यादि भी केन्द्र सरकार द्वारा निर्दिष्ट किए जाएंगे। (धारा 56)

साइबरअपीलीयन्यायाधिकरणकोअपील : इस अध्याय की धारा 57 के प्रावधानों के अनुसार नियंत्रक अथवा न्यायिक जांच अधिकारी द्वारा पारित आदेश के विरुद्ध किसी पीड़ित व्यक्ति द्वारा साइबर अपीलीय न्यायाधिकरण को अपील की जा सकेगी। परंतु न्यायिक अधिकारी द्वारा पारित एक ऐसे आदेश जिसे कि सभी पक्षकारों की सहमति द्वारा पारित किया गया हो, के विरुद्ध साइबर अपीलीय न्यायाधिकरण के समक्ष कोई अपील मान्य नहीं होगी।

नियंत्रक अथवा न्यायिक अधिकारी द्वारा पारित आदेश की प्रतिलिपि पीड़ित व्यक्ति द्वारा प्राप्त होने के उपरांत निर्दिष्ट प्रारूप में तथा निर्दिष्ट शुल्क के साथ 45 दिनों की अवधि के अंतर्गत यह अपील की जाएगी। यदि साइबर अपीलीय न्यायाधिकरण को यह संतुष्टि हो जाए कि निर्धारित समय सीमा में अपील फाइल नहीं करने का समुचित कारण मौजूद है तो वह इस अपील को 45 दिन की अवधि के पश्चात् भी स्वीकार कर सकता है।

साइबर अपीलीय न्यायाधिकरण अपील के सभी पक्षकारों को सुनवाई का अवसर प्रदान करते हुए अपने विवेक अनुसार अपील किए गए आदेश की पुष्टिकरण, परिवर्तित अथवा रद्द करने हेतु आदेश पारित कर सकते हैं।

साइबर अपीलीय न्यायाधिकरण अपने द्वारा पारित आदेश की प्रतिलिपि अपील से संबंधित पक्षकारों को एवं संबंधित नियंत्रक अथवा न्यायिक जांच अधिकारी को भेजेंगे।

साइबर अपीलीय न्यायाधिकरण उपधारा (1) के तहत प्रस्तुत अपील को शीघ्रता एवं सभी संभावित उपाय करते हुए इसका अंतिम रूप से निबटान अपील की प्राप्ति के 6 महीनों के अंदर करेगा।

धारा 58 के प्रावधानों के अनुसार साइबर अपीलीय न्यायाधिकरण दीवानी प्रक्रिया संहिता 1908 की प्रक्रिया तथा प्रावधान से बाध्य नहीं होगी परंतु उस पर इस अधिनियम के प्रावधान तथा प्राकृतिक न्याय के सिद्धांत लागू होंगे तथा न्यायाधिकरण को यह अधिकार होगा कि वह अपनी बैठकों हेतु स्वयं अपनी प्रक्रिया बनाएं।

प्रकरण की सुनवाई के दौरान साइबर अपीलीय न्यायाधिकरण को वही शक्तियां प्राप्त होंगी जो कि एक दीवानी न्यायालय को दीवानी प्रक्रिया संहिता के अनुसार एक प्रकरण की सुनवाई के दौरान प्राप्त होती है।

साइबर अपीलीय न्यायाधिकरण के समक्ष अपना प्रकरण प्रस्तुत करने हेतु प्रकरण से संबंधित पक्षकार स्वयं उपस्थित हो सकते हैं अथवा एक या अधिक अधिवक्ताओं अथवा अपने किसी अधिकारी को अधिकृत कर सकते हैं। (धारा 59)

दीवानीन्यायालयकेअधिकारक्षेत्रसेबाहर : किसी भी न्यायालय को किसी ऐसे मामले से संबंधित प्रकरण अथवा कार्रवाई को स्वीकार करने का न्याय क्षेत्र प्राप्त नहीं होगा जिनमें कि इस अधिनियम के अंतर्गत नियुक्त न्यायिक अधिकारी अथवा इस अधिनियम के तहत स्थापित साईबर अपीलीय न्यायाधिकरण को इस अधिनियम के तहत निर्णीत करने एवं सुनने का अधिकार है एवं कोई भी न्यायालय अथवा कोई प्राधिकारी इस अधिनियम की शक्तियों के अधीन की गई किसी कार्रवाई अथवा की जाने वाली कार्रवाई के विरुद्ध कोई निषेधाज्ञा प्रदान नहीं करेगा। (धारा 61)

उच्चन्यायालयकोअपील : साइबर अपीलीय न्यायाधिकरण द्वारा पारित किसी निर्णय अथवा आदेश से पीड़ित कोई व्यक्ति इस निर्णय अथवा आदेश सूचना के प्राप्ति के 60 दिनों के अंदर किसी तथ्य अथवा विधि के प्रश्न जो कि उस आदेश से उत्पन्न हुआ है, के विरुद्ध उच्च न्यायालय में अपील कर सकता है। (धारा 62)

यदि उच्च न्यायालय संतुष्ट है कि अपील करने वाले व्यक्ति के पास निर्धारित समय सीमा में अपील दाखिल नहीं करने हेतु समुचित कारण मौजूद हैं, तो वह इस अवधि को अगले 60 दिनों की अवधि तक और बढ़ा सकता है।

उल्लंघनराजीनामाकरना : धारा 63 के प्रावधानों के अनुसार इस अध्याय के अंतर्गत किए गए किसी उल्लंघन को न्यायिक प्रक्रिया शुरू होने के पूर्व अथवा बाद में नियंत्रक अथवा न्यायिक अधिकारी अथवा किसी अन्य अधिकारी जिसे कि इस बारे में विशिष्ट रूप से अधिकृत किया गया हो, के द्वारा उन शर्तों के तहत जो कि नियंत्रक अथवा अन्य अधिकारी अथवा न्यायिक अधिकारी द्वारा लगाई जाएं, समझौता अथवा राजीनामा किया जा सकता है।

यह भी प्रावधान है कि इस समझौते की राशि किसी भी परिस्थिति में इस उल्लंघन हेतु इस अधिनियम के तहत लगाई जाने वाली अधिकतम शास्ति की राशि से अधिक नहीं होगी।

उपधारा (1) के प्रावधान उस व्यक्ति पर लागू नहीं होंगे जिसे कि अपने द्वारा किए गए प्रथम समान प्रकृति के उल्लंघन को राजीनामा कराए जाने के बाद 3 वर्ष की अवधि पूरी नहीं हुई है।

स्पष्टीकरण : इस उपधारा के उद्देश्यों हेतु कोई दूसरा अथवा अन्य अगला उल्लंघन यदि यह पिछले राजीनामे के 3 वर्षों की अवधि के बाद किया जाता है तो इसे प्रथम उल्लंघन माना जाएगा।

जब किसी उल्लंघन का उपधारा (1) के अनुसार राजीनामा किया जाता है तो उस व्यक्ति के विरुद्ध चल रही कार्रवाई रोक दी जाएगी तथा अगली कार्रवाई हेतु कोई कदम नहीं उठाया जाएगा।

धारा 64 के प्रावधानों के अनुसार इस अधिनियम के तहत अधिरोपित की गई किसी शास्ति अथवा जुर्माने का यदि भुगतान नहीं किया जाता तो इसकी वसूली भू-राजस्व के समान की जा सकती है तथा वह अनुज्ञप्ति अथवा आंकिक हस्ताक्षर प्रमाणपत्र तब तक निलंबित होंगे जब तक कि जुर्माने का भुगतान नहीं कर दिया जाता।

अध्याय–X
अपराध

अध्याय XI में धारा 65 से 78 तक कुछ कंप्यूटर अपराधों का वर्णन किया गया है। इन अपराधों हेतु सजा के प्रावधान निहित हैं, जिनमें :

1. धारा 65 में प्रावधानित किया गया है कि यदि कोई व्यक्ति जानबूझकर अथवा इरादे के साथ किसी कंप्यूटर कूट संकेत अथवा स्रोत कार्यक्रम को जिसे किसी एक कंप्यूटर, कंप्यूटर कार्यक्रम, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र में उपयोग किया जाना है एवं जिसे कि रखा जाना उस समय प्रचलित कानून के अनुसार आवश्यक है, को छिपाता है, नष्ट करता है अथवा परिवर्तित करता है अथवा किसी अन्य व्यक्ति को छिपाने, नष्ट करने, अथवा परिवर्तित करने हेतु प्रेरित करता है, तो उसे तीन वर्ष तक का कारावास अथवा 2,00,000 रुपये तक का जुर्माना अथवा दोनों से ही दण्डित किया जा सकता है।

इस धारा हेतु कंप्यूटर स्रोत कोड से आशय कार्यक्रमों की सूची, कंप्यूटर निर्देश, कंप्यूटर स्रोत की किसी प्रारूप में डिजाइन अथवा कार्यक्रम विश्लेषण है।

2. ***कंप्यूटरप्रणालीकोतितर-बितरकरना*** : धारा 66 में एक कंप्यूटर स्रोत में निहित किसी सूचना को नष्ट करने अथवा मिटाने अथवा इसे परिवर्तित करने अथवा इसकी मूल्य अथवा उपयोगिता को घटाने अथवा इसे हानिकारक रूप से प्रभावित करने हेतु किए गए कार्यों को परिभाषित किया गया है। यह क्रिया जानते हुए भी की जाती है कि वह कार्य किसी व्यक्ति को अथवा आम जनता को हानि अथवा क्षति पहुंचाने का कारक होगा, धारा 66 में यह प्रावधानित किया गया है कि एक व्यक्ति जो कि हैकिंग का अपराध करता है उसे 2,00,000 रुपये तक जुर्माना अथवा तीन वर्ष का कारावास अथवा दोनों से दण्डित किया जाएगा।

3. धारा 67 में प्रावधान है कि जो व्यक्ति अश्लील सामग्री को वैद्युतिक रूप में प्रेषित करता है अथवा प्रकाशित करता है अथवा प्रेषित अथवा प्रकाशित कराता है उसे 5 वर्ष तक का कारावास एवं 1,00,000 रुपये तक के जुर्माने से प्रथम बार दण्डित किया जाएगा। दूसरे एवं अगले अपराध की दशा में कारावास की अवधि 10 वर्षों तक एवं 2,00,000 रुपये तक के जुर्माने से दण्डित किया जाएगा।

4. धारा 68 के प्रावधानों के अनुसार इस अधिनियम के प्रावधानों तथा इसके तहत बने नियमों अथवा विनियमों के पालन हेतु नियंत्रक आदेश द्वारा एक प्रमाणीकरण प्राधिकारी अथवा उसके किसी कर्मचारी को निर्देशित कर सकते हैं कि वह आदेश में निर्दिष्ट कदम उठाएं अथवा आदेश में वर्णित कार्यों को किए जाना बंद कर दें।

यदि किसी व्यक्ति द्वारा उपरोक्त आदेश का पालन नहीं किया जाता तो यह जुर्म माना जाएगा एवं उस व्यक्ति को 2,00,000 रुपये तक जुर्माना अथवा तीन वर्ष तक का कारावास अथवा दोनों से दण्डित किया जा सकता है।

5. धारा 69 द्वारा नियंत्रक को शक्तियां प्रदान की हैं कि यदि वह संतुष्ट हैं कि भारत की विश्वसनीयता एवं सम्प्रभुता, राज्य की सुरक्षा, विदेशी राज्यों से मित्रतापूर्ण संबंध अथवा लोकशांति कायम रखने हेतु यह करना आवश्यक है, तो वह कोई कंप्यूटर प्रणाली अथवा कंप्यूटर नेटवर्क के द्वारा भेजी गई किसी सूचना को मार्ग में रोक सकता है।

6. धारा 70 उपयुक्त सरकार को शक्ति प्रदान करती है कि वे अधिसूचना जारी करके किसी कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र को एक संरक्षित

प्रणाली घोषित करें। इन प्रणालियों तक कोई अनधिकृत पहुंच अथवा प्रवेश को जुर्माने अथवा 10 वर्ष के कारावास तक से दण्डित किया जा सकता है।

7. धारा 71 के प्रावधानों के अनुसार यदि कोई व्यक्ति नियंत्रक अथवा प्रमाणीकरण प्राधिकारी के समक्ष गलत बयान करता है अथवा कोई महत्त्वपूर्ण तथ्य छिपाता है तो उसे 2 वर्षों तक के कारावास अथवा 1,00,000 रुपये तक जुर्माना अथवा दोनों से दण्डित किया जा सकता है।

8. ***(धारा72)गोपनीयताएवंविश्वसनीयताकोभंगकरना*** : एक व्यक्ति जो कि वैद्युतिक अभिलेखों, पुस्तकों, सूचना इत्यादि तक पहुंच रखता हो अथवा इनमें प्रवेश कर सकता हो, को जिस व्यक्ति से ये संबंधित हैं उसकी अनुमति के बिना यदि इनकी गोपनीयता एवं विश्वसनीयता को भंग करता है तो उसे दो वर्ष तक के कारावास अथवा 1,00,000 रुपये तक का जुर्माना अथवा दोनों से दण्डित किया जा सकता है।

9. धारा 73 में प्रावधान है कि यदि कोई व्यक्ति एक ऐसे आंकिक हस्ताक्षर प्रमाणपत्र जिसके महत्त्वपूर्ण विवरण गलत हैं, का प्रकाशन करता है अथवा इसे किसी अन्य व्यक्ति को उपलब्ध कराता है तो इस जुर्म के हेतु 2 वर्षों तक के कारावास अथवा 1,00,000 रुपये तक के जुर्माने अथवा दोनों से दण्डित किया जा सकता है।

10. धारा 74 यदि एक व्यक्ति जो कि जानबूझकर धोखा-धड़ी करने के उद्देश्य से किसी आंकिक हस्ताक्षर प्रमाणपत्र को प्रकाशित करता है तो धारा 74 में प्रावधानित किया गया है इस व्यक्ति को 2 वर्ष तक के कारावास अथवा 1,00,000 रुपये तक के जुर्माने अथवा दोनों से दण्डित किया जा सकता है।

11. ***भारतवर्षकेबाहरकिएगएअपराध*** : धारा 75 के अंतर्गत एक व्यक्ति को बिना उसकी राष्ट्रीयता की परवाह किए इस अधिनियम के तहत उसके द्वारा भारतवर्ष के बाहर किए गए किसी जुर्म अथवा उल्लंघन हेतु समान रूप से दण्डित किया जाएगा। यदि यह कार्य अथवा व्यवहार भारतवर्ष में स्थित एक कंप्यूटर, कंप्यूटर प्रणाली अथवा कंप्यूटर तंत्र से संबंधित जुर्म अथवा उल्लंघन की स्थापना करता है।

12. ***'जब्ती'*** : धारा 76 के प्रावधानों के अनुसार इस अधिनियम के किसी प्रावधान, नियम, विनियम अथवा आदेशों के उल्लंघन की दशा में किसी

कंप्यूटर, कंप्यूटर प्रणाली, फ्लॉपी, कम्पैक्ट डिस्क अथवा सी.डी., टेप अथवा अन्य सहायक उपकरणों की जब्ती की जाएगी।

यदि जब्ती प्रकरण की सुनवाई कर रहे न्यायालय के समक्ष यह स्थापित कर दिया जाए एवं न्यायपूर्ण रूप से संतुष्ट हो जाए कि ये कंप्यूटर, कंप्यूटर प्रणाली, फ्लॉपी, सी.डी. इत्यादि जिस व्यक्ति के अधिकार, शक्ति अथवा नियंत्रण में है वह व्यक्ति इस अधिनियम के किसी प्रावधान, नियम, आदेश अथवा विनियमों के उल्लंघन हेतु उत्तरदायी नहीं है तो न्यायालय उस कंप्यूटर प्रणाली अथवा फ्लॉपी इत्यादि की जब्ती का आदेश देने की बजाए इस अधिनियम के प्रावधानों, नियमों, आदेशों अथवा विनियमों का उल्लंघन करने वाले व्यक्ति के विरुद्ध इस अधिनियम द्वारा अधिकृत कोई अन्य आदेश पारित कर सकता है।

धारा 77 के प्रावधानों के अनुसार इस अधिनियम के अंतर्गत प्रावधानित जुर्माने एवं जब्ती उस समय में प्रचलित किसी अन्य कानून के अंतर्गत दिए जाने योग्य अन्य सजाओं को प्रभावित नहीं करेंगे।

धारा 78 प्रावधानित करता है कि इस अधिनियम के तहत किए गए जुर्म की विवेचना का अधिकार पुलिस उपअधीक्षक से निचले स्तर के किसी अधिकारी को नहीं होगा।

अध्याय–XI

कईप्रकरणोंमेंतंत्रसेवाप्रदाताउत्तरदायीनहींहोंगे : अध्याय 12 की धारा 79 में प्रावधान है कि एक नेटवर्क सेवा प्रदाता किसी तृतीय पक्ष सूचना अथवा समंक जो कि उसके द्वारा उपलब्ध कराए गए हैं, हेतु इस अधिनियम अथवा इसके तहत बनाए गए नियमों एवं विनियमों के अंतर्गत उत्तरदायी नहीं होगा। यदि वह सिद्ध कर देता है कि वह जुर्म अथवा उल्लंघन बिना उसकी जानकारी के किया गया है अथवा उसने उस जुर्म अथवा उल्लंघन के किए जाने को रोकने हेतु आवश्यक सभी सावधानियां बरती थीं।

स्पष्टीकरण :

(अ) 'नेटवर्क सेवा प्रदाता' से आशय एक मध्यस्थ से होता है।

(ब) 'तृतीय पक्ष सूचना' से आशय ऐसी सूचना से होता है जिसे कि एक

तंत्र सेवा प्रदाता ने एक मध्यस्थ के रूप में व्यवहारित किया हो।

अध्याय–XII
विविध

1. धारा 80 के अनुसार भारतीय दण्ड संहिता 1973 के प्रावधानों से परे कोई पुलिस अधिकारी जो कि एक पुलिस उप अधीक्षक से नीचे पद का नहीं हो अथवा केन्द्र सरकार अथवा एक राज्य सरकार का कोई अन्य अधिकारी जिसे कि केन्द्र ने अधिकृत किया हो, बिना वारंट के किसी सार्वजनिक स्थान में प्रवेश कर सकते हैं एवं छानबीन कर सकते हैं एवं किसी व्यक्ति को जो कि उसके अंदर पाया जाता है एवं जिस पर समुचित तौर पर संदेह है कि वह इस अधिनियम के तहत कोई अपराध कर चुका है, अथवा कर रहा है, अथवा करने जा रहा है, को गिरफ्तार कर सकते हैं।

सार्वजनिक स्थान से आशय किसी होटल, किसी दुकान अथवा किसी अन्य स्थान से है जो कि आम जनता के उपयोग एवं पहुंच हेतु बनाया गया हो। यदि गिरफ्तारी पुलिस अधिकारी के अलावा किसी अन्य अधिकारी ने की है तो वह गिरफ्तार व्यक्ति को तुरंत प्रकरण में क्षेत्राधिकार रखने वाले एक दण्डाधिकारी के समक्ष अथवा एक पुलिस थाना प्रभारी के समक्ष प्रस्तुत करेगा।

इस धारा के अंतर्गत किसी प्रवेश, छानबीन अथवा गिरफ्तारी के संबंध में 'भारतीय दण्ड प्रक्रिया संहिता' 1973 के प्रावधान लागू होंगे।

2. इस अधिनियम के प्रावधान उस समय में प्रचलित किसी अन्य विधि के प्रावधानों पर रद्दकारी प्रभाव रखेंगे (धारा 81)।

3. धारा 82 के अनुसार अपीलीय न्यायाधिकरण के पीठासीन अधिकारी एवं कर्मचारी, नियंत्रक, उपनियंत्रक एवं सहायक नियंत्रक इत्यादि भारतीय दण्ड संहिता की धारा 21 के अर्थों में सार्वजनिक सेवक समझे जाएंगे।

4. केन्द्र सरकार किसी राज्य सरकार को इस राज्य में उस अधिनियम के किसी प्रावधान अथवा इसके तहत बनाए गए किसी नियम, उपनियम अथवा आदेश के क्रियान्वयन हेतु आवश्यक निर्देश जारी कर सकती है। (धारा 83)

5. कम्पनियों द्वारा किए गए अपराध :

(अ) यदि एक व्यक्ति जिसने कि इस अधिनियम के प्रावधानों अथवा इसके तहत बनाए गए किसी नियम, निर्देश अथवा आदेश का उल्लंघन किया है वह एक कम्पनी है तो कम्पनी के साथ-साथ प्रत्येक व्यक्ति जो कि उस समय कम्पनी का प्रभारी रहा हो, एवं कम्पनी के व्यापार परिचालन हेतु उत्तरदायी हो, को उल्लंघन का दोषी माना जाएगा एवं उनके विरुद्ध इस उल्लंघन हेतु कार्रवाई की जा सकती है एवं उन्हें दण्डित भी किया जा सकता है।

इस उपधारा के उपबंधों हेतु ऐसे किसी व्यक्ति को दण्ड हेतु उत्तरदायी नहीं ठहराया जा सकता जो कि यह सिद्ध कर देता है कि वह उल्लंघन उसकी जानकारी के बिना हुआ था अथवा उस उल्लंघन को रोकने हेतु उसने समुचित सावधानी बरती थी।

(ब) यदि इस अधिनियम के प्रावधानों व नियमों अथवा आदेशों इत्यादि का उल्लंघन एक कम्पनी द्वारा किया गया है एवं यह सिद्ध कर दिया जाता है कि यह उल्लंघन उस कम्पनी के किसी निर्देशक, प्रबंधक, सचिव अथवा अन्य अधिकारी की सहमति अथवा सहयोग से किया गया था अथवा उनकी लापरवाही अथवा उपेक्षा के कारण उत्पन्न हुआ था, तो ऐसे निर्देशक, प्रबंधक, सचिव एवं अन्य अधिकारी उल्लंघन के दोषी माने जाएंगे एवं उनके विरुद्ध कार्रवाई की जा सकेगी तथा वे दण्डित किए जा सकेंगे।

स्पष्टीकरण :

(i) 'कम्पनी' से आशय एक निगमित व्यक्ति से होता है एवं इसमें फर्म तथा अन्य व्यक्तियों के समूह को भी शामिल किया जाता है।

(ii) ***'संचालक'*** : एक फर्म के संबंध में संचालक से आशय उस फर्म के भागीदार से होता है (धारा 85)

6. ***केन्द्रसरकारकीनियमबनानेकीशक्ति*** :

(1) केन्द्र सरकार इस अधिनियम के प्रावधानों को क्रियान्वित करने हेतु अधिकारिक गजट एवं वैद्युतिक गजट में अधिसूचना जारी करके नियमों को बना सकती है (धारा 87)।

(2) उपधारा (1) में वर्णित शक्तियों को कोई क्षति पहुंचाए बिना विशेष रूप में इन नियमों द्वारा सभी अथवा किन्हीं निम्नलिखित मामलों हेतु प्रावधान बनाए जा सकते हैं

(3) कोई सूचना अथवा मद किस तरीके से धारा 5 के अंतर्गत वर्णित आंकिक हस्ताक्षरों द्वारा सत्यापित की जाएगी;

(4) धारा 6 की उपधारा (1) के अंतर्गत वर्णित दायर करना, जारी करना, प्रदान करना, अथवा भुगतान करने हेतु विभिन्न वैद्युतिक प्रारूप;

(5) धारा 6 की उपधारा (2) के अंतर्गत वैद्युतिक अभिलेखों के दायर करने अथवा जारी करने एवं भुगतानों की विधि एवं प्रारूप;

(6) धारा 10 के अंतर्गत आंकिक हस्ताक्षरों के प्रकार, इसके नत्थी करने के तरीके एवं प्रारूप से संबंधित विषय;

(7) धारा 16 के अंतर्गत सुरक्षित वैद्युतिक अभिलेख एवं सुरक्षित आंकिक हस्ताक्षर तैयार अथवा निर्मित करने हेतु आवश्यक सुरक्षा प्रक्रिया;

(8) धारा 17 के अधीन नियंत्रक, उपनियंत्रकों एवं सहायक नियंत्रकों की सेवाओं हेतु योग्यता, अनुभव तथा अन्य शतेड;

(9) धारा 20 की उपधारा (2) के खण्ड (b) में वर्णित नियंत्रक द्वारा अनुसरण करने योग्य अन्य मानक;

(10) धारा 21 की उपधारा (2) में वर्णित वे आवश्यकताएं जिन्हें एक आवेदक को पूरा करना जरूरी है;

(11) धारा 21 की उपधारा (3) के खण्ड (अ) में वर्णित प्रदान किए जाने वाली अनुज्ञप्ति की वैधता की अवधि;

(12) धारा 22 की उपधारा (1) के अधीन प्रदान किए जाने वाली अनुज्ञप्ति हेतु एक आवेदन का प्रारूप;

(13) धारा 22 की उपधारा (2) के खण्ड (स) के अंतर्गत भुगतान किए जाने वाले शुल्क की राशि;

(14) धारा 22 की उपधारा (2) के खण्ड (द) के अंतर्गत जारी किए जाने वाली अनुज्ञप्ति हेतु एक आवेदन के साथ नत्थी किए जाने वाले अन्य दस्तावेज;

(15) धारा 23 के अंतर्गत एक अनुज्ञप्ति के नवीनीकरण हेतु आवेदन का प्रारूप एवं भुगतान किए जाने वाले शुल्क;

(16) धारा 35 की उपधारा (1) के अंतर्गत एक आंकिक हस्ताक्षर प्रमाणपत्र जारी किए जाने हेतु आवेदन का प्रारूप;

(17) धारा 35 की उपधारा (2) के अंतर्गत एक आंकिक हस्ताक्षर प्रमाणपत्र जारी किए जाने हेतु प्रमाणीकरण प्राधिकारी को भुगतान किए जाने वाला शुल्क;

(18) धारा 46 की उपधारा (1) के तहत वर्णित न्यायिक अधिकारी के द्वारा की जाने वाली जांच का तरीका;

(19) योग्यता एवं अनुभव जो कि धारा 46 की उपधारा (3) के अनुसार एक न्यायिक जांच अधिकारी में होना चाहिए;

(20) धारा 52 के अंतर्गत पीठासीन अधिकारी की सेवाओं हेतु वेतन, भत्ते एवं अन्य शर्तें;

(21) धारा 54 की उपधारा (3) के अंतर्गत पीठासीन अधिकारी के दुर्व्यवहार अथवा अक्षमता के अन्वेषण की प्रक्रिया;

(21) धारा 56 की उपधारा (3) के अंतर्गत अन्य अधिकारियों एवं कर्मचारियों की सेवा हेतु वेतन, भत्ते तथा अन्य शर्तें;

(22) धारा 57 की उपधारा (3) के तहत अपील दाखिल करने हेतु प्रारूप एवं इसका शुल्क;

(23) एक दीवानी न्यायालय की अन्य शक्तियां जिन्हें कि धारा 58 की उपधारा (2) के वाक्य (जी) में प्रावधानित करना आवश्यक है; एवं

(24) कोई अन्य मामला जिसका प्रावधान किया जाना आवश्यक हो अथवा किया जा सकता हो।

(ग) उपधारा (3) के अंतर्गत जारी की जाने वाली अधिसूचनाएं एवं बनाए जाने वाले नियमों को संसद में प्रस्तुत करने हेतु विभिन्न प्रावधानों का वर्णन है।

7. ***सलाहकारसमितिकागठन*** : (धारा 88)

(i) केन्द्र सरकार इस अधिनियम के प्रारंभ हो जाने के पश्चात् शीघ्र ही एक समिति का गठन करेगी जिसे कि 'साइबर नियमन सलाहकार समिति' के नाम से पुकारा जाएगा।

(ii) साइबर नियमन सलाहकारी समिति में एक सभापति तथा कुछ सरकारी एवं गैर-सरकारी व्यक्ति जो कि मुख्यतः सभी संबंधितों का प्रतिनिधित्व करते हों अथवा विषयवस्तु के बारे में विशिष्ट ज्ञान रखते हों जैसा कि केन्द्र सरकार उचित समझे सदस्य नियुक्त किए जाएंगे।

(iii) साइबर नियमन सलाहकारी समिति

(अ) इस अधिनियम के किन्हीं नियमों अथवा इससे जुड़े अन्य उद्देश्यों के संबंध में केन्द्र सरकार को सलाह देगी।

(ब) इस अधिनियम के तहत विनियमों के बनाने की प्रक्रिया नियंत्रक को सलाह देगी।

(घ) इस समिति के गैर-सरकारी सदस्यों को केन्द्र सरकार द्वारा निर्धारित यात्रा एवं अन्य भत्तों का भुगतान किया जाएगा।

8. ***नियंत्रककीविनियमोंकोबनानेकीशक्ति*** : (धारा 89)

(i) नियंत्रक साइबर नियमन सलाहकारी समिति से सलाह करने के पश्चात् एवं केन्द्र सरकार की पूर्व अनुमति प्राप्त करते हुए अधिकारिक गजट में अधिसूचना जारी करके इस अधिनियम एवं इसके तहत बनाए गए नियमों के अनुरूप विनियमों को बना सकता है जो कि इस अधिनियम के उद्देश्यों को प्राप्त करने में सहयोगी होंगे।

(ii) विशेष रूप में बिना पिछली शक्तियों की साधारणता को कोई नुकसान पहुंचाए, ये विनियम निम्नलिखित सभी अथवा किसी विषय का प्रावधान कर सकते हैं

(1) धारा 18 के वाक्य (एम) में वर्णित प्रत्येक प्रमाणीकरण प्राधिकारी के द्वारा प्रदर्शनीय, अभिलेखों से निहित समंक आधार (डाटाबेस) के रख-रखाव से संबंधित विषय;

(2) धारा 19 की उपधारा (1) के अनुसार वे शर्तें एवं प्रतिबंध जिनके अनुसार नियंत्रक किसी विदेशी प्रमाणीकरण प्राधिकारी को मान्यता प्रदान करते हैं;

(3) वे नियम तथा शर्तें जिनके तहत धारा 21 की उपधारा (3) के वाक्य (सी) के तहत एक अनुज्ञप्ति प्रदान की जाती है;

(4) धारा 30 के वाक्य (d) के तहत एक प्रमाणीकरण प्राधिकारी द्वारा अनुसरणीय अन्य मानक;

(5) वह तरीका जिसमें कि प्रमाणीकरण प्राधिकारी धारा 34 की उपधारा (1) में वर्णित मामलों को प्रकट करेगा;

(6) धारा 35 की उपधारा (3) के तहत दिए जाने वाले ज्ञान के साथ प्रस्तुत किए जाने वाले प्रतिवेदनों के विवरण;

(7) वह तरीका जिसमें कि एक अंशदाता प्रमाणीकरण प्राधिकारी को धारा 42 की उपधारा (2) के तहत निजी कुंजी के विवादग्रस्त हो जाने की सूचना देगा।

(iii) उपधारा (3) में इस अधिनियम के तहत बनाए गए विनियमों के संसद में प्रस्तुतीकरण एवं उसके पारित कराने संबंधी प्रक्रियाओं एवं समयसीमा इत्यादि का वर्णन किया गया है।

9. *राज्यसरकारद्वारानियमोंकोबनानेकीशक्ति* : (धारा 90)

(i) राज्य सरकार अधिकारिक गजट में अधिसूचना जारी करके इस अधिनियम के प्रावधानों को क्रियान्वित करने हेतु नियम बना सकती है।

(ii) विशेष तौर पर एवं पिछली शक्तियों की सामान्यता को बिना कोई नुकसान पहुंचाए इन नियमों द्वारा निम्नलिखित सभी अथवा किसी मामले हेतु प्रावधान बनाए जा सकते हैं

(अ) वैद्युतिक प्रारूप जिसमें कि धारा (6) की उपधारा (1) के तहत दाखिल, जारी प्राप्ति अथवा भुगतान प्रभावकारी किए जाएंगे;

(ब) धारा 6 की उपधारा (2) में निर्दिष्ट मामलों हेतु;

(स) कोई अन्य मामला जिसे कि राज्य सरकार द्वारा नियम बनाते हुए प्रावधानित किया जाना आवश्यक हो;

(iii) राज्य सरकार द्वारा इस धारा के अधीन बनाए गए प्रत्येक नियम इन्हें बनाने के तुरंत बाद राज्य विधान सभा के एक अथवा दोनों सदनों (जैसी परिस्थिति हो) के समक्ष प्रस्तुत किए जाएंगे।

10. *अन्यविधियोंमेंसंशोधन*

(i) भारतीय दण्ड संहिता 1860 को इस अधिनियम की प्रथम अनुसूची

में वर्णित तरीके से संशोधित किया जाएगा (धारा 91)।

(ii) भारतीय साक्ष्य अधिनियम को इस अधिनियम की द्वितीय अनुसूची में वर्णित तरीके से संशोधित किया जाएगा (धारा 92)।

(iii) बैंकर्स पुस्तकें साक्ष्य अधिनियम को इस अधिनियम की तृतीय अनुसूची में वर्णित तरीके द्वारा संशोधित किया गया है (धारा 93)।

(iv) भारतीय रिजर्व बैंक अधिनियम को इस अधिनियम की चतुर्थ अनुसूची में वर्णित तरीके द्वारा संशोधित किया गया है (धारा 94)।

आंकड़ोंमेंसाइबरअपराध: साइबर अपराध भारत में अपराधों का एक नया वर्ग है लेकिन इंटरनेट और सूचना प्रौद्योगिकी के लगातार बढ़ते उपयोग के कारण अब हमारे यहां साइबर अपराध के मामले भी बहुत तेजी से बढ़ रहे हैं। सूचना प्रौद्योगिकी अधिनियम, 2000 के मुताबिक साइबर अपराध के तहत आने वाले प्रमुख कृत्य निम्नलिखित हैं :

1. कंप्यूटर स्रोत विभाग की टैम्परिंग
2. कंप्यूटर तंत्र की हैकिंग
3. अश्लील सामग्री का इलैक्ट्रॉनिक रूप में प्रकाशन/प्रसारण
4. किसी कंप्यूटर-तंत्र तक अनाधिकृत पहुंच
5. गुमराह करके इलैक्ट्रॉनिक हस्ताक्षर प्राप्त करना
6. फर्जी/झूठे डिजिटल सिग्नेचर सर्टिफिकेट का प्रकाशन
7. डिजिटल हस्ताक्षर का फर्जीवाड़ा
8. गोपनीयता भंग करना

सन् 2006 के दौरान सूचना प्रौद्योगिकी अधिनियम के अंतर्गत देश भर में कुल 142 मामले दर्ज किए गए जबकि सन् 2005 में ऐसे कुल 179 मामले दर्ज किए गए थे। इस प्रकार सन् 2005 के मुकाबले सन् 2006 में साइबर अपराध के मामलों में 20.7 फीसदी की गिरावट दर्ज की गई। साइबर अपराध के सबसे अधिक मामले (35) महाराष्ट्र में दर्ज किए गए जबकि 27 मामलों के साथ कर्नाटक दूसरे स्थान पर और 14 मामलों के साथ आंध्र प्रदेश तीसरे स्थान पर रहा। केरल और पंजाब में भी साइबर

अपराध के 12-12 मामले दर्ज किए गए। सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत कुल मामलों में से 48.6 प्रतिशत मामले अश्लील प्रकाशन/प्रसारण से संबंधित थे। इसके अलावा कुल 59 मामले हैकिंग के देशभर में दर्ज किए गए। साइबर अपराध के कुल 311 मामले, सन् 2006 के दौरान, भारतीय दण्ड संहिता की विभिन्न धाराओं के तहत भी दर्ज किए गए थे।

●

6

बैंकिंग अपराध और प्रौद्योगिकी

आज के इस आर्थिक युग में पैसों का लेनदेन काफी बढ़ गया है जिस कारण बैंकिंग व्यवसाय काफी तीव्र गति से विकास कर रहा है। एक समय था जब कुछ सरकारी बैंक ही भारत में बैंकिंग सेवाएं प्रदान कर रहे थे लेकिन अब अनेक निजी बैंक भी अस्तित्व में आ चुके हैं। निजी और विदेशी बैंकों द्वारा बैंकिंग सेवाओं का परिचालन प्रारंभ कर दिए जाने के बाद विभिन्न बैंकों के बीच प्रतिस्पर्धा बढ़ी है तो ग्राहकों को अधिक सुविधाएं भी मिलने लगी हैं। बैंकिंग व्यवसाय और सुविधाओं के इस बढ़ते दौर में बैंकिंग संबंधी अपराध भी तेजी से बढ़े हैं। इस संदर्भ में संतुष्टि की बात सिर्फ यह है कि टेक्नोलॉजी एवं प्रौद्योगिकी ने हमें ऐसे उपकरण उपलब्ध करा दिए हैं जिनके आधार पर बैंकिंग अपराधों की रोकथाम की जा सकती है।

प्रौद्योगिकी के इस्तेमाल के कारण विभिन्न प्रकार के बैंकिंग अपराधों को रोकना अब काफी आसान हो गया है। बैंकिंग क्षेत्र में सबसे अधिक अपराध, क्रेडिट कार्डों से संबंधित होते हैं लेकिन व्यक्तिगत पहचान संख्या *(पर्सनल आइडेंटीफिकेशन नंबर),* दूरभाष पहचान संख्या *(टेलीफोन आइडेंटीफिकेशन नंबर)* और कार्ड के पीछे मैग्नेटिक-स्ट्रिप के इस्तेमाल के कारण क्रेडिट कार्डों से संबंधित अपराधों को रोकना अपेक्षाकृत काफी सरल हो गया है। इसके कारण *सी.बी.एस. (कोर बैंकिंग साल्यूशन)* तंत्र के विकास के कारण भी फर्जी बैंक खातों पर आधारित अपराधों को रोकना सरल हो गया है। बैंकिंग क्षेत्र में आजकल बायोमैट्रिक्स जैसी अत्याधुनिक तकनीक का भी प्रयोग होने लगा है जिस कारण फर्जी तरीके से किसी और के खाते से रकम निकाल लेने के मामलों

की रोकथाम संभव हो पाई है।

विभिन्न बैंकिंग अपराध

जैसे-जैसे बैंकिंग व्यवसाय बढ़ रहा है वैसे-वैसे बैंकिंग संबंधी अपराध भी बढ़ रहे हैं। बैंकिंग संबंधी विभिन्न अपराधों में क्रेडिट कार्डों के जरिए फर्जीवाडा और धोखाधड़ी, फर्जी क्रेडिट कार्ड, बेनामी बैंक खाते, फर्जी डिजिटल हस्ताक्षर और ऑटोमैटिक ट्रेलर मशीन (ए.टी.एम.) से संबंधित अपराध प्रमुख हैं। यहां हम विभिन्न बैंकिंग अपराध और प्रौद्योगिकी द्वारा उनकी रोकथाम के उपायों की चर्चा करेंगे।

प्लास्टिककार्डसंबंधीअपराधएवंप्रौद्योगिकी: आजकल जमाना 'प्लास्टिक मुद्रा' का है। प्लास्टिक मुद्रा के अंतर्गत डेबिट और क्रेडिट कार्ड आते हैं। क्रेडिट कार्ड के द्वारा हम अपने बैंक से उधार लेकर खरीदारी करते हैं अथवा नगद धन की निकासी करते हैं। इसके विपरीत डेबिट कार्ड के जरिए हम अपने बैंक खाते में उपलब्ध धन का ही प्रयोग कर पाते हैं। इन प्लास्टिक कार्डों के जरिए बाजार में खरीदारी की जा सकती है, ए.टी.एम. से नगद धन की निकासी की जा सकती है और इंटरनेट पर खरीदारी *(ई-शॉपिंग)* भी की जा सकती है। हमारे देश में *ई-शॉपिंग* के प्रति लोगों का आकर्षण किस तेजी से बढ़ रहा है, इसका खुलासा 'नीलसन' नामक सर्वेक्षण कम्पनी ने दुनियाभर में किए अपने एक ऑनलाइन सर्वेक्षण के बाद किया है। 'नीलसन' की रिपोर्ट के मुताबिक ऑनलाइन खरीदारी करने के मामले में भारतीय, दुनियाभर में तीसरे स्थान पर पहुंच गए हैं। सर्वेक्षण के अनुसार 85 प्रतिशत इंटरनेट प्रयोगकर्ता, सेवा प्राप्त करने या उत्पाद खरीदने के लिए इंटरनेट का प्रयोग करते हैं और ये लोग भुगतान करने के लिए क्रेडिट कार्ड का उपयोग करते हैं। इस सर्वेक्षण के मुताबिक 70 प्रतिशत भारतीय हवाई सेवा के टिकट आरक्षित कराने के लिए इंटरनेट (ई-टिकटिंग) का इस्तेमाल करते हैं।

भारत में प्लास्टिक कार्डों का उपयोग बढ़ा है तो इससे जुड़े अपराध भी बढ़े हैं। अभी तक तो क्रेडिट कार्डों के दुरुपयोग के मामले ही सामने आते थे लेकिन अब फर्जी *(क्लोन्ड)* क्रेडिट कार्ड भी बनने लगे हैं। तकनीक के इस्तेमाल से कुछ आपराधिक तत्व, किसी अन्य व्यक्ति के क्रेडिट कार्ड का प्रतिरूप

(क्लोन) तैयार कर लेते हैं और फिर इस प्रतिरूप क्रेडिट कार्ड से वे खरीदारी आदि कर लेते हैं। इसके अलावा किसी अन्य व्यक्ति के क्रेडिट कार्ड से अनाधिकृत रूप से खरीदारी करने और धन-निकासी के मामले भी अक्सर सामने आते रहते हैं। खो गए या चोरी चले गए क्रेडिट कार्डों का इस प्रकार का दुरुपयोग बेहद आम है। निम्नलिखित उपाय अपना कर आप अपने क्रेडिट कार्ड का गलत इस्तेमाल होने से बचा सकते हैं :

1. रेस्टोरेंट आदि में अपने कार्ड को अपने सामने ही भुगतान हेतु *स्वैप* कराएं। यदि ऐसा नहीं किया जाए तो आपके क्रेडिट कार्ड से आपकी व्यक्तिगत जानकारी चुरायी जा सकती है अथवा आपके कार्ड का प्रतिरूप (क्लोन) तैयार किया जा सकता है।
2. यदि कोई व्यक्ति ई-मेल के जरिए आपके क्रेडिट कार्ड से संबंधित जानकारियां मांगे तो ऐसे ई-मेल का कोई जवाब न दें।
3. असुरक्षित साइट पर अपने कार्ड से संबंधित कोई भी जानकारी उपलब्ध न कराएं।
4. क्रेडिट कार्ड के पीछे अपने हस्ताक्षर अवश्य करें।
5. अपने क्रेडिट कार्ड पर अपना पिन *(पर्सनल आइडेंटीफिकेशन नंबर)* कदापि न लिखें। ऐसा करने पर चोर के लिए आपके कार्ड का दुरुपयोग करना आसान हो जाएगा।
6. केवल उन्हीं कार्डों को अपने साथ रखें जिनका आप प्रयोग करते हैं। बाकी के कार्डों को घर पर किसी सुरक्षित स्थान पर रख दें।

विज्ञान और प्रौद्योगिकी ने आज ऐसी कई तकनीकें हमें उपलब्ध करा दी हैं जिनकी सहायता से क्रेडिट कार्ड संबंधी अपराधों की रोकथाम की जा सकती है। क्रेडिट कार्ड की सुरक्षा के लिए ऐसा प्रबंध किया गया है कि बिना व्यक्तिगत पहचान संख्या (पिन) के क्रेडिट कार्ड का प्रयोग, ऑटोमैटिक ट्रेलर मशीन (एटीएम) में नहीं हो सकता। यह पिन आमतौर पर 4 अंकों का होता है। अपने क्रेडिट और डेबिटकार्ड की सुरक्षा के लिए जरूरी है कि :

1. अपनी 'व्यक्तिगत पहचान संख्या' (पिन) किसी को भी न बताएं।
2. अपने पिन को लिखकर जेब में कदापि न रखें। उसे याद करके रखें।

3. अपनी टेलीफोन संख्या, जन्मतिथि, मकान संख्या, वैवाहिक वर्षगांठ और वाहन की संख्या आदि के आधार पर अपना पिन कभी न बनाएं।
4. अपना पिन समय-समय पर बदलते रहें।

क्रेडिट कार्ड की सुरक्षा के लिए उस पर धारक का चित्र भी अंकित किया जाता है जिस कारण चोरी हो जाने के बावजूद कोई अनाधिकृत व्यक्ति उसका प्रयोग खरीददारी में नहीं कर सकता है। क्रेडिट कार्ड पर एक मैग्नेटिक-स्ट्रिप भी लगी होती है जिसमें धारक की सभी सूचनाएं दर्ज होती हैं। इसके कारण भी क्रेडिट कार्ड के दुरुपयोग की आशंका काफी कम हो जाती है।

ए.टी.एम.संबंधीअपराधऔरप्रौद्योगिकी: भारत में प्लास्टिक-मुद्रा का प्रचलन बढ़ा है तो ए.टी.एम *(ऑटोमैटिक ट्रेलर मशीन)* का उपयोग भी काफी बढ़ गया है क्योंकि किसी ए.टी.एम. में ही आप अपने कार्ड का प्रयोग करके नगद धन की निकासी कर सकते हैं। ए.टी.एम. से संबंधित बहुत से अपराध आजकल प्रकाश में आ रहे हैं। अक्सर देखने-सुनने में आता है कि किसी अनाधिकृत व्यक्ति ने किसी व्यक्ति के प्लास्टिक कार्ड का प्रयोग करके ए.टी.एम. से नगद धन निकाल लिया। इसके अलावा ए.टी.एम. कक्ष को तोड़ कर लूटने के प्रयास के मामले भी यदाकदा प्रकाश में आते रहते हैं। प्रौद्योगिकी ने हमें ऐसे उपकरण एवं विधियां उपलब्ध करा दी हैं जिनकी सहायता से ए. टी.एम. से संबंधित अपराधों की रोकथाम की जा सकती है।

पूरा ए.टी.एम. कक्ष, *क्लोज-सर्किट टेलीविजन* की निगरानी में रहता है ताकि ए.टी.एम. कक्ष में आने वाले व्यक्ति की प्रत्येक गतिविधि पर नजर रखी जा सके। क्लोज-सर्किट टेलीविजन को प्रभावी बनाए रखने के लिए ही ग्राहकों से अनुरोध किया जाता है कि वे हेलमेट या टोपी पहन कर ए.टी.एम. कक्ष में प्रवेश न करें। इसके अलावा ग्राहकों के समूह में ए.टी.एम. कक्ष में प्रवेश की भी मनाही होती है। इस प्रकार अपराध को होने से पहले ही रोक लिया जाता है। ऐसे भी कई मामले प्रकाश में आए हैं जिनमें ए.टी.एम. कक्ष में लगे क्लोज-सर्किट टेलीविजन की फुटेज को देखकर अपराधी की पहचान की गई। कुछ समय पहले राजधानी दिल्ली में 'पुश्किन हत्याकांड' काफी चर्चा में रहा था। पुश्किन नामक एक व्यक्ति की हत्या कर हत्यारे उसके घर से अन्य वस्तुओं के

साथ-साथ पुश्किन का क्रेडिट कार्ड भी चुरा कर ले गए थे। पुलिस छानबीन में पता चला कि पुश्किन की हत्या के बाद उसके क्रेडिट कार्ड का प्रयोग, कनॉट-प्लेस स्थित एक ए.टी.एम. में किया गया था। पुलिस ने उस ए.टी.एम. में लगे क्लोज-सर्किट टेलीविजन की फुटेज देखी तो पता चला कि पुश्किन की हत्या कर उसके क्रेडिट कार्ड चुराने वाला और कोई नहीं बल्कि उसका नेपाली नौकर ही था।

ए.टी.एम. में इस प्रकार की व्यवस्था की गई होती है कि उसमें प्लास्टिक कार्ड तभी कार्य करता है जब ग्राहक द्वारा ए.टी.एम. के कंप्यूटर में पिन *(पर्सनल आइडेंटिटी नंबर)* का प्रयोग किया जाए। इस प्रकार कोई अनाधिकृत व्यक्ति किसी क्रेडिट कार्ड का प्रयोग, ए.टी.एम. में नहीं कर सकता है। यदि कोई अनाधिकृत व्यक्ति, ग्राहक के 'पिन' का अंदाजा लगाने का प्रयास करता है तो उससे बचने के तकनीकी इंतजाम भी ए.टी.एम. में किए गए हैं। यदि कोई व्यक्ति लगातार 3 बार गलत पिन दर्ज करता है तो प्लास्टिक कार्ड, ब्लॉक हो जाता है और फिर कहीं भी उसका इस्तेमाल नहीं किया जा सकता है।

फोन-बैंकिंगमेंप्रौद्योगिकीसेसुरक्षाः आजकल लगभग सभी बैंक अपने ग्राहकों को फोन-बैंकिंग की सुविधा उपलब्ध कराते हैं। इस सुविधा के अंतर्गत बैंक अपने ग्राहकों को एक 'टिन' *(टेलीफोन आइडेंटिटी नंबर)* जारी करता है। ग्राहक, बैंक के 'ग्राहक सेवा केन्द्र' को फोन करके कोई भी बैंकिंग कार्य कर सकता है। उदाहरण के लिए, ग्राहक मात्र फोन करके ही बैंक से कोई मांग-पत्र बनवा सकता है अथवा अपने खाते से कोई धनराशि, किसी दूसरे व्यक्ति के खाते में स्थानांतरित करवा सकता है। ग्राहक, मात्र फोन-बैंकिंग के जरिए वे सारे कार्य कर सकता है जो वह बैंक की शाखा के काउंटर पर करता है। इस प्रकार फोन-बैंकिंग, ग्राहकों के लिए बेहद सुविधाजनक होती है।

हम जानते हैं कि सुविधा के साथ-साथ अपराध घटित होने की आशंका भी बढ़ जाती है। किसी अनाधिकृत व्यक्ति द्वारा फोन-बैंकिंग का इस्तेमाल कर किसी व्यक्ति के बैंक खाते का परिचालन करने के अपराध को रोकने के लिए प्रौद्योगिकी ने कुछ उपकरण भी उपलब्ध कराए हैं। आवाज-पहचान-तंत्र *(वायस रिकोगनिशन सिस्टम)* की सहायता से ऐसे अपराधों को रोका जा सकता है

इसलिए अधिकतर बैंक अब इस तकनीक का इस्तेमाल करने लगे हैं। इस तकनीक के अंतर्गत बैंक के ग्राहक की आवाज के नमूने को बैंक के कंप्यूटर में सुरक्षित रख लिया जाता है और ऐसी व्यवस्था कर दी जाती है कि कोई व्यक्ति अपने खाते को तभी संचालित कर पाता है जब बैंक का कंप्यूटर उस व्यक्ति की आवाज को पहचान ले। यदि वास्तविक ग्राहक, बैंक के 'ग्राहक सेवा केन्द्र' को फोन करता है तो बैंक का कंप्यूटर उस आवाज का मिलान अपने डाटाबेस में रखे ग्राहक की आवाज के नमूने से करता है और दोनों के एक समान होने पर ग्राहक को अपना खाता संचालित करने की अनुमति मिल जाती है अन्यथा बैंक, ग्राहक के रूप में फोन-बैंकिंग की सुविधा का इस्तेमाल करने का प्रयास करने वाले अनाधिकृत व्यक्ति को खाते का परिचालन करने से रोक देता है। इस प्रकार प्रौद्योगिकी व टेक्नोलॉजी के इस्तेमाल से फोन-बैंकिंग द्वारा हो सकने वाले आशंकित अपराधों की रोकथाम की जा सकती है।

वीडियोसर्विलांससेसुरक्षा: वीडियो सर्विलांस एक ऐसी सुविधा है जिसकी सहायता से बहुत से बैंकिंग अपराधों की रोकथाम में सफलता मिल रही है। वर्तमान समय में लगभग सभी अत्याधुनिक बैंकों की शाखाएं, पूरी तरह से वीडियो सर्विलांस की निगरानी में रहती हैं। बैंक परिसर में आने वाले व्यक्ति की प्रत्येक गतिविधि की निगरानी, वीडियो सर्विलांस द्वारा की जाती है और किसी भी असामान्य गतिविधि की स्थिति में बैंक के सुरक्षाकर्मी तुरंत स्थिति को काबू में कर लेते हैं।

वीडियो सर्विलांस तंत्र में एक अचल वीडियो कैमरा लगा होता है जो एक वी.सी.पी. (वीडियो कैसेट प्लेयर) से जुड़ा होता है। कैमरे द्वारा प्रत्येक गतिविधि की फिल्म तैयार की जाती है जिसे उसी समय वी.सी.पी. की सहायता से नियंत्रण-कक्ष में देखा जा सकता है। अत्याधुनिक वीडियो सर्विलांस तकनीक में वीडियो कैमरे को इंटरनेट से जोड़ दिया जाता है और फिर किसी स्थान (बैंक आदि) पर चल रही गतिविधियों को दुनिया के किसी भी हिस्से से इंटरनेट के जरिए देखा जा सकता है।

धातु-खोजकयंत्रसेजांच: बैंक को लूटने की घटनाएं अक्सर प्रकाश में आती रहती हैं। हालांकि बैंक परिसर में किसी भी तरह के हथियार आदि को लाना प्रतिबंधित होता है लेकिन लुटेरे, कपड़ों आदि के नीचे छिपा कर

हथियार बैंक के भीतर ले जाते हैं और फिर हथियार के बल पर बैंक कर्मियों और वहां उपस्थित ग्राहकों को अपने नियंत्रण में लेकर बैंक को लूट लेते हैं। ऐसी घटनाओं को रोकने के लिए विज्ञान और प्रौद्योगिकी ने धातु-खोजक यंत्र (मेटल डिटेक्टर) के रूप में हमें एक प्रभावशाली उपकरण उपलब्ध करा दिया है।

बैंक परिसर के प्रवेश-द्वारों पर मेटल डिटेक्टर लगे होते हैं। इसके अलावा वहां उपस्थित सुरक्षाकर्मी भी मेटल डिटेक्टर द्वारा प्रत्येक आगंतुक की जांच करते हैं जिस कारण हथियारों के साथ बैंक परिसर में प्रवेश करना काफी मुश्किल हो जाता है।

मेटल डिटेक्टर की सहायता से धातु से बनी किसी भी वस्तु को खोज निकाला जा सकता है। अत्याधुनिक मेटल डिटेक्टर, बालू, मिट्टी या लकड़ी आदि के भीतर छिपा कर रखी गई धातु की वस्तु को भी खोज लेते हैं। मेटल डिटेक्टर में एक दोलक होता है जो प्रतिवर्तित धारा उत्पन्न करता है। यह विद्युत धारा एक कुंडली में प्रवाहित होती है जिस कारण एक चुंबकीय क्षेत्र पैदा हो जाता है। चुंबकीय पदार्थ (कोई धातु) के आसपास होने पर मेटल डिटेक्टर को चुंबकीय क्षेत्र में परिवर्तन हो जाता है, जिसके आधार पर धातु की पहचान/खोज संभव हो जाती है। मेटल डिटेक्टर में लगे माइक्रोप्रोसेसर द्वारा यह भी पता लगा लिया जाता है कि खोजी गई धातु कौन सी है। मेटल डिटेक्टर, वैद्युत चुंबकत्व के सिद्धांत पर कार्य करते हैं। उपयोग की दृष्टि से विभिन्न मेटल डिटेक्टरों की संवेदनशीलता अलग-अलग होती है। सबसे पहला मेटल डिटेक्टर, सन् 1937 में जेरार्ड फिशर नामक वैज्ञानिक ने बनाया था। प्रारंभिक मेटल डिटेक्टर आकार में बड़े होते थे और उनमें ऊर्जा की खपत भी अधिक होती थी जिस कारण उनका उपयोग करना बेहद असुविधाजनक होता था लेकिन अत्याधुनिक मेटल डिटेक्टर आकार में बेहद छोटे होते हैं और वे बैटरी द्वारा परिचालित किए जा सकते हैं। इस प्रकार वर्तमान समय के मेटल डिटेक्टर अपेक्षाकृत अधिक सुविधाजनक और अधिक संवेदनशील होते हैं।

डिजिटलहस्ताक्षरऔरअपराधोंकीरोकथाम: आज जमाना 'ऑनलाइन' का है। हर चीज ऑनलाइन है। ऑनलाइन बैंकिंग, ऑनलाइन खरीदारी, ऑनलाइन टिकटिंग और ऑनलाइन चैटिंग आदि। कुछ भी काम

ऑनलाइन करने में कई बार धोखाधड़ी का शिकार होने की आशंका भी रहती है। क्योंकि ऑनलाइन व्यवहार में अक्सर व्यक्ति की पहचान स्थापित नहीं हो पाती है जिस कारण कई प्रकार के अपराध होने की आशंका सदैव बनी रहती है। इस समस्या के समाधान का एक बहुत कारगर साधन हमें प्रौद्योगिकी ने डिजिटल हस्ताक्षर के रूप में उपलब्ध कराया है।

डिजिटल हस्ताक्षरों के कारण इंटरनेट द्वारा भेजे जाने वाले दस्तावेज़ों को प्रामाणिकता मिलती है जिस कारण इंटरनेट के जरिए भेजे जाने वाले दस्तावेज़ों पर डिजिटल हस्ताक्षरों का इस्तेमाल किया जाता है। डिजिटल हस्ताक्षरों की विशेषता यह होती है कि इनमें हस्तलिखित हस्ताक्षरों की भांति कोई परिवर्तन नहीं किया जा सकता। उदाहरण के लिए, यदि किसी बैंक का मुख्यालय अपनी किसी शाखा से किसी खाते विशेष में कोई परिवर्तन करने का निर्देश इंटरनेट के जरिए देता है तो शाखा के बैंककर्मी को आशंका रहती है कि कहीं बैंक मुख्यालय द्वारा दिया गया निर्देश, फर्जी तो नहीं है अथवा उसे किसी अनाधिकृत व्यक्ति ने तो नहीं भेजा है। डिजिटल हस्ताक्षर की उपस्थिति के कारण बैंककर्मी को किसी प्रकार की कोई आशंका नहीं रहती है। सूचना प्रौद्योगिकी अधिनियम की धारा-7 के अंतर्गत डिजिटल हस्ताक्षरों को विधिक मान्यता भी प्राप्त है।

डिजिटल हस्ताक्षरों को मान्यता, प्रमाणन एजेंसियों द्वारा प्रदान की जाती है। नियंत्रक की कड़ी निगरानी में प्रमाणन एजेंसियों को लायसेंस दिए जाते हैं। डिजिटल हस्ताक्षर के अंतर्गत सब्सक्राइबर के पास दो कोड होते हैं, पहला निजी कोड और दूसरा सार्वजनिक कोड। निजी कोड, सब्सक्राइबर को अथवा उसके द्वारा अधिकृत किए गए किसी व्यक्ति को ही पता होता है। इस कोड के जरिए ही किसी ऑनलाइन दस्तावेज़ पर डिजिटल हस्ताक्षर हो सकते हैं। सार्वजनिक कोड किसी भी व्यक्ति के पास हो सकता है और इस सार्वजनिक कोड के जरिए कोई भी व्यक्ति इन दस्तावेज़ों को देख सकता है। डिजिटल हस्ताक्षर युक्त दस्तावेज़ को कोई भी व्यक्ति देख तो सकता है लेकिन वह उसका दुरुपयोग नहीं कर सकता। इस प्रकार डिजिटल हस्ताक्षरों के जरिए महत्त्वपूर्ण दस्तावेज़ों की सुरक्षा सुनिश्चित होती है। निम्नलिखित प्रक्रिया का पालन करके डिजिटल हस्ताक्षरों को पंजीकृत किया जा सकता है।

एम.सी.ए. के होम पेज पर जाएं

⇓

रजिस्टर डी.एस.सी. पर क्लिक करें

⇓

डायरेक्टर लिंक पर क्लिक करें

⇓

अपना डी.आई.एन. भरें

⇓

अगले बटन (नेक्स्ट) का चयन करें

⇓

डी.एस.सी. का चयन करें

⇓

सर्टिफिकेट का चयन करें

⇓

'आई एग्री' बटन पर क्लिक करें

'आई एग्री' बटन पर क्लिक करते ही आपका डी.एस.सी. पंजीकृत हो जाएगा। डी.एस.सी. का पंजीयन करने के बाद *'सबमिट'* बटन क्लिक करें। प्रयोगकर्ता को स्क्रीन पर एक संदेश दिखाई देगा जो बताएगा कि आपका डी. एस.सी. पंजीकृत हो चुका है। डिजिटल हस्ताक्षरों का लाभ यह है कि ये संदेश या दस्तावेज़ भेजने वाले स्रोत को प्रमाणित करते हैं। अक्सर इंटरनेट के द्वारा संदेश भेजते समय, संदेश भेजने वाले और संदेश प्राप्त करने वाले के मन में आशंका बनी रहती है कि कहीं संदेश को बीच रास्ते में ही बदल न दिया गया हो लेकिन डिजिटल हस्ताक्षर युक्त संदेश (दस्तावेज़) के मामले में इस प्रकार की कोई आशंका नहीं रहती है। यदि डिजिटल हस्ताक्षर युक्त दस्तावेज या संदेश में बीच रास्ते कोई परिवर्तन करने का प्रयास करता है तो कंप्यूटर-तंत्र, हस्ताक्षर को अवैध घोषित कर देता है जिस कारण प्रयोगकर्ता को पता चल जाता है कि संदेश (दस्तावेज़) में कोई अवांछनीय परिवर्तन किया गया है।

डिजिटल हस्ताक्षरों का इस्तेमाल करते समय कुछ सावधानियां बरतने की भी जरूरत है। प्रयोगकर्ता को चाहिए कि वह किसी दस्तावेज़ को अपने कंप्यूटर

पर ही हस्ताक्षरित करे। इसके अलावा डिजिटल हस्ताक्षरों का इस्तेमाल ऐसे एप्लीकेशंस में ही करें, जिनमें हैकिंग किए जाने की आशंका न्यूनतम हो। डिजिटल हस्ताक्षर की प्रौद्योगिकी के कारण विभिन्न प्रकार के ऑनलाइन दस्तावेज़ आधारित अपराधों को रोकने में खासी सफलता मिली है।

इंटरनेट-बैंकिंगमेंसुरक्षाउपाय: निजी और अंतर्राष्ट्रीय बैंकों द्वारा आजकल ग्राहकों को कई सुविधाएं उपलब्ध कराई जा रही हैं। फोन बैंकिंग और इंटरनेट बैंकिंग ऐसी सुविधाएं हैं जो ग्राहकों के बीच काफी लोकप्रिय हैं। इन सुविधाओं की लोकप्रियता का कारण यह है कि इनका इस्तेमाल करके ग्राहक बैंक जाने और वहां भीड़भाड़ का सामना करने से बच जाता है। इंटरनेट बैंकिंग आज अगर काफी लोकप्रिय हो रही है तो इससे संबंधित अपराध भी अब काफी संख्या में प्रकाश में आने लगे हैं।

इंटरनेट बैंकिंग में बैंक का ग्राहक, बैंक की वेबसाइट के जरिए अपनी बैंकिंग संबंधी जरूरतों को पूरा कर सकता है। वह अपने खाते की जांच कर सकता है, धनादेश (बैंक ड्राफ्ट) बनवा सकता है और अपने खाते से धनराशि को किसी दूसरे खाते में स्थानांतरित करवा सकता है। बैंक अपने ग्राहकों को प्लास्टिक कार्ड जारी करते समय पिन, ई-पिन और टी-पिन भी जारी करता है। पिन का इस्तेमाल, ऑटोमैटिक ट्रेलर मशीन से नगद धनराशि का आहरण करते समय किया जाता है तो टी-पिन (टेलीफोन पिन) का इस्तेमाल ग्राहक *'टेलीफोन बैंकिंग'* के दौरान करते हैं। इंटरनेट-बैंकिंग की सुविधा का उपयोग करने के लिए बैंक अपने ग्राहकों को 'ई-पिन' (इंटरनेट पिन) भी जारी करते हैं। ई-पिन (पासवर्ड) का इस्तेमाल करके ग्राहक अपने बैंक खाते को परिचालित कर सकता है।

कुछ मामलों में देखा गया है कि कोई व्यक्ति किसी दूसरे व्यक्ति के बैंक खाते को 'इंटरनेट बैंकिंग' द्वारा अनाधिकृत रूप से परिचालित कर लेता है जिस कारण वास्तविक ग्राहक या बैंक को काफी बड़ा नुकसान हो सकता है। यह एक आपराधिक कृत्य है और ऐसे अपराधों की रोकथाम के लिए टेक्नोलॉजी आधारित कई विधियां विकसित की गई हैं। ऐसी ही एक प्रमुख विधि है, पासवर्ड का इस्तेमाल। वास्तव में इंटरनेट-बैंकिंग का इस्तेमाल करने के लिए एक पासवर्ड की आवश्यकता होती है। यदि आप अपने पासवर्ड को सुरक्षित रख

सकें तो आप विभिन्न बैंकिंग अपराधों का शिकार होने से बच सकते हैं।

जरूरत इस बात की है कि अपना पासवर्ड बनाते समय काफी सावधानी का परिचय दें। कुछ लोग अलग-अलग उद्देश्यों के लिए अलग-अलग पासवर्ड बनाते हैं जिस कारण अक्सर वे भ्रम का शिकार हो जाते हैं कि कौन सा पासवर्ड किस का है। लेकिन यदि आप विभिन्न उद्देश्यों (सोशल नेटवर्किंग साइट, डेटिंग साइट, ऑनलाइन खरीदारी साइट और इंटरनेट बैंकिंग आदि) उद्देश्यों के लिए एक ही पासवर्ड बनाते हैं तो आपके परिचितों के लिए आपका पासवर्ड हैक करना काफी आसान हो जाएगा। अपने टेलीफोन नंबर, जन्मतिथि या अपने वाहन संख्या के आधार पर पासवर्ड कदापि न बनाएं क्योंकि ऐसे पासवर्ड को हैक करना काफी आसान हो जाता है। पासवर्ड इस प्रकार का होना चाहिए, जिसे आसानी से तोड़ा न जा सके। निम्नलिखित सावधानियां अपना कर आप अपने पासवर्ड को सुरक्षित बना सकते हैं :

1. वेबसाइट द्वारा सुझाए गए पासवर्ड से मिलता-जुलता पासवर्ड न बनाएं।
2. आपका नया पासवर्ड, आपके किसी पुराने पासवर्ड जैसा नहीं होना चाहिए। उदाहरण के लिए, यदि आपका पुराना पासवर्ड 'Sanjay 33' है तो नया पासवर्ड 'Sanjay 44' कदापि निर्धारित न करें।
3. अपने या अपने जीवनसाथी के नाम, पालतू जानवर, घर के पते, 12345..., a b c d e f..., जन्मतिथि, वाहन संख्या, मोबाइल नंबर आदि बेहद असुरक्षित पासवर्ड माने जाते हैं इसलिए इन्हें अपना पासवर्ड न बनाएं।
4. पासवर्ड बनाने के लिए किसी वाक्यांश का इस्तेमाल करते हुए इससे स्वरों को हटा सकते हैं। जैसे 'i won the game' के स्थान पर 'i w d t h g m' को अपना पासवर्ड बनाएं।
5. दो-तीन माह में अपने पासवर्ड को बदलते रहें। ऐसा करने पर आप अपने पासवर्ड को हैक होने के खतरे से बचा सकते हैं।
6. पासवर्ड को लंबा रखने का प्रयास करें क्योंकि पासवर्ड जितना लंबा होगा, उसे (हैक) करना उतना ही कठिन हो जाएगा।

इंटरनेट-बैंकिंग का इस्तेमाल करते समय काफी सावधानी बरतने की जरूरत है। ध्यान रखें कि अपने ई-मेल खाते के आई.डी. और पासवर्ड को अपने व्यक्तिगत कंप्यूटर में दर्ज करके न रखें। ऐसा करने पर पासवर्ड का आशंकित दुरुपयोग संभव नहीं रहेगा। साइबर कैफे में इंटरनेट बैंकिंग करने से बचें क्योंकि ऐसे स्थानों पर कुछ कंप्यूटरों में *'कीलॉगर्स'* जैसे वायरस होते हैं जो कंप्यूटर पर की गई किसी भी एंट्री को लॉग कर लेते हैं। उपरोक्त चर्चा से स्पष्ट है कि आज यदि बैंकिंग संबंधी अपराध बढ़ रहे हैं तो ऐसी तकनीकें और प्रौद्योगिकी भी उपलब्ध हैं जिसकी सहायता से बैंकिंग अपराधों की रोकथाम काफी सरल हो गई है। जरूरत है तो बस थोड़ी सी सावधानी बरतने की।

●

7

वित्तीय अपराध और प्रौद्योगिकी

हम चर्चा कर चुके हैं कि विभिन्न प्रकार के अपराधों को कारित करने के लिए अपराधी तत्व आजकल नई-नई टेक्नोलॉजी एवं प्रौद्योगिकी का इस्तेमाल करने लगे हैं। बढ़ते अपराध के इस दौर में विभिन्न प्रकार के वित्तीय अपराध भी आज तेजी से बढ़ते जा रहे हैं। अपराधियों द्वारा प्रौद्योगिकी के इस्तेमाल के कारण वित्तीय अपराधों की वृद्धि-दर भी बढ़ी है। यहां एक सुखद तथ्य यही है कि अब विभिन्न सुरक्षा एजेंसियां भी तकनीक और प्रौद्योगिकी से लैस हो रही हैं जिस कारण वित्तीय अपराधों की रोकथाम सरल हो गई है।

सबसे पहले बात वित्तीय अपराध की परिभाषा की। ऐसा कोई भी अपराध जिसके कारण किसी देश की वित्तीय व्यवस्था ही खतरे में पड़ जाए, वित्तीय अपराध कहलाता है। इस प्रकार वित्तीय अपराध एक बेहद विस्तृत शब्द है जिसके प्रभाव भी एक विस्तरित क्षेत्र पर पड़ते हैं और ये प्रभाव दूरगामी प्रकार के होते हैं। आतंकवाद के इस दौर में वित्तीय अपराध अपेक्षाकृत ज्यादा होने लगे हैं क्योंकि विभिन्न अंतर्राष्ट्रीय आतंकी संगठनों द्वारा भी वित्तीय अपराधों को अंजाम दिया जा रहा है। आतंकी संगठनों द्वारा वित्तीय अपराधों में संलग्न रहने के दो कारण हैं। प्रथम, वित्तीय अपराधों के कारण उस देश की अर्थव्यवस्था लड़खड़ा जाती है जिस देश के खिलाफ कोई आतंकी संगठन लड़ रहा होता है। द्वितीय, वित्तीय अपराधों के कारण आतंकी संगठनों को बेशुमार धन प्राप्त होता है जिसका उपयोग आतंकी संगठन, अत्याधुनिक हथियार खरीदने और प्रशिक्षण कार्यक्रमों में व्यय करते हैं। बैंकिंग अपराध और वित्तीय अपराध को कुछ लोग समान समझते हैं लेकिन ऐसा नहीं है। वास्तव में इन दोनों अपराधों

में एक छोटा सा अंतर होता है। सभी बैंकिंग अपराध, वित्तीय अपराध की श्रेणी में आते हैं लेकिन सभी वित्तीय अपराध, बैंकिंग अपराध नहीं होते हैं।

विभिन्न वित्तीय अपराध

तकनीक के इस युग में प्रतिदिन नये-नये वित्तीय अपराध प्रकाश में आ रहे हैं। जाली करेंसी नोटों का चलन तो पुराना है अब तो जाली राजस्व स्टाम्प पेपर भी बाजार में आ गए हैं जिनके कारण सरकार को अरबों रुपये के राजस्व की हानि हो रही है। इसी प्रकार शेयर बाजार में भी तकनीक के आधार पर भिन्न-भिन्न प्रकार के अपराध घटित किए जा रहे हैं। यहां सकारात्मक तथ्य यही है कि प्रौद्योगिकी ने हमें ऐसे उपकरण उपलब्ध करा दिए हैं जिनकी सहायता से विभिन्न वित्तीय अपराधों की रोकथाम की जा सकती है। यहां हम प्रमुख वित्तीय अपराध और प्रौद्योगिकी के इस्तेमाल के कारण उनकी रोकथाम की चर्चा करेंगे।

जालीकरेंसीनोटऔरप्रौद्योगिकी: करेंसी नोट किसी भी देश की अर्थव्यवस्था के एक प्रमुख घटक होते हैं। जाली करेंसी नोटों के जरिए किसी भी अर्थव्यवस्था को मिट्टी में मिलाया जा सकता है। जाली नोटों द्वारा किसी देश की अर्थव्यवस्था को कितना नुकसान पहुंचाया जा सकता है, इसे समझने के लिए इस तथ्य को जानना ही काफी होगा कि हमारे पड़ोसी देश पाकिस्तान की खुफिया एजेंसी, 'आई.एस.आई.', भारतीय बाजार में चल रहे जाली नोटों की सबसे बड़ी स्रोत है। आई.एस.आई, आतंकवाद के साथ-साथ जाली नोटों के सहारे भी भारत के खिलाफ एक लड़ाई लड़ रही है।

आई.एस.आई. के एजेंट नेपाल के रास्ते भारतीय बाजार में जाली नोट पहुंचाते हैं। हाल ही में नेपाल से लगे उत्तर प्रदेश के डुमरियागंज में करोड़ों रुपये के जाली नोट पकड़े गए थे। अधिकतर जाली नोट, 1000 रुपये और 500 रुपये के हैं। आज हमारी अर्थव्यवस्था में अरबों रुपये के जाली नोट मौजूद हैं। अभी तक एक हजार और पांच सौ के नोट ही जाली हुआ करते थे लेकिन ताजा रिपोर्ट बताती है कि अब जालसाज, 10, 20 और 50 रुपये के जाली नोट भी बनाने लगे हैं। ये नोटों के वे प्रकार हैं जो गरीब से गरीब व्यक्ति की जेब में भी होते हैं। इस प्रकार जाली नोटों के कारण भारतीय अर्थव्यवस्था को बहुत

ज्यादा नुकसान पहुंच रहा है।

जाली करेंसी नोटों ने किस प्रकार भारतीय अर्थव्यवस्था में अपनी घुसपैठ बना ली है, इसका अंदाजा इसी बात से लगाया जा सकता है कि अब बैंकों और ए.टी.एम. में भी जाली नोट पाए जाने लगे हैं। तकनीक ने हमें ऐसे उपकरण उपलब्ध करा दिए हैं जिनकी सहायता से जाली नोटों को बेहद आसानी से पहचाना जा सकता है। अल्ट्रा वायलेट मशीन द्वारा जाली नोटों को आसानी से पहचाना जा सकता है। दिल्ली के कनाट प्लेस स्थित पीवीआर सिनेमा कम्प्लैक्स में ऐसी ही एक मशीन लगाई गई है ताकि ग्राहकों द्वारा दिए गए जाली करेंसी नोटों को तुरंत पहचाना जा सके। जाली नोटों को प्रचलन में आने से रोकने के लिए सरकार द्वारा काफी प्रयास किए जा रहे हैं। प्रौद्योगिकी का इस्तेमाल करके अब इस प्रकार के नोट छापे जा रहे हैं, जिनकी नकल करना लगभग असंभव है। नोट छापने के लिए निम्नलिखित तकनीकों का इस्तेमाल अब किया जा रहा है :

(1) वाटरमार्क का प्रयोग: प्रत्येक नोट में महात्मा गांधी का वाटरमार्क लगा होता है। इस वाटरमार्क पर गहरी व हल्की छाया होती है। प्रकाश के सामने रख कर इस वाटरमार्क को आसानी से देखा जा सकता है।

(2) अंकों की छपाई: नोटों पर 100, 500 या 1000 के अंक, आधे सामने की ओर तथा आधे पीछे की ओर छापे जाते हैं। ये आधे-आधे अंक इतनी सफाई से छापे जाते हैं कि प्रकाश के सम्मुख रखने पर ये अंक, पूरे दिखाई देते हैं। प्रकाश के सामने आगे और पीछे के आधे-आधे अंक मिल कर पूरा अंक दिखाई देता है। जाली करेंसी नोटों पर इस प्रकार की छपाई लगभग असंभव है।

(3) चमकीला धागा: असली नोटों में एक चमकीले धागे का प्रयोग किया जाता है और जाली नोट पहचानने का यह सबसे सुविधाजनक तरीका है क्योंकि जाली करेंसी नोटों में इस चमकीले धागे का अभाव होता है। 10 रुपये से लेकर 1000 रुपये तक के करेंसी नोटों में इस धागे का प्रयोग किया जाता है। कुछ जाली नोटों में भी यह चमकीला धागा होता है लेकिन जाली नोटों का चमकीला धागा पहली नजर में देखने पर ही कटा-फटा दिखाई देता है। असली नोट में इस धागे पर 'भारत' और 'आर.बी.' भी लिखा होता है।

(4) वर्टिकलबैंड : असली नोट के दाहिने किनारे पर एक लंबवत बैंड होता है। इसके अलावा इसमें महात्मा गांधी का एक चित्र भी होता है। इनमें छिपे हुए चित्र (लेटेंट इमेज) का प्रभाव आता है जिसके जरिए नोट का मूल्य सामने आ जाता है। इसके मूल्य को चौड़ाई में अर्थात क्षैतिज ढंग से रखने पर ही देखा जा सकता है। यह तभी दिखाई देता है जब इस पर 45 डिग्री से प्रकाश की किरण पड़ती है। ऐसा न होने पर यह वर्टिकल बैंड मात्र एक खड़ी पट्टी के रूप में ही दिखाई देता है।

भारतीय अर्थव्यवस्था को जाली नोटों के साए से बचाने के लिए भारतीय रिजर्व बैंक ने कई उपाय किए हैं। सरकारी छापेखाने में करेंसी नोटों को छापने की प्रक्रिया में इस प्रकार की प्रौद्योगिकी का इस्तेमाल किया जाने लगा है कि जालसाजों के लिए उनकी नकल करना आसान नहीं रह गया है। करेंसी नोट में चांदी के एक तार का इस्तेमाल किया जाता है जिसके आधार पर वास्तविक और जाली नोटों की पहचान करना काफी सरल हो जाता है। अत्याधुनिक तकनीक का प्रयोग करते हुए करेंसी नोट में राष्ट्रपिता महात्मा गांधी का चित्र इस प्रकार अंकित किया जाता है कि उसे केवल तभी देखा जा सकता है जब नोट को किसी प्रकाश-स्रोत के सामने रख कर देखा जाए। इसके अलावा करेंसी नोट पर उसका मूल्य (1000 या 500 रुपये), उभरे हुए अक्षरों में छापा जाता है जिस कारण नोट को स्पर्श करके भी वास्तविक या जाली नोट की पहचान की जा सकती है। एक हजार और पांच सौ रुपये के नोट में कागज और स्याही इस प्रकार की प्रयुक्त की जाती है कि उसकी नकल करना जालसाजों के लिए काफी मुश्किल हो जाता है। यह बात सही है कि भारतीय बाजार में अरबों रुपये के जाली नोट प्रचलन में हैं लेकिन दूसरा तथ्य यह भी है कि प्रौद्योगिकी के इस्तेमाल से बने वास्तविक (असली) नोटों को आसानी से पहचाना जा सकता है।

सिर्फ तकनीक और प्रौद्योगिकी के कारण ही जाली नोटों को पहचानना इतना सुविधाजनक हो गया है। आजकल इन्फ्रारेड किरणों पर आधारित ऐसे उपकरण भी बाजार में आ गए हैं जो रुपयों के ढेर के बीच से भी जाली नोट को पहचान सकते हैं। इन उपकरणों का उपयोग विभिन्न बैंकों के मुख्यालयों और राजकीय कोषागार आदि में किया जाता है।

शेयर बाजार और प्रौद्योगिकी

शेयर बाजार किसी भी अर्थव्यवस्था की रीढ़ के समान होते हैं क्योंकि यहां पर प्रतिदिन अरबों रुपये का कारोबार किया जाता है। शेयर बाजार के उछाल भरने या गिरने का सीधा असर, अर्थव्यवस्था पर पड़ता है। चूंकि शेयर बाजार में प्रतिदिन अरबों रुपयों का व्यापार होता है इसलिए अपराधियों की नजर भी शेयर बाजार पर लगी रहती है और वे विभिन्न अपराधों के द्वारा शेयर बाजार को नुकसान पहुंचाने का प्रयास करते रहते हैं।

कुछ वर्षों पूर्व हुए प्रतिभूति घोटाले ने भारतीय अर्थव्यवस्था को हिलाकर रख दिया था। इस बहुचर्चित घोटाले का मुख्य आरोपी हर्षद मेहता नामक एक शेयर दलाल था जिसने फर्जी प्रतिभूति खातों का प्रयोग करके और एक ही प्रतिभूति/ शेयर को कई-कई बार बेच कर, भारतीय अर्थव्यवस्था को अरबों रुपयों की चोट पहुंचाई थी। तकनीक और प्रौद्योगिकी ने आज इतनी तरक्की कर ली है कि हर्षद मेहता द्वारा कारित प्रतिभूति घोटाले जैसे वित्तीय अपराधों के होने की आशंका अब लगभग समाप्त हो गई है। शेयर बाजार और शेयर खातों के पूर्णतया कंप्यूटरीकरण के कारण ही ऐसा संभव हो पाया है। अब शेयर बाजार में कारोबार करने वाले प्रत्येक व्यक्ति और दलाल के लिए आवश्यक कर दिया गया है कि वे शेयरों की खरीद-फरोख्त अपने 'डी-मैट खाते' के द्वारा ही करें। डी-मैट खाते में शेयरों का इलैक्ट्रॉनिक स्थानांतरण होता है जिस कारण शेयरों के भौतिक स्थानांतरण के समय होने वाली जालसाजी और फर्जीवाडे पर पूर्णतया रोक लग गई है। डी-मैट खातों ने भारतीय शेयर बाजार की तस्वीर ही बदल कर रख दी है। अब वहां किसी भी प्रकार के घोटाले की आशंका लगभग समाप्त हो गई है। टेक्नोलॉजी और प्रौद्योगिकी के इस्तेमाल के कारण ही ऐसा हो पाया है।

बेनामीबैंकखातेऔरप्रौद्योगिकी: देश का अधिकांश काला धन, बेनामी बैंक खातों में रखा होता है। एक ही खाते में सारा धन जमा करके रखने में बहुत से खतरे होते हैं इसलिए भ्रष्टाचारी और अपराधी लोग अपने काले धन को बेनामी और फर्जी बैंक खातों में रखा करते थे। इसके लिए ये लोग अपने मिलते-जुलते नामों से विभिन्न बैंकों की विभिन्न शाखाओं में कई-कई खाते

खोल लिया करते थे। चूंकि विभिन्न शाखाओं के रिकॉर्ड का परस्पर मिलान करना संभव नहीं था इसलिए बेनामी और फर्जी बैंक खातों के जरिए भारत की अर्थव्यवस्था को खोखला किया जा रहा था। लेकिन तकनीक एवं प्रौद्योगिकी के इस्तेमाल के चलते अब ऐसा संभव नहीं रह गया है।

अब सभी बैंक शाखाओं का कंप्यूटरीकरण किया जा रहा है। बैंक की शाखा का संपूर्ण रिकॉर्ड कंप्यूटरीकृत है जिसे इंटरनेट द्वारा अन्य शाखाओं से जोड़ दिया गया है। इस प्रकार किसी बैंक की सभी शाखाओं के रिकॉर्ड को किसी भी स्थान से इंटरनेट द्वारा मिलान किया जा सकता है। विभिन्न बैंक परस्पर एक-दूसरे के रिकॉर्ड (ग्राहक के रिकॉर्ड) का भी साझा प्रयोग कर सकते हैं। इस प्रकार किसी व्यक्ति विशेष के बारे में आसानी से यह पता लगाया जा सकता है कि देशभर में उस व्यक्ति के किस-किस बैंक में कुल कितने खाते हैं।

पूर्णतया कंप्यूटरीकृत बैंक शाखा को 'सी.बी.एस.' *(कोर बैंकिंग साल्यूशन)* शाखा कहा जाता है। सी.बी.एस. शाखाओं के कारण एक ओर जहां ग्राहकों को बेहद सुविधाजनक स्थिति प्राप्त हो गई है वहीं इनके कारण फर्जी और बेनामी बैंक खातों के परिचालन जैसे वित्तीय अपराधों पर भी प्रभावी रोक लग गई है। सी.बी.एस. बैंक शाखा के ग्राहक, उस बैंक की देशभर में फैली किसी भी सी.बी.एस. शाखा में जाकर बैंकिंग कर सकते हैं। उदाहरण के लिए, यदि आपका बैंक खाता हाथरस स्थित भारतीय स्टेट बैंक की *सी.बी.एस.* शाखा में है तो आप कोयम्बतूर की भारतीय स्टेट बैंक की *सी.बी.एस.* शाखा में जाकर भी अपने खाते को परिचालित कर सकते हैं। आप कोयम्बतूर की शाखा से भी अपने खाते से नगद राशि का आहरण कर सकते हैं अथवा खाते में धन जमा करवा सकते हैं। इस प्रकार *'कोर बैंकिंग साल्यूशन'* ने भारतीय बैंकिंग की तस्वीर ही बदल कर रख दी है।

फर्जीस्टाम्पऔरप्रौद्योगिकी: स्टाम्प पेपर, सरकार द्वारा राजस्व एकत्रित करने का एक प्रमुख साधन है। भूमि, मकान, दुकान आदि के स्वामित्व परिवर्तन के समय क्रेता द्वारा एक निर्धारित मूल्य के स्टाम्प पेपर लगाना आवश्यक होता है। इसके अलावा न्यायालयों का शुल्क भी स्टाम्प पेपरों द्वारा ही देय होता है। इस प्रकार स्टाम्प पेपर का विक्रय करके सरकार को करोड़ों रुपये के राजस्व की प्राप्ति प्रतिवर्ष होती है। कुछ समय पूर्व फर्जी या जाली

स्टाम्प पेपर कांड प्रकाश में आया था जिसका मुख्य अभियुक्त अब्दुल करीम तेलगी नामक एक व्यक्ति था।

अब्दुल करीम तेलगी ने सरकारी छापेखानों की पुरानी मशीनों और स्टाम्प पेपरों के ब्लाक, नीलामी के द्वारा खरीद लिए और फिर इनकी सहायता से वह सरकारी स्टाम्प पेपरों जैसे ही स्टाम्प पेपर छापने लगे। अब्दुल करीम तेलगी द्वारा छापे जाने वाले स्टाम्प पेपर हू-ब-हू सरकारी स्टाम्प पेपरों जैसे ही थे और इनकी पहचान करना काफी कठिन था। अब्दुल करीम तेलगी अपने जाली स्टाम्प पेपर सरकारी मूल्य के मुकाबले काफी कम दाम पर बाजार में बेचता था जिस कारण समूचे भारतवर्ष में उसके जाली स्टाम्प पेपर बिकने लगे। राजस्व विभाग, बीमा कम्पनी और बैंक आदि के कर्मचारी भी अपने स्वार्थ के कारण, अब्दुल करीम तेलगी के जाली स्टाम्प पेपरों को वरीयता देने लगे। जब इस कांड का खुलासा हुआ तो चारों ओर हड़कम्प मच गया क्योंकि अब्दुल करीम तेलगी और उसके साथियों ने फर्जी स्टाम्प पेपरों के द्वारा सरकार को अरबों रुपये का चूना लगा दिया था।

फर्जी/जाली स्टाम्प पेपरों के प्रकाश में आने के बाद सरकार हरकत में आई और उसने प्रौद्योगिकी का प्रयोग करते हुए स्टाम्प पेपरों की छपाई की प्रक्रिया को पूरी तरह से बदल दिया। वर्तमान में स्टाम्प पेपरों की छपाई में कई ऐसे तकनीकी प्रयोग किए गए हैं जिनके कारण अब फर्जी स्टाम्प पेपर छापना काफी कठिन हो गया है। करेंसी नोटों की तरह स्टाम्प पेपरों में भी अब चांदी के तार, महात्मा गांधी के छिपे हुए चित्र और एक क्रम-संख्या का प्रयोग किया जाता है। इसके अलावा स्टाम्प पेपरों में 'बार कोड' का प्रयोग भी किया जाने लगा है जिस कारण फर्जी स्टाम्प पेपर छापना और उन्हें बाजार में चलाना लगभग असंभव हो गया है। इसके अलावा दिल्ली सहित कुछ अन्य राज्यों में भी आजकल 'ई-स्टाम्प पेपर' प्रचलन में आ गए हैं। ई-स्टाम्प पेपर में स्टाम्प शुल्क का भुगतान इंटरनेट के द्वारा होता है और इंटरनेट के जरिए ही क्रेता को रसीद भी प्राप्त हो जाती है। इस प्रकार ई-स्टाम्प पेपर में स्टाम्प पेपरों का भौतिक अस्तित्व नहीं होता है जिस कारण स्टाम्प पेपर संबंधी किसी भी धोखाधड़ी की आशंका अब लगभग समाप्त हो गई है। इस प्रकार प्रौद्योगिकी के इस्तेमाल के कारण स्टाम्प पेपरों का कारोबार पूरी तरह से सुरक्षित हो गया

है और अब इसमें किसी भी प्रकार के फर्जीवाडे की आशंका नहीं रह गई है।

स्वामित्व परिवर्तन और प्रौद्योगिकी

अक्सर ऐसे मामले सामने आते रहे हैं जिनमें किसी व्यक्ति की भूमि, मकान, दुकान आदि को किसी अन्य व्यक्ति द्वारा अनाधिकृत रूप से बेच दिया गया। इस प्रकार का फर्जीवाडा करने वाले अपराधी, जाली हस्ताक्षरों और फर्जी गवाहों के सहारे यह अपराध करते रहे हैं। उत्तर प्रदेश के गाजियाबाद में तो एक ऐसा मामला प्रकाश में आया जिसमें एक अभियुक्त ने राजस्व विभाग के कर्मचारियों की मिलीभगत से राजस्व विभाग के रिकॉर्ड से छेड़छाड़ करके सरकारी भूमि को ही अपने नाम करा लिया। जांच एजेंसियों ने अरबों रुपये की ऐसी सरकारी भूमि का पता लगाया है जिसे इस अभियुक्त ने फर्जी तरीके से अपने नाम करा लिया था।

तकनीक और प्रौद्योगिकी का इस्तेमाल करते हुए अब ऐसी विधियां विकसित कर ली गई हैं जिनकी सहायता से ऐसे अपराधों की रोकथाम की जा सकती है। किसी भी संपत्ति (भूमि, मकान, दुकान आदि) के स्वामित्व परिवर्तन के समय अब क्रेता और विक्रेता के अंगुलि चिह्न, राजस्व अधिकारी के सम्मुख ही संबंधित दस्तावेजों पर लिए जाते हैं। इसके अलावा क्रेता और विक्रेता के डिजिटल चित्र भी दस्तावेजों पर लगाए जाते हैं जिस कारण भविष्य में स्वामित्व परिवर्तन संबंधी अपराधों पर प्रभावी रोक लग सकेगी क्योंकि अंगुलि चिह्न और डिजिटल चित्र अंकित किसी संपत्ति के दस्तावेज़ों के स्वामित्व परिवर्तन के समय विक्रेता के अंगुलि चिह्नों और चित्र का मिलान राजस्व विभाग के डेटा में उपलब्ध उसके अंगुलि चिह्नों व चित्र से किया जाएगा। इस प्रकार बायोमैट्रिक्स का उपयोग करके इस प्रकार के वित्तीय अपराधों की रोकथाम काफी सरल हो गई है।

राजस्व विभाग के रिकार्ड से होने वाली किसी भी छेड़छाड़ या फर्जीवाडे को रोकने के लिए राजस्व विभाग के समूचे रिकार्ड का कंप्यूटरीकरण किया जा रहा है। उत्तर प्रदेश के अधिकतर जिलों में ऐसा किया जा चुका है और अन्य राज्यों में भी अब राजस्व विभाग के रिकार्ड का कंप्यूटरीकरण किया जा रहा है जिस कारण सरकारी भूमि का स्वामित्व अपने नाम करा लेने के अपराध अब

नहीं हो सकेंगे। राजस्व विभाग के रिकॉर्ड का कंप्यूटरीकरण होने के कारण विभिन्न प्रकार के वित्तीय अपराधों की तो रोकथाम हुई ही है साथ ही इसके कारण आम जनता विशेषकर ग्रामीणों को भी बेहद सुविधा हो गई है। अब कोई भी व्यक्ति एक निर्धारित शुल्क जमा करवा कर राजस्व विभाग से अपनी संपत्ति की 'नकल-खतौनी' प्राप्त कर सकता है। कंप्यूटरीकरण होने से पहले इस काम में भारी श्रम तथा समय व्यर्थ हो जाता था।

बीमा क्षेत्र में भी आजकल प्रौद्योगिकी का खूब इस्तेमाल हो रहा है जिस कारण विभिन्न प्रकार के बीमा संबंधी अपराधों की रोकथाम में सफलता मिली है। बीमा संबंधी दस्तावेज़ों में बायोमैट्रिक्स का इस्तेमाल करके फर्जी दावा करने वालों पर रोक लगा दी है। हाल ही में निजी बीमा कंपनी, *'आई.सी.आई.सी.आई. लोम्बार्ड'* ने *'ई-इंश्योरेंस'* की सुविधा भी प्रारंभ कर दी है। अब मात्र कंप्यूटर के माउस से क्लिक करके ही आप किसी भी बीमा-योजना का लाभ उठा सकते हें। कंपनी ने ई-सोल्यूशंस' नामक एक पोर्टल भी लांच किया है। कहा जा सकता है कि तकनीक और प्रौद्योगिकी का इस्तेमाल करते हुए अब विभिन्न प्रकार के वित्तीय अपराधों की रोकथाम काफी सरल हो गई है। वैसे इस दिशा में अभी काफी कुछ किया जाना शेष है। बैंकिंग, राजस्व, शेयर बाजार आदि के पूर्ण कंप्यूटरीकरण से वित्तीय अपराधों को पूरी तरह से रोका जाना संभव हो सकेगा इसलिए इस दिशा में गंभीर प्रयास किए जाने की आवश्यकता है।

●

8

आतंकवाद और प्रौद्योगिकी

समूची दुनिया आज आतंकवाद की गिरफ्त में है। चाहे पूर्व हो या पश्चिम, विकसित देश हों या विकासशील देश, आतंकवाद चारों ओर पसरा हुआ है। 9/11 की घटना ने तो सिद्ध कर दिया है कि दुनिया का सबसे ताकतवर देश अमेरिका भी आतंकवाद के आगे बौना है। आतंकवाद के संदर्भ में एक दुर्भाग्यपूर्ण तथ्य यह है कि अब दहशतगर्द भी आतंकी कार्रवाइयों में तकनीक व प्रौद्योगिकी का खूब इस्तेमाल करने लगे हैं। लेकिन यहां अमनपसंद लोगों के लिए अच्छी बात यह है कि आधुनिक प्रौद्योगिकी ने हमें कई ऐसी तकनीकें जैसे विभिन्न प्रकार के डिटेक्टर आदि उपलब्ध करा दिए हैं, जिनकी सहायता से आतंकी घटनाओं को रोका जा सकता है। सरकारी खुफिया तंत्र को विभिन्न आतंकी कार्रवाइयों का पहले से ही पता चल जाता है क्योंकि ये खुफिया एजेंसियां आतंकवादियों के खिलाफ मोबाइल सर्विलांस और साइबर सर्विलांस का प्रयोग बहुतायत से कर रही हैं।

आतंकवादियों की पहचान उनके लिए सबसे बड़ा खतरा होती है इसलिए विभिन्न आतंकवादी समूह अपनी पहचान छिपा कर ही कार्य करते हैं। यदि आतंकवादियों की पहचान स्थापित हो जाए तो बहुत सी आतंकी कार्रवाइयों को होने से पहले ही रोका जा सकता है। आतंकवादियों की पहचान के लिए संयुक्त राज्य अमेरिका के कुछ अंतर्राष्ट्रीय हवाई अड्डों पर *'फेशियल रिकोगनिशन सिस्टम'* परीक्षण के तौर पर लगाया गया है जिसमें *'इंजीन फेसेज'* की सहायता से किसी आतंकवादी को जहाज में चढ़ने से रोका जा सकता है। बनारस हिंदू विश्वविद्यालय, वाराणसी के वैज्ञानिक आजकल *'नैनो नोज'* नामक एक अद्भुत

उपकरण विकसित करने में लगे हुए हैं, जो किसी भी प्रकार के विस्फोटक को उसकी गंध मात्र से ही पहचान लेगा। इनके अलावा भी प्रौद्योगिकी आधारित अनेक ऐसी तकनीकें हैं जिनकी सहायता से आतंकी कार्रवाइयों की रोकथाम की जा सकती है।

आतंकवादकाबढ़तासाया: विश्व के अनेक देश आज आतंकवाद की पीड़ा झेल रहे हैं। इन देशों में कुछ सिरफिरे लोगों के समूह अपनी जायज-नाजायज बात मनवाने के लिए चुनी हुई लोकतांत्रिक सरकारों के खिलाफ हिंसा का रास्ता अपनाए हुए हैं। विश्व का कोई भी हिस्सा ऐसा नहीं है, जहां आतंकवाद न पसरा हो, दहशतगर्दी का आलम न हो। वस्तुतः ईश्वर की तरह आज आतंकवाद भी सर्वव्यापी हो गया है, अपरिमित और अनियंत्रित हो गया है। बात चाहे अमेरिका की हो या अफगानिस्तान की, हम बात चाहे चीन, लीबिया, इस्राइल, रूस की करें या फिर इराक और कोरिया की, चहुंओर दहशतगर्दी व आतंक का राज है और मजहबी वहशीपन है। सारे विश्व को शांति का पाठ पढ़ाने वाला 'गांधी का भारत' भी आतंकवाद से जूझ रहा है तो महात्मा बुद्ध और सम्राट अशोक की कर्मस्थली श्रीलंका में भी आतंकवाद ने कहर ढा रखा है। और तो और नेपाल, मालदीव, बांग्लादेश, चेचेन्या, तातरस्तान, बास्किरिया, इन्गुसेतिया, इथोपिया, बोस्निया, जोर्डन और सीरिया जैसे छोटे-छोटे देशों में भी आतंकवाद के कारण जीना मुहाल है।

आतंकवाद के कारण ताकत और सजगता का अमेरिकी मिथक टूट कर बिखर चुका है 11 सितंबर, 2001 को आतंकवाद दबे पांव अमेरिका तक पहुंच गया और देखते ही देखते अमेरिकी पूंजीवाद का प्रतीक 'वर्ल्ड ट्रेड सेंटर' और अमेरिका को दंभ का सांस देने वाला 'पेंटागन', धराशायी हो गया। यह आतंकी ताकत के एक नये पैमाने का प्रस्फुटन था। अमेरिका पर हुए इस कल्पनातीत हमले के सदमे से दुनिया अभी उबरी भी नहीं थी कि दहशतगर्दों ने भारतीय लोकतंत्र, राजनीतिक संप्रभुता और राष्ट्रीय अस्मिता की प्रतीक, हमारी संसद पर भी दुस्साहसिक हमला बोल दिया। भारत मां के कुछ सपूतों ने अगर बहादुरी नहीं दिखायी होती और आतंकवादी, संसद के मुख्य कक्ष में प्रवेश कर गए होते तो क्या होता, यह सोचकर ही सौ करोड़ भारतीय कांप उठते हैं। तब शायद भारत, नेतृत्वविहीन हो चुका होता।

राज्य	*नागरिक*	*सुरक्षाकर्मी*	*आतंकवादी*	*कुल*
जम्मू-कश्मीर	54	72	256	382
असम	98	7	89	194
गुजरात	55	0	0	55
महाराष्ट्र	1	0	0	1
कर्नाटक	0	0	2	2
मणिपुर	91	9	210	310
मेघालय	0	0	7	7
नागालैंड	35	2	82	119
राजस्थान	80	0	0	80
त्रिपुरा	5	1	13	19
पश्चिमी बंगाल	146	160	168	474
उत्तर प्रदेश	1	7	0	8
कुल	**566**	**258**	**827**	**1651**

तालिका : आतंकवाद के कारण हुई मौतें (जनवरी–अगस्त, 2008)

आत्मघात के जरिए दहशतगर्दी फैलाना आतंकवाद की एक नई खौफनाक प्रवृत्ति है। चूंकि इसमें दहशत फैलाने वाले आत्मघाती को मौत का कोई डर नहीं होता है, वरन वह तो मौत का वरण करने ही आता है, इसलिए यह आत्मघाती आतंकवाद कहीं अधिक खतरनाक है, खौफनाक है। समूचा भारतवर्ष आज आतंकवाद की गिरफ्त में है। जम्मू-कश्मीर से लेकर कन्याकुमारी तक और मुंबई से लेकर नगालैंड तक भारत को आतंकवाद लहूलुहान कर रहा है। आतंकवाद के कारण सैकड़ों भारतीयों को प्रत्येक वर्ष असमय अपनी जान गंवानी पड़ती है। एक जनवरी, 2008 से लेकर 31 अगस्त, 2008 तक ही कुल 1651 व्यक्ति भारत में आतंकवाद की भेंट चढ़ चुके हैं।

आतंकवादियोंद्वाराप्रौद्योगिकीकाइस्तेमालः आज लगभग समूची दुनिया आतंकवाद की गिरफ्त में है और दुर्भाग्य से अब आतंकवादी भी तकनीक व प्रौद्योगिकी का इस्तेमाल मानवता के खिलाफ कर रहे हैं। आज

आतंकवादी कंप्यूटर और इंटरनेट का खुलकर दुरुपयोग कर रहे हैं। स्वयं हमारे देश में ही आतंकवादियों ने *'साइबर वार'* को अपना नया हथियार बना लिया है। भारत में *'साइबर वार'* नामक नये आतंकी हथियार का इस्तेमाल 'इंडियन मुजाहिदीन' नामक आतंकी संगठन खूब कर रहा है। अंतर्राष्ट्रीय दबाव के चलते हरकत-उल-जिहाद-ए-इस्लामी अर्थात 'हूजी' नामक आतंकवादी संगठन ने 'इंडियन मुजाहिदीन' नाम का नया चोला ओढ़ लिया है। 'इंडियन मुजाहिदीन' की सहायता 'सिमी' *(स्टूडेंट इस्लामिक मूवमेंट ऑफ इंडिया)* नामक संगठन भी कर रहा है। अब नाम नया है तो काम करने का ढंग भी नया होना चाहिए और इसीलिए इंडियन-मुजाहिदीन ने *'साइबर वार'* को अपना नया हथियार बनाया है।

'साइबर वार' के अंतर्गत आतंकी संगठन, खुफिया एजेंसियों और पुलिस को *ई-मेल* द्वारा बम-विस्फोटों की धमकियां देकर उलझाए रखने का काम करते हैं। जब पुलिस व सुरक्षा-तंत्र, धमकियों में उलझे रहते हैं तो शहर में मौजूद 'आतंकी माड्यूल' किसी आतंकी गतिविधि को अंजाम दे देते हैं। खुफिया रिपोर्टों के मुताबिक उत्तर प्रदेश के लगभग 25 शहरों में *'टेरर माड्यूल'* काम कर रहे हैं। *'टेरर माड्यूल'* में एक बम बनाने वाला होता है जिसका नाम गोपनीय रखा जाता है। बम बनाने वाला आतंकी किसी गोपनीय स्थान से आता है और अपना काम निपटा कर वहीं वापस लौट जाता है। इसके बाद 'होल्डर' सक्रिय होते हैं जिनका काम होता है किसी सार्वजनिक स्थान पर बम रखना। इनके अलावा भी माड्यूल में 3-4 व्यक्ति और होते हैं जो ई-मेल करने, फर्जी धमकियां देने आदि का कार्य करते हैं। भारत में आतंकवादियों के साथ-साथ नक्सलवादियों द्वारा भी अत्याधुनिक तकनीकों का इस्तेमाल, दहशत फैलाने के लिए किया जा रहा है। कुछ समय पूर्व केन्द्रीय गृह राज्यमंत्री ने लोकसभा में स्वीकार किया था कि आतंकवादी अब टैक्नोसैवी हो रहे हैं और अपने नापाक इरादों को अंजाम देने के लिए वे सैटेलाइट फोन, इंटरनेट, कंप्यूटर, अत्याधुनिक वायरलैस यंत्र तथा अन्य हाईटेक साधनों का इस्तेमाल कर रहे हैं।

भारत में कई नक्सली संगठन खुलेआम अपनी वेबसाइटें चला रहे हैं। वेबसाइटों के जरिए आतंकी और नक्सली, दुनियाभर से धन व समर्थन मांग रहे हैं और नई भर्ती कर रहे हैं। साइबर-आतंक से निपटने के लिए सरकार ने *'इंडियन*

कंप्यूटर इमरजेंसी रेस्पांस टीम' (सी.ई.आर.टी. इन.) का गठन किया है। अमेरिका व यूरोप सहित अब हमारे देश में भी तमाम सरकारी व गैर-सरकारी प्रणालियां, पूरी तरह से कंप्यूटर पर आधारित हैं। हमारी रक्षा-प्रणाली, वायु सेवा, रेल सेवा, वित्तीय संस्थान, बैंक और सूचना-तंत्र पूरी तरह से कंप्यूटर आधारित हैं। यदि इन संस्थाओं के कंप्यूटर तंत्र को हैक कर लिया जाए तो सारी व्यवस्था चरमरा सकती है और आतंकवादी ऐसा करने का ही कुत्सित प्रयास कर रहे हैं।

सितंबर, 2008 में गृह मंत्रालय ने आतंकवाद पर एक रिपोर्ट तैयार की जिसमें कहा गया है कि भारत के कुछ आतंकवादी संगठन अब बम और गोली का प्रयोग छोड़कर रासायनिक, जैविक, आणविक और रेडियोलॉजिकल हथियारों से भारत में तबाही मचाने की तैयारी कर रहे हैं। इस प्रकार के नये खतरे को गृह मंत्रालय ने 'सुपर टेररिज्म' नाम दिया है। अपनी रिपोर्ट में गृह मंत्रालय ने कहा है कि आतंकवादी, बिहार में भारत-नेपाल सीमा का इस्तेमाल हथियारों, विस्फोटकों और नकली नोटों की तस्करी के लिए कर रहे हैं। इस रिपोर्ट के अनुसार पाकिस्तानी खुफिया एजेंसी आई एस आई अब भारत से लड़ने के लिए 'सुपर टेररिज्म' नाम के नये हथियार का इस्तेमाल करने की तैयारी कर रही है। कहा जा सकता है कि आने वाले समय में भारत को अत्याधुनिक हथियारों और प्रौद्योगिकी से लैस आतंकवादियों का सामना करना पड़ेगा।

आतंकवादी किस प्रकार अत्याधुनिक तकनीक व प्रौद्योगिकी से लैस हो रहे हैं, यह जानने के लिए 13 सितंबर, 2008 को राजधानी दिल्ली में हुए शृंखलाबद्ध बम विस्फोटों के लिए जिम्मेदार माने जा रहे आतंकवादी तौकीर का उदाहरण दिया जा सकता है। तौकीर उर्फ अब्दुल सुभान कुरैशी, सॉफ्टवेयर इंजीनियर है और आतंकी कार्रवाईयों में तकनीक का इस्तेमाल करने में उसे महारत हासिल है। उसके नेटवर्क (समूह) में भी तकनीक के ज्ञाता आतंकवादी ही शामिल हैं। अपने समूह के लोगों से तौकीर केवल जंगलों में मिलता है ताकि किसी भी प्रकार की सर्विलांस से वह बचा रह सके। खुफिया एजेंसियों के अनुसार तौकीर के पास मोबाइल फोनों के तीन दर्जन से भी अधिक सिमकार्ड हैं और वह एक सिमकार्ड का इस्तेमाल कुछ मिनटों से अधिक समय के लिए बिल्कुल नहीं करता है। तकनीक का इस्तेमाल तौकीर, सुरक्षा एजेंसियों को गुमराह करने के लिए करता है। नेटवर्क हैकिंग में उसे महारत हासिल है और

वह किसी अन्य व्यक्ति के बाई-फाई नेटवर्क को हैक करके उसके ई-मेल से खुफिया एजेंसियों को मेल करके उन्हें गुमराह करता रहता है।

हैकिंग और प्रौद्योगिकी द्वारा रोकथाम

सूचना-प्रौद्योगिकी के इस युग में आतंकवादियों ने हैकिंग को अपना नया हथियार बना लिया है। हैकिंग के द्वारा किसी भी देश की सुरक्षा व्यवस्था और वित्तीय स्थिति को तार-तार किया जा सकता है इसलिए अत्याधुनिक तकनीक से लैस आतंकवादी अब हैकिंग द्वारा आतंक फैलाने का प्रयास कर रहे हैं। पिछले दिनों भारतीय विदेश मंत्रालय की वेबसाइट को हैक करने की असफल कोशिश की गई। यह बात और है कि भारतीय विदेश मंत्रालय ने तकनीक व प्रौद्योगिकी का इस्तेमाल करके अपनी वेबसाइट की सुरक्षा दीवार इतनी पुख्ता कर रखी है कि उसे भेद पाना लगभग असंभव है। किसी भी आशंकित हैकिंग से बचने के लिए विदेश मंत्रालय अक्सर अपनी सुरक्षा-दीवार को बदलता रहता है।

इसी प्रकार सन् 2008 के प्रारंभ में *नेशनल इनफॉरमेटिक्स सेंटर* (एन. आई.सी.) की वेबसाइट और सर्वर को हैक करने की कोशिश की गई। नेशनल इनफॉरमेटिक्स सेंटर, केन्द्र व राज्य सरकारों को नेटवर्क उपलब्ध कराता है। सरकारी योजनाओं से जुड़े आंकड़े व सारा लेखा-जोखा भी एन.आई.सी. के सर्वर में ही सुरक्षित रहता है। एन.आई.सी. के सर्वर के ठप्प होने से सारा सूचना-तंत्र ध्वस्त हो सकता है। इसके ठप्प हो जाने पर सरकारी कामकाज और यहां तक कि पुलिस मुख्यालयों के डाटाबेस पर भी खतरा मंडरा सकता था। किसी देश के प्रमुख वेबसाइटों को हैक करने से क्या-क्या खतरे पैदा हो सकते हैं, यह समझने के लिए जरूरी है यह जानना कि कौन-कौन से सरकारी तंत्र, कंप्यूटर नेटवर्क पर आधारित होते हैं। आतंकवादी, हैकिंग द्वारा निम्नलिखित व्यवस्थाओं को ध्वस्त कर सकते हैं :

रक्षाप्रणाली: भारत सहित सभी प्रमुख राष्ट्रों के रक्षा-तंत्र कंप्यूटरों पर ही आधारित हैं। रक्षा-मंत्रालय की वेबसाइट को हैक करके सेना की पूरी संचार-प्रणाली को ध्वस्त किया जा सकता है और सामरिक महत्त्व के डाटाबेस की चोरी की जा सकती है।

वायुसेवा: आज समूची वायु सेवा प्रणाली, कंप्यूटर पर ही आधारित है। वायुसेवा की निगरानी और मार्गदर्शन प्रणाली भी कंप्यूटरीकृत होती है। हैकिंग द्वारा आतंकवादी, किसी भी देश की वायुसेवा को पूरी तरह से बाधित कर सकते हैं।

रेलसेवा: विभिन्न रेलगाड़ियों का स्टेशन से संपर्क और पथ-संचालन कंप्यूटरों पर ही आधारित होता है। हैकिंग द्वारा समूचे रेल यातायात को बाधित किया जा सकता है।

वित्तीयव्यवस्था: भारत सहित अधिकतर देशों के आधुनिक शेयर बाजार आजकल पूरी तरह से कंप्यूटरीकृत हैं और यहां शेयरों की खरीद-फरोख्त कंप्यूटर के जरिए ही होती है। बिना कंप्यूटर/नेटवर्क के शेयर बाजार बिल्कुल अपंग सा हो जाता है। शेयर बाजार और वित्तीय संस्थानों के कंप्यूटर हैक करके किस प्रकार कोहराम मचाया जा सकता है, इसका अंदाजा सहज ही लगाया जा सकता है।

सरकारीसूचना-तंत्र: भारत में केन्द्र व राज्य सरकारों के बीच सूचनाओं का आदान-प्रदान और सरकारी कामकाज का लेखा-जोखा कंप्यूटरों में ही दर्ज रहता है। सरकारी कंप्यूटर तंत्र को हैक करके सरकारी सेवाओं और केन्द्र-राज्य समन्वय को ध्वस्त किया जा सकता है।

यदि आतंकवादी किसी बैंक की वेबसाइट को हैक कर लें तो पूरी बैंकिंग व्यवस्था धराशायी हो सकती है। सरकारी वेबसाइटों की हैकिंग के बढ़ते खतरे के संदर्भ में हमारी सुरक्षा एजेंसियों की नींद उड़ी हुई है। पिछले कुछ समय के दौरान ही विदेश मंत्रालय, रक्षा मंत्रालय, नेशनल इंफॉरमेटिव सेंटर और दूरसंचार नियामक आयोग (ट्राई) की वेबसाइटें हैक हो चुकी हैं। अब हैकरों के निशाने पर बैंक भी आ चुके हैं। बैंकों की साइटों को हैक करने के पीछे इरादा, बैंकिंग व्यवस्था को चौपट करना ही है। यदि कोई हैकर, किसी बैंक की वेबसाइट को हैक करने में कामयाब हो जाता है तो डेबिट और क्रेडिट कार्डों से संबंधित सूचनाओं में हेराफेरी की जा सकती है। इसके कारण गलत दिशा-निर्देश जारी होने का भी खतरा पैदा हो जाता है। सरकार को साइबर हमले से बचाने के लिए *'सी.ई.आर.टी. इन'* (संचार मंत्रालय के अंतर्गत एक विभाग) काफी प्रयास कर रहा है।

हैकर के रूप में आतंकवादी, राष्ट्रपति और प्रधानमंत्री अथवा उच्च सैन्याधिकारियों के बीच होने वाली ई-मेल बातचीत को भी सुन सकते हैं। इसके अलावा सामरिक महत्त्व के राष्ट्रीय सुरक्षा से संबंधित दस्तावेज़ों को भी हैक किया जा सकता है। हैकिंग के खतरे से बचने के लिए दुनिया की कई बड़ी सूचना-प्रौद्योगिकी कंपनियां आजकल शोध व विकास कार्य कर रही हैं। भारत की एक सूचना प्रौद्योगिकी प्रमाण कंपनी *'अप्पीन'* ने हैकिंग के खतरे से देश को बचाने के लिए *'इंटरटेक'* नामक कम्पनी से समझौता किया है। समझौते के अंतर्गत दोनों कम्पनियां, 'ए.पी.पी.एस.ई.सी.' नाम से *'सॉफ्टवेयर एप्लीकेशन सिक्युरिटी सर्टिफिकेट'* प्रदान करेंगी। यह प्रमाण पत्र जारी करने से पहले 'अप्पीन' और 'इंटरटेक' दोनों ही कम्पनियां मिलकर कुल 20 मानदण्डों पर सॉफ्टवेयर का परीक्षण करेंगी। 'ए.पी.पी.एस.ई.सी.' को संयुक्त राज्य अमेरिका, इंग्लैंड और अन्य पश्चिमी देशों में पहले से ही मान्यता प्राप्त है।

वाई-फाईकीसुरक्षाः आतंकवादियों द्वारा किसी अन्य व्यक्ति के *वाई-फाई* नेटवर्क का इस्तेमाल करने के मामले भी अब प्रकाश में आने लगे हैं। ऐसा करके आतंकवादी अपनी पहचान गुप्त रखने में कामयाब हो जाते हैं। दरअसल, वाई-फाई एक प्रचलित वायरलैस तकनीक है, जिसका इस्तेमाल होम नेटवर्क, मोबाइल फोन और वीडियो गेम में किया जाता है। यह तकनीक सामान्यतः सभी ऑपरेटिंग सिस्टमों पर काम कर सकती है। वाई-फाई दो प्रकार का होता है खुला क्षेत्र और बंद क्षेत्र वाई-फाई। खुले वाई-फाई का प्रयोग कोई भी व्यक्ति कर सकता है जबकि बंद वाई-फाई का प्रयोग करने के लिए पासवर्ड की आवश्यकता होती है। वाई-फाई नेटवर्क के माध्यम से नेटवर्क कार्ड वाले कंप्यूटर, वायरलैस रूटर से जुड़े होते हैं। वाई-फाई में सूचना के आदान-प्रदान के लिए रेडियो फ्रीक्वेंसी तकनालॉजी का प्रयोग किया जाता है।

यह नेटवर्क की एक वायरलैस तकनीक है और इसके कारण तार, प्लग, स्विच, एडाप्टर, पिन और कनेक्टर आदि से मुक्ति मिल गई है। यह तकनीक जिस दायरे में होती है, उस दायरे के किसी भी स्थान से इंटरनेट का इस्तेमाल किया जा सकता है। इस तकनीक के द्वारा व्यक्तिगत कंप्यूटर या लैपटॉप को एक कनेक्टर की सहायता से इंटरनेट से जोड़ा जाता है। यह एक बेहद सुविधाजनक तकनीक है लेकिन अब इसका इस्तेमाल आतंकवादी भी करने लगे

हैं। सन् 2008 में अहमदाबाद में हुए बम विस्फोटों की जिम्मेदारी लेने के लिए इंडियन मुजाहिदीन नामक आतंकवादी संगठन ने मुम्बई के एक अमेरिकी नागरिक के वाई-फाई नेटवर्क को हैक कर लिया और फिर उस अमेरिकी नागरिक के ई-मेल से सुरक्षा एजेंसियों और मीडिया को मेल किए गए। वाई-फाई के दायरे में उपस्थित कोई भी व्यक्ति, इंटरनेट का प्रयोग तो कर ही सकता है, साथ ही वह इसके 'इनक्रिप्टेड स्टैंडर्ड वायरलैस इक्विवेलेंट प्राइवेसी' को हैक कर उसे तोड़ भी सकता है।

तकनीक ने यदि आतंकवादियों को वाई-फाई जैसी एक विधि उपलब्ध कराई है तो उसने सुरक्षा एजेंसियों और आम नागरिकों को वे उपकरण भी उपलब्ध करा दिए हैं जिनका उपयोग करके, किसी अनाधिकृत व्यक्ति द्वारा वाई-फाई के दुरुपयोग की रोकथाम की जा सकती है :

(1) सबसे पहले अपने 'रूटर' का स्विच-ऑन करें और फिर नेटवर्क कनेक्शन के विकल्प को क्लिक करें। इसमें प्रयोगकर्ता का नाम और पासवर्ड डालिए और 'ओ.के.' बटन को क्लिक कर दें। ऐसा करते ही कंप्यूटर को वाई-फाई का संकेत मिल जाएगा और यह इंटरनेट से जुड़ जाएगा यह वाई-फाई इस्तेमाल करने का सबसे सुरक्षित तरीका है।

(2) अपने 'रूटर' को स्विच ऑन करके न छोड़े। ऐसा करना बेहद असुरक्षित हो सकता है क्योंकि कोई भी व्यक्ति आपके वाई- फाई संकेतों का दुरुपयोग कर सकता है।

(3) वाई-फाई का प्रयोग करने के लिए सदैव प्रयोगकर्ता के नाम और पासवर्ड का प्रयोग करें तथा एक निश्चित अवधि के बाद अपना पासवर्ड बदलते रहें।

(4) यदि उपयोग न किया जा रहा हो तो अपने वाई-फाई कनेक्शन को बंद कर दें।

(5) समय-समय पर इस बात की जांच करते रहें कि कोई व्यक्ति आपके कंप्यूटर/वाई-फाई का दुरुपयोग तो नहीं कर रहा है। नेटवर्क आइकन को क्लिक करते ही आप जान सकते हैं कि आपके वाई-फाई से कौन-कौन से कंप्यूटर जुड़े हुए हैं।

चूंकि आतंकवादी इंटरनेट का दुरुपयोग भी करने लगे हैं इसलिए जरूरत इस बात की है कि आप अपने इंटरनेट कनेक्शन को सुरक्षित रखें। असुरक्षित वाई-फाई कनेक्शन का प्रयोग कदापि न करें और अपने वाई-फाई में सदैव प्रयोगकर्ता का नाम *(यूजर नेम)* और पासवर्ड का इस्तेमाल करें।

इलैक्ट्रॉनिक सर्विलांस से आतंकवाद की रोकथाम

आज अगर आतंकवादी कंप्यूटर, इंटरनेट, मोबाइल और सैटेलाइट फोन जैसे अत्याधुनिक संचार साधनों का इस्तेमाल कर रहे हैं तो इलैक्ट्रॉनिक सर्विलांस द्वारा आतंकवाद की रोकथाम करना भी काफी सरल हो गया है। मोबाइल और वीडियो सर्विलांस के जरिए आतंकवाद के पर कतरना बेहद सुविधाजनक हो गया है। हाल ही में भारतीय प्रौद्योगिकी संस्थान, कानपुर ने *'ऑटोमैटिक वीडियो सर्विलांस'* नामक एक ऐसी तकनीक विकसित की है, जिसके जरिए संदिग्ध आतंकवादियों को दबोचना आसान हो जाएगा। इस तकनीक की सहायता से धार्मिक व सार्वजनिक स्थलों पर पैनी नजर रखी जा सकेगी। इस तकनीक को जल्द ही मुंबई स्थित भाभा परमाणु केन्द्र (बार्क) में संस्थापित किया जाएगा। भाभा परमाणु अनुसंधान केन्द्र का परिसर लगभग 20 वर्ग किलोमीटर के क्षेत्रफल में विस्तृत है। अब इस केन्द्र की सुरक्षा, ऑटोमैटिक वीडियो सर्विलांस के जरिए की जा सकती है। इस तकनीक के अंतर्गत एक नियंत्रण-कक्ष बनाया जाएगा जिसकी सहायता से संदिग्ध व्यक्तियों पर निगाह रखी जा सकेगी। ऑटोमैटिक वीडियो सर्विलांस की सहायता से हथियार या विस्फोटक सामग्री लेकर परिसर में घुसने वाले व्यक्ति की पहचान की जा सकेगी। हथियार या विस्फोटक सामग्री लेकर परिसर में प्रवेश करते ही नियंत्रण-कक्ष में लालबत्ती जल उठेगी जिससे सुरक्षाकर्मी सतर्क हो जाएंगे।

भारतीय प्रौद्योगिकी संस्थान (कानपुर) द्वारा विकसित यह तकनीक, इसी प्रकार की विदेशी तकनीकों के मुकाबले काफी सस्ती है और इसमें चूक होने की आशंका लगभग नगण्य है। ऑटोमैटिक वीडियो सर्विलांस की तकनीक को अब केन्द्रीय गृह मंत्रालय को सौंपने की तैयारी चल रही है ताकि विभिन्न धार्मिक व सार्वजनिक स्थलों की सुरक्षा व्यवस्था मजबूत की जा सके। सर्विलांस, फ्रेंच भाषा का शब्द है जिसका अर्थ होता है अतिरिक्त नजर। हिंदी में इसे

निगरानी-तंत्र भी कहा जा सकता है। निगरानी-तंत्र के माध्यम से व्यक्ति के व्यवहार पर निगरानी रखी जाती है। आतंकवादियों के खतरनाक मंसूबों की रोकथाम के लिए इलैक्ट्रॉनिक सर्विलांस के निम्नलिखित माध्यमों का उपयोग किया जाता है :

- ☆ टेलीफोन टैपिंग
- ☆ डारेक्टनल माइक्रोफोन
- ☆ कर्वर लिस्टिंग डिवाइस
- ☆ क्लोज सर्किट टेलीविजन
- ☆ रात्रि में देखने के उपकरण
- ☆ जी.पी.एस. ट्रैकिंग
- ☆ इंटरनेट सर्विलांस
- ☆ इलैक्ट्रॉनिक ट्रायल्स

मोबाइलसर्विलांस: आतंकवादियों के बीच होने वाली बातचीत और उन्हें धर दबोचने में मोबाइल सर्विलांस काफी महत्त्वपूर्ण भूमिका अदा कर रही है। मोबाइल फोनों ने आतंकवादियों के हमलों के रुख को बदल कर रख दिया है। सॉफ्टवेयर इंजीनियरों ने मोबाइल जैमर और सर्विलांस जैसी तकनीक का आविष्कार कर आतंकवाद की रोकथाम को संभव कर दिखाया है। आतंकवादियों के लिए मोबाइल फोन जहां बेहद सुविधाजनक हैं वहीं इनके कारण आतंकवादियों के छिपने का पता भी लगाया जा सकता है।

कुछ आतंकवादी और अपराधी सोचते हैं कि यदि वे अपने मोबाइल फोन को बंद कर दें अथवा उसमें से सिमकार्ड निकाल कर फेंक दें तो वे मोबाइल सर्विलांस से बच सकते हैं। लेकिन वास्तव में ऐसा नहीं है। यदि कोई आतंकवादी अपने मोबाइल फोन को बंद कर दे, उसकी बैटरी निकाल दे अथवा मोबाइल के सिमकार्ड को नष्ट कर दे, तो भी तकनीक का उपयोग करके मोबाइल फोन को ट्रैप किया जा सकता है और तो और यदि आतंकवादी अपने मोबाइल फोन को फेंककर किसी दूसरे मोबाइल फोन का इस्तेमाल करने लगे, तो भी *'इम्जी'* नामक सॉफ्टवेयर के द्वारा आतंकवादी की लोकेशन का पता लगाया जा सकता है। किसी आतंकवादी के व्यक्तिगत विवरण की जानकारी भले ही सुरक्षा एजेंसियों के पास न हो लेकिन उसके साथ साए की तरह हमेशा साथ रहने वाला

उसका मोबाइल फोन, बताता चलता है कि अब आतंकवादी किस क्षेत्र विशेष में है।

'इम्जी' नामक सर्विलांस प्रणाली आज आतंकवादियों को पकड़ने में एक वरदान की तरह है। अगर आतंकवादी अपने मोबाइल फोन को फेंक कर उसके सिमकार्ड का उपयोग किसी दूसरे मोबाइल फोन में करने लगे तो 'इम्जी' की सहायता से उसे फिर से ट्रैप किया जा सकता है। यही नहीं अगर मोबाइल टॉवर पर एक 'ई.एम.आई.ई.' आ गई है तो आतंकवादी चाहे कितने ही मोबाइल फोन बदल ले लेकिन यदि उसने दूसरे मोबाइल नेटवर्क पर उसी 'ई.एम.आई.ई.' से फोन कर दिया तो आतंकवादी की लोकेशन की पहचान आसानी से की जा सकती है।

मोबाइलजैमरः किसी क्षेत्र-विशेष में मोबाइल फोन के नेटवर्क को बाधित कर देने वाले उपकरण को *'मोबाइल जैमर'* कहा जाता है। महत्त्वपूर्ण स्थलों की सुरक्षा में ये मोबाइल जैमर महत्त्वपूर्ण भूमिका अदा कर रहे हैं। महत्त्वपूर्ण स्थलों व इमारतों की सुरक्षा की दृष्टि से तथा अनावश्यक व्यवधान से बचने के लिए मोबाइल फोन जैमर का इस्तेमाल किया जाता है। इसके इस्तेमाल से आतंकवादियों के संचार-संपर्क को भी नष्ट कर दिया जाता है। यही कारण है कि भारत की संसद, राष्ट्रपति भवन और इसी प्रकार की अन्य इमारतों में शक्तिशाली मोबाइल फोन जैमर लगाए गए हैं।

मोबाइल फोन जैमर एक ऐसा उपकरण है, जो इस्तेमाल किए जाने वाले मोबाइल फोन की समान आवृत्ति वाले संकेत उत्पन्न करता है जिस कारण ट्रांसमिशन बाधित हो जाता है और उस क्षेत्र विशेष का मोबाइल नेटवर्क काम करना बंद कर देता है। प्रत्येक मोबाइल फोन दो अलग-अलग आवृत्तियों का इस्तेमाल करता है, एक बोलने के लिए और दूसरी सुनने के लिए। मोबाइल फोन से उत्पन्न संकेत को बेस स्टेशन भेजा जाता है और जब बेस स्टेशन से इन संकेतों को प्राप्तकर्ता के पास भेजा जाता है तो समान आवृत्ति के होने के कारण दोनों संकेत रद्द हो जाते हैं। अधिकतर जैमर्स के माध्यम से एक तरफ की आवृत्ति को ही रद्द किया जाता है जिस कारण क्षेत्र विशेष में नेटवर्क बाधित हो जाता है और मोबाइल फोन काम करना बंद कर देते हैं। प्रत्येक जैमर में एक एंटीना, मुख्य सर्किट और एक विद्युत स्रोत लगा होता है। मोबाइल फोन

जैमर, प्रत्येक नेटवर्क को बाधित कर सकते हैं।

ब्लैकबेरीसेवाऔरआतंकवादः तकनीक और प्रौद्योगिकी ने आतंकवादियों को संचार के कई अत्याधुनिक साधन उपलब्ध कराए हैं और ऐसी ही एक विधि है ब्लैकबेरी मोबाइल सेवा। हमारी सुरक्षा एजेंसियों ने केन्द्रीय गृह मंत्रालय को सौंपी एक रिपोर्ट में कहा है कि कुछ आतंकवादी संगठन और हवाला संचालक, ब्लैकबेरी सेवा का दुरुपयोग कर रहे हैं। सुरक्षा एजेंसियों ने आगाह करते हुए कहा है कि ब्लैकबेरी सेवा की विषय सामग्री *(कंटेंट)* पर निगरानी रखने के पुख्ता इंतजाम किए बगैर ब्लैकबेरी सेवा, राष्ट्रविरोधी तत्वों के हाथों का खिलौना हो सकती है। सरकार इससे पहले ही मोबाइल फोन सेवा प्रदाता कम्पनियों से कह चुकी है कि वे ब्लैकबेरी के जरिए भेजी गई सामग्री की निगरानी करें अन्यथा सेवा को बंद कर दें क्योंकि इससे देश की सुरक्षा में सेंध लग सकती है। इससे पहले आसूचना राजस्व महानिदेशालय (डी.आर. आई.) ने ब्लैकबेरी सेवा के जरिए भेजी जाने वाली सामग्री की निगरानी में मुश्किल जाहिर की थी। उस समय कहा गया था कि आंकड़ों की पैकेजिंग, कोड में किए जाने के कारण सामग्री को समझा नहीं जा सकता। इस टेक्नोलॉजी में डेटा पैकेट, कोड रूप में भेजे जाते हैं जिन तक पहुंचने के लिए पासवर्ड का होना आवश्यक होता है। इस पासवर्ड में ग्राहक-कोड और कम्पनी-कोड होता है। इस प्रकार डेटा के पैकिट की डाउनलोडिंग कठिन हो जाती है।

चूंकि ब्लैकबेरी सेवा का दुरुपयोग, आतंकवादी संगठन कर सकते हैं इसलिए भारत सरकार इस सेवा की निगरानी को लेकर गंभीर हो गई है और उसने ब्लैकबेरी सेवा के जरिए भेजे जाने वाले ई-मेल के संदेशों पर निगरानी का काम एक विदेशी कम्पनी को सौंपने का फैसला किया है। हमारे पास अभी तक ब्लैकबेरी सेवा के जरिए भेजे जाने वाले संदेशों को पढ़ने की कोई तकनीक उपलब्ध नहीं है। ब्लैकबेरी सेवा प्रदाता तकनीक लायसेंस रखने वाली कम्पनी, *'रिसर्च-इन-मोशन'* (रिम) भी कह चुकी है कि उसके पास इस माध्यम से संचारित संदेशों को पढ़ने की कोई प्रणाली नहीं है। यहां यह जानना प्रासंगिक होगा कि ब्लैकबेरी के माध्यम से ग्राहक, मोबाइल फोन के द्वारा ही ई-मेल को 'एस.एम.एस.' के रूप में भेज सकते हैं अथवा प्राप्त कर सकते हैं। देश में ब्लैकबेरी सेवा तब अधिकारिक रूप से निगरानी में आ गई

थी जब विदेशों में स्थापित सर्वरों के माध्यम से संदेशों का आदान-प्रदान होने लगा और हमारी सुरक्षा एजेंसियां इसे रोक पाने में नाकाम हो गईं।

स्विटजरलैण्ड और कनाडा की कुछ सॉफ्टवेयर कम्पनियों ने ब्लैकबेरी जैसी सेवाओं की निगरानी हेतु एक सॉफ्टवेयर विकसित करने का दावा किया है। एक स्विस कम्पनी *'यूटिमाको'* ने ब्लैकबेरी सेफगार्ड का एक नया संस्करण जारी किया है, जिसकी सहायता से ब्लैकबेरी सेवा द्वारा भेजे जाने वाले सभी प्रकार के ई-मेल संदेशों को पढ़ा जा सकता है। कहा जा सकता है कि तकनीक व प्रौद्योगिकी ने आज इतनी तरक्की कर ली है कि ब्लैकबेरी जैसी सेवाओं को भी निगरानी-तंत्र (सर्विलांस) के अंतर्गत लाया जा सकता है। इस प्रकार आतंकवादियों द्वारा ब्लैकबेरी सेवा के दुरुपयोग के मामलों को प्रभावी ढंग से रोका जा सकता है।

धातु-खोजकऔरआतंककीरोकथामः भीड़भाड़ वाले सार्वजनिक स्थलों की सुरक्षा करना सुरक्षा एजेंसियों के लिए एक चुनौतीपूर्ण कार्य है क्योंकि ऐसी जगहों पर आने वाले प्रत्येक व्यक्ति और उसके सामान की तलाशी लेना संभव नहीं होता है। इस संदर्भ में धातु-खोजक (मेटल डिटेक्टर) एक महत्त्वपूर्ण भूमिका अदा करता है। आतंकवाद के इस दौर में प्रत्येक सार्वजनिक और धार्मिक स्थल की सुरक्षा मेटल डिटेक्टरों के जरिए ही की जा रही है। लगभग सभी हवाई अड्डों, रेलवे स्टेशनों, सिनेमाघरों, शॉपिंग माल्स और मेट्रो रेल स्टेशनों के परिसर में प्रवेश करने वाले प्रत्येक व्यक्ति की तलाशी में मेटल डिटेक्टरों का इस्तेमाल किया जाता है।

जैसा कि नाम से ही स्पष्ट है, मेटल डिटेक्टर का इस्तेमाल छिपाकर रखी गई किसी धातु को खोजने के लिए किया जाता है। इसके अलावा आजकल भूमिगत सुरंगों और विस्फोटकों का पता लगाने वाले डिटेक्टर भी अस्तित्व में आ चुके हैं। मेटल डिटेक्टर में एक दोलक होता है जो प्रतिवर्ती वैद्युत धारा उत्पन्न करता है। यह वैद्युत धारा एक कुंडली में प्रवाहित होती है जिस कारण एक चुंबकीय क्षेत्र पैदा हो जाता है। इसमें एक कुंडली का इस्तेमाल चुंबकीय क्षेत्र को मापने के लिए किया जाता है। चुंबकीय पदार्थ (धातु) होने पर चुंबकीय क्षेत्र में परिवर्तन होता है और इस परिवर्तन के आधार पर ही किसी धातु की उपस्थिति का पता चल जाता है। इसमें लगे

माइक्रोप्रोसेसर से यह भी पता चल जाता है कि खोजी गई धातु कौन सी है। इस प्रकार मेटल डिटेक्टर, वैद्युत चुंबकत्व के आधार पर कार्य करते हैं।

विश्व का सबसे पहला मेटल डिटेक्टर सन् 1937 ई. में जेरार्ड फिशर ने बनाया था। इसके बाद विभिन्न प्रकार के मेटल डिटेक्टर बनाए जाने लगे। भिन्न-भिन्न आवश्यकताओं के अनुरूप अलग-अलग संवेदनशीलता वाले मेटल डिटेक्टर बनाए जाते हैं। आधुनिक मेटल डिटेक्टर इतने संवेदनशील होते हैं कि वे बालू, मिट्टी और लकड़ी के भीतर छिपी धातु का भी पता लगा लेते हैं। विभिन्न आतंकी गतिविधियों की रोकथाम में ये मेटल डिटेक्टर, बेहद कारगर साबित हो रहे हैं।

मेट्रोस्टेशनोंकीसुरक्षा: बेहद अल्प समय में ही मेट्रो रेल, दिल्ली की शान बन चुकी है और शायद इसलिए दिल्ली-मेट्रो आतंकवादियों के निशाने पर है। आतंकवादियों के खतरे को भांपते हुए दिल्ली मेट्रो रेल कार्पोरेशन ने तकनीक व प्रौद्योगिकी का इस्तेमाल करते हुए ऐसे प्रबंध किए हैं कि आतंकवादियों के लिए मेट्रो रेल परिसर में कोई वारदात करना काफी कठिन है।

दिल्ली मेट्रो के वर्तमान में कुल 59 स्टेशन हैं और ये सभी मेट्रो स्टेशन, पूरी तरह से क्लोज-सर्किट टेलीविजन कैमरों की निगरानी में हैं। दिल्ली मेट्रो रेल कार्पोरेशन ने अपने सभी स्टेशनों में कुल 1237 सी.सी.टी.वी. कैमरे लगाए हैं जिनकी सहायता से मेट्रो रेल परिसर में आने वाले प्रत्येक व्यक्ति पर गहरी नजर रखी जाती है। दिल्ली मेट्रो की तीन लाइनों के सभी स्टेशनों पर क्लोज सर्किट टेलीविजन कैमरे लगा दिए जाने के बाद अब वहां आने वाले प्रत्येक व्यक्ति की संदिग्ध गतिविधियों पर नजर रखना सरल व आसान हो गया है। सी.सी.टी.वी. कैमरों के अलावा मेट्रो परिसर में प्रवेश करने से पहले प्रत्येक व्यक्ति को मेटल डिटेक्टर और भारी सुरक्षा व्यवस्था से गुजरना पड़ता है जिस कारण मेट्रो परिसरों में किसी भी आतंकी कार्रवाई को अंजाम देना काफी मुश्किल है।

दिल्ली मेट्रो के अलावा दिल्ली की अन्य महत्त्वपूर्ण इमारतों को आतंकी खतरे से बचाने के लिए भी व्यापक प्रबंध किए गए हैं। संसद भवन और दिल्ली सचिवालय की सुरक्षा के लिए वहां मेटल डिटेक्टर, क्लोज सर्किट टेलीविजन कैमरे, फ्लैप बैरियर, व्यक्ति की पहचान हेतु बायोमैट्रिक उपकरण, बार-कोड

युक्त स्मार्ट पहचान-पत्र, स्कैनर, बैगेज स्क्रीनिंग प्रणाली, विशेष प्रकार के होलोग्राम युक्त स्टीकर आदि अत्याधुनिक तकनीकों व उपकरणों का इस्तेमाल किया जा रहा है। आतंकवाद को मात देने के लिए तकनीक व प्रौद्योगिकी का इस्तेमाल करने के लिए अब हमारे वैज्ञानिकों ने भी कमर कस ली है। वैसे भी जिस देश में कुल 833 व्यक्तियों पर मात्र एक पुलिसकर्मी हो वहां आतंकवाद का मुकाबला केवल तकनीक और बेहतर योजना से ही किया जा सकता है।

उत्तर प्रदेश स्थित एक कम्पनी ने एक ऐसा सॉफ्टवेयर बनाया है, जिसकी मदद से ई-मेल से धमकी देने या बम-विस्फोट की सूचना देने वाले की पहचान, तुरंत हो सकेगी। *'क्रिस' (कस्टमर रजिस्ट्रेशन एंड आइडेंटीफिकेशन सिस्टम)* नामक इस सॉफ्टवेयर का विकास, लखनऊ स्थित कम्पनी 'जी.आई. बायोमैट्रिक्स' ने किया है। इस सॉफ्टवेयर का विकास मुख्य रूप से साइबर कैफों के लिए किया गया है ताकि साइबर कैफों में जाकर आतंकी कार्रवाइयों की सूचना देने या धमकी देने वाले आतंकवादियों की पहचान की जा सके। इस सॉफ्टवेयर के लगाने के बाद साइबर कैफे पर जाने वाले व्यक्ति को पहचान-पत्र दिखाने के अलावा अपने अंगूठे का निशान (अंगुलि चिह्न) भी देना होगा। इसके बाद वेबकैम से ग्राहक का चित्र भी ले लिया जाएगा ग्राहक के बारे में यह सब जानकारियां, स्वयं ही कंप्यूटर के डाटाबेस में दर्ज हो जाएंगी। इसके अलावा यह भी कंप्यूटर में दर्ज हो जाएगा कि किस व्यक्ति ने, किस समय और किस कंप्यूटर का इस्तेमाल, इंटरनेट द्वारा अपराध करने के लिए किया।

इस सॉफ्टवेयर के डाटाबेस को कोई व्यक्ति हैक भी नहीं कर पाएगा क्योंकि ग्राहक का विवरण, अंगुलि चिह्न और चित्र आदि एनक्रिप्टेड फार्म (बाइट या आंकड़ों में) में बदल जाते हैं। ये सभी आंकड़े तभी प्राप्त हो सकेंगे जब कोई पुलिसकर्मी इसकी रिपोर्ट तैयार करने वाला बटन दबाएगा। इस सॉफ्टवेयर से छेड़छाड़ करने की आशंका लगभग नगण्य है। प्रौद्योगिकी का इस्तेमाल करके आतंकवाद से मुकाबला करने का प्रयास आज समूची दुनिया में किया जा रहा है। अमेरिका में मधुमक्खी के आकार का एक चालक-रहित विमान बनाया गया है जिसका प्रयोग आतंकवाद की रोकथाम के लिए किया जाएगा। आकाश में उड़ते हुए भूमि पर निगरानी करने वाले इस छोटे से उपकरण का आविष्कार, होनेइवेल अंतर्राष्ट्रीय एस.ओ.एन.एन. नामक संस्था ने किया है। हवा में चक्कर

काटने और आकाश में स्थिर रहने वेऽ लिए इस उपकरण में इलैक्ट्रो-ऑपटिक/इंफ्रारेड सेंसॉरस का प्रयोग किया गया है। इस उपकरण के द्वारा भूमि पर होने वाली किसी भी आतंकी गतिविधि पर नजर रखी जा सकेगी।

सारतः कहा जा सकता है कि आज अगर आतंकी संगठन, विभिन्न अत्याधुनिक तकनीकों व प्रौद्योगिकी का इस्तेमाल कर रहे हैं तो आतंकवादी घटनाओं की रोकथाम के लिए भी प्रौद्योगिकी का खूब प्रयोग हो रहा है। मोबाइल ट्रैकिंग व्यवस्था, इलैक्ट्रॉनिक सर्विलांस, साइबर सर्विलांस, ऑटोमैटिक वीडियो सर्विलांस, जी.पी.आर. एस. आदि तकनीकों का इस्तेमाल आज आतंकवाद की रोकथाम के लिए दुनियाभर में किया जा रहा है। यहां यह जानना प्रासंगिक रहेगा कि हमारे देश में आतंकियों के खिलाफ प्रौद्योगिकी का इस्तेमाल कर सकने वाले प्रशिक्षित कर्मियों की भारी कमी है। विभिन्न तकनीकें और उपकरण तो उपलब्ध हैं लेकिन उनका उपयोग कर सकने वाले दक्ष लोगों का अभाव है इसलिए जरूरत इस संबंध में गहन प्रशिक्षण की भी है।

●

9

इलैक्ट्रॉनिक सर्विलांस का महत्त्व

अत्याधुनिक तकनीक और सूचना प्रौद्योगिकी ने यदि अपराधियों को एक से एक नये हथियार दिए हैं तो इनके कारण सुरक्षा एजेंसियों को भी कई ऐसे उपकरण व तकनीकें मिल गई हैं जिनकी सहायता से अपराधों की रोकथाम भी संभव हो गई है। ऐसी ही एक जादुई तकनीक है इलैक्ट्रॉनिक सर्विलांस, जिसके कारण आज अपराधियों के होश उड़े हुए हैं। इसमें कोई शक नहीं है कि *'इलैक्ट्रॉनिक सर्विलांस'* अपराधों की रोकथाम में आज सबसे कारगर साबित हो रही है। इस तकनीक के प्रयोग से अपराधियों द्वारा टेलीफोन या मोबाइल फोन से की जाने वाली बातचीत को तो सुना ही जा सकता है साथ ही इसकी सहायता से उनकी भौगोलिक स्थिति *(लोकेशन)* का भी पता लगाया जा सकता है। इसके अलावा इलैक्ट्रॉनिक सर्विलांस के जरिए इंटरनेट और ई-मेल पर भी नजर रखी जा सकती है।

'सर्विलांस', फ्रेंच भाषा का एक शब्द है जिसका शाब्दिक अर्थ होता है 'अतिरिक्त नजर'। हिंदी में इसे हम निगरानी-तंत्र भी कहते हैं। निगरानी तंत्र *(सर्विलांस सिस्टम)* के माध्यम से व्यक्ति के व्यवहार पर निगरानी रखी जाती है। सर्विलांस के कई रूप हैं, जैसे टेलीफोन टैपिंग, मोबाइल सर्विलांस, जी.पी. ट्रैकिंग, कर्वर लिस्टिंग उपकरण, क्लोज सर्किट टेलीविजन, डायरेक्टनल माइक्रोफोन, इंटरनेट सर्विलांस और इलैक्ट्रॉनिक ट्रायल्स आदि। टेलीफोन टैपिंग से दो उत्पाद सुरक्षा एजेंसियों को मिलते हैं काल डिटेल रिकार्ड और लिसनिंग वॉच। इनकी सहायता से किसी टेलीफोन से की जाने वाली बातचीत तो सुनी ही जा सकती है साथ ही उस टेलीफोन से की जाने वाली और

उस टेलीफोन पर आने वाली सभी कॉल्स का विवरण भी प्राप्त किया जा सकता है। इलैक्ट्रॉनिक सर्विलांस के अंतर्गत *'इलैक्ट्रॉनिक ट्रायल्स'* एक ऐसी तकनीक है जिसकी सहायता से इलैक्ट्रॉनिक डाटा पर नजर रखी जा सकती है।

मोबाइल सर्विलांस

यदि कहा जाए कि आज हम मोबाइल फोन के युग में जी रहे हैं तो शायद कुछ गलत नहीं होगा। मोबाइल फोन आज हर व्यक्ति की जरूरत बन गया है। अपराधियों और आतंकवादियों द्वारा भी मोबाइल फोन का इस्तेमाल खूब हो रहा है। मोबाइल फोन अपराधियों के लिए एक बेहद सुविधाजनक संचार माध्यम है तो सर्विलांस के कारण यह उनके लिए मौत का सबब भी बन रहा है। आज अधिकतर अपराधी मोबाइल सर्विलांस के कारण ही पकड़े जा रहे हैं। अपराधियों की पहचान के साथ-साथ मोबाइल सर्विलांस, अपराधों की रोकथाम के लिए भी एक कारगर उपकरण साबित हो रहा है।

मोबाइलफोनकाबढ़ताप्रयोग: टेलीफोन का आविष्कार करने के बाद ग्राहम बेल ने सोचा तक नहीं होगा कि जब उनकी इस तार-सेवा का बेतार प्रसार होगा तो वो इतनी विकसित हो जाएगी कि उसके बिना मनुष्य के जीवन की कल्पना भी नहीं की जा सकेगी। गार्टनर इंक नामक एक सर्वेक्षण कम्पनी का कहना है कि सन् 2012 तक भारत में मोबाइल प्रयोगकर्ताओं की संख्या 27 करोड़ से बढ़कर 73.7 करोड़ हो जाएगी। यह वृद्धि लगभग 21 फीसदी सालाना की दर से होगी। आज 10 भारतीयों में से प्रत्येक 5 के पास मोबाइल फोन हैं जबकि सन् 2012 में यह आंकड़ा प्रति 10 व्यक्ति 6 का हो जाएगा। अभी भारत के लगभग 6 लाख गांवों में से आधे गांव, मोबाइल नेटवर्क के घेरे में हैं। सन् 2012 तक भारत में लगभग 25 करोड़ मोबाइल फोन धारक, ग्रामीण क्षेत्र से होंगे। गार्टनर इंक का कहना है कि मोबाइल सेवा का राजस्व प्रतिवर्ष 18 प्रतिशत की वृद्धि के साथ 2012 तक 1.58 लाख करोड़ हो जाएगा।

मोबाइलप्रयोगकर्ता	*अनुमानितसंख्या (सन् 2012)*
चीन	800 मिलियन
भारत	560 मिलियन
रूस	189 मिलियन
ब्राजील	76 मिलियन

तालिका : मोबाइल धारकों की अनुमानित संख्या

मोबाइल फोन को अब स्मार्टफोन में बदलने की तैयारी की जा रही है। मोबाइल फोन जिस प्लेटफार्म पर चलते हैं, उसे ऑपरेटिंग सिस्टम कहा जाता है। अधिकतर मोबाइल फोन, विंडोज और सिंबियन प्लेटफार्म पर चलते हैं। मोबाइल फोन के क्षेत्र में प्रतिदिन नई-नई तकनीकें आ रही हैं। शीघ्र ही हमारे देश में मोबाइल फोन पर '3जी' सेवा प्रारंभ होने जा रही है जिसकी सहायता से मोबाइल उपभोक्ता अपने हैंडसेट पर टेलीविजन देख सकेंगे, ई-मेल कर सकेंगे, फैक्स भेज सकेंगे और मंगवा सकेंगे तथा वीडियो कांफ्रेसिंग कर सकेंगे। इंटरनेशनल टेलीकम्युनिकेशन यूनियनों के मापदण्डों के अनुसार 3-जी, तीसरी पीढ़ी की मोबाइल सेवा है जिसमें सीमित फ्रीक्वेंसी स्पैक्ट्रम के जरिए ही तीव्र डाटा भेजा जा सकेगा।

मोबाइल सेवा के क्षेत्र में अब *'नंबर पोर्टेबिलिटी'* के लिए भी प्रयास शुरू हो चुके हैं जिसके अंतर्गत मोबाइल फोन सेवा प्रदाता कम्पनी को बदल लेने पर भी आपका मोबाइल नंबर नहीं बदलेगा। इस सुविधा के लिए सभी मोबाइल सेवा प्रदाता कम्पनियों को जोड़कर एक वेयर हाउस बनाया जाएगा। जब भी कोई उपभोक्ता अपनी मोबाइल कम्पनी बदलेगा तो उसे इस वेयरहाउस के जरिए पुराने नंबर पर ही मोबाइल सेवा प्रदान की जाती रहेगी। सभी ऑपरेटर्स वेयर हाउस से संबद्ध रहेंगे। इस सुविधा का लाभ उठाने के लिए उपभोक्ता को शुल्क चुकाना होगा और इस शुल्क का निर्धारण, सरकार करेगी।

मोबाइलसर्विलांसकीप्रक्रिया: किसी व्यक्ति से संबंधित सूचनाएं एकत्र करने को जब सुरक्षा एजेंसियां उस व्यक्ति के मोबाइल फोन को निगरानी पर लगाती हैं तो इसे मोबाइल सर्विलांस कहा जाता है। मोबाइल सर्विलांस के द्वारा, जिस नंबर को निगरानी में रखा जाता है उसकी कॉल-डिटेल-रिकार्ड (सी डी आर), उसकी भौगोलिक स्थिति (ग्लोबल पॉजिशिनिंग तंत्र द्वारा) का पता

तो लगाया ही जा सकता है साथ ही जरूरत पड़ने पर *'लिसनिंग वॉच'* प्रणाली के द्वारा उस नंबर से होने वाली प्रत्येक बातचीत को भी सुना जा सकता है। इस प्रकार मोबाइल सर्विलांस के निम्नलिखित दो रूप होते हैं :

(1) कॉल डिटेल रिकार्ड की जानकारी प्राप्त करना

(2) *'लिसनिंग वाच'* द्वारा बातचीत को सुनना

किसी व्यक्ति के मोबाइल फोन को सर्विलांस पर लगाने से पहले विधिक प्रक्रिया का पालन करना होता है। जब पुलिस किसी भी संदिग्ध व्यक्ति के बारे में जानकारी प्राप्त करना चाहती है तो कानूनी प्रक्रिया के आधार पर उस व्यक्ति विशेष के मोबाइल फोन को सर्विलांस पर लगाया जा सकता है। सामान्य तौर पर आम आदमी को किसी व्यक्ति का मोबाइल फोन, सर्विलांस पर लगवाने की अनुमति नहीं होती है। कॉल-डिटेल-रिकार्ड (सी.डी.आर.) प्राप्त करने के लिए सहायक पुलिस आयुक्त स्तर के ऐसे पुलिस अधिकारी के प्रस्ताव, जिसका ई-मेल आई.डी. सेवा प्रदाता कम्पनी के पास पंजीकृत हो, पर सेवा प्रदाता कम्पनी, सर्विलांस की व्यवस्था करती हैं। इस सेवा की सुविधा प्राप्त करने के लिए पुलिस द्वारा सेवा प्रदाता कम्पनी को मोबाइल नंबर और 'आई.एम.ई. आई.' *(इंटरनेशनल मोबाइल इक्युपमेंट आइडेंटीफिकेशन)* नंबर का विवरण देना पड़ता है। इसके विपरीत जब किसी व्यक्ति के मोबाइल को *'लिसनिंग वॉच'* पर लगाने की जरूरत पड़ती है तो जिले की पुलिस का एक पुलिस उपायुक्त स्तर का अधिकारी, संयुक्त आयुक्त के जरिए इस संबंध में एक प्रस्ताव पुलिस आयुक्त को भेजता है। पुलिस आयुक्त इस प्रस्ताव को गृह मंत्रालय के मुख्य सचिव को अनुमोदन हेतु भेजता है। इस प्रकार किसी संदिग्ध व्यक्ति के मोबाइल फोन से होने वाली बातचीत को सुनने के लिए मुख्य सचिव (गृह) की अनुमति आवश्यक होती है।

किसी संदिग्ध व्यक्ति का *'कॉल-डिटेल-रिकॉर्ड'*, मोबाइल सेवा प्रदाता कम्पनी द्वारा पुलिस को उपलब्ध कराया जाता है। इस रिकॉर्ड में उन सभी फोन नंबरों की सूची रहती है जिन नंबरों से सर्विलांस पर लगे फोन नंबर पर बात (आने वाली और जाने वाली दोनों कॉल) की गई। इसके अलावा यह विवरण भी दर्ज रहता है किस नंबर पर किस समय और कितनी देर बात की गई। मोबाइल सर्विलांस के समय जी.पी.आर.एस. सेवा का उपयोग भी किया जाता

है ताकि यह पता लग सके कि सर्विलांस पर लगे मोबाइल फोन की भौगोलिक स्थिति (लोकेशन) क्या है। *'लिसनिंग वॉच'* प्रक्रिया के अंतर्गत किसी संदिग्ध व्यक्ति की बातचीत सुनने के लिए पुलिस, *'वॉयस लॉगर'* नामक एक उपकरण के जरिए बातचीत रिकार्ड करती है। उस व्यक्ति द्वारा की जाने वाली बातचीत के आधार पर पुलिस उस व्यक्ति के खिलाफ सबूत जुटाती है।

बहुचर्चित शिवानी भटनागर हत्याकाण्ड की जांच में भी पुलिस को अहम जानकारियां, शिवानी भटनागर के मोबाइल फोन कॉल डिटेल से ही मिली थीं। लगभग ऐसा ही दिल्ली के पार्षद आत्माराम गुप्ता हत्याकाण्ड में भी हुआ था। आतंकवाद की रोकथाम करने में भी मोबाइल सर्विलांस महत्त्वपूर्ण भूमिका अदा कर रहा है। पुलिस और खुफिया एजेंसियां अक्सर संदिग्ध आतंकवादियों के मोबाइल फोन को सर्विलांस पर लगा देती हैं जिस कारण उन्हें आतंकवादियों की भावी योजनाओं की जानकारी पहले से ही मिल जाती है जिस कारण आतंकी गतिविधियों की रोकथाम आसानी से हो जाती है।

सवाल उठता है कि मोबाइल की सर्विलांस किस प्रकार काम करती है। प्रत्येक मोबाइल के बैटरी भाग में 16 अंकों की एक संख्या लिखी होती है, जिसे 'ई.एम.आई.डी.' *(इंटरनेशनल मोबाइल आइडेंटिटी इक्यूपमेंट)* कहते हैं। यह मोबाइल का एक कोड होता है जो अंतर्राष्ट्रीय होता है। इस कोड की कभी भी डबलिंग नहीं होती है। यह कोड मोबाइल फोन का पंजीकरण होता है और जब मोबाइल फोन चलता है तो मोबाइल फोन सबसे पहले इस कोड को ही स्वीकार करता है और इसी के बाद मोबाइल सेवा प्रारंभ होती है। यदि आपका मोबाइल फोन गुम हो जाए या चोरी हो जाए तो अपने फोन की 'ई.एम.आई.ई.' को मोबाइल नेटवर्क पर चलवा कर आप अपने फोन की भौगोलिक स्थिति का पता लगा सकते हैं क्योंकि ई.एम.आई.ई., मोबाइल फोन की परछाई की तरह होती है। सर्विलांस के जरिए किसी मोबाइल फोन की भौगोलिक स्थिति का पता या उसकी स्थिति की जानकारी, मोबाइल टॉवर या उपग्रह के जरिए पता की जाती है। यदि किसी आपराधिक घटना के बाद कोई मोबाइल फोन भी गायब हो जाता है तो लगभग 90 प्रतिशत मामलों में 4-5 दिनों में ही मामले का खुलासा हो जाता है।

मोबाइल फोन के क्षेत्र में दो प्रकार के नेटवर्क कार्य करते हैं *जी.एस.*

एम. और *सी.डी.एम.ए.*। मोबाइल सर्विलांस का अर्थ जी. एम. एम सर्विलांस से ही है क्योंकि इसी को सर्विलास के लिए मोबाइल टॉवर की आवश्यकता पड़ती है। *सी.डी.एम.ए.* मोबाइल की सर्विलांस के लिए मोबाइल टॉवर की जरूरत नहीं पड़ती है क्योंकि इस प्रकार के फोन सीधे सेवा प्रदाता कम्पनी के नियंत्रण कक्ष से जुड़े रहते हैं। *सी.डी.एम.ए.* सेवा प्रदाता कम्पनी ही सीधे बता सकती है कि उसका मोबाइल फोन किस क्षेत्र में है।

इम्जीप्रणाली: कुछ व्यक्ति सोचते हैं कि यदि वे मोबाइल फोन को बंद कर दें अथवा उसका सिम कार्ड निकाल कर फेंक दे तो वे सर्विलांस से बच सकते हैं। आमतौर पर ऐसा ही होता भी था लेकिन प्रौद्योगिकी ने *'इम्जी'* नामक एक ऐसी प्रणाली का विकास कर लिया है जिसकी सहायता से यदि व्यक्ति मोबाइल को बंद कर दे, तब भी उस पर निगरानी रखी जा सकती है। यदि कोई अपराधी बेहद शातिर है और वह 'ई.एम.आई.ई.' के बारे में जानता है तथा वह सर्विलांस से बचने के लिए अपने फोन को फेंक कर सिम का प्रयोग किसी दूसरे मोबाइल फोन में करने लगता है तो इम्जी सॉफ्टवेयर की सहायता से उसे भी पकड़ा जा सकता है। उदाहरण के लिए, यदि किसी अपराधी ने चोरी के फोन को फेंक दिया और उसके सिम कार्ड को किसी दूसरे मोबाइल फोन में लगा चला दिया, तब भी उसे इम्जी प्रणाली के अंतर्गत ट्रैप किया जा सकता है। यही नहीं अगर मोबाइल टॉवर पर एक 'ई.एम.आई.ई.' आ गई है, तब अपराधी व्यक्ति चाहे कितने ही मोबाइल फोन क्यों न बदल ले लेकिन अगर अपराधी व्यक्ति ने दूसरे नेटवर्क पर उसी सिम कार्ड से फोन कर दिया तो फिर उसे कभी भी पकड़ा जा सकता है।

कैसेबचतेहैंअपराधी: मोबाइल सर्विलांस से बचने के लिए अपराधी विभिन्न तकनीकों का इस्तेमाल करते रहते हैं। निम्नलिखित तकनीकों का इस्तेमाल करते हुए अपराधी, सर्विलांस से बचने का प्रयास करते हैं :

1. मोबाइल फोन को बंद किए बगैर ही सीधे बैटरी निकाल कर,
2. एक फोन से एक कॉल करने के बाद दूसरी बार फोन का इस्तेमाल न करके,
3. मोबाइल का सिम कार्ड किसी दूसरे फोन में इस्तेमाल नहीं करके,
4. कभी भी एक ही जगह खड़े होकर बातचीत नहीं करके,

5. सी.डी.एम.ए. मोबाइल के सेटेलाइट नेटवर्क से बाहर निकल कर किसी दूसरे नेटवर्क की खोज करके।

मोबाइल सर्विलांस, सेटेलाइट-फोन में काम नहीं करती है। पहले सेटेलाइट फोन का इस्तेमाल केवल सेना व पुलिस ही करती थी लेकिन नये संचार नियमों के अंतर्गत अब आम व्यक्ति भी सेटेलाइट फोन का इस्तेमाल कर सकते हैं। सेटेलाइट, छोटे-छोटे नेटवर्क बना कर सेटेलाइट फोन को सेवा प्रदान करता है। सीधे उपग्रह से जुड़े होने के कारण सेटेलाइट फोन की भौगोलिक स्थिति का पता लगाना काफी मुश्किल काम है। यही कारण है कि आतंकवादी आजकल उपग्रह-फोन का इस्तेमाल करने लगे हैं। सन् 2008 के अंत में मुंबई पर हुए आतंकी हमले में आतंकवादियों ने परस्पर संपर्क में रहने के लिए सेटेलाइट फोनों का ही इस्तेमाल किया था। आजकल ऐसी तकनीक के विकास के लिए प्रयास किए जा रहे हैं, जिसकी सहायता से उपग्रह-फोन को भी सर्विलांस के दायरे में लाया जा सके।

भारत की प्रमुख मोबाइल सेवा प्रदाता कम्पनी 'एयरटेल' ने एक अत्याधुनिक तकनीक का इस्तेमाल शुरू किया है जिसकी सहायता से गुम हो जाने पर भी ग्राहकों के हैंडसेट्स को आसानी से खोजा जा सकेगा। इसके लिए 'एयरटेल' ने 'माइक्रो टेक्नोलॉजी' से एक समझौता किया है। इस नई तकनीक का नाम *'लॉस्ट मोबाइल ट्रैकिंग सिस्टम'* (एल.एम.टी.एस.) है। यह तकनीक केवल जी. एस.एम. मोबाइल फोनों में ही कार्य करेगी। यदि किसी उपभोक्ता का मोबाइल फोन गुम हो जाता है तो उसे पाने वाला व्यक्ति जैसे ही मूल सिम कार्ड को निकाल कर फोन में नया सिम कार्ड डालेगा, वैसे ही उसमें लगा सॉफ्टवेयर, उपभोक्ता के ई-मेल पर संदेश भेजकर उस नये मोबाइल नंबर की जानकारी दे देगा। इसके अलावा मोबाइल फोन की स्थिति (लोकेशन) की जानकारी भी उपभोक्ता को उसके ई-मेल पर भेज दी जाएगी। इस तरह खो गए अथवा चोरी हो गए मोबाइल फोन का पता आसानी से लगाया जा सकता है।

मोबाइलट्रैकिंगउपकरण: हाल ही में भारतीय प्रौद्योगिकी संस्थान (कानपुर) ने एक नई तकनीक का विकास किया है जिस कारण मोबाइल सर्विलांस और भी अधिक प्रभावी हो गई है। अभी तक सर्विलांस पर रखे मोबाइल फोन की स्थिति की जानकारी तो मिलती थी लेकिन मात्र इतना ही

पता चल पाता था कि मोबाइल फोन किस बी.टी.एस. टॉवर के क्षेत्र में है। एक टॉवर लगभग 2-3 किलोमीटर क्षेत्रफल के मोबाइल धारकों को सेवा प्रदान करता है इसलिए इतने बड़े क्षेत्र में छिपे किसी अपराधी को पकड़ना काफी मुश्किल काम होता था। भारतीय प्रौद्योगिकी संस्थान (कानपुर) द्वारा विकसित 'मोबाइल ट्रैकिंग उपकरण' की सहायता से टॉवर के स्थान पर मोबाइल फोन की स्थायी स्थिति (लोकेशन) का पता चल सकेगा।

इस प्रकार मोबाइल ट्रैकिंग उपकरण, सर्विलांस का एक नया हथियार बनेगा और इसके कारण सर्विलांस को एक नई धार मिल जाएगी। इस उपकरण की सहायता से गुप्तचर एजेंसियां, शहर के किसी भी कोने में छिपे बैठे अपराधी तक भी पहुंच सकेंगी। यदि मोबाइल फोन बंद होगा तो यह उपकरण काम नहीं करेगा। इस उपकरण/तकनीक का विकास, भारतीय प्रौद्योगिकी संस्थान, कानपुर के विद्युत अभियंत्रण एवं संचार विभाग ने किया है और अब इस आधुनिक तकनीक को इंटेलीजेंस ब्यूरो, नारकोटिक्स कन्ट्रोल ब्यूरो, रॉ और केन्द्रीय अन्वेषण ब्यूरो जैसी एजेंसियों को उपलब्ध कराए जाने की तैयारी चल रही है। इस तकनीक के विकास के लिए केन्द्रीय गृह मंत्रालय ने अथक प्रयास किए थे ताकि आतंकवादियों और अपराधियों पर प्रभावी शिकंजा कसा जा सके।

यहां यह बताना प्रासंगिक रहेगा कि चीन निर्मित मोबाइल फोनों ने भारत की सुरक्षा एजेंसियों के लिए एक नई मुसीबत पैदा कर दी है। अक्सर जब कोई मोबाइल फोन चोरी हो जाता है अथवा किसी अपराधी की स्थिति (लोकेशन) का पता लगाना हो तो पुलिस, *'इंटरनेशनल मोबाइल इक्यूपमेंट आइडेंटिटी'* (आई.एम.ई.आई.) नंबर की सहायता लेती है। चीन निर्मित मोबाइल फोनों के सॉफ्टवेयर भारत में उपलब्ध नहीं होने के कारण पुलिस के लिए चीनी मोबाइलों की सर्विलांस काफी कठिन हो जाती है। आमतौर पर होता यह है कि जब किसी मोबाइल फोन का पता लगाना हो अथवा मोबाइल फोन की स्थिति की जानकारी प्राप्त करनी हो तो पुलिस, *'आई.एम.ई.आई.'* नंबर की तकनीक का इस्तेमाल करती है। पुलिस, मोबाइल कम्पनी के सॉफ्टवेयर से आसानी से यह पता लगा लेती है कि संबंधित मोबाइल फोन में कौन-सा नंबर चल रहा है। मोबाइल नंबर का पता चल जाने पर पुलिस संबंधित सेवा प्रदाता कम्पनी की सहायता लेती है और मोबाइल धारक के पते के साथ-साथ यह भी जानकारी

प्राप्त कर लेती है कि संबंधित मोबाइल फोन किस क्षेत्र में काम कर रहा है।

चीनी मोबाइलों को खोजना, पुलिस के लिए काफी मुश्किल काम है, क्योंकि पुलिस के पास न तो चीनी मोबाइल निर्माता कम्पनियों की जानकारी है और न ही उसे यह पता है कि बाजार में चीनी मोबाइल फोनों की कौन-कौन सी कम्पनियां और मॉडल उपलब्ध हैं। इसके अलावा पुलिस के पास चीन निर्मित फोनों का सॉफ्टवेयर भी नहीं है जिसकी सहायता से *'आई.एम.ई.आई.'* नंबर के जरिए फोन पर चल रहे नये नंबर की जानकारी प्राप्त होती है। इससे भी खतरनाक तथ्य यह है कि चीनी मोबाइलों का *'आई.एम.ई.आई.'* नंबर भारत की अन्य कम्पनियों की अपेक्षा अलग प्रकार का होता है। चीन निर्मित मोबाइल फोनों में *'आई.एम.ई.आई.'* नंबर मात्र 11 अंकों का होता है जबकि अंतर्राष्ट्रीय स्तर पर (भारत सहित) यह नंबर 18 अंकों का होता है। भारतीय 'आई.एम.ई.आई.' नंबर विशुद्ध रूप से गणितीय अंकों का होता है (जैसे) : 157988997117989920) जबकि चीन निर्मित मोबाइलों में यह नंबर, अंकों व अक्षरों का मिश्रित रूप (जैसे : 12PQ8AC7117) होता है, जिस कारण उन्हें पहचान पाना लगभग असंभव होता है। इस समस्या के निदान के लिए 6 जनवरी, 2009 से भारत में ऐसे सभी मोबाइल फोनों पर मोबाइल सेवा बंद कर दी गई है, जिन मोबाइल फोनों में आदर्श 'आई.एम.ई.आई.' नंबर नहीं था।

फोन टैपिंग

टेलीफोन टैपिंग, सर्विलांस का ही एक रूप है। इसके अंतर्गत किसी टेलीफोन विशेष से होने वाली सारी बातचीत को सीधे सुना जा सकता है। टेलीफोन टैपिंग को संयुक्त राज्य अमेरिका में *वायर-टैपिंग* भी कहा जाता है और इसका अर्थ होता है, टेलीफोन या इंटरनेट का परीवीक्षण, किसी तीसरे व्यक्ति द्वारा करना। फोन-टैपिंग को यह नाम इसलिए मिला क्योंकि प्रारंभ में जब टेलीफोन टैपिंग प्रारंभ हुई थी तो एक छोटा सा उपकरण उस टेलीफोन के तार में लगाया जाता था, जिस टेलीफोन को टैप किया जाना होता था। इस उपकरण की सहायता से ध्वनि के कुछ संकेत, टैपिंग मशीन तक पहुंच जाते थे जिस कारण उस टेलीफोन से होने वाली बातचीत को सुनना संभव हो पाता था। फोन टैपिंग जब विधिक रूप से होती है और इसे सरकारी प्राधिकरण से

मान्यता प्राप्त होती है तो फोन टैपिंग को 'विधिक इंटरसेप्शन' कहा जाता है।

संयुक्त राज्य अमेरिका में वायर-टैपिंग दो प्रकार की होती है अक्रिय और सक्रिय वायर टैपिंग। अक्रिय वायर टैपिंग में टेलीफोन द्वारा की गई बातचीत की सूचना को प्राप्त किया जाता है जबकि सक्रिय वायर टैपिंग में की जा रही बातचीत को सीधे सुना जा सकता है। टेलीफोन टैपिंग को सभी देशों में समान रूप से विधिक मान्यता नहीं मिली है। कुछ देशों में व्यक्ति की निजता का ध्यान रखते हुए टेलीफोन टैपिंग को पूरी तरह से प्रतिबंधित किया गया है तो कुछ देशों में सुरक्षा एजेंसियों को कुछ छूट देते हुए इसे प्रतिबंधित किया गया है। अधिकतर विकसित प्रजातांत्रिक व्यवस्थाओं में टेलीफोन टैपिंग को अच्छी चीज नहीं माना जाता है। सैद्धांतिक रूप से टेलीफोन टैपिंग की अनुमति किसी सक्षम न्यायालय द्वारा ही दी जाती है। कुछ मामलों में टेलीफोन टैपिंग की अनुमति बिना किसी अधिक लिखित कार्रवाई के मिल जाती है। अवैध और अनाधिकृत फोन टैपिंग को आपराधिक कृत्य माना जाता है। जर्मनी जैसे कुछ देश ऐसे भी हैं जहां अनाधिकृत रूप से की गई फोन टैपिंग को भी न्यायालय, सबूत के रूप में स्वीकार कर लेता है।

संयुक्त राज्य अमेरिका के संघीय कानून और कुछ राज्यों के कानूनों में फोन टैपिंग को तब तक अवैध नहीं माना जाता है जब तक टैपिंग द्वारा सुनी जा रही बातचीत करने वाले दो व्यक्तियों में से कम से कम एक को पता हो कि उसका फोन टैप हो रहा है। हमारे देश में टेलीफोन टैपिंग के लिए सक्षम प्राधिकारी से पूर्वानुमति लेनी आवश्यक है, अन्यथा टेलीफोन टैपिंग को अवैध, अनाधिकृत और आपराधिक कृत्य माना जाता है। अधिकतर देशों में किसी टेलीफोन सेवा प्रदाता कम्पनी को दूरसंचार सेवाएं उपलब्ध कराने का लायसेंस इसी शर्त पर दिया जाता है कि वे टेलीफोन टैप करने की सुविधा, पुलिस व सुरक्षा एजेंसियों को उपलब्ध कराएंगी।

कुछ समय पहले तक जब अधिकतर टेलीफोन एक्सचेंज, यांत्रिक हुआ करते थे, उस समय किसी टेलीफोन को टैप करने के लिए एक छोटा सा टेप, टेलीफोन के तारों से जोड़ दिया जाता था ताकि तार में जा रहे ध्वनि संकेतों का कुछ हिस्सा, टेप के जरिए टैपिंग मशीन तक पहुंच जाए और उस टेलीफोन से हो रही बातचीत को सुना जा सके। टेलीफोन एक्सचेंजों के कंप्यूटरीकरण

और डिजिटलीकरण के बाद टेलीफोन टैपिंग की प्रक्रिया काफी सरल और सुविधाजनक हो गई है। यह अब इतनी सुविधाजनक हो गई है कि अब दूर स्थान से कंप्यूटर के जरिए भी टेलीफोन टैपिंग की जा सकती है। स्थिर टेलीफोन और मोबाइल टेलीफोन के साथ-साथ टेलीविजन केबल द्वारा दूरभाष सेवाएं उपलब्ध कराने वाली कम्पनियां भी अत्याधुनिक स्विचिंग टेक्नोलॉजी का प्रयोग कर रही हैं। जब टेप को डिजिटल स्विच के साथ जोड़ा जाता है तो स्विचिंग कंप्यूटर उन डिजिट्स की नकल कर लेता है जो टेलीफोन पर की जा रही बातचीत का प्रतिनिधित्व करती हैं। स्विचिंग कंप्यूटर नकल की गई डिजिट्स को एक दूसरी लाइन पर डाल देता है जहां से टेलीफोन पर होने वाली बातचीत को सुना जा सकता है। इस तकनीक में टेलीफोन पर बात कर रहे व्यक्तियों को पता तक नहीं चल पाता कि उनका टेलीफोन टैप किया जा रहा है। इस तकनीक का प्रयोग इतनी सफाई से किया जाता है कि काफी प्रयास करने पर भी यह पता लगाना लगभग असंभव है कि क्या टेलीफोन टैप किया जा रहा है। टेलीफोन सेवा प्रदान कम्पनी के बिलिंग विभाग से यह जानकारी भी आसानी से प्राप्त की जा सकती है कि संबंधित फोन से किस नंबर पर कॉल की गईं, किस नंबर से उस पर कॉल आई और प्रत्येक कॉल कुल कितने समय (अवधि) तक चली। ये सभी जानकारियां, *'पेन रजिस्टर'* नामक एक छोटे से यंत्र की सहायता से भी प्राप्त की जा सकती हैं।

कुछ लोग अनाधिकृत रूप से भी किसी व्यक्ति के फोन को टैप करके उससे की जा रही बातचीत को सुन लेते हैं। यह एक आपराधिक कृत्य है। किसी व्यक्ति के फोन की निगरानी करने के लिए आजकल बहुत से उपकरण बाजार में उपलब्ध हैं। बाजार में *'कॉइल टेप'* और *'इन-लाइन-टेप'* जैसे उपकरण उपलब्ध हैं जिन्हें टैप किए जाने वाले टेलीफोन के रिसीवर में लगा कर उस टेलीफोन से होने वाली सारी बातचीत को सुना जा सकता है। आजकल इन उपकरणों का एक अच्छा विकल्प भी 'रिकॉडिंग सॉफ्टवेयर' के रूप में उपलब्ध है जिसे कंप्यूटर में लगाकर बातचीत को सीधे सुना जा सकता है अथवा उसे रिकॉर्ड किया जा सकता है। किसी व्यक्ति के टेलीफोन को अनाधिकृत रूप से टैप करने के लिए बटसेट, बीज बॉक्स अथवा इंटक्शन-कॉइल का प्रयोग भी किया जा सकता है।

वेबटैपिंग: सूचना तकनीक के इस युग में वेब टैपिंग के रूप में एक नया हथियार, सुरक्षा एजेंसियों को मिल गया है। इस तकनीक के जरिए इंटरनेट प्रयोगकर्ता के 'आई.पी. पते' *(इंटरनेशनल प्रोटोकाल एड्रेस)* तक पहुंच बना ली जाती है। वेब टैपिंग के जरिए ऐसी वेबसाइटों पर नजर रखी जाती है जो संवेदनशील और खतरनाक सामग्री युक्त होती हैं और इंटरनेट प्रयोगकर्ता जिन तक पहुंचते हैं।

आजकल आतंकवादी संगठन अपने सदस्यों से बात करने के लिए इंटरनेट का इस्तेमाल अधिक करते हैं। कुख्यात आतंकवादी सरगना ओसामा-बिन-लादेन अपने सदस्यों को सभी आवश्यक दिशा-निर्देश ई-मेल के जरिए ही देता है। सिविल इंजीनियरिंग की पढ़ाई कर चुके ओसामा-बिन-लादेन को इंटरनेट के प्रयोग में महारत हासिल है। किसी ज्वलंत मद्दे पर वह अपने वीडियो टेप भी जारी करता रहता है ताकि लोगों को पता लग सके कि वह जिंदा है और आतंकी कार्रवाइयों में व्यस्त है। वेब टैपिंग, सुरक्षा एजेंसियों के लिए वरदान की तरह है। सुरक्षा एजेंसियां, संदिग्ध आतंकवादियों के ई-मेल टैप करती हैं ताकि उनके द्वारा बनाई जा रही किसी आतंकी योजना का पता समय रहते चल सके और उस आतंकी कार्रवाई को क्रियान्वित होने से पहले ही रोका जा सके।

आतंकवादी किस प्रकार सूचना प्रौद्योगिकी का इस्तेमाल करने लगे हैं इसका पता इसी बात से लग सकता है कि सन् 2004 में पाया गया कि ग्रीस के प्रधानमंत्री और उच्चाधिकारियों समेत सरकार के लगभग 100 मंत्रियों व प्रशासनिक अधिकारियों के टेलीफोन पिछले लगभग एक वर्ष से भी अधिक समय से टैप किए जा रहे थे। सरकार ने अपनी जांच में पाया कि एक विदेशी खुफिया एजेंसी द्वारा यह टैपिंग की जा रही थी ताकि सन् 2004 के ग्रीस ओलंपिक खेलों के दौरान बड़ी आतंकी कार्रवाइयों को अंजाम दिया जा सके। इस कांड में ग्रीक के वोडाफोन मोबाइल नेटवर्क को ही हैक कर लिया गया था ताकि किसी भी मोबाइल नंबर की निगरानी व टैपिंग की जा सके। सर्विलांस/टैपिंग के द्वारा सुरक्षा एजेंसियों ने पता लगा लिया कि आतंकवादी क्या करने जा रहे हैं, इस प्रकार एक बड़ी आतंकी कार्रवाई को घटित होने से पहले ही रोक दिया गया।

वेब टैपिंग जैसा ही एक और शब्द *'कंप्यूटर सर्विलांस'* आजकल प्रचलन

में है जिसका अर्थ है कंप्यूटर प्रयोगकर्ता को पता चले बिना उसकी कंप्यूटर संबंधी गतिविधियों पर निगरानी रखना। इस प्रकार वेब टैपिंग, कंप्यूटर सर्विलांस का ही एक अवयव है। कंप्यूटर-सर्विलांस बेहद सरल होती है और इसमें प्रयोगकर्ता को पता ही नहीं चलता कि उसका कंप्यूटर निगरानी पर है। अधिकतर कंप्यूटर, किसी न किसी नेटवर्क का हिस्सा होते हैं जिस कारण उनमें रखे गए डाटा तक पहुंचना काफी आसान हो जाता है। इंटरनेट पर बहुत से ऐसे सॉफ्टवेयर उपलब्ध हैं जिनका प्रयोग कंप्यूटर-सर्विलांस उपकरण के रूप में किया जा सकता है।

यदि किसी कंप्यूटर में सर्विलांस सॉफ्टवेयर (प्रोग्राम) डाल दिया गया हो तो वह सॉफ्टवेयर, किसी संदिग्ध डाटा की खोज कर सकता है, कंप्यूटर के प्रयोग पर निगरानी रख सकता है, पासवर्ड एकत्र कर सकता है और संबंधित सारी रिपोर्टें, इंटरनेट के माध्यम से सर्विलांस-ऑपरेटर को भेज सकता है। सबसे ज्यादा इस्तेमाल में लाया जाने वाला 'स्पाईवेयर' नामक सॉफ्टवेयर, आमतौर पर बाजार के व्यावसायिक डाटा तक पहुंचने के लिए प्रयोग में लाया जाता है लेकिन इससे डाटा को चुराया भी जा सकता है और उसमें संपादन (बदलाव) भी किया जा सकता है। सॉफ्टवेयर के अतिरिक्त हार्डवेयर सर्विलांस उपकरण भी अब उपलब्ध हैं। ऐसा ही एक उपकरण (बग), की-पैड में लगाया जाता है जिसे *'की-स्ट्रोक लॉगर'* कहते हैं। इसके अलावा और भी कई ऐसे उपकरण उपलब्ध हैं, जिन्हें कंप्यूटर तंत्र के किसी भाग में लगाकर उस कंप्यूटर की निगरानी की जा सकती है। इस प्रकार के हार्डवेयर निगरानी उपकरणों की सबसे बड़ी कमी यही है कि इनका इस्तेमाल करने के लिए कंप्यूटर तक भौतिक रूप से पहुंचना पड़ता है और फिर कंप्यूटर तंत्र में उस उपकरण को लगाना पड़ता है।

विज्ञान ने सुरक्षा एजेंसियों को कुछ ऐसे संवेदनशील निगरानी यंत्र भी उपलब्ध करा दिए हैं जिन्हें कंप्यूटर में लगाने की भी जरूरत नहीं पड़ती है। ये यंत्र, सी.आर.टी. मॉनीटर से निकलने वाली किरणों का पीछा करके कंप्यूटर तंत्र तक पहुंच कर उसकी निगरानी करते हैं। आजकल *'ट्रैकिंग सॉफ्टवेयर'* भी उपलब्ध है जो कंप्यूटर पर की जाने वाली गतिविधियों को नोट करते रहते हैं। इस प्रकार 'ट्रैकिंग सॉफ्टवेयर' के आधार पर पता चल जाता है कि कंप्यूटर प्रयोगकर्ता चैट, ई-मेल आदि कर रहा है अथवा अपने की-पैड के कौन-कौन से बटन दबा रहा है। इसके अतिरिक्त इस बात का पता भी सरलतापूर्वक चल

जाता है कि कंप्यूटर प्रयोगकर्ता ने कौन-कौन सी वेबसाइटों को देखा। 'ट्रैकिंग सॉफ्टवेयर' का प्रयोग अग्रलिखित समूहों द्वारा किया जाता है :

- ☆ बच्चे के माता-पिता/अभिभावक
- ☆ नियोक्ता
- ☆ सरकारी विभाग
- ☆ अवैध प्रयोगकर्ता

आधुनिक युग में बच्चे और किशोर, वेबसाइटों तक पहुंचने का कार्य अधिक करते हैं। कुछ वेबसाइटें अश्लील और आतंकवाद फैलाने वाली होती हैं, इसलिए बच्चे/किशोर के अभिभावक उसकी वेब-गतिविधियों पर नजर रखने के लिए 'ट्रैकिंग सॉफ्टवेयर' का प्रयोग करते हैं। इसी प्रकार निजी क्षेत्र के अधिकतर नियोक्ता भी अपने कर्मचारियों की वेब-गतिविधियों पर नजर रखने के लिए इस सॉफ्टवेयर/प्रोग्राम का प्रयोग करते हैं। सरकारी विभाग यह देखने के लिए इस सॉफ्टवेयर का प्रयोग करते हैं कि कहीं उसके कर्मचारी, सरकारी कंप्यूटरों का दुरुपयोग तो नहीं कर रहे हैं। विभिन्न सरकारी एजेंसियां, आपराधिक मामलों की जांच में भी इस सॉफ्टवेयर का प्रयोग करती हैं। इसके अलावा कंप्यूटर आधारित अपराधों की रोकथाम में भी 'ट्रैकिंग सॉफ्टवेयर' का प्रयोग किया जाता है।

इस सॉफ्टवेयर का प्रयोग सदैव विवादों में रहा है। हालांकि इस सॉफ्टवेयर को बेचने वाली कम्पनियां यही दावा करती हैं कि इसका प्रयोग अभिभावकों और पुलिस द्वारा किया जाता है लेकिन व्यवहार में देखा गया है कि इस सॉफ्टवेयर का इस्तेमाल कुछ ऐसी गतिविधियों में भी किया जाता है जिनके कारण सामाजिक व पारिवारिक स्तर पर कई समस्याएं पैदा हो जाती हैं। आजकल 'ट्रैकिंग सॉफ्टवेयर' का इस्तेमाल जीवनसाथी की संदिग्ध गतिविधियों पर नजर रखने के लिए भी किया जा रहा है। इसके अलावा इस सॉफ्टवेयर के कारण व्यक्ति की निजता को भी खतरा पैदा हो जाता है। यदि ट्रैकिंग सॉफ्टवेयर में *'की लॉगिंग'* की सुविधा भी हो तो इसका इस्तेमाल अनाधिकृत रूप से किसी व्यक्ति के कंप्यूटर तंत्र तक पहुंचने के लिए भी किया जा सकता है। ऐसी कम्पनियों की कमी नहीं है जो एक ओर तो ट्रैकिंग सॉफ्टवेयर की बिक्री को प्रोत्साहित करती हैं तो दूसरी ओर वे इस प्रकार के ट्रैकिंग सॉफ्टवेयरो को खोज कर अक्रिय कर देने वाले सॉफ्टवेयर भी बेचती हैं।

अपराधों की रोकथाम के लिए सुरक्षा एजेंसियों द्वारा *'स्पाईवेयर'* नामक सॉफ्टवेयर का इस्तेमाल काफी अधिक किया जाता है। *'स्पाईवेयर'* एक ऐसा कंप्यूटर सॉफ्टवेयर है जिसे किसी कंप्यूटर में लोड करके उस कंप्यूटर का प्रयोग करने वाले व्यक्ति की कंप्यूटर संबंधी सभी गतिविधियों की निगरानी की जा सकती है और प्रयोगकर्ता को पता भी नहीं चल पाता कि कोई उसकी निगरानी कर रहा है। इस सॉफ्टवेयर के नाम से ही स्पष्ट है कि यह सॉफ्टवेयर छिप कर कार्य करता है और प्रयोगकर्ता को इसकी उपस्थिति का पता नहीं चल पाता है। *'स्पाईवेयर'* द्वारा निम्नलिखित प्रकार से निगरानी की जा सकती है :

1. कंप्यूटर प्रयोगकर्ता के व्यवहार पर नजर
2. कंप्यूटर पर आंशिक नियंत्रण
3. व्यक्तिगत जानकारी में सेंध
4. प्रयोगकर्ता के इंटरनेट सर्फिंग व्यवहार पर नजर
5. देखी गई वेबसाइटों का लेखा-जोखा
6. अतिरिक्त सॉफ्टवेयर जोड़ना
7. भेजे जाने वाले डाटा को पुनः निर्देशित करना
8. कंप्यूटर प्रारूप में परिवर्तन

स्पाईवेयर शब्द का सर्वप्रथम प्रयोग 16 अक्तूबर, 1995 को किया गया था। स्पाईवेयर सॉफ्टवेयर को इंटरनेट की सहायता से भी लोड किया जा सकता है इसलिए इसका इस्तेमाल काफी अधिक होता है। अपराधों की रोकथाम में 'कवर्ट लिसनिंग उपकरण' का भी काफी अधिक प्रयोग किया जाता है। इसे आम बोलचाल की भाषा में 'बग' कहते हैं तथा इसके इस्तेमाल को 'बगिंग' कहा जाता है। इसमें एक छोटा सा रेडियो ट्रांसमीटर और माइक्रोफोन होता है। इसके द्वारा कार्डलैस फोन से होने वाली बातचीत को भी सुना जा सकता है। इसके अतिरिक्त इसकी सहायता से वायरलैस कंप्यूटर नेटवर्क से डाटा भी प्राप्त किया जा सकता है।

वीडियो सर्विलांस

वीडियो सर्विलांस का अर्थ है किसी स्थान विशेष की चलते-फिरते चित्रों द्वारा निगरानी करना। प्रारंभ में वीडियो सर्विलांस के अंतर्गत एक वीडियो कैमरे व वी.सी.पी./वी.सी.आर. का इस्तेमाल किया जाता था लेकिन आजकल इसके

कई रूप अस्तित्व में आ चुके हैं। आधुनिक युग में एक डिजिटल वीडियो कैमरे को इंटरनेट से जोड़ दिया जाता है और इस प्रकार दुनिया के किसी भी हिस्से में रहकर इंटरनेट के द्वारा किसी स्थान विशेष की निगरानी की जा सकती है। वीडियो सर्विलांस का उपयोग, आतंकी कार्रवाइयों की रोकथाम में प्रमुखता से होता है। वीडियो सर्विलांस का उपयोग, अपराध व अपराधी की पहचान के साथ-साथ अपराधों की रोकथाम में भी किया जाता है।

अक्सर ऐसे मामले प्रकाश में आते रहते हैं जिनमें कोई व्यक्ति किसी अन्य व्यक्ति का क्रेडिट/डेबिट कार्ड चुरा कर, ए.टी.एम. *(आटोमैटिक ट्रेलर मशीन)* द्वारा धन निकासी कर लेता है। प्रत्येक ए.टी.एम. कक्ष, वीडियो सर्विलांस पर रहता है इसलिए ऐसे मामलों में जांच एजेंसी सबसे पहले संबंधित बैंक से यह पता करती है कि बैंक के किस ए.टी.एम. से धन की निकासी की गई है और उसके बाद जांच एजेंसी, संबंधित ए.टी.एम. के क्लोज सर्किट टेलीविजन की वीडियो फुटेज को देख कर अपराधी की पहचान स्थापित करती है। इसी प्रकार शॉपिंग मॉल्स और गहनों आदि की दुकानों से होने वाली चोरियों का पता भी वीडियो सर्विलांस के द्वारा आसानी से लगा लिया जाता है। ये वीडियो सर्विलांस द्वारा अपराध और अपराधी की पहचान के उदाहरण हैं।

विभिन्न धार्मिक व सार्वजनिक स्थलों पर आतंकी कार्रवाइयों का खतरा सदैव बना रहता है इसलिए ऐसे स्थानों को आजकल वीडियो सर्विलांस के अंतर्गत ला दिया गया है। वीडियो सर्विलांस के अंतर्गत विभिन्न ऐतिहासिक, धार्मिक और राजनैतिक महत्त्व के स्थलों पर क्लोज सर्किज टेलीविजन कैमरे लगा दिए जाते हैं, जिनको नियंत्रण कक्ष से जोड़ दिया जाता है। इस प्रकार नियंत्रण कक्ष में बैठे पुलिसकर्मी, टेलीविजन पर देखकर ही काफी बड़े क्षेत्र पर नजर रख सकते हैं। ऐसा करने पर उस क्षेत्र विशेष में आने वाले प्रत्येक व्यक्ति की प्रत्येक गतिविधि पर नजर रखना संभव हो गया है। इस प्रकार वीडियो सर्विलांस के अंतर्गत निगरानी में रहने वाले स्थलों पर आपराधिक व्यक्ति कोई अपराध कारित करने की हिम्मत नहीं कर पाते हैं और यदि वे ऐसा करने का प्रयास भी करते हैं तो तुरंत सुरक्षाकर्मियों को पता चल जाता है और अपराध घटित होने से पहले ही उसे रोक लिया जाता है। वैसे आजकल वीडियो सर्विलांस का प्रयोग उद्योगों और कम्पनियों में उत्पादकता बढ़ाने के लिए भी किया जा रहा है।

हाल ही में भारतीय प्रौद्योगिकी संस्थान, कानपुर ने स्वचालित वीडियो निगरानी प्रणाली का विकास किया है। इस स्वचालित प्रणाली के जरिए संदिग्ध आतंकवादियों को पकड़ने में सहायता मिलेगी। इस प्रणाली को मुंबई के भाभा परमाणु अनुसंधान केन्द्र में लगाया जा रहा है और जल्द ही इसे अन्य संवेदनशील धार्मिक स्थलों पर भी लगा दिया जाएगा। इस स्वचालित वीडियो निगरानी प्रणाली का विकास भारतीय प्रौद्योगिकी संस्थान (कानपुर) के वैद्युत अभियंत्रण विभाग ने किया है। इस प्रणाली के विकास का प्रारंभ जून, 2004 में किया गया था और 4 वर्षों के गहन शोध के बाद जून, 2008 में इस प्रणाली को विकसित कर लिया गया। इस प्रणाली के विकास पर लगभग 25 लाख रुपये खर्च किए गए हैं। इस प्रणाली के सफल परीक्षण के बाद अब इसे 20 वर्ग किलोमीटर क्षेत्र में फैले भाभा परमाणु अनुसंधान केन्द्र (मुंबई) में लगाया जा रहा है। स्वचालित वीडियो निगरानी प्रणाली की मदद से, इस केन्द्र में प्रवेश करने वाले प्रत्येक व्यक्ति की एक-एक गतिविधि पर नजर रखी जाएगी और यदि कोई व्यक्ति हथियार या विस्फोटक सामग्री लेकर परिसर में प्रवेश करने का प्रयास करेगा तो उसे तुरंत दबोच लिया जाएगा। इस स्वचालित वीडियो निगरानी प्रणाली को जल्द ही केन्द्रीय गृह मंत्रालय को सौंपने की तैयारी की जा रही है ताकि अन्य संवेदनशील स्थलों पर भी इस प्रणाली को स्थापित किया जा सके।

न्यायालयों में न्यायाधीश के सम्मुख पेशी के लिए विभिन्न अपराधियों को लाया जाता है। अक्सर देखा गया है कि अपराधी के विरोधी लोग, न्यायालय में ही उस पर हमला कर देते हैं। इसके अलावा न्यायालय परिसर से अपराधियों को पुलिस के कब्जे से छुड़वाने के प्रयास भी यदा-कदा किए जाते रहते हैं। इस प्रकार के अपराधों को रोकने के लिए प्रमुख न्यायालयों को वीडियो सर्विलांस के अंतर्गत लाने की योजना है। दिल्ली स्थित कड़कड़डूमा न्यायालय के हर हिस्से में क्लोज-सर्किट टेलीविजन कैमरे लगाए जा रहे हैं। समूचे न्यायालय में कुल 50 क्लोज-सर्किट टेलीविजन लगाए जा रहे हैं ताकि न्यायालय परिसर के चप्पे-चप्पे पर नजर रखी जा सके। ये सभी कैमरे मॉनीटर-कक्ष में लगे मॉनीटर से जुड़े होंगे ताकि वहां बैठकर परिसर में चल रही किसी भी संदिग्ध गतिविधि का पता लगाया जा सके। इससे पहले दिल्ली के ही रोहिणी न्यायालय में जगह-जगह सी.सी.टी.वी. कैमरे लगा दिए हैं। हाल ही

में इन कैमरों की मदद से पुलिस ने न्यायालय परिसर से स्कूटर-मोटर साइकिल चुराने वाले एक गिरोह की पहचान कर ली क्योंकि एक मोटर साइकिल को चुराने और उसे न्यायालय परिसर से बाहर ले जाने की पूरी प्रक्रिया, वहां लगे क्लोज-सर्किट कैमरों में दर्ज हो गई थी।

आवास-निगरानी प्रणाली

एक समय था जब रात को घरों समय की रखवाली का काम चौकीदार किया करते थे। उस समय दिन में महिलाएं घर पर रहती थीं और रात के समय जब सब सो जाते थे तो घर की रखवाली चौकीदार किया करते थे। आधुनिक युग में लोगों की जीवनशैली बदल गई है। एकल-परिवार के इस युग में महिलाएं भी घर से बाहर निकल कर नौकरी करती हैं, व्यवसाय संभालती हैं अथवा कोई अन्य कार्य करती हैं जिस कारण दिन में घर खाली रहते हैं। चोरों से घरों को बचाने के लिए विज्ञान और प्रौद्योगिकी ने 'आवास निगरानी प्रणाली' का विकास कर लिया है।

प्रौद्योगिकी के इस युग में घरों की देखभाल की जिम्मेदारी अब इलैक्ट्रॉनिक सुरक्षा प्रणाली के जिम्मे छोड़ दी गई है। इस प्रणाली के अंतर्गत आवास के प्रत्येक प्रवेश और निकास द्वारों पर वीडियो सर्विलांस उपकरण लगा दिए जाते हैं ताकि आप घर से दूर रहकर भी इंटरनेट के जरिए अपने घर की देखभाल कर सकें। इसके अलावा ऐसे उपकरण भी विकसित हो चुके हैं जिनकी सहायता से चोरों द्वारा घर के ताले को खोलने का प्रयास करने पर तुरंत पता चल जाता है। यदि कोई व्यक्ति अनाधिकृत रूप से प्रवेश-द्वार के ताले को खोलने/तोड़ने का प्रयास करता है तो स्वामी के मोबाइल फोन पर तुरंत एक *एस.एम.एस.* (मोबाइल-संदेश) भेज कर उसे सावधान कर दिया जाता है। घर की सुरक्षा के अतिरिक्त घर में रहने वाले बच्चों और बुजुर्ग लोगों की देखभाल और सुरक्षा भी इस निगरानी तंत्र द्वारा सुनिश्चित की जा सकती है। घर में अकेले रह गए नौकरों की गतिविधियों पर भी इस प्रणाली द्वारा निगरानी रखी जा सकती है।

निगरानी-तंत्र द्वारा कार को चोरी होने से भी बचाया जा सकता है। आजकल कार में कई ऐसे उपकरण लगाए जाने लगे हैं जिनकी सहायता से कार को चोरी होने से बचाया जा सकता है। जी.पी.आर.एस. युक्त कार सुरक्षा

प्रणाली में एक माइक्रोचिप का प्रयोग किया जाता है जिसे कार में कहीं छिपा कर लगा दिया जाता है। इस प्रणाली द्वारा मात्र एक *एस.एम.एस.* (मोबाइल-संदेश) द्वारा ही किसी भी समय कार की भौगोलिक स्थिति (लोकेशन) का पता लगाया जा सकता है। कार को चोरी हो जाने से बचाने और उस पर निगरानी रखने के लिए निम्नलिखित उपकरणों का इस्तेमाल किया जाता है :

- ☆ जी.पी.एस. ट्रैकिंग प्रणाली
- ☆ इग्नीशन कॉलम गार्ड
- ☆ इग्नीशन कटऑफ
- ☆ ईंधन कटऑफ
- ☆ दरवाजों में बायोमैट्रिक ताले

इलैक्ट्रॉनिक निगरानी प्रणाली के अतिरिक्त आजकल बायोमैट्रिक्स निगरानी प्रणाली का खूब इस्तेमाल किया जा रहा है। इसमें व्यक्ति के भौतिक अथवा व्यवहार के लक्षणों के आधार पर उसकी पहचान स्थापित की जाती है और फिर बायोमैट्रिक्स उपकरण यह निर्धारित करते हैं कि उस व्यक्ति को प्रवेश देना है या नहीं। इसके अंतर्गत अंगुलि चिह्नों, आंख के रेटिना व आइरिस, डी. एन.ए., चेहरे के प्रतिरूप, हाथों की बनावट और कद-काठी का प्रयोग, व्यक्ति की पहचान स्थापित करने के लिए किया जाता है। आजकल आवास, कार्यालय, कार और महत्त्वपूर्ण स्थलों की निगरानी तथा वहां आने-जाने वाले व्यक्तियों को पहचानने के लिए बायोमैट्रिक्स प्रणाली का खूब इस्तेमाल किया जा रहा है।

सारतः कहा जा सकता है कि सर्विलांस के जरिए विभिन्न प्रकार के अपराधों की रोकथाम काफी आसान है। यही कारण है कि आज अपराधों की रोकथाम के लिए सर्विलांस प्रणाली का प्रयोग ही अधिक किया जा रहा है। इसके प्रयोग से हम घर, मकान, दुकान, कार्यालय, महत्त्वपूर्ण धार्मिक व ऐतिहासिक स्थलों को अपराधियों व आतंकवादियों के हमले से बचा सकते हैं। निगरानी-तंत्र (सर्विलांस सिस्टम) की उपस्थिति के कारण अपराधों की रोकथाम तो आसान है ही साथ ही इसके कारण अपराध व अपराधी की पहचान भी की जा सकती है। सर्विलांस के महत्त्व को इसी से समझा जा सकता है कि आजकल अधिकतर अपराधी, सर्विलांस के कारण ही पकड़े जा रहे हैं।

●

10

प्रमुख अत्याधुनिक तकनीकें

टेक्नोलॉजी और प्रौद्योगिकी के इस दौर में यदि अपराधी और आतंकवादी, टेक्नोलॉजी के विभिन्न उत्पादों व उपकरणों का प्रयोग कर रहे हैं तो सुरक्षा एजेंसियां और पुलिस भी प्रौद्योगिकी के बल पर अपराधों की रोकथाम कर रही हैं। एक समय था जब विज्ञान का प्रयोग, अपराध व अपराधी की पहचान करने के लिए ही संभव था लेकिन अब विज्ञान ने हमें ऐसे उपकरण व तकनीकें उपलब्ध करा दी हैं कि अपराध को घटित होने से पहले ही रोकना संभव हो गया है। सुरक्षा एजेंसियों ने इस तथ्य को समझ लिया है कि केवल तकनीक के आधार पर ही अत्याधुनिक उपकरणों से लैस अपराधियों का मुकाबला किया जा सकता है और इसीलिए सुरक्षा एजेंसियों द्वारा प्रौद्योगिकी के इस्तेमाल को बढ़ावा दिया जा रहा है।

अपराधों की रोकथाम करने के लिए भारतीय सुरक्षा एजेंसियों द्वारा भी टेक्नोलॉजी का खूब इस्तेमाल किया जाने लगा है। हम पढ़ चुके हैं कि किस प्रकार बायोमैट्रिक विधियों द्वारा व्यक्ति की शत-प्रतिशत सही पहचान की जाती है और किस प्रकार हम विभिन्न बायोमैट्रिक उपकरणों का इस्तेमाल करके अपने घर व कार आदि की सुरक्षा कर सकते हैं। अभी तक अंगुलि चिह्नों का प्रयोग, अपराधी की पहचान करने के लिए ही किया जाता था लेकिन अब इनके आधार पर अपराधों की रोकथाम भी संभव हो गई है। आजकल ऐसे प्रवेश-द्वार *(डोर-सिस्टम)* और ताले *(लॉक-सिस्टम)* अस्तित्व में आ चुके हैं जो स्वामी (अधिकृत व्यक्ति) के अंगुलि चिह्नों को पहचानने के बाद ही सक्रिय होते हैं। बायोमैट्रिक्स आधारित इस प्रकार के तालों का उपयोग आवास और कार आदि

की सुरक्षा में काफी किया जा रहा है।

सूचना-प्रौद्योगिकी ने तो पुलिस व अन्य सुरक्षा एजेंसियों को कई ऐसी तकनीकें उपलब्ध करा दी हैं जिनके आधार पर अपराध को प्रभावी ढंग से रोका जा सकता है। इलैक्ट्रॉनिक सर्विलांस, स्वचालित वीडियो निगरानी तंत्र, जी.पी. आर. एस., नोकिया ट्रेटा प्रणाली और रेडियो फ्रीक्वेंसी हथियार, ऐसी ही कुछ विधियां हैं जिनकी सहायता से अपराध व अपराधियों पर नकेल कसना काफी सरल व सुविधाजनक हो गया है। इसके अलावा कोर-बैंकिंग साल्यूशन, डी-मैट शेयर खाते, प्लास्टिक कार्डों पर मैग्नेटिक-स्ट्रिप का इस्तेमाल, पिन (व्यक्तिगत पहचान संख्या), पासवर्ड, टिन (टेलीफोन पहचान संख्या) और वायस रिकोगनिशन प्रणाली आदि कुछ ऐसी विधियां हैं जिन्होंने विभिन्न प्रकार के बैंकिंग और वित्तीय अपराधों को रोकने में महत्त्वपूर्ण भूमिका अदा की है।

यह बात और है कि आज आतंकवादी संगठन भी आधुनिक वैज्ञानिक उपकरणों व तकनीकों का इस्तेमाल कर रहे हैं लेकिन यहां यह तथ्य उल्लेखनीय है कि विज्ञान और प्रौद्योगिकी ने हमें कई उपकरण भी उपलब्ध कराए हैं जिनके आधार पर विभिन्न आतंकी कार्रवाइयों की रोकथाम संभव हो पायी है। धातु-खोजक यंत्र, विस्फोटक खोजक यंत्र, नैनो-नोज, फेशियल रिकोगनिशन प्रणाली, बायोमैट्रिक प्रणाली और स्वचालित वीडियो निगरानी प्रणाली आदि ऐसी विधियां हैं जिनकी सहायता से आतंकी हमलों की रोकथाम संभव हो पायी है। इसी प्रकार इलैक्ट्रॉनिक सर्विलांस प्रणाली भी आज अपराधों की रोकथाम में बेहद कारगर साबित हो रही है और अधिकतर अपराधी आज इसी प्रणाली के कारण पुलिस की गिरफ्त में आ रहे हैं। इनके अलावा सरकार द्वारा और भी अनेक तकनीकों का इस्तेमाल अपराधों की रोकथाम के लिए किया जा रहा है जैसे राष्ट्रीय पहचान-पत्र परियोजना (स्मार्ट कार्ड) एवं *'सीपा' (कॉमन इंटीग्रेटेड पुलिस एप्लीकेशन्स)* आदि।

राष्ट्रीय पहचान-पत्र परियोजना

हमारे देश में पड़ोसी देशों से अवैध घुसपैठ के मामले लगातार बढ़ते जा रहे हैं। इस प्रकार अवैध रूप से भारत की सीमा में घुसपैठ करने वाले लोग, भारत में आकर आपराधिक गतिविधियों में संलग्न हो जाते हैं। स्वयं राजधानी

दिल्ली में पकड़े जाने वाले अधिकतर अपराधियों में बांग्लादेशी घुसपैठियों की संख्या काफी अधिक होती है। भारत में विदेशी घुसपैठियों को नियंत्रित करने और व्यक्ति की व्यक्तिगत पहचान स्थापित करने के लिए भारत सरकार द्वारा एक अति-महत्त्वाकांक्षी परियोजना प्रारंभ की गई है। इस परियोजना के अंतर्गत प्रत्येक भारतीय नागरिक को एक 'राष्ट्रीय पहचान-पत्र' जारी किया जाएगा। यह पहचान-पत्र, एक स्मार्ट कार्ड के रूप में होगा जिसको तैयार करने में अत्याधुनिक तकनीक का प्रयोग किया जाएगा।

हालांकि सरकार द्वारा मतदाता पहचान-पत्र, राशन कार्ड और अन्य सरकारी दस्तावेज, नागरिकों को जारी किए जाते हैं जिनके आधार पर कोई व्यक्ति अपनी पहचान स्थापित कर सकता है लेकिन आज जरूरत एक ऐसे राष्ट्रीय पहचान-पत्र की है जिसका प्रयोग विभिन्न विकास कार्यक्रमों, जनगणना, कर एकत्रीकरण और स्वास्थ्य सेवाओं के साथ-साथ पुलिस रिकॉर्ड एवं घुसपैठ रोकने के लिए भी किया जा सके। सन् 2003 में भारत सरकार ने नागरिकता अधिनियम, 1955 में संशोधन किया और नागरिकों के पंजीकरण एवं नागरिकों को एक राष्ट्रीय पहचान-पत्र जारी करने का प्रावधान इसमें जोड़ दिया। इस अधिनियम में सरकार ने एक नया अनुच्छेद 14-ए जोड़ा जिसमें कहा गया था कि सरकार प्रत्येक नागरिक का पंजीकरण करेगी और उसे एक राष्ट्रीय पहचान-पत्र जारी करेगी। इस पहचान-पत्र में प्रत्येक नागरिक की एक 'राष्ट्रीय पहचान संख्या' होगी। इन प्रस्तावित पहचान-पत्रों में किसी भी प्रकार के फर्जीवाडे को रोकने के लिए सरकार ने इन पहचान-पत्रों के निर्माण में *'एम्बेडेड डिजिटल सिग्नेचर टेक्नोलॉजी'* का प्रयोग करने का फैसला किया है। एक बार जब किसी पहचान-पत्र (स्मार्ट कार्ड) पर डिजिटल हस्ताक्षरों को उकेर दिया जाएगा तो फिर उसमें किसी प्रकार का कोई बदलाव करना संभव नहीं होगा और कोई भी व्यक्ति, फर्जी पहचान-पत्र नहीं बना सकेगा। इसी प्रकार की एक परियोजना मलेशिया सरकार द्वारा पहले से ही चलाई जा रही है और उसके काफी सकारात्मक परिणाम मिल रहे हैं।

प्रस्तावित राष्ट्रीय पहचान-पत्र को *'एम.एन.आई.सी.' (मल्टीपर्पज नेशनल आइडेंटिटी कार्ड)* नाम दिया गया है। यह राष्ट्रीय सुरक्षा की दृष्टि से बेहद महत्त्वपूर्ण है और इसकी सहायता से विभिन्न प्रकार के अपराधों की रोकथाम

भी की जा सकेगी। इस परियोजना का शुभारंभ, भारत सरकार द्वारा सन् 2002 में किया गया था। यह भारत सरकार की एक 'स्वप्निल परियोजना' है, और इसकी सहायता से विदेशी घुसपैठ, आतंकवाद और अवैध प्रवेश जैसे अपराधों की रोकथाम की जानी संभव हो सकेगी। '*एम.एन.आई.सी.* परियोजना' के निम्नलिखित उद्देश्य हैं :

(1) एक राष्ट्रीय जनसंख्या रजिस्टर बनाना ताकि वास्तविक जनसंख्या का पता चल सके।
(2) भारतीय नागरिकों की एक राष्ट्रीय पंजिका तैयार करना, ताकि विदेशी घुसपैठ को रोका जा सके।
(3) गैर-नागरिकों के लिए एक राष्ट्रीय अधिवास पंजिका तैयार करना।
(4) प्रत्येक भारतीय नागरिक को एक राष्ट्रीय पहचान-पत्र जारी करना।
(5) प्रत्येक भारतीय नागरिक को एक 'राष्ट्रीय पहचान संख्या' आवंटित करना।

बहुउद्देश्यीयराष्ट्रीयपहचान-पत्रकाप्रारूपः प्रत्येक भारतीय नागरिक को जो राष्ट्रीय पहचान-पत्र दिया जाना है, उसमें एक 'माइक्रो प्रोसेसर चिप' लगा होगा, जिसकी क्षमता 16 के.बी. मेमोरी की होगी। इस पहचान-पत्र के न तो नकली पहचान-पत्र बनाए जा सकेंगे और न ही इनका प्रतिरूप (क्लोन) बनाना संभव होगा क्योंकि इस कार्ड को बनाने में अत्याधुनिक *'की-क्रिप्टोग्राफी'* तकनीक का इस्तेमाल किया जाएगा। प्लास्टिक से निर्मित इस स्मार्ट कार्ड में धारक के निम्नलिखित विवरण दर्ज होंगे :

☆ राष्ट्रीय पहचान-पत्र संख्या (NIN)
☆ धारक का नाम व उपनाम
☆ लिंग
☆ पिता का नाम
☆ माता का नाम
☆ जन्म तिथि
☆ जन्म स्थान
☆ वैवाहिक स्थिति

- ☆ जीवन साथी (पति/पत्नी) का नाम
- ☆ निवास का वर्तमान पता
- ☆ स्थायी निवास का पता
- ☆ दिखायी देने योग्य पहचान का चिह्न
- ☆ धारक का डिजिटल चित्र
- ☆ अंगुलियों का बायोमैट्रिक विवरण
- ☆ पंजीकरण की तिथि
- ☆ जारी करने की तिथि

प्रत्येक भारतीय नागरिक को एक राष्ट्रीय पहचान-पत्र जारी करने की प्रायोगिक परियोजना, 12 राज्यों और एक केन्द्र शासित प्रदेश पांडिचेरी में चलाई जा रही है। इस परियोजना के अंतर्गत किए जाने वाले स्मार्ट कार्डों को तैयार करने के काम में कई महत्वपूर्ण एजेंसियां अपना योगदान दे रही हैं जैसे राष्ट्रीय डिजायन संस्थान, नेशनल इंफार्मेटिक्स सेंटर और भारतीय प्रौद्योगिकी संस्थान, कानपुर। अत्याधुनिक तकनीक से बना यह राष्ट्रीय पहचान-पत्र, विभिन्न अपराधों की रोकथाम में कारगर भूमिका अदा करेगा, ऐसा विश्वास है।

सीपा (कॉमन इंटीग्रेटिड पुलिस एप्लीकेशन)

विभिन्न प्रकार के अपराधों की रोकथाम करने और अपराध-पीड़ितों को त्वरित न्याय दिलाने के लिए, भारत सरकार द्वारा 'सीपा' नामक एक महत्वाकांक्षी परियोजना पर काम किया जा रहा है। इस परियोजना के अंतर्गत प्रत्येक पुलिस थाने का पूर्णतः कंप्यूटरीकरण किया जाएगा ताकि पुलिस-प्रक्रिया को तेज और सुगम बनाया जा सके। प्रत्येक पुलिस-थाने का कंप्यूटरीकरण करके उसे जिला अपराध रिकार्ड ब्यूरो से जोड़ा जाएगा। ये जिला स्तरीय ब्यूरो, आगे राज्य अपराध रिकार्ड ब्यूरो और राष्ट्रीय अपराध रिकार्ड ब्यूरो से जुड़े रहेंगे। *'सीपा'* का सॉफ्टवेयर, राष्ट्रीय सूचना केन्द्र (नेशनल इंफार्मेटिक्स सेंटर) द्वारा विकसित किया जा रहा है। 'सीपा' के अनुवीक्षण और क्रियान्वयन की जिम्मेदारी, राष्ट्रीय अपराध रिकार्ड ब्यूरो को सौंपी गई है।

'सीपा' के क्रियान्वयन पर निगरानी रखने के लिए केन्द्रीय गृह मंत्रालय

द्वारा एक 'सीपा क्रियान्वयन समिति' का गठन किया है। इस समिति के अध्यक्ष, राष्ट्रीय अपराध रिकार्ड ब्यूरो के निदेशक हैं और निम्नलिखित व्यक्ति इस महत्वपूर्ण समिति के सदस्य हैं :

(1) निदेशक, राष्ट्रीय अपराध विज्ञान एवं विधि विज्ञान संस्थान
(2) निदेशक (पुलिस आधुनिकीकरण), गृह मंत्रालय, भारत सरकार
(3) उप-महानिदेशक, राष्ट्रीय सूचना केन्द्र
(4) राज्यों के प्रतिनिधि।

समय से और प्रासंगिक डाटा/रिकार्ड मिलने से पुलिस व अन्य सुरक्षा एजेंसियों को कार्य करने में अत्याधिक सुविधा मिलती है। आज के युग में अपराधी भी टेक्नोलॉजी एवं प्रौद्योगिकी का अत्याधिक इस्तेमाल कर रहे हैं। अपराध को कारित करने में वे नई-नई तकनीकों का प्रयोग कर रहे हैं। 'सीपा' परियोजना के अंतर्गत अपराध और अपराधियों का कंप्यूटरीकृत (डिजिकृत) डाटाबेस तैयार किया जाना है। इस परियोजना के अंतर्गत प्रत्येक पुलिस थाने का कंप्यूटरीकरण किया जाना है ताकि पुलिस-कार्य को अधिक प्रभावी बनाया जा सके और उसे गति प्रदान की जा सके।

बम निरोधक तकनीक

आज आतंकवाद का दौर है। भारत सहित दुनिया के सभी प्रमुख राष्ट्र, आतंकवाद की चपेट में हैं। आतंकवादी विभिन्न प्रकार की आतंकी गतिविधियों को अंजाम देते हैं लेकिन उनमें सबसे प्रमुख है बम विस्फोट। भीड़-भाड़ वाले सार्वजनिक स्थलों पर बम विस्फोट करके आतंकवादी, एक साथ अनेक लोगों को मौत के घाट तो उतारते ही हैं, साथ ही लाखों लोगों के मन-मस्तिष्क में दहशत भी भर देते हैं। बम बनाने और फिर उसका विस्फोट करने में आजकल आतंकवादी विभिन्न अत्याधुनिक तकनीकों का इस्तेमाल करने लगे हैं। वे दिन अब अतीत के पन्नों में सिमट गए हैं जब आतंकवादी बम फोड़ते थे। अत्याधुनिक तकनीक से लैस आतंकवादी आजकल रिमोट-कंट्रोल का बटन दूर से ही दबाकर, बम का विस्फोट कर देते हैं।

प्रौद्योगिकी ने अगर आतंकवादियों को बम-विस्फोट की एक से एक नई तकनीकें उपलब्ध करायी हैं तो इस प्रौद्योगिकी ने सुरक्षा एजेंसियों को ऐसे

उपकरण भी उपलब्ध करा किए हैं जिनकी सहायता से बम की खोज कर उन्हें निष्क्रिय किया जा सकता है। धातु-खोजक (मेटल डिटेक्टर) द्वारा छिपे हुए बमों की खोज तो काफी समय से की जाती रही है लेकिन अब तो 'नैनो नोज' जैसे अत्याधुनिक विस्फोटक खोजक यंत्र भी अस्तित्व में आ गए हैं। बनारस हिन्दू विश्वविद्यालय (वाराणसी) के वैज्ञानिकों ने *'नैनो नोज'* नामक एक अत्याधिक संवेदनशील यंत्र का विकास किया है। इसकी सहायता से छिपे हुए विस्फोटक को भी खोजा जा सकता है। इस प्रकार अत्याधुनिक तकनीक का इस्तेमाल करके सुरक्षा एजेंसियां, खतरनाक आतंकी कार्रवाइयों की रोकथाम करती हैं।

आतंकवादियों द्वारा आमतौर पर दो प्रकार के बमों का इस्तेमाल किया जाता है क्रूड बम और आई.ई.डी. बम। क्रूड बम वास्तव में परंपरागत प्रकार के बम होते हैं। क्रूड बम को हम देशी बम भी कह सकते हैं क्योंकि इसके निर्माण में देशी नुस्खों का इस्तेमाल किया जाता है। जैसे खुले बाजार में मिलने वाले रसायन, कील, बैटरी, टिफिन आदि। इन देशी बमों की मारक क्षमता अपेक्षाकृत कम अवश्य होती है लेकिन इनसे निकलने वाले स्पिंटर्स से एक साथ बहुत सारे लोगों को नुकसान पहुंचाया जा सकता है। भारत में आतंकवादियों द्वारा देशी बमों का इस्तेमाल अधिक किया जाता है क्योंकि इनके निर्माण में प्रयुक्त होने वाली वस्तुएं आसानी से बाजार में उपलब्ध होती हैं। वैसे आजकल आतंकवादियों द्वारा अत्याधुनिक 'आई. ई. डी.' (इप्रोवाइज्ड एक्सप्लोसिव डिवाइस) बमों का इस्तेमाल भी किया जाने लगा है। 'आई. ई. डी.' बमों की मारक क्षमता कई किलोमीटर के क्षेत्र में हो सकती है। इन बमों में डेटोनेटर, उच्च क्षमता वाली बैटरी और आवश्यकता के अनुरूप विस्फोटक सामग्री का इस्तेमाल किया जाता है। इन बमों में टाइमर व रिमोट कंट्रोल के अतिरिक्त ध्वनि से भी विस्फोट किया जा सकता है। इन बमों में एक बैटरी की सहायता से विद्युत की आपूर्ति की जाती है और विद्युत की आपूर्ति प्रारंभ होते ही डेटोनेटर फट जाता है जिस कारण विस्फोट के साथ बम फट जाता है जो भारी तबाही का कारण बनता है। चूंकि इन बमों का विस्फोट करने के लिए भावी घटनास्थल पर रहना आवश्यक नहीं है इसलिए अपनी सुरक्षा के लिए आतंकवादी इन बमों का प्रयोग अधिक करते हैं।

'आई. ई. डी.' बमों के इस दौर में ऐसी तकनीकें भी उपलब्ध हैं जिनकी

सहायता से इन बमों को निष्क्रिय किया जा सकता है। बमों को निष्क्रिय करने के लिए सुरक्षाकर्मियों को विशेष प्रशिक्षण दिया जाता है। कुछ पश्चिमी देशों में तो बमों को निष्क्रिय करने के लिए रोबोट की सहायता भी ली जाने लगी है। इन रोबोट में कैमरे व एक्सरे मशीन लगी होती है ताकि बम के बारे में पता लगाया जा सके। हमारे देश में बम-निरोधक दस्ते के सदस्य को हाथ से बम को निष्क्रिय करना पड़ता है और इसके लिए विभिन्न प्रकार के उपकरणों व कवच को धारण करना पड़ता है। बम निष्क्रिय करने की यह विधि काफी खतरनाक हो सकती है क्योंकि बम निष्क्रिय करते समय ही फट सकता है। हाल ही में *'जियूस-हलोंस'* नामक एक नई तकनीक प्रकाश में आई है। इस तकनीक में बम के खोल में लेजर किरणों से छेद करके विस्फोटक सामग्री को नष्ट कर दिया जाता है। इस अत्याधुनिक तकनीक का इस्तेमाल, फिलहाल तो अमेरिकी सेना द्वारा ही किया जा रहा है लेकिन जल्द ही विश्व के अन्य हिस्सों में भी इस तकनीक का इस्तेमाल होने लगेगा।

आतंकवादियों द्वारा बम धमाकों में आजकल 'आर.डी.एक्स.' का इस्तेमाल भी खूब किया जाता है। आतंक का पर्याय बन चुका 'आर.डी.एक्स.' वास्तव में साइक्लो-ट्राई-मिथाईलीन-ट्राई-नाइट्रामाइन' है। यह शुद्ध सफेद रंग का एक ठोस होता है और इसकी गंध व स्वाद से इसका पता नहीं लगाया जा सकता। किसी अन्य विस्फोटक के साथ मिला कर इसका प्रयोग करने पर यह अत्यंत घातक हो सकता है। द्वितीय विश्वयुद्ध में दोनों पक्षों द्वारा 'आर.डी.एक्स.' का जमकर इस्तेमाल किया गया था। आजकल ऐसे संवेदनशील उपकरण अस्तित्व में आ चुके हैं जो छिपे हुए 'आर.डी.एक्स.' को भी खोज निकालते हैं। इस प्रकार 'आर.डी.एक्स.' के कहर से मानवता को बचाना संभव हो गया है।

सुरक्षा एजेंसियों और पुलिस में अलग से बम निरोधक दस्तों का गठन किया जाता है। जैसे ही किसी स्थान पर बम रखे होने की सूचना इस दस्ते को मिलती है, इसके विशेषज्ञ, घटनास्थल पर पहुंच कर बम को निष्क्रिय कर देते हैं। बम को निष्क्रिय करने के लिए विशेषज्ञ, कंट्रोल-प्लास या कटर का प्रयोग करते हैं। बम को निष्क्रिय करने के लिए उसकी विद्युत आपूर्ति काटना महत्वपूर्ण होता है। सबसे पहले एक्सरे मशीन द्वारा यह पता लगाया जाता है कि बम में विद्युत आपूर्ति का प्रबंध किस प्रकार किया गया है और इसके बाद धनात्मक

या ऋणात्मक तार में से किसी एक को काट दिया जाता है। एक बम को निष्क्रिय करने में 15 मिनट से लेकर एक घण्टा तक लग सकता है। तारों की सरल संरचना वाले बमों को निष्क्रिय करने में कम समय लगता है जबकि अधिक जटिल संरचना वाले बमों को निष्क्रिय करने में कुछ ज्यादा समय लगता है।

बम निष्क्रिय करने वाले दस्ते के उपयोग हेतु अत्याधुनिक उपकरणों का इस्तेमाल किया जाता है। विशेषज्ञ के परिधान व जूतों सहित अधिकतर उपकरणों का आयात, इजरायल से किया जाता है। इजरायल, सदैव से

आतंकवाद से पीड़ित रहा है इसलिए उसने आतंकी गतिविधियों की रोकथाम के लिए पुख्ता इंतजाम दिए हुए हैं। यही कारण है कि इजरायल में ऐसे उपकरणों का विकास अधिक हुआ है। बम-निरोधक दस्ते के पास *'डीप माइन मेटल डिटेक्टर'* नामक उपकरण होता है जिसकी सहायता से जमीन में गड़े विस्फोटक का भी पता लगाया जा सकता है। आशंकित स्थान से ऐसे विस्फोटक का पता लगाकर, बम निरोधक दस्ते के विशेषज्ञ उसे निष्क्रिय कर देते हैं। इसी प्रकार का एक और उपकरण, 'विस्फोटक-97' नाम से सुरक्षा एजेंसियों के पास होता है जिसकी सहायता से सुरक्षा एजेंसियां, नियमित जांच करती हैं। बम निष्क्रिय करने वाला विशेषज्ञ एक विशेष परिधान पहनता है जिसे 'बम सूट' कहा जाता है। यह परिधान, आग और बारूद से विशेषज्ञ की रक्षा करता है। इस विशेष परिधान का मूल्य लगभग 10 लाख रुपये है। बम निष्क्रिय करते समय विशेषज्ञ एक विशेष प्रकार का 'बम मास्क' भी लगाते हैं ताकि सिर व चेहरे की सुरक्षा की जा सके।

यदि समय रहते किसी बम या विस्फोटक सामग्री का पता लग जाए तो उसे आसानी से निष्क्रिय किया जा सकता है। स्पष्ट है कि तकनीक ने हमें ऐसे उपकरण उपलब्ध करा दिए हैं जिनकी सहायता से बम-विस्फोटों की रोकथाम भी संभव हो गई है। प्रौद्योगिकी ने यदि अपराधियों को तकनीक से लैस कर दिया है तो इसके कारण विभिन्न प्रकार के अपराधों व आतंकवाद की रोकथाम भी संभव हो गई है। जरूरत इस बात की है कि अपराधों की रोकथाम के लिए प्रौद्योगिकी व तकनीक का अधिक से अधिक इस्तेमाल किया जाए।

●●●

डा. निशांत सिंह

डा. निशांत सिंह अपराध, अपराधी और पुलिस तकनीक पर विभिन्न पत्र-पत्रिकाओं में अनवरत लिखते रहे हैं। आकाशवाणी से आपकी वार्ताओं का नियमित प्रसारण भी होता रहा है। साइबर अपराध, महिला अपराध अंगुलि चिह्न विज्ञान और भारत में अपराध सहित कुल डेढ़ दर्जन महत्वपूर्ण ग्रंथों का प्रकाशन हो चुका है।

आप इंदिरा गाँधी राजभाषा पुरस्कार, विधि पुरस्कार, भारतेंदु हरिशचंद्र पुरस्कार, डा. मेघनाद साहा पुरस्कार और मेदिनी सम्मान सहित भारत सरकार द्वारा कुल 8 राष्ट्रीय पुरस्कारों से सम्मानित हो चुके हैं।

अभी आप राष्ट्रीय अपराध रिकार्ड ब्यूरो (गृह मंत्रालय, भारत सरकार) में अंगुलि चिह्न विशेषज्ञ के पद पर कार्य कर रहे हैं।