TECH BITES

ક્લિનિકની બહાર આંખોની તપાસ

આંખોની તપાસ હવે પરંપરાગત ક્લિનિક પૂરતી સીમિત રહી નથી. પહેરી શકાય તેવી ટેક્નોલોજીના વિકાસથી આંખોની તપાસ વધુ સરળ અને પોર્ટેબલ બની રહી છે. બેંગલુરુ સ્થિત રેમિડિયો ઇનોવેટિવ સોલ્યુશન્સે તેની વેરેબલ 3D આઇ-ઇમેજિંગ ટેક્નોલોજી માટે અમેરિકામાં પેટન્ટ મેળવ્યું છે. VR પ્રકારના હેડસેટ જેવી રચના ધરાવતું આ ઉપકરણ એક જ પોર્ટેબલ યુનિટમાં આંખની પાંચથી વધુ તપાસને સમાવી શકે છે. આ ટેક્નોલોજી ખાસ કરીને દૂરના વિસ્તારો અને પ્રાથમિક આરોગ્ય કેન્દ્રોમાં ઉપયોગી બની શકે છે. રેમિડિયોની ઓક્યુલોમિક્સ પહેલ રેટિનાની તસવીરો દ્વારા આંખ સિવાયની કેટલીક સ્વાસ્થ્ય સમસ્યાઓના સંકેતો ઓળખવાની શક્યતાઓ પણ શોધી રહી છે.

વર્લપૂલની લક્ઝ્યુરીયમ 4-ડોર રેફ્રિજરેટર રેન્જ લોન્ચ

વર્લપૂલ ઓફ ઇન્ડિયા લિમિટેડે પ્રીમિયમ 4-ડોર રેફ્રિજરેટર રેન્જ 'લક્ઝ્યુરીયમ' લોન્ચ કરી છે. 654 લિટરની ક્ષમતા ધરાવતી આ રેન્જમાં 360 ટ્રિપલ કૂલિંગ ટેકનોલોજી સાથે ત્રણ સ્વતંત્ર કૂલિંગ સિસ્ટમ આપવામાં આવી છે, જે વિવિધ ખાદ્ય પદાર્થોની તાજગી, સ્વાદ અને ગુણવત્તા જાળવવામાં મદદ કરે છે. કન્વર્ટિબલ કમ્પાર્ટમેન્ટ 30 મિનિટથી ઓછા સમયમાં ફ્રીઝરથી રેફ્રિજરેટર મોડમાં બદલી શકાય છે. 4-ડોર ડિઝાઇન ભારતીય રસોડાની સ્ટોરેજ જરૂરિયાતોને અનુરૂપ છે. પ્રીમિયમ ફિનિશ, ઝીરો-બેન્ડિંગ ક્રિસ્પર ડ્રોઅર્સ અને સ્માર્ટ સ્ટોરેજ જેવી સુવિધાઓ ઉપલબ્ધ છે. રેન્જની શરૂઆતની કિંમત રૂ. 98,000 છે.

રોજિંદી વાતચીતમાં AIનો પ્રવેશ

આર્ટિફિશિયલ ઇન્ટેલિજન્સ હવે રોજિંદી ડિજિટલ વાતચીતનો પણ હિસ્સો બની રહ્યું છે. ઓપનએઆઇએ ChatGPTમાં 'સ્ટિકર્સ' નામનું નવું ફીચર રજૂ કર્યું છે, જે AIની મદદથી વ્યક્તિગત સ્ટિકર પેક બનાવવાની સુવિધા આપે છે. મોબાઇલ પર ChatGPTનો ઉપયોગ કરતા લોકો કોઈ થીમ, પાત્ર અથવા વિચારનું વર્ણન કરીને તેના આધારે સ્ટિકર્સ બનાવી શકે છે. આ સુવિધા ChatGPT Images 2.0 દ્વારા સંચાલિત છે અને વિશ્વભરમાં મફત વપરાશકર્તાઓ માટે ઉપલબ્ધ છે. રમૂજી પાત્રોથી લઈને વ્યક્તિગત રિએક્શન સુધી, AI આધારિત સ્ટિકર્સ ડિજિટલ વાતચીતને વધુ સર્જનાત્મક અને વ્યક્તિત્વસભર બનાવી શકે છે. આ સાથે જનરેટિવ AI સામાન્ય જીવનમાં વધુ ઊંડે પ્રવેશી રહ્યું છે.

GCCને નવા અંદાજથી ઘડતી ભાગીદારી

વિશ્વભરની કંપનીઓ હવે AI આધારિત ગ્લોબલ કેપેબિલિટી સેન્ટર્સ (GCCs) તરફ આગળ વધી રહી છે. આ દિશામાં Kyndryl અને Bridgepath Innovations વચ્ચે નવી ભાગીદારી થઈ છે. બંને કંપનીઓનો હેતુ સાહસોને AI-નેટિવ GCCની ડિઝાઇન, નિર્માણ અને વિસ્તરણમાં મદદ કરવાનો છે. આ મોડેલમાં ડિલિવરી, ઓપરેશન્સ અને ગવર્નન્સ સહિતના વિવિધ ક્ષેત્રોમાં AIને સામેલ કરવામાં આવશે. સાથે જ ડિજિટલ અને ડેટા આધારભૂત માળખાને પણ મજબૂત બનાવાશે. બંને કંપનીઓ ગ્રાહકોની એન્ટરપ્રાઇઝ સિસ્ટમ્સ, ડેટા અને બિઝનેસ જરૂરિયાતોને ધ્યાનમાં રાખીને કસ્ટમાઇઝ્ડ AI સોલ્યુશન્સ પણ વિકસાવશે. આ ભાગીદારી GCCને માત્ર સપોર્ટ સેન્ટર નહીં, પરંતુ નવીનતા અને ટેક્નોલોજીનું કેન્દ્ર બનાવવાની દિશામાં મહત્વનું પગલું છે.

ઘર -ઓફિસમાં CCTV કેમેરા સિસ્ટમ પર સતત મંડરાતો સાયબર-ફિઝિકલ હુમલો

આજના સમયમાં ઘર, દુકાન અને ઓફિસની સુરક્ષા માટે CCTV કેમેરાનો ઉપયોગ ખૂબ સામાન્ય બની ગયો છે. પરંતુ માત્ર કેમેરા લગાવી દેવાથી સંપૂર્ણ સુરક્ષા મળી જાય છે તેવું માનવું ભૂલભરેલું છે. જો CCTV સિસ્ટમનું નેટવર્ક અને તેની ભૌતિક વ્યવસ્થા સુરક્ષિત ન હોય તો તે જ સિસ્ટમ સુરક્ષા માટે જોખમ બની શકે છે. ઈન્ટરનેટ સાથે જોડાયેલા કેમેરાને હેક કરીને કોઈ અજાણ્યો વ્યક્તિ ખાનગી દૃશ્યો સુધી પહોંચી શકે છે, જ્યારે ચોર અથવા અસામાજિક તત્ત્વો વાયર કાપીને કે રેકોર્ડિંગ સિસ્ટમને નુકસાન પહોંચાડીને પુરાવાનો નાશ કરવાનો પ્રયાસ કરી શકે છે. તેથી CCTV સુરક્ષામાં સાયબર અને ફિઝિકલ એમ બંને પાસાં પર ધ્યાન આપવું જરૂરી છે. સુરક્ષા અંગે સામાન્ય ભૂલો પણ ઘણી વખત ગંભીર પરિણામ લાવી શકે છે.

ઉદાહરણ તરીકે, દુકાનમાં ચોરી થયા બાદ પોલીસને ફૂટેજ આપવાની જરૂર પડે ત્યારે ખબર પડે કે હાર્ડડિસ્ક મહિનાઓથી

મયુર ભુસાવળકર
આઈટી એક્સપર્ટ

ખરાબ હતી. આ સ્થિતિ ટાળવા માટે નિયમિત રીતે રેકોર્ડિંગ તપાસવું જરૂરી છે. તેવી જ રીતે, કોઈ વ્યક્તિ ડિફોલ્ટ પાસવર્ડ બદલવાનું ભૂલી જાય તો તેના ઈન્ટરનેટ સાથે જોડાયેલા કેમેરાની સુરક્ષા જોખમાઈ શકે છે. CCTV ખરીદતી વખતે વિશ્વસનીય ઉત્પાદક અને નિયમિત સોફ્ટવેર અપડેટ આપતી કંપનીને પ્રાથમિકતા આપવી જોઈએ. રાત્રિના સમયે સ્પષ્ટ દૃશ્ય માટે યોગ્ય નાઈટ વિઝન, વિશ્વસનીય સ્ટોરેજ અને સુરક્ષિત નેટવર્ક વ્યવસ્થા પણ મહત્વપૂર્ણ છે. CCTV સર્વેલન્સ અંગે જરૂરી હોય ત્યાં સ્પષ્ટ સૂચના બોર્ડ લગાવવાથી પણ લોકોમાં જાગૃતિ વધે છે. ભારતીય કાયદા અને સ્થાનિક નિયમોનું પાલન કરવું પણ જરૂરી છે. પોતાના સુરક્ષા કેમેરાને એવી રીતે ગોઠવવા જોઈએ નહીં કે તે પડોશીની ખાનગી જગ્યા, બારી અથવા અન્ય અંગત વિસ્તારનું અનાવશ્યક રેકોર્ડિંગ કરે. CCTV કેમેરા માત્ર એક ઈલેક્ટ્રોનિક ઉપકરણ નથી, પરંતુ ઘર, દુકાન અને ઓફિસની સમગ્ર સુરક્ષા વ્યવસ્થાનો મહત્વપૂર્ણ ભાગ છે. મજબૂત પાસવર્ડ, 2FA, નિયમિત સોફ્ટવેર અપડેટ, સુરક્ષિત Wi-Fi, યોગ્ય પાવર બેકઅપ, છુપાવેલા અને સુરક્ષિત વાયર, મજબૂત સ્ટોરેજ વ્યવસ્થા તથા પ્રાઈવસીનું ધ્યાન રાખવાથી CCTV સિસ્ટમને સાયબર અને ફિઝિકલ બંને પ્રકારના જોખમોથી વધુ સારી રીતે સુરક્ષિત બનાવી શકાય છે. ટેક્નોલોજીનો સમજદારીપૂર્વક ઉપયોગ અને નિયમિત ચકાસણી જ અસરકારક સુરક્ષાનું સાચું કવચ છે.

ડિફોલ્ટ પાસવર્ડ બદલવોએ સૌથી પહેલું કામ હોવુ જોઈએ

ઘણા લોકો CCTV કેમેરા, DVR અથવા NVR ઇન્સ્ટોલ થયા બાદ કંપની દ્વારા આપવામાં આવેલ ડિફોલ્ટ પાસવર્ડ જ ચાલુ રાખે છે. admin/admin અથવા 123456 જેવા સરળ પાસવર્ડ હેકર્સ માટે સરળ નિશાન બની શકે છે. તેથી સિસ્ટમ શરૂ કરતાં જ મજબૂત અને અલગ પાસવર્ડ રાખવો જોઈએ. પાસવર્ડમાં મોટા અને નાના અક્ષરો, અંકો અને ખાસ ચિહ્નોનો સમાવેશ કરવો વધુ સુરક્ષિત છે. ઉદાહરણ તરીકે S3cur3@Home»2026 જેવા પાસવર્ડનો ઉપયોગ કરી શકાય.આ સાથે, જ્યાં શક્ય હોય ત્યાં Two-Factor Authentication એટલે કે 2FA પણ ચાલુ કરવું જોઈએ. આમ, કોઈ વ્યક્તિને પાસવર્ડ મળી જાય તો પણ મોબાઇલ પર આવતા OTP અથવા કન્ફર્મેશન કોડ વગર સિસ્ટમમાં પ્રવેશ મેળવવો મુશ્કેલ બને છે.CCTV કેમેરાના ફર્મવેર અને સિક્યોરિટી અપડેટ પણ નિયમિત રીતે કરવા જરૂરી છે. ઉત્પાદક કંપનીઓ સમયાંતરે સુરક્ષાની ખામીઓ દૂર કરવા અપડેટ બહાર પાડતી હોય છે. મહિનામાં ઓછામાં ઓછું એક વખત મોબાઇલ એપ્લિકેશન અથવા DVR/NVR સેટિંગ્સમાં અપડેટ ઉપલબ્ધ છે કે નહીં તેની તપાસ કરવી જોઈએ.

Wi-Fi રાઉટરની સુરક્ષા પણ મહત્વની

વાયરલેસ CCTV કેમેરા હોય તો Wi-Fi રાઉટરની સુરક્ષા પણ એટલી જ મહત્વપૂર્ણ બને છે. CCTV ઉપકરણો માટે અલગ નેટવર્ક અથવા Guest Network બનાવવાથી મુખ્ય ઘર કે ઓફિસ નેટવર્કથી તેને અલગ રાખી શકાય છે. રાઉટરમાં WPA2 અથવા WPA3 જેવી સુરક્ષા પદ્ધતિનો ઉપયોગ કરવો જોઈએ.જૂની પદ્ધતિ મુજબ CCTVને મોબાઇલમાં જોવા માટે Port Forwarding કરવામાં આવતું હતું, પરંતુ આ પદ્ધતિ કેટલાક કિસ્સાઓમાં સિસ્ટમને ઇન્ટરનેટ પર વધુ ખુલ્લી મૂકી શકે છે. તેથી જરૂરિયાત મુજબ સુરક્ષિત VPN અથવા ઉત્પાદક દ્વારા આપવામાં આવતી વિશ્વસનીય રિમોટ-એક્સેસ પદ્ધતિનો ઉપયોગ કરવો જોઈએ.

આ મહત્વપૂર્ણ બાબતો ક્યારેય ભૂલશો નહીં

પ્રાઈવસીનું ધ્યાન રાખો : ઘરમાં બેડરૂમ, બાથરૂમ અથવા અન્ય અત્યંત અંગત સ્થળોએ કેમેરા લગાવવા ટાળવા જોઈએ. ઓફિસમાં પણ રેસ્ટરૂમ અને અન્ય ખાનગી વિસ્તારોમાં CCTV ન હોવા જોઈએ. કેમેરાનું ફોકસ માત્ર સુરક્ષા માટે જરૂરી વિસ્તારો તરફ જ હોવું જોઈએ.

એક્સેસ કંટ્રોલ રાખો : CCTVનું એડમિન એક્સેસ મર્યાદિત લોકો પાસે જ હોવું જોઈએ. ઘરમાં જવાબદાર પરિવારજનોને જ સંપૂર્ણ એક્સેસ આપવો જોઈએ, જ્યારે ઓફિસમાં જરૂરી કર્મચારીઓને માત્ર View Only જેવી મર્યાદિત પરવાનગી આપી શકાય.

મોશન એલર્ટનો ઉપયોગ કરો : ઘરના બહારના વિસ્તારો માટે રાત્રિના સમયે Motion Alert ઉપયોગી બની શકે છે. ઓફિસમાં કામકાજના સમય બાદ અનધિકૃત હલચલ અંગે એલર્ટ ગોઠવી શકાય છે.

ટેકનિશિયનનું એક્સેસ દૂર કરો : CCTV ઇન્સ્ટોલેશન અથવા મરામત કરનાર ટેકનિશિયનનું કામ પૂર્ણ થયા પછી તેની પાસે રહેલો એક્સેસ દૂર કરવો જોઈએ. જરૂર પડે તો પાસવર્ડ બદલીને તમામ લોગિન સત્રોની તપાસ કરવી જોઈએ.

કેમેરાની નિયમિત સફાઈ કરો : ધૂળ, વરસાદના ડાઘ અથવા કરોળિયાના જાળાને કારણે કેમેરાનું દૃશ્ય ધૂંધળું બની શકે છે. તેથી લેન્સ અને કેમેરાની બહારની સપાટી સમયાંતરે સાફ કરવી જોઈએ.

વીજળી બંધ થાય તો પણ CCTV ચાલુ રહે તેવુ ગોઠવો

ચોર કે અસામાજિક તત્ત્વો મુખ્ય વીજ પુરવઠો બંધ કરીને CCTV સિસ્ટમને નિષ્ક્રિય કરવાનો પ્રયાસ કરી શકે છે. વીજળીના સામાન્ય કટ દરમિયાન પણ કેમેરા બંધ થઈ શકે છે. તેથી મહત્વપૂર્ણ CCTV સિસ્ટમ, DVR/NVR અને જરૂર મુજબ નેટવર્ક ઉપકરણોને UPS અથવા યોગ્ય પાવર બેકઅપ સાથે જોડવા જોઈએ. પાવર બેકઅપની ક્ષમતા એવી હોવી જોઈએ કે વીજ પુરવઠો બંધ થયા બાદ પણ જરૂરી સમય સુધી રેકોર્ડિંગ ચાલુ રહી શકે. સમયાંતરે UPS અને બેટરીની કામગીરી પણ તપાસવી જરૂરી છે.

CCTV કેમેરાની ભૌતિક સુરક્ષા પણ એટલી જ જરૂરી

સોફ્ટવેર અને પાસવર્ડ ગમે તેટલા મજબૂત હોય, પરંતુ જો કોઈ વ્યક્તિ સરળતાથી કેમેરા સુધી પહોંચી શકે તો તેને નુકસાન પહોંચાડી શકાય છે. તેથી કેમેરા સામાન્ય રીતે એવી ઊંચાઈએ લગાવવા જોઈએ જ્યાં સુધી સરળતાથી હાથ ન પહોંચી શકે અને સાથે જ જરૂરી વિસ્તારનું સ્પષ્ટ કવરેજ મળી રહે.કેમેરાનું ક્રોસ-એંગલ કવરેજ પણ ઉપયોગી બની શકે છે. એક કેમેરાની આસપાસની પ્રવૃત્તિ બીજા કેમેરામાં કેદ થાય તેવી ગોઠવણ કરવાથી કોઈ વ્યક્તિ કેમેરા સાથે છેડછાડ કરે તો તેની ઘટના બીજા કેમેરામાં રેકોર્ડ થઈ શકે છે.કેમેરાના વાયર ખુલ્લા રાખવા જોખમી બની શકે છે. વાયરને યોગ્ય રીતે PVC પાઇપ અથવા કન્ડ્યુઇટ દ્વારા પસાર કરવા જોઈએ. બહારના કનેક્શન માટે હવામાન-પ્રતિરોધક જંક્શન બોક્સનો ઉપયોગ કરવો યોગ્ય છે.

કિશોરો માટે સોશિયલ મીડિયા પર 'સેફ્ટી લોક' Instagram અને Facebookમાં નવા નિયમો

સુરક્ષા વધશે કે સ્વતંત્રતા ઘટશે?

ટાઈમ લિમિટથી લઈને પેરેન્ટલ કંટ્રોલ સુધી–કિશોરોના ડિજિટલ જીવન પર કડક નજર

સોશિયલ મીડિયા આજના કિશોરોના જીવનનો મહત્વનો હિસ્સો બની ગયું છે. મિત્રો સાથે જોડાવાથી લઈને મનોરંજન અને અભ્યાસ સુધી Instagram અને Facebook જેવા પ્લેટફોર્મનો ઉપયોગ વધી રહ્યો છે. જોકે, વધતા સ્ક્રીન ટાઈમ, ઊંઘમાં ખલેલ, સાયબરબુલિંગ, બોડી-ઈમેજ અંગેનો દબાણ અને માનસિક સ્વાસ્થ્યને લઈને ઊભી થતી ચિંતાઓએ ટેક કંપનીઓને નવી સુરક્ષા વ્યવસ્થા તરફ ધકેલી છે. Meta હવે કિશોરો માટે સોશિયલ મીડિયા અનુભવને વધુ સુરક્ષિત બનાવવા નવા પગલાં અમલમાં મૂકવાની તૈયારીમાં છે. 13થી 17 વર્ષની ઉંમરના યુઝર્સ માટે સમય મર્યાદા, નોટિફિકેશન નિયંત્રણ અને વય આધારિત પ્રતિબંધો જેવા ફીચર્સ પર ભાર મૂકવામાં આવી રહ્યો છે. નવી વ્યવસ્થામાં કિશોરો રાત્રિના સમયે સોશિયલ મીડિયા ઉપયોગને મર્યાદિત કરી શકે તેવી સુવિધાઓ હશે. ઉપરાંત, માતા-પિતા પોતાના સંતાનના એકાઉન્ટ પર કેટલીક સેટિંગ્સનું નિયંત્રણ રાખી શકશે. ખાસ કરીને મોડરેશન, કન્ટેન્ટ અને પ્રાઈવસી અંગેના વિકલ્પોમાં પેરેન્ટલ દેખરેખને મહત્વ આપવામાં આવશે.

AIની નજર, પેરેન્ટ્સની મંજૂરી અને કન્ટેન્ટ ફિલ્ટર–પણ સવાલ છે 'કેટલું અસરકારક?'

સુરક્ષા વ્યવસ્થાનો બીજો મહત્વનો ભાગ AI આધારિત વય ચકાસણી છે. જો પ્લેટફોર્મને લાગે કે કોઈ યુઝર 13 વર્ષથી નાની ઉંમરનો છે, તો તેની ઓળખ અને ઉંમર અંગે વધુ ચકાસણી થઈ શકે છે. 13થી 17 વર્ષના કિશોરો માટે પણ કેટલીક સેટિંગ્સ માતા-પિતાની મંજૂરી વગર બદલી શકાશે નહીં. Instagram પર કિશોરો દ્વારા જોવામાં આવતા કન્ટેન્ટને વધુ સુરક્ષિત બનાવવાનો પ્રયાસ પણ થશે. ભલામણો, સંવેદનશીલ કન્ટેન્ટ અને બોડી-ઈમેજને અસર કરી શકે તેવી સામગ્રી પર નિયંત્રણ વધારવાની દિશામાં પગલાં લેવાઈ રહ્યા છે. બાળકોને ટાર્ગેટ કરતા મેકઅપ ફિલ્ટર્સ અને અન્ય કેટલાક ફીચર્સ પર પણ પ્રતિબંધ અથવા મર્યાદા આવી શકે છે.પરંતુ અહીં સૌથી મોટો સવાલ છે–શું ટેક્નોલોજી કિશોરોને ખરેખર સુરક્ષિત કરી શકશે?નિષ્ણાતોનું માનવું છે કે માત્ર ટેકનિકલ નિયંત્રણ પૂરતું નથી. માતા-પિતા અને બાળકો વચ્ચેનો સંવાદ, ડિજિટલ સાક્ષરતા અને જવાબદાર સોશિયલ મીડિયા ઉપયોગ પણ એટલો જ જરૂરી છે.Metaની સાથે TikTok, YouTube અને Snapchat જેવા પ્લેટફોર્મ પર પણ સમાન પ્રકારના નિયંત્રણો લાવવાની ચર્ચા થઈ રહી છે. જોકે, વધુ પડતા નિયંત્રણો કિશોરોની સ્વતંત્રતા અને પ્રાઈવસી સામે પ્રશ્નો ઊભા કરી શકે છે.અંતે વાત માત્ર 'સોશિયલ મીડિયા કેટલું વાપરવું?' તેની નથી, પરંતુ 'તેનો સુરક્ષિત અને સમજદારીપૂર્વક ઉપયોગ કેવી રીતે કરવો?' તેની છે. ટેક્નોલોજી સુરક્ષાનું સાધન બની શકે, પરંતુ કિશોરોના ડિજિટલ જીવન માટે સૌથી મજબૂત 'સેફ્ટી ફીચર' કદાચ જાગૃત માતા-પિતા અને સમજદાર બાળક વચ્ચેનો વિશ્વાસ જ છે.

નવી ટેક્નોલોજી માટે હવે ગેટકીપિંગ જરૂરી

AIની અદૃશ્ય લગામ

કૃત્રિમ બુદ્ધિમત્તા એટલે કે AI માનવ જીવનને સરળ, ઝડપી અને વધુ કાર્યક્ષમ બનાવવાની અદભૂત ક્ષમતા ધરાવે છે. આરોગ્ય, શિક્ષણ, સરકારી સેવાઓથી લઈને રોજગાર અને વ્યવસાય સુધી AI અનેક ક્ષેત્રોમાં પરિવર્તન લાવી રહ્યું છે. પરંતુ માઈક્રોસોફ્ટના સહ-સ્થાપક અને પરોપકારી બિલ ગેટ્સ હવે AIની વધતી ક્ષમતાઓ સાથે તેના જોખમો અંગે પણ ગંભીર ચેતવણી આપી રહ્યા છે. ગેટ્સના મતે, AIથી સમાજને મોટા પ્રમાણમાં ફાયદો થઈ શકે છે, પરંતુ આ લાભ આપોઆપ દરેક વ્યક્તિ સુધી પહોંચશે એવું માનવું યોગ્ય નથી. ટેક્નોલોજીનો ઉપયોગ કેવી રીતે થાય છે, તેના પર નિયંત્રણ અને યોગ્ય નિયમો કેટલા અસરકારક છે–આ બાબતો આગામી વર્ષોમાં અત્યંત મહત્વપૂર્ણ બનવાની છે. AIની ઝડપથી વધી રહેલી ક્ષમતાઓએ ગેટ્સની ચિંતામાં વધારો કર્યો છે. તેઓ ખાસ કરીને સાયબર હુમલા, ખોટી માહિતી, નોકરીઓ પર પડનારી અસર, સ્વાયત્ત ટેક્નોલોજી અને માનવ સંબંધો પર થતી અસર જેવા જોખમો તરફ ધ્યાન દોરે છે. AI વધુ શક્તિશાળી બનશે તેમ તેના સારા અને ખરાબ બંને ઉપયોગની શક્યતાઓ પણ વધશે.

ફાયદા સામે જોખમ : AIને રોકવું નહીં, જવાબદારીથી ચલાવવું

ગેટ્સનો અભિગમ AIના વિકાસને સંપૂર્ણપણે અટકાવવાનો નથી. તેના બદલે તેઓ માને છે કે AIનો વિકાસ માનવ હિત સાથે સુસંગત રહે તે માટે મજબૂત દેખરેખ અને નિયમન જરૂરી છે. સરકારો, ટેક્નોલોજી કંપનીઓ અને નિષ્ણાતોએ સાથે મળીને એવા નિયમો ઘડવા પડશે જે નવીનતાને અટકાવ્યા વિના તેના દુરુપયોગને નિયંત્રિત કરી શકે. ખાસ કરીને આરોગ્ય અને શિક્ષણ જેવા ક્ષેત્રોમાં AI માનવ જીવનમાં મોટા સુધારા લાવી શકે છે. ગરીબ અને વિકાસશીલ દેશોમાં પણ AI આધારિત સરકારી સેવાઓ તથા શૈક્ષણિક સાધનો નવી તકો ઊભી કરી શકે છે. પરંતુ બીજી તરફ, જો AIના લાભો માત્ર મોટા કોર્પોરેટ્સ અથવા સમૃદ્ધ વર્ગ સુધી મર્યાદિત રહી જાય, તો ટેક્નોલોજી અસમાનતા ઘટાડવાને બદલે વધારી શકે છે.

AIથી ડરો નહીં, સમજદારીથી સ્વીકારો

નોકરીઓ માટે પડકાર, પરંતુ નવી તકોના દરવાજાઓ પણ ખુલશે

આર્ટિફિશિયલ ઈન્ટેલિજન્સ એટલે કે AI હવે માત્ર ટેક્નોલોજીની દુનિયાનો વિષય રહ્યો નથી. તે રોજગાર, શિક્ષણ અને સમગ્ર કાર્યસંસ્કૃતિને બદલી રહ્યો છે. AIના વધતા ઉપયોગથી અનેક પરંપરાગત નોકરીઓ પર જોખમ ઊભું થઈ રહ્યું છે, પરંતુ સાથે જ નવી કુશળતા અને નવા પ્રકારની નોકરીઓ માટેની તકો પણ સર્જાઈ રહી છે.ભારતીય IT ક્ષેત્રમાં આ પરિવર્તનની અસર ખાસ નોંધપાત્ર બની રહી છે. કેટલાક અંદાજ મુજબ આગામી થોડાં વર્ષોમાં મોટી સંખ્યામાં નોકરીઓમાં ફેરફાર અથવા ઘટાડો થઈ શકે છે. ખાસ કરીને ડેટા એન્ટ્રી, બેઝિક કોડિંગ, ગ્રાહક સેવા, ટેલિકોલિંગ, રૂટીન IT સપોર્ટ અને કેટલાક એકાઉન્ટિંગ જેવા પુનરાવર્તિત કામો AI અને ઓટોમેશનથી વધુ પ્રભાવિત થઈ શકે છે.

AI માણસનો વિકલ્પ કે સહયોગી?

AIની સૌથી મોટી શક્તિ પુનરાવર્તિત અને નિયમિત કામ ઝડપથી કરવાની છે. પરંતુ નિર્ણયક્ષમતા, સહાનુભૂતિ, નેતૃત્વ, સર્જનાત્મકતા અને જટિલ માનવીય પરિસ્થિતિઓને સમજવાની ક્ષમતા હજુ પણ માણસની વિશેષતા છે. એટલે ભવિષ્યની સ્પર્ધા કદાચ 'માણસ વિરુદ્ધ AI' નહીં, પરંતુ 'AIનો શ્રેષ્ઠ ઉપયોગ કરનાર માણસ વિરુદ્ધ AIનો ઉપયોગ ન કરનાર માણસ' વચ્ચેની બની શકે છે.

પડકાર કરતાં મોટો છે 'રીસ્કિલિંગ'નો મોકો

AIનો અર્થ દરેક માનવીની નોકરી ખતમ થવી એવો નથી. હકીકતમાં AI સાથે કામ કરવાની ક્ષમતા ધરાવતા કર્મચારીઓની માંગ વધી શકે છે. કંપનીઓ હવે માત્ર ટેક્નિકલ જ્ઞાન નહીં, પરંતુ AI ટૂલ્સનો ઉપયોગ, ડેટા સમજવાની ક્ષમતા, સમસ્યા ઉકેલવાની કુશળતા, સર્જનાત્મક વિચારસરણી અને માનવીય સંવાદ જેવી કુશળતાઓને પણ મહત્વ આપી રહી છે. ભારતીય IT કંપનીઓ માટે સૌથી મોટો પ્રશ્ન એ છે કે હાલના કર્મચારીઓને નવી ટેક્નોલોજી સાથે ઝડપથી કેવી રીતે તાલમેલ કરાવવામાં આવે. માત્ર નવા કર્મચારીઓની ભરતી કરતાં હાલના કર્મચારીઓને રીસ્કિલ અને અપસ્કિલ કરવાથી સંસ્થાઓ માટે લાંબા ગાળે વધુ ફાયદો થઈ શકે છે.

'AI અપનાવો, માણસને પાછળ ન છોડો'

કંપનીઓ માટે પડકાર માત્ર AI અપનાવવાનો નથી, પરંતુ AI સાથે કર્મચારીઓનું ભવિષ્ય પણ સુરક્ષિત રાખવાનો છે. નવી ટેક્નોલોજીથી ઉત્પાદકતા વધે અને ખર્ચ ઘટે તે જરૂરી છે, પરંતુ કર્મચારીઓને તાલીમ આપ્યા વિના માત્ર ઓટોમેશન તરફ આગળ વધવું લાંબા ગાળે અસંતોષ અને કુશળતાના અંતરને વધારી શકે છે.ભવિષ્યમાં સફળ કંપની એ હશે જે ટેક્નોલોજી અને માનવીય પ્રતિભા વચ્ચે સંતુલન જાળવી શકે. AIને માણસના વિકલ્પ તરીકે નહીં, પરંતુ માણસની ક્ષમતાને અનેકગણી વધારતા શક્તિશાળી સહયોગી તરીકે સ્વીકારવો એ જ આગળ વધવાનો માર્ગ બની શકે છે.