የኮምፒውተር ወንጀል አዋጅ ማብራሪያ

መግቢያ

በኢንፎርሜሽን ኮምኒዩኬሽን ቴክኖሎጂ እና ሌሎች የቴክኖሎጂ ውጤቶች መስፋፋትና የሰው ልጅ የእለት ተእለት እንቅስቃሴ በእነዚህ ቴክኖሎጂዎች ጥገኛ እየሆነ መምጣቱ ለአዳዲስ ወንጀሎች መፈጠር ብቻ ሳይሆን መደበኛ ወይም ነባር ወንጀሎችም ውስብስብና ሊገመቱ በማይችሉ መንገዶች እንዲፈፀሙ መንስኤ ሆኗል:: እነዚህ ወንጀሎች የቴክኖሎጂው ተደራሽነት ተከትሎ በሃገራችንም ኢኮኖሚያዊ፣ ፖለቲካዊ፣ ማህበራዊና ግለሰባዊ ስጋት እየሆኑ መጥቷል:: ለዚህም በርካታ መንስኤዎች ያሉት ቢሆንም ጠንካራና ከቴክኖሎጂው ውስብስብነት ጋር አብሮ መጓዝ የሚችል የሕግ ማዕቀፍ አለመኖር አንዱ በመሆኑ የኮምፒውተር ወንጀል አዋጅ ማዘጋጀት አስፈልጓል::

ዓላማ

የዚህ ማብራሪያ ሰነድ ዋና ዋና አላማዎች፣

- ጥቅል በሆነ መልኩ የተገለፁ የህጉ ድንጋጌዎችን በውስጣቸው ምን ምን ቁምነገሮች እንደቋጠሩ በማሳየት በሕጉ አፈፃፀም ሂደት ሊከሰቱ የሚችሉ ብዥታዎችን ማስቀረት፣
- በእያንዳንዱ ድንጋጌ ጀርባ ያሉ እሳቤዎችና መነሻዎች ማሳየት፣
- በህጉ ላይ ለሚደረጉ ቀጣይ ጥናቶች መነሻ ሆኖ እንዲያገለግልና ሕጉ በሚዘጋጅበት ወቅት የነበሩ አስተሳሰቦች ማሳየት፣
- እያንዳንዱ የሕጉ ድንጋጌ መንፈስ በማብራራት የሳይበር ምህዳርን የሚመለከቱ ሌሎች ሕጎች በሚዘጋጁበት ወቅት ሊፈጠር የሚችልን ግጭት ማስቀረት፣ እና
- በሕጉ አፈፃፀም ዙሪያ ለፍትህ አካላት በሚሰጡ የአቅም ግንባታ ስልጠናዎች እንደ ግብአት ሆኖ እንዲያገለግል ማድረግ

ናቸው::

እሳቤዎች

የረቂቅ ህጉ ዝግጅት በዋናነት በሚከተሉት መሰረታዊ እሳቤዎች ላይ የተመሰረተ ነው፤

- የኮምፒውተር ወንጀል አለም አቀፍ ባህሪ ያለው መሆኑና ወንጀሉን ለመከላከል አለም አቀፍ ተሞክሮዎችን መሰረት ያደረገ የህግ ማእቀፍ ማዘጋጀት ማስፈለጉ፤
- በሳይበር ምህዳር መስፋፋት ምክንያት አዳዲስ ወንጀሎችና አዳዲስ የወንጀል አፈፃፀም ስልቶች መፈጠራቸው፤
- በሃገሪቱ የኮምፒውተር ወንጀልን የሚገዙ መሰረታዊም ሆነ የሥነ-ሥርዓት ህጎች በበቂ ሁኔታ አለመኖር፤
- በሃገሪቱ የኢንፎርሜሽን መሰረተ ልማቶች መስፋፋትና ከዲጂታላይዜሽን ሥራዎች ጋር ተያይዞ የተፈጠረ ሰፊ የደህንነት ታጋላጭነት፤
- የኮምፒውተር ወንጀልን ለመከላከልና ለመቆጣጠር የተወሰዱ አካባቢያዊና አለም አቀፋዊ የጋራ ግንዛቤዎችና ስምምነቶች መፈጠራቸው፡፡

የሕጉ የዝግጅት ሂደት

የአዋጁ ዝግጅት ከሁለት ዓመት በላይ የወሰደ እና በርካታ ሂደቶችም ያለፈ ሲሆን ረቂቅ ሕጉ ተጠናቅቆ እስከቀረበበት ድረስ የተከናወኑ አበይት ተግባራት ወይም ሂደቶች በሚከተለው መልኩ ተጠቃለዋል፡፡

1/ **ሰፊ ጥናት ማካሄድ፡-** ዘርፉ አዲስና ውስብስብ ከመሆኑ የተነሳ በርካታ ጥናቶች ማካሄድና በጥልቀት መረዳት የሚጠይቅ ሲሆን ይህንን ለማሳካትም ለሁለት አመት ያህል በርካታ የጥናት ሰነዶች ተዘጋጅቷል፡፡ በእነዚህ ጥናቶች አማካኝነትም ረቂቅ ህጉ ከማዘጋጀት ባሻገር በቀጣይነት ህጉ ለማስፈፀም ሊያጋጥሙ የሚችሉ ፈተናዎችና መሰራት የሚገባቸው ጉዳዮች ተለይቷል፡፡

2/ **በሀገራችን በተጨባጭ እየደረሱ ያሉ የሳይበር ጥቃቶች እና ተጋላጭነቶች መለየት፦** ህጉ በተግባራዊ ችግሮች ላይ የተመሰረተ እንዲሆን በማሰብ በሃገራችን በተጨባጭ እየደረሱ ያሉ የሳይበር ጥቃቶችና ተጋላጭነቶች እንዲሁም ያሉ ክፍተቶች ለመለየት የተለያዩ ጥረቶች የተደረጉ ሲሆን ለዚህም ሁለት የመረጃ (የዳታ) ምንጮች ጥቅም ላይ ውለዋል፡፡ እነዚህም በተመረጡ የፌዴራል መንግስት ተቋማት፣ በICT ዘርፍ ላይ በተሰማሩ ካምፓኒዎች፣ በባንኮች እና በፍትህ ተቋማት ላይ በተደረጉ የዳሰሳ ጥናቶች

የተገኙ ዳታዎች እንዲሁም የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ (ኢመደኤ) በተለያዩ ወቅቶች የሰበሰባቸው ቴክኒካዊ መረጃዎችና ሪፖርቶች ናቸው:: በዚህ መሰረትም በርካታ የሳይበር ጥቃቶች መለየት የተቻለ ሲሆን ሁሉም በረቂቅ ሕጉ ሽፋን እንዲያገኙ ጥረት ተደርጓል::

3/ **በስራ ላይ ያሉ የሀገሪቱ ሕጎች ያለባቸው ክፍተት መለየት፦** የሳይበር ምህዳር ለአዳዲስ ወንጀሎች መፈጠር ብቻ ሳይሆን ነባር ወንጀሎችም በአዳዲስና ውስብስብ መንገዶች እንዲፈፀሙ ያስቻለ በመሆኑ ከዚህ አንፃር በስራ ላይ ያሉ ተዛማጅ ሕጎቻችን ያሉባቸው ክፍተቶች ማጥናት ያስፈልጋል:: በዚህ መሰረትም በተለያዩ ሕጎች ውስጥ ከኮምፒውተር ወንጀል ጋር ግንኙነት ያላቸው የተወሰኑ ድንጋጌዎች የተካተቱ ቢሆንም በርካታ ክፍተቶች ያሉባቸውና ሕጎቹ ማስፈፀም የሚያስችሉ የሥነ-ሥርዓትና የማስረጃ ድንጋጌዎች ያላካተቱ በመሆናቸው የነበሩ ክፍተቶች በዚህ ረቂቅ አዋጅ እንዲሞሉ ተደርጓል::

4/ **ለረቂቅ ሕጉ ዝግጅት ግብአት የሚሆኑ ሞዴል ሕጎችና ተሞክሮዎች መምረጥ፦** የኮምፒውተር ወንጀል ዓለም አቀፍ ይዘት ያለው በመሆኑ ወንጀለኞች ከየትኛውም የዓለም ጫፍ ሆነው ጥቃት ሊፈፅሙ ይችላሉ:: ስለሆነም ይህንን ችግር ለመፍታት ያለው ብቸኛ መፍትሄ ሃገሮች ወንጀሉን ለመከላከል በጋራ መስራትና ወንጀለኞችን የሚለዋወጡበት ስምምነት መፍጠር ነው:: ነገር ግን እንደዚህ አይነቱ ስምምነት ተግባራዊ ሊሆን የሚችለው አንድን ድርጊት በተስማሚ ሀገሮች ዘንድ እንደ ወንጀል የሚቆጠር (double criminality principle) ተግባራዊ ሲሆን ብቻ በመሆኑ ሀገሮች በዘርፉ ያሏቸው የሕግ ማዕቀፎች አንድ ዓይነት ማድረግ ባይቻልም ተመሳሳይነት እንዲኖራቸው ማድረግ ያስፈልጋል:: ይህንን ከግምት ውስጥ በማስገባት በርካታ ዓለም አቀፍ ሞዴል ሕጎች የተዘጋጁ ሲሆን ዋና ዓላማቸውም የየሃገራቱ ተጨባጭ ሁኔታዎች ከግምት ውስጥ ማስገባት እንደተጠበቀ ሆኖ የሳይበር ምህዳሩን የሚገዙ ሕጎችን ተመሳሳይነት እንዲኖራቸው ማድረግ (legal harmonization) ነው:: ስለሆነም ይህንን የአለም አካሄድ መከተል አስፈላጊ በመሆኑና የህጉንም ይዘት አለም አቀፍ ደረጃው የጠበቀ ይሆን ዘንድ የሚከተሉት አለም አቀፍ ህጎች በሞዴልነት ተመርጧል::

- የአፍሪካ ህብረት የሳይበር ደህንነት ረቂቅ ስምምነት (2011)፣
- የአውሮፓ ህብረት የሳይበር ወንጀል ስምምነት (2001)፣

- የአለም አቀፉ የቴሌኮምኒዩኬሽን ህብረት የሳይበር ወንጀል ሞዴል ሕግ (2010)፣
- የምዕራብ ኤሲያ አገሮች የኢኮኖሚና ማህበራዊ ኮሚሽን(ESCWA) የሳይበር ወንጀል ሞዴል ሕግ (2002)
- የቡድን 8 የኮምፒዩተር ወንጀል መከላከል መርሆች(1997)
- አለም አቀፍ የሳይበር ደህንነትና የሳይበር ወንጀል ረቂቅ ፕሮቶኮል (2009)
- የተባበሩት መንግስታት ድርጅት የኮምፒዩተር ወንጀል አስመልክቶ በተለያዩ ጊዜያቶች ያስተላለፋቸው ውሳኔዎች(1990-2004)

ከዚህም በተጨማሪ በረቂቅ አዋጁ ዝግጅት ሂደት በርካታ የአፍሪካ፣ የአውሮፓ፣ የአሜሪካና የኤስያ አገሮች የኮምፒውተር ወንጀል ሕግ ተሞክሮዎችን በስፋት የተዳሰሱ ሲሆን የረቂቅ አዋጁ ይዘት አጠቃላይ ማብራሪያም እንደሚከተለው ቀርቧል::

ባለድርሻ አካላትን ማወያየት

ረቂቅ ህጉን ለማዳበር የሚከተሉት ሶስት ወርክ ሾፖች ተዘጋጅቷል፦

- ከፌዴራል የመንግስት መስሪያ ቤቶች ከተውጣጡ የተለያዩ ባለሙያዎችና ሃላፊዎች ጋር የሁለት ቀን ወርክሾፕ፤
- የመንግስት መስሪያ ቤቶች የወከሉና በግል የሚሰሩ የሕግ ባለሙያዎች ብቻ የተሳተፉበት የሁለት ቀን ወርክሾፕ፤
- በመላው ሃገሪቱ ካሉ ትላልቅ ዩኒቨርሲቲዎች ከተውጣጡ ሙሁራን ጋር የሁለት ቀን ወርክሾፕ::

የረቂቅ አዋጁ አጠቃላይ ይዘት

- **የቋንቋ አጠቃቀም**፦ የኮምፒውተር ወንጀል ከኢንፎርሜሽን ኮምኒዩኬሽን ቴክኖሎጂ ፈጣን እድገትና ውስብስብነት ጋር አብሮ የሚለዋወጥና እየተወሳሰበ የሚሄድ እንዲሁም የሳይበር ምህዳር በየቀኑ አዳዲስ የወንጀል አይነቶች የሚፈጠሩበት በመሆኑ እያንዳንዱን ወንጀል መዘርዘርና የህግ ሽፋን እንዲኖረው ማድረግ አዳጋች ብቻ ሳይሆን ወንጀሎቹ በተለዋወጡ ቁጥር የህግ ስርዓቱም በዚያው ፍጥነት መለወጥ አለበት ማለት ነው:: ይህም ፈፅሞ የማይቻልና የፍትህ ስርዓቱንም የሚያመሰቃቅል በመሆኑ የሚቀረፀው የህግ ማዕቀፍ በተቻለ መጠን በሳይበር ምህዳሩ በሚከሰቱ ሁሉም የወንጀል ድርጊቶች ተፈፃሚ እንዲሆንና አሁን የተፈጠሩትን የወንጀል አይነቶች ብቻ ሳይሆን ወደፊት ሊፈጠሩ በሚችሉት ላይም ተፈፃሚ እንዲሆን ተደርጎ ሊቀረፅ ይገባል:: ይህንንም

ለማሳካት በበርካታ መስፈርቶች የሚመሳሰሉ የኮምፒውተር ወንጀል አይነቶችን በአንድ ምድብ ማስቀመጥና የህጉ ተፈፃሚነት ቀጣይነት ይኖረው ዘንድ ቴክኖሎጂያዊ ያልሆነ (technology neutral) ቋንቋ ወይም አገላለፅ መጠቀም ያስፈልጋል:: ይህም ማለት የወንጀሉ የአፈፃፀም ስልት ወይም ጥቅም ላይ የሚውሉ የቴክኖሎጂ አይነቶች ግምት ውስጥ አይገቡም ማለት ነው:: ይህ አካሄድ በተለያዩ አለም አቀፍ ሞዴል ህጎችና ስምምነቶች የሚመከር ሲሆን የአፍሪካ ህብረት የሳይበር ሕግ ረቀቅ ስምምነትም እንደ ግዴታ አስቀምጦታል:: በዚህ መሰረትም ረቂቅ አዋጁ በዋናነት ቴክኖሎጂያዊ ባልሆነ (technology neutral) ቋንቋ ወይም አገላለፅ ተዘጋጅቷል::

- **የወንጀል ፈፃሚዎች የሃሳብ ክፍል፦** በዚህ ረቂቅ አዋጅ የተካተቱት አብዛኞቹ ድርጊቶች በወንጀል ሊያስቀጡ የሚችሉት **“ሆን ተብለው”** የተፈፀሙ እንደሆነ ብቻ ሲሆን ይህም የሆነበት ምክንያት በሃገራችን ያለው የኮምፒዩተር አጠቃቀምና ደህንነት ግንዛቤ አነስተኛ በመሆኑ **በቸልተኝነት** የሚፈፀሙ ጥፋቶችን ወንጀል ማድረግ ከጥቅሙ ይልቅ ጉዳቱ ሊያመዝን ይችላል በሚል እሳቤ ነው:: ይህ ማለት ግን ቸልተኝነት በኮምፒውተር ወንጀል ፈፅሞ አያስቀጣም ማለት አይደለም:: *(ለምሳሌ አንቀፅ 7 (5) ይመልከቱ)*
- **የወንጀል ህግ አጠቃላይ መርሆች ተፈፃሚነት፦** ይህ ረቂቅ አዋጅ ምንም እንኳን አዲስ የወንጀል ሕግ ቢሆንም በ1997 ተሻሽሎ በወጣው የወንጀል ሕግ አንቀፅ 3 ላይ እንደተመለከተው አጠቃላይ የወንጀል ህጉ መርሆችን በዚህ አዋጅ ላይም ተፈፃሚ እንደሚሆኑ ግንዛቤ ሊወሰድ ይገባል *(የ1997ቱ የወንጀል ሕግ አንቀፅ 3 ይመልከቱ)::*

ክፍል አንድ
ጠቅላላ

አንቀፅ 2-ትርጓሜ

በዚህ ክፍል በርካታ ቃላትና ሐረጋት በረቂቅ ህጉ ባላቸው አገባብ መሰረት የተተረጎሙ ሲሆን የዋና ዋናዎቹ ማብራሪያ እንደሚከተለው ቀርቧል::

አንቀፅ 2 (2) “ **ኮምፒውተር ወይም የኮምፒዩተር ስርዓት**” ማለት በሶፍትዌር እና ማይክሮቺፕ ቴክኖሎጂ ላይ የተመሰረተ የዳታ ፕሮሴሲንግ፣ ክምችት፣ ትንተና፣ ስርጭት፣ ግንኙነት፣ ወይም ሌሎች ሂሳባዊ ወይም አመክንዮአዊ ተግባራትን የሚያከናውን ማንኛውም መሳሪያ ነው::

ይህም የኮምፒዩተር ስርዓት ያለ ሰው ቀጥተኛ ድጋፍ (automatic) ዲጂታል ዳታዎችን ለመተንተን፣ ለማከማቸትና ለማሰራጨት ተብለው የሚሰሩ የተለያዩ መሳሪያዎች (ሃርድዌርና ሶፍትዌር) እና መሰረተ ልማቶች የሚመለከት ሲሆን ለምሳሌ ያህልም እንደሰርቨሮች፣ ራውተሮች፣ የዳታ ማከማቻ መሳሪያዎች (storage devices) እንዲሁም እነዚህን ተክተው የሚሰሩ ተንቀሳቃስ ስልኮች እና የመሳሰሉ መሳሪያዎች ያጠቃልላል:: ከዚህም ባሻገር ኮምፒውተርን መሰረት ያደረጉ የትራንስፖርት እና የኢንዱስትሪ የቁጥጥር ስርአቶች (ለምሳሌ የኢነርጂ፣ የባቡር ኔትዎርክ፣ የአቬሽን፣ የውሃ አቅርቦት ስርዓቶች)፣ የቴሌኮሚኒኬሽን ስርዓቶች፣ የመንግስት የኢንፎርሜሽን ማኔጅሜንት ስርአቶች (ለምሳሌ ለብሔራዊ መታወቂያ የሚያገለግል ዳታ ቋት፣ የጂኦ ስፓሻል ብሔራዊ የዳታ ቋት፣ የከተሞች መሬት ኢንፎርሜሽን የዳታ ቋት፣ የኢ-ባንኪንግ (e-banking)፣ ኢ-ችሎት (e-chilot)፣ ኢ-ሄልዝ (e-health)፣ ወረዳ ኔት፣ ስኩል ኔት፣ ኢ-ታክሴሽን (e-taxation) ሥርዓቶችና አውቶሜሽኖች፣ የሳይበርና የኤሌክትሮኒክ ሚዲያ እንዲሁም ኮምፒውተርን መሰረት ያደረገ ወታደራዊ የዕዝና የቁጥጥር ሲስተሞች እና የመሳሰሉ ስርዓቶች ያጠቃልላል:: የኮምፒዩተር ስርዓት በሁሉም የረቂቅ ህጉ መሰረታዊና የስነ-ስርዓት ድንጋጌዎች ጥቅም ላይ የዋለ ሲሆን ምክንያቱም የኮምፒዩተር ስርዓት የኮምፒውተር ወንጀለኞች እንደ ኢላማና ማስፈፀሚያ እንዲሁም ለመርማሪዎች እንደ ማስረጃና የምርመራ መሳሪያ ሆኖ ስለሚያገለግል ነው:: በዚህ ንኡስ አንቀጽ በተሰጠው ትርጓሜ መሰረት የኮምፒዩተር ስርዓት ከሌሎች የቴክኖሎጂ ውጤቶች የተለየ የሚያደርጉት ቁልፍ መስፈርቶች በኮምፒዩተር ፕሮግራም (ሶፍትዌር፣ ማይክሮቺፕ ቴክኖሎጂ) ብቻ የሚሰራ መሆኑና ቀጥተኛ የሆነ የሰው ድጋፍ ሳያስፈልገው ዳታን የመቀበል፣ የማከማቸት፣ የመተንተን፣ የማሰራጨት፣ የማጓጓዝ ወይም የማስተላለፍ (የዳታ ፕሮሲንግ) አገልግሎት ለመስጠት የሚያስችል መሆኑ ናቸው::

አንቀፅ 2 (3) “የኮምፒዩተር ዳታ”፦ በዚህ ንኡስ አንቀፅ መሰረት የኮምፒዩተር ዳታ አቶማቲክ በሆነ መንገድ በኮምፒዩተር ስርዓት ሊተነተን በሚችል መልክ የሚገኝ (suitable for automatic processing) ማንኛውም ዲጂታል ኢንፎርሜሽን ሲሆን በዋናነትም **የይዘት ዳታን ፣ ትራፊክ ዳታን ፣ የኮምፒዩተር ፕሮግራምንና የደንበኞች መረጃን** ይመለከታል:: እነዚህ የኮምፒዩተር ዳታ አይነቶች የኮምፒዩተር ወንጀል ኢላማና ማስፈፀሚያ ሊሆኑ የሚችሉ እንዲሆም ለወንጀል ምርመራ ትልቅ ፋይዳ ያላቸው ናቸው::

የይዘት ዳታ (content) የዳታውን ሙሉ ትርጓሜ (substance) ወይም መልእክት የሚመለከት ሲሆን “**ትራፊክ ዳታ**” ደግሞ በኮምፒዩተር መረብ አማካኝነት የሚደረግን ግንኙነት ሰንሰለት በተመለከተ የግንኙነቱን መነሻ፣ መድረሻ፣ ዑደት፣ ጊዜ፣ መጠን ወይም የአገልግሎት ዓይነት የሚያሳይ ነው *(አንቀፅ 2(5 እና 6) ይመልከቱ)::* “ትራፊክ ዳታ” የአንድን የኮምፒዩተር ግንኙነት መነሻና መድረሻ (IP address)፣ ከየት ወዴት እንደተላከ፣ መልእክቱ/ግንኙነቱ የተጓዘባቸው መስመሮች/ኔትዎርኮች፣ ሰርቨሮች፣ ግንኙነቱ መቼና ለምን ያህል ጊዜ እንደተከናወ፣ የመልእክቱ መጠን (size)፣ የግንኙነቱ አይነት (phone, email, chat, file transfer, share, download, site visited …) እና የመሳሰሉ መረጃዎች የሚሰጥና የኮምፒውተር ስርዓት በራሱ የሚያመነጨው (computer generated) ዳታ ሲሆን አንድን ወንጀለኛ አድኖ ለመያዝ ወይም የወንጀሉን ምንጭ ለመለየት (በተለይም ራስን በመደበቅ በሚፈፀሙ ወንጀሎች ላይ) ከፍተኛ አስተዋፅኦ አለው:: ትራፊክ ዳታ በዋናነት በአገልግሎት ሰጪዎች እጅና በወንጀሉ ተጠቂ የኮምፒዩተር ስርዓት የሚገኝ ሲሆን የደህንነት ጥበቃ ካልተደረገለት በፍጥነት ሊጠፋ የሚችል የዳታ አይነት ነው::

ሌላው የኮምፒዩተር ዳታ አይነት “**የኮምፒዩተር ፕሮግራም**” ሲሆን ይህም አንድን የኮምፒዩተር ስርዓት መደበኛ ተግባሩን እንዲያከናውን ወይም የታለመለትን ውጤት እንዲያስገኝ የሚያስችልና በቃላት፣ በኮዶች ወይም በዘዴዎች የሚገለፅ የመመሪያዎች ወይም ትእዛዞች ስብስብ ነው (**አንቀፅ** 2 (4)) :: የኮምፒዩተር ፕሮግራም የተለያዩ ሶፍትዌሮችን የሚመለከት ሲሆን በአንድ በኩል ወንጀለኞች ራሳቸውን ለመደበቅ፣ ግንኙነታቸውን ሚስጢራዊ ለማድረግ፣ የተመሰጠሩ ግንኙነቶችን ለመፍታት፣ የደህንነት አጥሮችን ለመስበር፣ በኮምፒዩተር ስርዓትና ዳታ ላይ ጉዳት ለማድረስና ለመሳሰሉ ድርጊቶች የሚጠቀሙባቸው ሲሆን በሌላ በኩል ደግሞ የኮምፒውተር ወንጀሎችን ለመመርመርና ለመከታተል በስፋት ጥቅም ላይ ይውላሉ:: ስለሆነም ጠቃሚና ጎጂ የኮምፒዩተር ፕሮግራሞች አሉ ማለት ነው:: (*አንቀፅ 7 ይመልከቱ)*

አንቀፅ 2 (10) “ቁልፍ መሰረተ ልማት” ማለት በዚህ አዋጅ ከአንቀፅ 3 እስከ 6 የተመለከተውን ማናቸውም የወንጀል ድርጊት ቢፈፀምበት በህዝብ ደህንነት እና በሃገሪቱ ብሄራዊ ደህንነት ላይ ከፍተኛ ጉዳት ሊያደርስ የሚችል የኮምፒዩተር ስርዓት፣ የኮምፒዩተር ኔትዎርክ ወይም የኮምፒዩተር ዳታ ነው:: በዚህ ንኡስ አንቀፅ መሰረት የአንድ የኢንፎርሜሽን መሰረት ልማት ወይም ዳታ ቁልፍነት የሚወሰነው የሳይበር ደህንነት አደጋ ቢደርስበት ሊያስከትል በሚችለው ተፅእኖ (impact) ሲሆን በዋናነትም ፦

- የመከላከያ ወታደራዊ የእዝና ቁጥጥር ሲስተሞች፣
- የደህንነት፣ የፍትህና የፀጥታ ተቋማት ሚስጢራዊ ዳታዎችና የኢንፎርሜሽን መሰረተ ልማቶች (ኔትዎርኮች)፣
- የፋይናንስ ተቋማት ሚስጢራዊ ዳታዎችና የኮምፒዩተር ስርዓቶች (ኔትዎርኮች)፣
- መሰረታዊ የህዝብ አገልግሎት (ለምሳሌ የውሃ፣ ሃይልና መገናኛ አገልግሎቶች) ለመስጠት የሚያስችሉ የኮምፒዩተር መቆጣጠሪያ ስርዓቶች (SCADA))፣
- የትራንስፖርት ሲስተሞች (በተለይም የአየርና የባቡር ትራንስፖርት ሲስተም)፣
- የሚዲያና ኮምኒዩኬሽን ሲስተሞች፣
- የትምህርት፣ የጤና እና ከፍተኛ የምርምር ተቋማት ሲስተሞች እና የመሳሰሉትን ይመለከታል፡፡

በኢንፎርሜሽን ኮምኒዩኬሽን ቴክኖሎጂ እድገት ምክንያት በርካታ የሃገራችን ቁልፍ የመንግስትና የግል ተቋማት እርስበርሳቸው እየተሳሰሩና አውቶሜትድ እየሆኑ በመምጣታቸው ምክንያት ለበርካታ የሳይበር ደህንነት ስጋቶች የተጋለጡ ናቸው፡፡ ስለሆነም በእነዚህ የኮምፒዩተር ስርዓቶችና ዳታዎች ላይ የሚደርሱ ጥቃቶች/ወንጀሎች ከፍተኛ ቅጣት ያስከትላሉ፡፡ (*ከአንቀፅ 3-8 ይመልከቱ)*

አንቀፅ 2(13) “**አገልግሎት ሰጪ**” በኮምፒዩተር ስርዓት አማካኝነት የዳታ ፕሮሰሲግ አገልግሎት ማለትም የኮምፒዩተር ዳታን የማከማቸት፣ የመተንተን፣ የማሰራጨት፣ የማጓጓዝ ወይም የማስተላለፍ አገልግሎት እንዲሁም የኔትዎርክ አገልግሎት የሚሰጡ አካላት የሚመለከት ሲሆን በዋናነትም የኢንተርኔት አገልግሎት ሰጪዎች፣ ድረ-ገፅ ኦፕሬተሮች፣ በኢንተርኔትና መሰል ኔትዎርክ አማካኝነት የተለያዩ አገልግሎቶች የሚሰጡ አካላት፣ የሰርቨር አገልግሎት ሰጪዎች፣ ወዘተ ያጠቃልላል፡፡

ክፍል ሁለት

የኮምፒውተር ወንጀሎች

የኮምፒውተር ወንጀልን ለመከላከል ቅድሚያ መወሰድ ካለባቸው ህጋዊ እርምጃዎች አንዱ እንደ ወንጀል የሚቆጠሩ ድርጊቶችና ለእነዚህ ድርጊቶች ተገቢ የሆኑ ቅጣቶችን በግልፅ ማስቀመጥ ነው፡፡ ይህም የወንጀል ድርጊቶችን አስቀድሞ በማሳወቅ ሰዎች ይህንን አውቀው ከጥፋት እንዲቆጠቡ ማድረግና ይህንን ማስጠንቀቂያ በማይቀበሉ ሰዎች ላይ ቅጣቱን ተግባራዊ

ማድረግ ያለመ ነው፡፡ በመሆኑም በዚህ ክፍል በአህጉራዊና አለም አቀፍ ስምምነቶች እንዲሁም በአብዛኞቹ ሀገራት ህጎች ከስምምነት የተደረሰባቸውና በሃገራችን ላይም በተጨባጭ እየተፈፀሙ ያሉ መሰረታዊ (substantive) የኮምፒዩተር ወንጀሎች ተደንግጓል፡፡

ንኡስ ክፍል አንድ

በኮምፒዩተር ስርዓትና በኮምፒዩተር ዳታ ላይ የሚፈፀሙ ወንጀሎች

በተለያዩ ጥናቶችና አለም አቀፍ መድረኮች እንደተመለከተው የዲጂታል ዘመን ከወለዳቸው ቀዳሚ ስጋቶች ወይም ወንጀሎች በኢንፎርሜሽንና በኢንፎርሜሽን መሰረተ ልማት ሚስጢራዊነት፣ ተአማኒነትና ተደራሽነት ላይ የሚፈፀሙ ናቸው፡፡ እነዚህ ህገ-ወጥ ድርጊቶች በዋናነት የኮምፒዩተር ስርዓትን ወይም የኮምፒዩተር ዳታን ኢላማ የሚያደርጉ ሲሆን ከዚህም በተጨማሪ የቴክኖሎጂው እድገት የወለዳቸው አዳዲስ ወንጀሎች በመሆናቸው በስራ ላይ ባሉ ህጎች ሽፋን ያላገኙ ናቸው፡፡ በመሆኑም የኮምፒዩተር ስርዓት ወይም የኮምፒዩተር ዳታ ኢላማ የሚያደርጉ ወንጀሎች በሁሉም አለም አቀፍና ሃገራዊ ህጎች ዘንድ በክብደታቸውና በውስብስብነታቸው በቀዳሚነት የሚጠቀሱ የኮምፒዩተር ወንጀሎች ሆነዋል፡፡ የዚህ ንኡስ ክፍል አላማም እነዚህ ቀዳሚ የሳይበር ደህንነት ስጋቶችን መከላከል ሲሆን በዋናነት እነዚህ ድርጊቶች በወንጀል ሊያስቀጡ የሚችሉት ያለፈቃድ ወይም ፈቃድን ያለአግባብ በመጠቀም ሲፈፀሙ ብቻ ሲሆን የእነዚህ ቅድመ ሁኔታዎች ማብራሪያና አስፈላጊነትም እንደሚከተለው ይሆናል፡፡

“ያለፈቃድ (without right)” የሚለው አገላለፅ አንድን ድርጊት በራሱ እንደማያስቀጣ የሚያመለክት ሲሆን ይህም ማለት ውልን፣ ሕግን፣ አስተዳደራዊ መመሪያ ወይም የፍርድ ቤት ውሳኔን ወይም ሌላ ስልጣን ያለው አካል በሚሰጠው ፈቃድ ወይም አስገዳጅ ትእዛዝ መሰረት የሚፈፀሙ ድርጊቶች በኮምፒዩተር ወንጀል አያስቀጡም ማለት ነው፡፡ ከዚህም በተጨማሪ ለወንጀል ምርመራ፣ ለህዝብ ጥቅም ወይም ለብሔራዊ ደህንነት ሲባል ሕግ በሚፈቅደው መልኩ የሚከናወኑ ተግባራት በዚህ ረቂቅ አዋጅ መሰረት አያስቀጡም፡፡ ለምሳሌ ያህል የኮምፒዩተር ስርሰራ (hacking) በራሱ ላያስቀጣ ይችላል፡፡ ይህ ድርጊት በሳይበር ደህንነት ባለሙያዎችና መማሪዎች ወይም ሌሎች በተፈቀደላቸው አካላት ሊፈፀም ስለሚችል የኮምፒዩተር ስርሰራ በወንጀል ሊያስቀጣ የሚችለው ከላይ በተመለከተው መልኩ ያለፈቃድ የተከናወነ እንደሆነ ነው፡፡ ለምሳሌ ያህል እንደ የይለፍ ቃልና ሌሎች የደህንነት አጥሮችን ሰብሮ

መግባት (breaking security measures)፣ ክፍያ የሚጠይቁ የኮምፒዩተር አገልግሎቶችን ያለ ክፍያ መጠቀም እና የመሳሰሉ ድርጊቶችን መጥቀስ ይቻላል::

“ከተሰጠው ፈቃድ ውጪ” የሚለው አገላለፅ ደግሞ የተፈቀደለት ሰውም ቢሆን (ለምሳሌ የአንድ ተቋም ሰራተኛ) የተሰጠው ፈቃድ ያለአግባብ በመጠቀም ፈቃድ ከተሰጠው ተግባር ውጪ በዚህ ረቂቅ አዋጅ በወንጀልነት የተደነገጉ ተግባራት መካከል ፈፅሞ ሲገኝ ከወንጀል ተጠያቂነት እንደማያመልጥ የሚያመለክት ነው:: ለምሳሌ ያህል አንድ የባንክ የኮምፒዩተር ስርዓት የደህንነት ፍተሻ እንዲያደርግ የደራሽነት (access) ፈቃድ የተሰጠው ባለሙያ የተሰጠውን ፈቃድ ያለአግባብ በመጠቀም ሚስጢራዊ ዳታዎች የወሰደ ወይም ለሌሎች አሳልፎ የሰጠ እንደሆነ በዚህ ረቂቅ አዋጅ መሰረት በወንጀል ተጠያቂ ይሆናል ማለት ነው:: በተጨማሪም ይህ ድንጋጌ የኮምፒዩተር ወንጀል ለመመርመር በሕግ ፈቃድ የሚሰጣቸው አካላት ስልጣናቸውን ያለአግባብ በመጠቀም ከወንጀሉ ጋር ግንኙነት የሌላቸው የኮምፒዩተር ስርዓቶችን እንዳይበረብሩ እንዲሁም በኮምፒዩተር መረብ አማካኝነት የሚሰጡ አገልግሎቶችን ተጠቃሚ የሆኑ ደንበኞች ከተፈቀደላቸው የአጠቃቀም ስርዓት (terms of use) ውጪ ህገ-ወጥ ድርጊቶች እንዳይፈፅሙ ለመከላከል ያለመ ነው::

ወንጀሎቹን የሚያከብዱ ሁኔታዎች፦ በዚህ ንኡስ ክፍል የተመለከቱ የወንጀል ድርጊቶች የግለሰቦችን የኮምፒዩተር ስርዓትና ዳታ ከማጥቃት ጀምሮ ከፍተኛ የመንግስትና የህዝብ ተቋማት የኮምፒዩተር ስርዓቶችን ኢላማ ሊያደርጉ የሚችሉ ጥቃቶች ናቸው:: ስለሆነም ከቀላል እስከ በጣም ከባድ የሚባሉ የወንጀል ድርጊቶችን የተለዩ ሲሆን የቅጣት መጠናቸውም በዚህ መሰረት የተለያዩ እንዲሆኑ ተደርጓል:: እነዚህ የወንጀል ደረጃዎች በዋናነት ሶስት የማይነጣጠሉ መስፈርቶችን መሰረት በማድረግ የተለዩ ሲሆን፣ የመጀመሪያው መስፈርት የድርጊቱ ፈፃሚዎች **ፍላጎት** (motive) መሰረት ያደረገ ነው:: ይህም ማለት የኮምፒዩተር/የሳይበር ጥቃት የደረሰባቸው የኮምፒዩተር ስርዓቶችን መሰረት በማድረግ ከጥቃቱ ፈፃሚዎች ጀርባ ያለውን ፍላጎትና የተዋንያኑ አደገኝነት ማወቅ ያስችላል ማለት :: ለምሳሌ ያህል የባንኮችን የኮምፒዩተር ስርዓት ስርሰራ ላይ የተሰማሩና የግለሰቦችን ኮምፒዩተር የሚሰረስሩ ወንጀለኞች ፍላጎታቸው ፈፅሞ የተለያየ ነው:: ወይም የሁሉም ፍላጎት ገንዘብ ማግኘት ቢሆንም የተዋንያኑ አደገኝነት ወይም የወንጀለኛነት ባህሪ አንድ አይነት ክብደት ሊሰጠው አይችልም:: በተመሳሳይ መልኩ የንግድ ተቋማት ሚስጢራዊ ዳታዎችን ለመስረቅ የተሰማራና ወታደራዊ ሚስጢሮችን ለመስረቅ ወይም ወታደራዊ የኮምፒዩተር መረቦችን

ለማቋረጥ የሚሞክር ሰው አንድ አይነት ፍላጎት አላቸው ማለት አይቻልም። ሁለተኛው መስፈርት ወንጀሉ ቢፈፀም ሊያስከትል የሚችለው **የጉዳት መጠን** (impact) መሰረት ያደረገ ነው። አንዳንዶቹ የሳይበር ጥቃቶች ግለሰባዊ ወይም ተቋማዊ ጉዳት የሚያስከትሉ ሲሆን ሌሎች ደግሞ ሃገራዊ ጉዳት ሊያስከትሉ ይችላሉ። ለምሳሌ ያህል በቁልፍ የኮምፒዩተር ስርዓቶች ላይ የሚፈፀሙ ጥቃቶች በሃገሪቱ ላይ ከፍተኛ ኢኮኖሚያዊና ማህበራዊ ጉዳት የሚያስከትሉ ከዚህም አልፎ ብሔራዊ ደህንነትን ለአደጋ የሚያጋልጡ ናቸው። ለምሳሌ ያህል በአንድ ግለሰብ ወይም አነስተኛ ተቋም ድረ-ገፅ ላይ የሚፈፀም አገልግሎትን የማቋረጥ ጥቃትና በሃገሪቱ ቁልፍ የአገልግሎት መሰረተ ልማቶች መቆጣጠሪያ ስርዓት (SCADA system) ላይ የሚደርስ አገልግሎትን የማቋረጥ ጥቃት (DOS) የሚያስከትለው የጉዳት መጠን ተመሳሳይ ሊሆን አይችልም። ከዚህም በተጨማሪ በግል ኮምፒዩተርና በመንግስት እንዲሁም በንግድ ተቋማት ኮምፒዩተሮችና ዳታ ቤዞች የሚከማቸው የኢንፎርሜሽን ሃብት አንድ አይነት ዋጋ አይኖረውም። ይህም ማለት በመንግስትና በንግድ ተቋማት ዳታ ቤዞችና ኔትዎርኮች ላይ የሚደርስ ማንኛውም ጥቃት ከፍተኛ ጉዳት የሚያስከትል በመሆኑ የወንጀሉ ክብደት ያሳያል ማለት ነው።

ሶስተኛው መስፈርት **የተጋላጭነት መጠን** (vulnerability) መሰረት ያደረገ ነው። እንደሚታወቀው የኮምፒዩተር ስርዓቶችና አገልግሎቶችን ትስስር እየሰፋ በሄደ ቁጥር የሳይበር ጥቃት ተጋላጭነትም አብሮ ያድጋል። በተመሳሳይ መልኩ ይህንን የተጋጭነት ስፋት የወንጀለኞችን ቀልብ የሚስብ ሲሆን የሚያስከትለው ጉዳትም ከፍተኛ ይሆናል። ስለሆነም የአንድን የኮምፒዩተር ወንጀል ክብደትና ቅለት ከሚለካባቸው መንገዶች አንዱ የተጋላጭነት መጠን ነው። ለምሳሌ ያህል በአንድ የቁልፍ ተቋም መቆጣጠሪያ ስርዓት ላይ ጥቃት ቢፈፀም የሚያስከትለው ጉዳት ጥቃቱ በተፈፀመበት ስርዓት ብቻ የሚወሰን ሳይሆን ከዚሁ የኮምፒዩተር ስርዓት በኔትዎርክ የተሳሰሩ ሌሎች ተቋማትና መሰረተ ልማቶችም ለጥቃቱ ተጋላጭ ያደርጋቸዋል። ከዚሁ በተቃራኒ ግን በአንድ ግለሰብ የግል ኮምፒውተር በቫይረስ ቢጠቃ ሌሎች ኮምፒውተሮችን ተጋላጭ የማድረግ እድሉ ዜሮ ነው ባይባልም በተነፃፃሪነት ግን አነስተኛ ነው ማለት ይቻላል። ስለሆነም በዚህ ንኡስ ክፍል የተመለከቱ ድርጊቶች አብዛኞቹ ከላይ በተጠቀሱ መስፈርቶች መሰረት የተለያየ ክብደት የተሰጣቸው ሲሆን የድንጋጌዎቹ ሙሉ ይዘት ማብራሪያም እንደሚከተለው ቀርቧል።

አንቀፅ 3- ህገ ወጥ ደራሽነት

በረቂቅ አዋጁ አንቀፅ 2 ንኡስ አንቀፅ 9 መሰረት “ደራሽነት” ማለት ከኮምፒውተር ስርዓት ጋር ግንኙነት የመፍጠር፣ ወደ ኮምፒዩተር ስርዓቱ የመግባት፣ ዳታ የማከማቸት፣ የተከማቸን ዳታ የማግኘት፣ የማየት፣ የመውሰድ፣ የማንቀሳቀስ፣ ወደ ሌላ ማከማቻ መሳሪያ የመገልበጥ ወይም ሌላ ማንኛውም የዳታ ፕሮሰሲንግ አገልግሎትን የማግኘት ተግባር ነው፡፡ በሌላ አባባል እነዚህ አገልግሎቶችን በህገወጥ መንገድ (ያለፈቃድ) ማግኘት በዚህ ድንጋጌ መሰረት የሚያስቀጣ የወንጀል ድርጊት ሲሆን ድርጊቱ በቀጥታም ሆነ በተዘዋዋሪ እንዲሁም በተጠቂው የኮምፒዩተር ስርዓት በአካል በመገኘት ወይም በኔትዎርክ አማካኝነት ሊፈፀም ይችላል፡፡ ህገ-ወጥ ደራሽነት በኮምፒዩተር ስርዓትና ዳታ ሚስጢራዊነት፣ ተአማኒነትና ተደራሽነት ላይ ከሚፈፀሙ በርካታ የኮምፒውተር ወንጀሎች በቀዳሚነት የሚጠቀስ ሲሆን ይህም በዋናነት የኮምፒዩተር ስርዓት ስርሰራ (hackning)፣ ሰርጎገብነት (intrusion)፣ ሚስጢራዊ የይለፍ ቃልን ሰብሮ መግባት (cracking)፣ ኢስፖኔጅ እና የመሳሰሉትን ይመለከታል፡፡ ህገ-ወጥ ደራሽነት በኮምፒውተር ወንጀል ዙሪያ እስከ አሁን ከወጡ በርካታ አለም አቀፍና ሃገራዊ ህጎች ውስጥ በቀዳሚነት የተካተተ ሲሆን ይህም የሆነበት ምክንያት ለሌሎች የኮምፒውተር ወንጀሎች መንስኤ መሆኑ፣ ወንጀሉ ለመፈፀም የሚያስችሉ መሳሪያዎች (hacking tools) በቀላሉ ከኢንተርኔት ማግኘት እና ጥቃቶችን አውቶሜት ማድረግ የሚቻል መሆኑ እና ህጋዊ ተጠቃሚዎች በተለይም ባንኮችና ሌሎች አገልግሎት ሰጪዎች የኮምፒዩተር ስርዓታቸውን በፈለጉት መልኩ መቆጣጠር እንዳይችሉ የሚያደርግ መሆኑን ይገኙበታል፡፡ ከዚህም በተጨማሪ የተለያዩ ጥናቶች እንደሚያሳዩት **ወንጀሉ በዋናነት የሚፈፀመው በፋይናንስ ተቋማትና አገልግሎት ሰጪዎች እንዲሁም በተለያዩ የመንግስት ተቋማት** ላይ ነው፡፡ የዚህ ወንጀል ፈፃሚዎች የተለየየ መንገድና ቴክኒክ የሚጠቀሙ ቢሆንም (ለምሳሌ፦ social engeenering, phishing, keyloggers, spywares) ድርጊቱን እንጂ የአፈፃፀም መንገዶቹና መሳሪያዎቹ በዝርዝር መከልከል የማይቻል በመሆኑ የህጉ ድንጋጌ በድርጊቱ ብቻ ያተኩራል፡፡ ይህም ህጉ አሁን ባሉ ቴክኖሎጂዎች ላይ ብቻ ሳይሆን በቀጣይነት በሚፈጠሩ አዳዲስ ቴክኖሎጂዎች ወይም መሳሪያዎች ላይም ተፈፃሚ እንዲሆን ያደርገዋል፡፡ ይህ ወንጀል በማንኛውም የኮምፒዩተር ስርዓት ወይም ዳታ ላይ ሊፈፀም የሚችል ቢሆንም የወንጀሉ ክብደት ግን ከላይ በተገለፁት መስፈርቶች ምክንያት (motive, impact, vulnerability) የተለያየ ነው፡፡ በመሆኑም በዚህ አንቀጽ ንኡስ አንቀፅ (1) መሰረት ማንኛውም ህገ-ወጥ ደራሽነት እንደ ጉዳዩ ሁኔታ ከሶስት 垸

ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር 30,000 ሺህ እስከ ብር 50,000 ሺህ በሚደርስ መቀጮ ወይም በሁለቱም የሚያስቀጣ ነው። በሕግ የሰውነት መብት በተሰጣቸው ተቋማት (የመንግስትም ሆነ የግል) የኮምፒዩተር ስርዓቶች ላይ የሚፈፀም ከሆነ ደግሞ ከሶስት ዓመት እስከ አምስት ዓመት በሚደርስ ፅኑ እስራት እና ከብር 50,000 ሺህ በማይበልጥ መቀጮ የሚያስቀጣ ሲሆን ምክንያቱም ከሚይዙት የዳታ ብዛትና የሚስጢራዊነት ደረጃ፣ ከሚሰጡት አገልግሎት እንዲሁም ጥቃቱ ከሚያስከትለው ሰፊ ጉዳት አንፃር ነው። ለምሳሌ ያህል የአንድ ተቋም ድረ-ገፅ ቢጠቃ (hack ቢደረግ) ከሚደርሱ በርካታ ጉዳቶች መካከል የሚከተሉትን መጥቀስ ይቻላል።

- በድረ-ገፁ አማካኝነት የሚሰጡ አገልግሎቶች ሊቋረጡ ይችላሉ፤
- የድረ-ገፁ ሰርቨር በአጥቂዎቹ ቁጥጥር ስር ሊውልና እነሱ በሚፈልጉት መልኩ ሊያሰሩት ይችላሉ፤
- በሰርቨሩ ውስጥ የተከማቹና በልዩ መብት (privillage) ብቻ ሊገኙ የሚችሉ ሚስጢራዊ የተቋሙና የተገልጋዮች ዳታዎችና የኢሜል መልእክቶች ማግኘትና መጠቀም ይችላሉ፤
- ከተቋሙ ፍላጎት ተቃራኒ የሆኑ መልእክቶች (የወንጀለኞቹ አጀንዳ) በድረ-ገፁ አማካኝነት እንዲሰራጭ ያደርጋሉ፤
- የድረ-ገፁ ተጠቃሚዎች ሚስጢራዊ ዳታዎች ማግኘት ወይም ማጋለጥ ይችላሉ፤
- የተቋሙን የኢሜል አድራሻዎች በመጠቀም ከሚፈልጉት አካል ግንኙነት መፈፀም ይችላሉ፤
- ድረ-ገፁን በሚጎበኙ ተጠቃሚዎች የኮምፒዩተር ስርዓቶች ላይ ጉዳት ሊደርስ ይችላል፤
- ድረ-ገፁ በአለም አቀፍ የሳይበር ደህንነት ተቋማት የስጋት ዝርዝር ውስጥ (blacklist) ሊገባ ይችላል፤

እንዲሁም በእነዚህ ድርጊቶች ምክንያት የተቋሙ ስም ይጠፋል፣ የአገልግሎቱ ተጠቃሚዎች አመኔታ ያጣሉ/ይሸሻሉ፣ ከጥቃቱ ለማገገም ለበርካታ ወጪዎች (recovery cost) ይዳረጋል። ከዚህም በተጨማሪ በጥቃቱ ምክንያት የሚደርሰው የገንዘብ ኪሳራና ሌሎች ጉዳቶች (operational risk) መገመት ይቻላል። ይህ ወንጀል በቁልፍ መሰረተ ልማቶች ላይ ቢፈፀም ጉዳቱ እጅግ ሰፊ በመሆኑ ቅጣቱ ከሆነ ከአምስት እስከ አስር ዓመት የሚደርስ ጽኑ እስራት እና ከብር 50,000ሺህ እስከ ብር 100,000 ሺህ በሚደርስ መቀጮ እንዲሆን ተደርጓል። (አንቀፅ 3(2) ለ)

አንቀፅ 4- ህገ-ወጥ የዳታ ጠለፋ

በአንቀፅ 2 ንኡስ አንቀፅ (11) ላይ እንደተመለከተው “ጠለፋ” ማለት በኮምኒዩኬሽን ሂደት ላይ ያለን የኮምፒዩተር ዳታ ወይም የዳታ ፕሮሰሲግ አገልግሎት መከታተል፣ መቅዳት፣ ማዳመጥ፣ መውሰድ፣ ማየት፣ መቆጣጠር ወይም ሌላ ተመሳሳይ ተግባር ነው። በሌላ አባባል ህገ-ወጥ የዳታ ጠለፋ የሚባለው በኮምፒዩተር ስርዓት ማለትም በተለያዩ ኔትዎርኮችና በኢንተርኔት አማካኝነት ግንኙነት ወይም የዳታ ዝውውር ወይም ሌላ ማንኛውም እንቅስቃሴ በሚደረግበት ወቅት ካለባለቤቱ ወይም ሌላ ስልጣን ካለው አካል ፈቃድ ውጭ እነዚህ ዳታዎችን (የዳታው ይዘት፣ ትራፊክ ዳታ፣ የደንበኞች መረጃ፣ የኮምፒዩተር ፕሮግራሞች እና መሰል መረጃዎች) በቀጥታ መከታተል፣ መቅዳት፣ ማዳመጥ፣ መውሰድ፣ ማየት፣ መቆጣጠር ወይም ሌላ ተመሳሳይ ተግባር ነው። ይህ ወንጀል እንደ ኤሌክትሮኒክ፣ ሜካኒካል፣ ኦፕቲካል፣ ኤሌክትሮ-ሜካኒካል እና የመሳሰሉ ፊዚካልና ሎጂካል መንገዶች ወይም መሳሪያዎች እንዲሁም የተለያዩ የስለላ ሶፍትዌሮችን በመጠቀም የሚፈፀም ሲሆን የንግድ ተቋማትና የመንግስት ሚስጢሮችን እንዲሁም የአእምሮ ንብረቶችን በመመዝበር በኮምፒዩተር ዳታ ሚስጢራዊነት ከሚፈፀሙ የኮምፒዩተር ወንጀሎች በቀዳሚነት የሚጠቀስ ነው። ከዚህም በተጨማሪ ህገ-ወጥ ጠለፋ ሰዎች እንደ ኢሜልና የመሳሰሉ መረጃዎች በሚለዋወጡበት ወይም ለማንኛውም ዓላማ ኢንተርኔት በሚጠቀሙበት ወቅት በስፋት የሚፈፀም ወንጀል በመሆኑ በሰዎች የግላዊነት መብቶች (privacy) እና በተያያዥ ሕገ መንግስታዊ መብቶች ላይ ከሚፈፀሙ የኮምፒዩተር ወንጀሎች በቀዳሚነት የሚጠቀስ ነው። የዚህ ድንጋጌ አላማም እንደዚህ አይነቱ ህገ ወጥ ድርጊት መከላከል ሲሆን በዚህ አንቀፅ መሰረት የኮምፒዩተር ዳታ ጠለፋ በወንጀል ሊያስጠይቅ የሚችላው፦

- ድርጊቱ ያለፈቃድ ወይም ፈቃድን ያለአግባብ በመጠቀም የተፈፀመ ከሆነ (ህግ ወይም ስምምነት በሚፈቅደው መንገድ የሚደረጉ ጠለፋዎች በወንጀል አያስቀጡም። ለምሳሌ ያህል የኮምፒውተር ወንጀልን ለመከላከልና ለመቆጣጠር በህግ አስፈፃሚዎች ወይም መርማሪዎች ህጉ በሚፈቅደው መሰረት የሚደረጉ ጠለፋዎች፣ የኮምፒዩተር አገልግሎት ሰጪዎች ከደንበኞቻቸው በሚያገኙት ፈቃድ ወይም በተለመዱ የንግድ አሰራሮች መሠረት (ለምሳሌ-cookies) የሚደረጉ የኮምፒዩተር ዳታ ጠለፋዎች በወንጀል አያስጠይቁም)

- ድርጊቱ የተፈጸመው ሆን ተብሎ (intentionally) መሆን አለበት። ምክንያቱም የኮምፒዩተር ዳታ ጠለፋ የተለያዩ መሳሪያዎችና ቴክኒካዊ መንገዶች በመጠቀም የሚፈፀምና እውቀት የሚጠይቅ ድርጊት በመሆኑ በስፋት የሚፈፀመው በታቀደ አኳሃን በመሆኑ ነው። የኮምፒዩተር ዳታ ጠለፋ በቸልተኝነት ፈፅሞ ሊከናወን አይችልም ባይባልም የኮምፒዩተር አጠቃቀም በአግባቡ ባልዳበረበትና ባልተስፋፋበት ሁኔታ በቸልተኝነት የሚፈፀሙ ስህተቶች በወንጀል ማስቀጣቱ ከጥቅሙ ጉዳቱ ስለሚያመዝን ነው።
- የተጠለፈው የኮምፒዩተር ግንኙነት ይፋዊ ያልሆነ (non-public) መሆን አለበት። ይህ መስፈርት የግንኙነቱ አይነት እንጂ የዳታው ይዘት አይመለከትም። ይህም ማለት የዳታው ይዘት ሚስጢራዊም ሆነ ማንም ሰው የሚያውቀው፤ ሚስጢራዊ በሆነ መንገድ እስከተሰራጨ ድረስ በህግ ጥበቃ ሊያገኝ ይገባል። ለምሳሌ ያህል ማንኛውም ሰው ሊያውቀው የሚችል መረጃ/ዳታ ከአንድን ግለሰብ ወይም ተቋም የኢሜይል አድራሻ መጥለፍ ዳታው ሚስጢራዊ ባለመሆኑ ብቻ ከተጠያቂነት አያድንም። ሚስጢራዊ በሆነ መንገድ (በኢሜይል) እስከተሰራጨ ድረስ ከህገ ወጥ ጠለፋ መጠበቅ አለበት። በሌላ አገላለፅ ይፋዊ የሆኑ የኮምፒዩተር ግንኙነቶች መጥለፍ በዚህ አንቀፅ መሰረት አያስቀጣም ማለት ነው (ለምሳሌ paltalks, public chatrooms, discussion forums)። ስለሆነም ዋናው መስፈርት የግንኙነቱ ሚስጢራዊነትን እንጂ የዳታው ሚስጢራዊነት አይደለም። ይህም ማለት ሚስጢራዊ ያልሆነን ዳታ ይፋዊ ካልሆነ የኮምፒዩተር ግንኙነት መጥለፍ የቅጣቱ መጠን ያቀለዋል እንጂ ከተጠያቂነት አያድንም እንዲሁም ሚስጢራዊ ይዘት ያለውን ዳታ መጥለፍ ነገሩ ከባድ ያደርገዋል ማለት ነው። በዚህ መሰረትም በተቋም ደረጃ የሚደረጉ የኮምፒዩተር ግንኙነቶች በግለሰብ ደረጃ ከሚደረጉ የኮምፒዩተር ግንኙነቶች የበለጠ የሚስጢራዊነት ደረጃ ይኖራቸዋል እንዲሁም በቁልፍ መሰረተ ልማቶች ደረጃ የሚደረጉ ግንኙነቶች እጅግ ሚስጢራዊ መሆናቸው አይቀርም። ስለሆነም የወንጀሉ ክብደት በሶስተ ደረጃ እንዲከፈል ተደርገል *(ንኡስ አንቀፅ 1-3 ያለውን ይመልከቱ)*።

አንቀፅ 5- በኮምፒዩተር ስርዓት ላይ ጣልቃ መግባት

በዚህ አንቀጽ ንኡስ አንቀፅ (1) ላይ እንደተመለከተው በኮምፒዩተር ስርዓት ላይ ጣልቃ መግባት (interference) ሲባል የኮምፒዩተር ስርዓት ወይም ኔትወርክን መደበኛ ተግባርን

ማደናቀፍ፣ ማወክ ወይም አገልግሎቱን ማቋረጥ የሚያካትት ሲሆን የተለያዩ አላስፈላጊ ዳታዎችን በማስገባት፣ ወደ ኮምፒውተር ስርዓቱ በማሰራጨት ወይም ያለውን ዳታ በማጥፋት፣ በመለወጥ ወይም ሌላ ማንኛውም ጉዳት በማድረስ የሚፈፀም ነው። ስለሆነም ጣልቃ ገብነት የኮምፒዩተር ስርዓትን በአላስፈላጊ ዳታ ፍሰት በማጨናነቅ፣ የተለያዩ ኮምፒውተር ቫይረሶች፣ ማልዌሮች፣ ዎርሞችና የመሳሰሉ ፕሮግራሞች በማሰራጨት አንድን የኮምፒዩተር ስርዓት ስራውን በአግባቡ እንዳይወጣ ወይም ጨርሶ እንዲያቆም በማድረግ በተደራሽነት ላይ የሚፈፀም ከባድ የኮምፒውተር ወንጀል ነው። የዚህ ድንጋጌ አላማም የኮምፒዩተር ስርዓቶች እንደ ማንኛውም ሃብት ሆነ ተብለው ከሚደርሱ ጥቃቶች መጠበቅና በኮምፒዩተር ስርዓት አማካኝነት የሚሰጡ አገልግሎቶች እንዳይቋረጡ ወይም ለሌላ ማንኛውም አደጋ እንዳይጋለጡ መጠበቅ ነው። ይህ ወንጀል ለከፍተኛ ኪሳራ የሚዳርግና የኮምፒዩተር አገልግሎትና አጠቃቀም ላይ አመኔታ የሚያሳጣ በመሆኑ በከባድነቱ በቀዳሚነት ይጠቀሳል። ከዚህም አልፎ ይህ ወንጀል ከግል የኮምፒዩተር ስርዓቶች ጀምሮ በተለያዩ የመንግስትና የንግድ ተቋማት እንዲሁም በቁልፍ መሰረተ ልማቶች ላይ የሚፈፀም በመሆኑ ይህንን ግምት ውስጥ ባስገባ መልኩ ረቂቅ አዋጁ ተዘጋጅቷል።

አንቀፅ 6-በኮምፒዩተር ዳታ ላይ ጉዳት ማድረስ

በአንቀፅ 2 (3) ላይ እንደተገለፀው “የኮምፒዩተር ዳታ” ማለት በኮምፒዩተር ስርዓት አማካኝነት ሊተነተን የሚችል ማንኛውም የኮምፒዩተር ዳታ ይዘት፣ ዳታ ትራፊክ፣ የኮምፒዩተር ፕሮግራም፣ የደንበኞች መረጃ ወይም ሌላ ማንኛውም ኢንፎርሜሽን ነው። የኢንፎርሜሽን ኮምኒዩኬሽን ቴክኖሎጂ ፈጣን እድገት ተከትሎ አብዛኞቹ ተቋማት (የንግድ፣ አስተዳደራዊ እና ሲቪል) በኮምፒዩተር ዳታ ትንተና (data processing) ላይ ጥገኛ እየሆኑ በመምጣታቸውና ለዚህ የሚያገለግሉ እጅግ በርካታ ዳታዎችም በኤሌክትሮኒክ መሳሪያዎች ውስጥ ስለሚከማቹ፤ የኮምፒዩተር ዳታን ኢኮኖሚያዊና ኦፕሬሽናል ዋጋ ከፍተኛ ደረጃ ላይ የደረሰ ሲሆን በሌላ በኩል ደግሞ በእነዚህ ዳታዎች ላይ የሚደርስ የመጥፋት፣ የመቀየር፣ የመፋለስ ወይም ሌላ ማንኛውም ጥቃት እጅግ ከፍተኛ ጉዳት እንደሚያስከትል ለማንም ግልፅ ነው። በተለይም ደግሞ በቁልፍ የቢዝነስ፣ የህዝብ አገልግሎትና አስተዳደር ተቋማት የኮምፒዩተር ዳታና ሶፍትዌሮች ላይ የሚደርስ ማንኛውም ጥቃት ለሃገሪቱ ኢኮኖሚያዊና ማህበራዊ ደህንነት ከፍተኛ ስጋት ሊሆን እንደሚችል መገንዘብ ያስፈልጋል። በመሆኑም የኮምፒዩተር ዳታ ከማንኛውም መሰረተ ልማት ወይም ሃብት በበለጠ የወንጀል ኢላማ እየሆነ መጥቷል። ይህንን

አላማ ለማሳካትም በዋናነት እንደ ኮምፒውተር ቫይረሶችና ዎርሞች እንዲሆም የኮምፒዩተር ዳታን ከጥቅም ውጪ ሊያደርጉ የሚችሉ የለያዩ የረቀቁ ቴክኖሎጂዎችና ሶፍትዌሮች (logic bomb, time bomb, crash programs) ጥቅም ላይ ይውላሉ፡፡

በኮምፒዩተር ዳታ ሙሉዕነት፣ ትክክለኛነትና ተደራሽነት ላይ የሚደርሱ ጥቃቶች በዋናነት ሁለት አላማዎች ይኖራቸዋል፡፡ የመጀመሪያው አላማ (intention) የዳታው ሙሉዕነት ወይም ትክክለኛነት በመቀየር ወይም በማፋለስ የተለያዩ የማጭበርበርና የማታለል ወንጀሎች (በዋናነት ኢኮኖሚያዊ መነሻ አላቸው) ለመፈፀም ሲሆን በአንቀፅ 9 እና 10 ላይ ባሉ ድንጋጌዎች የሚገዛ ይሆናል፡፡ ይህንን አላማ አድርገው የሚነሱ ሰዎች በኮምፒዩተር ዳታ ላይ ጉዳት ማድረስ የመጨረሻ ግባቸው ሳይሆን ሌላ ህገ ወጥ ተግባር ለማከናወን የሚጠቀሙበት መንገድ ነው፡፡ ሁለተኛው አላማ ደግሞ ሌላ ወንጀል ለመፈፀም ሳይሆን እንዲሁ ዳታውን የመጉዳት ወይም የማውደም አላማ ያለው ድርጊት ነው፡፡ በዚህ ህገ ወጥ ድርጊት የሚሰማሩ ሰዎች መነሻቸው ፖለቲካዊ፣ አይዲዮሎጂያዊ፣ ቂም በቀል ወይም የሕዝብን ቀልብ መሳብ ሊሆን ይችላል፡፡ ለምሳሌ ያህል በስራቸው የተከፉ ወይም ከስራ ገበታቸው የተባረሩ ሰራተኞች ቂም በቀላቸውን ለመወጣት በአሰሪ ተቋማት የኮምፒዩተር ዳታዎች ላይ የሚፈፅሙት ጥቃት እንዲሁም ሽብርተኞችና አክቲቪስቶች የአለም ህብረተሰብን ቀልብ ለመሳብ (በተለይም anonymous በሚል ስም የሚታወቁት ቡድኖች) በትላልቅ ዳታ ቤዞች ላይ የሚያደርሱት ውድመት መጥቀስ ይቻላል፡፡ ስለሆነም የወንጀለኞቹ ግብ ዳታውን ከማውደም፣ መቀየር ወይም ተደራሽ እንዳይሆን ከማድረግ የዘለለ ሌላ ማግኘት የሚፈልጉት ኢኮኖሚያዊ ጥቅም የለም ማለት ነው፡፡ ስለሆነም የድንጋጌው ዋና አላማ በኮምፒዩተር ዳታ ሙሉእነት (integrity) እና ትክክለኛነት ላይ የሚደርሱ ህገ ወጥ ድርጊቶች/ጥቃቶች መከላከል ነው፡፡

አንቀፅ 7- ከኮምፒውተር መሳሪያና ዳታ አጠቃቀም ጋር የተያያዙ ህገ-ወጥ ድርጊቶች

ከአንቀጽ 3 እስከ 6 የተጠቀሱትና በኮምፒዩተር ስርዓትና ዳታ ሚስጢራዊነት፣ ተአማኒነትና ተደራሽነት ላይ የሚያነጣጥሩ ወንጀሎች ለመፈፀም የተለያዩ የኮምፒዩተር መሳሪያዎችና ሶፍትዌሮች (ለምሳሌ hacking tools) መጠቀምን ይጠይቃል፡፡ ለምሳሌ የጠለፋ ወንጀል ለመፈፀም ለዚሁ የሚያገለግሉ ሶፍትዌሮችና ሃርድዌሮች ጥቅም ላይ ይውላሉ፡፡ ስለሆነም ለእንደዚህ አይነት ህገ-ወጥ ድርጊት ማስፈፀሚያ የሚውሉ መሳሪያዎችና የኮምፒዩተር ፕሮግራሞች ጥቅም ላይ ከመዋላቸው አስቀድሞ ወይም ከምርትና ዝግጅት ሂደታቸው ጀምሮ መከላከልና መቆጣጠር ያስፈልጋል፡፡   በዚህ መሰረትም አንቀጽ 7 ንኡስ አንቀጽ (1)

በኮምፒውተር ስርዓትና ዳታ ጉዳት የሚያደርሱ ፕሮግራሞችን ማሰራጨት የሚከለክል ሲሆን በዋናነትም እንደ ኮምፒውተር ቫይረሶችና የተለያዩ ማልዌሮች ማሰራጨትን የሚመለከት ነው::

ከዚህ በተጨማሪም የኮምፒውተር ወንጀሎች ማስፈፀሚያ አላማ ተብለው የሚመረቱ የኮምፒዩተር መሳሪያዎችን ወይም የኮምፒዩተር ፕሮግራሞችን ወደ ሃገር ውስጥ ማስገባት፣ ማምረት፣ ማከፋፈል፣ መሸጥ ወይም ሌሎች እንዲያገኙ በአንቀፅ 7 ንኡስ አንቀፅ (2) መሰረት በወንጀል የሚያስጠይቅ ሲሆን ህገ-ወጥ የኮምፒውተር ሃርድ ዌሮችንና ሶፍትዌሮችን ይመለከታል:: ለምሳሌ ያህል ለኮምፒውተር ስርሰራ የሚያገለግሉ ሶፍት ዌሮች (hacking tools) እና ሚስጢራዊ ዳታዎችን ማንበብ የሚያስችሉ ሃርድዌሮች (card reader) መጥቀስ ይቻላል::

ነገር ግን ለወንጀል ማስፈፀሚያ ብቻ ስለሚውል ማንኛውም መሳሪያ ወይም ፕሮግራም የሚከለከል ከሆነ በዘርፉ ለሚሠሩ የጥናትና ምርምር ስራዎች (innovation) ማነቆ እንዳይሆን መጠንቀቅ ያስፈልጋል:: ስለሆነም ለወንጀል ማስፈፀሚያ ሊውል የሚችል መሳሪያ ወይም ፕሮግራም በሙሉ መከልከል አለበት ማለት አይደለም:: ስለሆነም አንቀፅ 7 (2) በወንጀል ሊያስቀጣ የሚችለው፦

- የኮምፒዩተር መሳሪያው ወይም ፕሮግራሙ ከአንቀፅ 3-6 ላይ የተጠቀሱትን ድርጊቶች ማስፈፀሚያ (በህገወጥ መንገድ ደራሽነት ለማግኘት፣ ለጠለፋ፣ ወዘተ) ተብሎ የተሰራ ወይም የተሻሻለ እንደሆነ፤ እንዲሁም
- መሳሪያዎቹ ወይም ፕሮግራሞቹ ለእነዚህ ወንጀሎች ማስፈፀሚያ እንደሚውሉ በማወቅ የተመረቱ፣ የተሸጡ፣ የተከፋፈሉ፣ ወዘተ እንደሆነ ብቻ ነው:: ይህም ማለት መሳሪያዎቹ በአንቀፅ 3-6 ላይ የተጠቀሱትን ድርጊቶች ማስፈፀሚያ ተብለው የተሰሩ ቢሆኑም እንዲሁ እነዚህ መሳሪያዎች ማምረት፣ መሸጥ፣ ወደ ሃገር ውስጥ ማስገባት፣ ወዘተ በራሱ በወንጀል አያስቀጣም:: ምክንያቱም ለተለያዩ የደህንነት ፍተሻ ስራዎች (security test)፣ ለጥናትና ምርምር፣ ለወንጀል ምርመራ፣ ወዘተ ተብለው ሊመረቱ፣ ሊሸጡ፣ ወደ ሃገር ውስጥ ሊገቡ ስለሚችሉ:: እነዚህ መሳሪያዎች ማምረት፣ መሸጥ፣ ወዘተ በወንጀል የሚያስቀጣው የመሳሪያዎቹ ተጠቃሚዎች አላማ (intention) ወንጀል ለመፈፀም እስከሆነ ድረስ ብቻ ነው:: ለምሳሌ ያህል የኮምፒዩተር ቫይረስ በራሱ ጎጂ ፕሮግራም ቢሆንም ለተለያዩ አላማዎች ሊመረት ይችላል:: ይህም ማለት አንዱ ለጥናትና ምርምር ብሎ ሊያመርተው ይችላል ሌላውም የተለያዩ ወንጀሎችን ለመፈፀም

በማሰብ ሊያመርተው ይችላል፡፡ በመሆኑም በዚህ አንቀፅ ንኡስ አንቀፅ (2) መሰረት በወንጀል የሚጠየቀው የኮምፒዩተር መሳሪያውን ወንጀል ማስፈፀሚያ እንደሚውሉ እያወቀ ያመረተ፣ የገዛ፣ ወደ ሃገር ውስጥ የሚያስገባ ሰው ብቻ ነው፡፡

አንቀፅ 7 (4) የኮምፒዩተር ስርዓትን ደራሽነት ማግኘት የሚያስችሉ የኮምፒዩተር ፕሮግራሞች፣ የሚስጥር ኮዶች፣ ቁልፎች፣ የይለፍ ቃሎች ወይም ሌላ መሰል ዳታዎችን ለማስተዳደር ወይም ለመጠቀም ስልጣን ወይም ፈቃድ የተሰጣቸው ሰዎችን የሚመለከት ሲሆን ዋና አላማውም እነዚህ ውስጥ አዋቂዎች (insiders) ከወንጀል ፈፃሚዎች ጋር በመተባበር ወይም በመመሳጠር የሚፈፅሟቸው ህገ-ወጥ ድርጊቶች መቆጣጠር ነው፡፡ የተለያዩ ጥናቶች እንደሚያመለክቱት በኮምፒዩተር ስርዓትና ዳታ ሚስጢራዊነት፣ ተአማኒነትና ተደራሽነት ላይ ከሚፈፀሙ ጥቃቶች 70% የሚሆኑት በውስጥ አዋቂዎች ተባባሪነት ይፈፀማሉ፡፡ ስለሆነም አንቀፅ 7 (4) የአንድን የኮምፒዩተር ስርዓት ሚስጢራዊ አጠቃቀም ወይም አሰራር የሚያውቁ ሰዎች ማለትም የህግ ወይም የውል ግዴታ ያለባቸው ሰዎችና ዳታ አድሚኒስትሬተሮች ግዴታን፣ ደንብን ወይም ለጥንቃቄ አስፈላጊ የሆኑትን ድንጋጌዎች በመጣስ እና ከውጭ አካላት በመተባበር የሚፈፅሚችው ህገ-ወጥ ድርጊቶች ለመከላከል ያግዛል፡፡

ንኡስ ክፍል ሁለት

በኮምፒዩተር አማካኝነት የሚፈፀሙ የማጭበርበር፣ የማታለልና የስርቆት ወንጀሎች

በመግቢያው ላይ እንደተገለፀው የሳይበር ምህዳር ለአዳዲስ ወንጀሎች መፈጠር ብቻ ሳይሆን ነባር/መደበኛ ወንጀሎችም በአዲስና ውስብስብ በሆነ መንገድ እንዲፈፀሙ አስችሏል፡፡ በተለይም አሁን ባለንበት የኢንፎርሜሽን ዘመን ኢንተርኔት ትልቁ የአለም አቀፍ ንግድ ማዕከል ሆኗል፡፡ ሃገራችንም የኤሌክትሮኒክ ንግድ እንቅስቃሴ እንዲሁም የመረጃ መረብን መሰረት ያደረጉ የተለያዩ የፋይናንስ አገልግሎቶች በመስፋፋት ላይ በመሆናቸው ወደዚህ አይነቱ የፋይናንስና የግብይት ስርዓት እየተቀላቀለች መሆኗ የሚያሳይ ነው፡፡ ታዲያ ይህንን የሚያውቁ ወንጀለኞች በየቀኑ በኮምፒዩተር መረብ የሚንቀሳቀሰውን ገንዘብ ለመመዝበር ቢቋምጡና ሌት ተቀን ቢደክሙ የሚያስገርም አይሆንም፡፡ በመሆኑም በየትኛውም የአለማችን ክፍል ያሉ ማፍያዎችና የተደራጁ ወንጀለኞች ፊታቸውን ሙሉ በሙሉ ወደ ሳይበር አለም አዙረዋል፡፡ ይኸውም ማንነታቸው ሳይጋለጥና ያለምንም ስጋት፣ ብዙ ሳይደክሙ እና ወጪ ሳያወጡ በኮምፒዩተር መረብ የሚንቀሳቀሰውን ገንዘብ በቀላሉ መመዝበርና መክበር የሚያስችላቸው በመሆኑ ነው፡፡

የዚህ ንኡስ ክፍል አላማም በኢንተርኔት፣ በከባቢያዊ ኔትዎርኮች እና ተያያዥ ቴክኖሎጂዎች አማካኝነት በሚደረጉ የንግድና የፋይናንስ አገልግሎቶች ላይ የሚፈፀሙ ወንጀሎችን እንዲሁም በኢንተርኔትና መሰል ቴክኖሎጂዎች ተጠቃሚዎች ላይ የሚፈፀሙና ከጊዜ ወደ ጊዜ እየተስፋፉ የመጡ የተለያዩ የማታለልና የማጭበርበር ወንጀሎችን መከላከል ነው፡፡

አንቀፅ 9- የኮምፒዩተር ዳታን ወደ ሃሰት መለወጥ

ሰነዶችን ወደ ሃሰት መለወጥ የተለመደ የወንጀል አይነትና በነባር የህግ ማዕቀፎችም የተደነገገ ቢሆንም በአንድ በኩል ነባሮቹ ህጎች ኤሌክትሮኒክ ዳታዎች (በተለይም በማሽን የሚነበቡ) የማይመለከቱ በመሆናቸው በሌላ በኩል ደግሞ በዚህ በዲጂታል ዘመን አብዛኞቹ ግለሰቦችን፣ ተቋማትንና መንግስታትን የሚመለከቱ ሰነዶች ወደ ኤሌክትሮኒክ/ዲጂታል መልክ በመቀየራቸው ምክንያት ወንጀሉ እጅግ ውስብስብና ሰፊ የህግ ክፍተት የሚታይበት ሆኗል፡፡ ይህ የሆነበት ምክንያትም በአንድ በኩል ከዋናው ሰነድ (orginal document) በፍፁም መለየት በማይቻልበት መልኩ የሃሰት ሰነዶችን (ለምሳሌ የክፍያና የATM ካርዶች) ለመስራት የሚያስችሉ የረቀቁ የቴክኖሎጂ ውጤቶች መስፋፋታቸው ሲሆን በሌላ መልኩ ደግሞ የህግ አስፈፃሚ አካላትና መርማሪዎች እነዚህን በረቀቀ ቴክኒካዊ መንገድ ወደ ሃሰት የሚለወጡ ኤሌክትሮኒክ ሰነዶችና ዳታዎች ማረጋገጥ የሚያስችል አቅም፣ ቴክኖሎጂና መሰረተ ልማት በበቂ ሁኔታ አለመታጠቃቸው ነው፡፡

ከዚህም ሌላ በሰነድ መልክ ሊገለፁ የማይችሉ የኮምፒዩተር ዳታዎች (አብዛኞቹ የኮምፒዩተር ዳታዎች በአሃዛዊ ቀመሮች የሚገለፁ ናቸው) ለተለያዩ የማጭበርበር ድርጊቶች በሰፊው የተጋለጡ በመሆናቸው ትክክለኛነታቸውና ተአማኒነታቸው ማስጠበቅ የሚያስችል የህግ ማእቀፍ ያስፈልጋል፡፡ በዚህ አንቀፅ የተመለከተው የወንጀል ድርጊት በዋናነት የዳታውን ትክክለኛነት ወይም የዳታውን ባለቤት በመቀየር (ከትክክለኛው ስው የተላከ በማስመሰል) የሚገለፅ ሲሆን እንደ ‘phishing’ ያሉ ቴክኒኮች በመጠቀምና ሃሰተኛ ድረ-ገፆች በማዘጋጀት ሊፈፀም ይችላል፡፡ ስለሆነም የዚህ ህግ አላማ በስራ ላይ ባሉ ህጎች ከሳይበር ቴክኖሎጂ እድገት ጋር ተያይዞ የተከሰቱ የህግ ክፍተቶች መሙላት እንጂ አዲስ ወንጀል መፍጠር አይደለም፡፡ እንዲሁም በዚህ ድንጋጌ ጥበቃ የተደረገለት ጥቅም (interest) ህጋዊ ውጤት ወይም ተጠያቂነት የሚያስከትሉ ግንኙነቶችን የሚመለከቱ ኤሌክትሮኒክ ዳታዎች ወይም ሰነዶች ደህንነትና ተአማኒነት ወይም ትክክለኛነት ነው፡፡ ስለሆነም የህግ ውጤት ያላቸውን

የምፒውተር ዳታዎችን ወደ ሃሰት መለወጥ፣ የህግ ውጤት ያላቸው ሃሰተኛ ዳታዎች ማዘጋጀት እንዲሁም በእነዚህ መገልገል በዚህ አንቀጽ መሰረት የሚያስቀጣ ወንጀል ሆኗል።

አንቀፅ 10- በኮምፒዩተር አማካኝነት የሚፈፀም የማታለል ወንጀል

የኢንተርኔት መስፋፋትና አለም አቀፍ ተደራሽነት ተከትሎ የተለያዩ የማታለል ወንጀሎች የሚፈፅሙ ግለሰቦች ወይም ቡድኖች ሚሊዮኖችን ባሉበት የሚደርሱበት እድል ፈጥሮላቸዋል። በመሆኑም በኮምፒዩተር በተለይም በኢንተርኔት አማካኝነት የሚፈፀም የማታለል ወንጀል በኤሌክትሮኒክስ ንግድ ላይ ከሚፈፀሙ ወንጀሎች በቀዳሚነት የሚጠቀስ ሆኗል። በኮምፒዩተር አማካኝነት የማታለል ወንጀሎች ከሚፈፀምባቸው የኢኮመርስ ዘርፎች የሚከተሉትን በዋናነት የሚጠቀሱ ናቸው።

- በመረጃ መረብ አማካኝነት የሚደረግ ጨረታ (ለምሳሌ- የሌሉ ዕቃዎችን እንዳሉ አድርጎ በማቅረብ፣ ከሚፈለገው የጥራት ደረጃ የወረዱ ዕቃዎች በማቅረብ፣ የሌላ ሰውን ዕቃ የራስ አድርጎ በማቅረብ፣ የጨረታ መስፈርት ሳያሟሉ ለውድድር በመቅረብ፣ ወ.ዘ.ተ.)፤
- በመረጃ መረብ አማካኝነት የሚደረግ የባንክ አገልግሎት፤
- ኤሌክትሮኒክ ንግድ (በመረጃ መረብ አማካኝነት የሚደረግ የንግድ ልውውጥ ሻጭና ገዥ ሳይተዋወቁና በአካል ሳይገናኙ የሚፈፀም በመሆኑ ለዚህ ወንጀል የተጋለጠ ነው)፤
- የተጭበረበሩ የኢንቨስትመንት ማስታወቂያዎች (የተለያዩ ድርጅቶች የሃሰት ዌብሳይቶችን በመፍጠር የኢንቨስትመንት ዕድል እንደተፈጠረ በማስመሰል መላክ እና ለሌሎች በማሰራጨት የሚከናወን የወንጀል ዓይነት ነው)።

የአንቀፅ 10 (1) አላማም እነዚህና ሌሎች በኮምፒዩተር ስርዓት አማካኝነት የሚፈፀሙ የማታለል ወንጀሎች መከላከል ሲሆን በዋናነት ያልተገባ (በተጭበረበረ መንገድ) ጥቅም ለማግኘት ወይም ለሌላ ሰው ለማስገኘት በማሰብ የኮምፒዩተር ዳታን በመለወጥ፣ በማጥፋት ወይም ሌላ ማንኛውም ጉዳት በማድረስ የሚፈፀሙ ናቸው። ከዚህም በተጨማሪ እነዚህ ወንጀሎች የአሳሳች የሆኑ የኮምፒውተር ዳታዎች በማሰራጨት፣ ወንጀለኞች የራሳቸውን ማንነት ወይም ሁኔታ በመሰወር እንደሁም የተለያዩ አሳሳች ማስታወቂያዎች በማስነገር ሊፈፀሙ ይችላሉ።

አንቀፅ 11- የኤሌክትሮኒክ ማንነት ስርቆት

የኤሌክትሮኒክ ማንነት ስርቆት በግርድፉ ሲተረጎም እንደ ኤሌክትሮኒክ ባንክ አካውንት፣ ዲጂታል ፊርማ፣ ሚስጢራዊ የይለፍ ቃል፣ የኤሌክትሮኒክ መታወቂያ ቁጥር (ID number)፣ የታክስ መለያ ቁጥር እና የመሳሰሉ የግለሰቦችን ማንነት ማረጋገጥ የሚችሉ ሚስጢራዊ መረጃዎች ቴክኒካዊ በሆነ መንገድ የመሰብሰብ ወይም የማግኘት ተግባር ነው። ይህንን ተግባር ለመፈፀም የተለያዩ ዘዴዎችና ሶፍትዌሮች ጥቅም ላይ የሚውሉ ሲሆን ለምሳሌ ያህልም እንደ ፊሺንግ፣ ሶሻል ኢንጂኔሪንግ እና ሰዎች በኮምፒውተራቸው ወይም በኮምፒዩተር መረባቸው ላይ በሚፅፉበት ወይም ዳታ በሚያስገቡበት ወቅት እየለቀሙ ለወንጀለኞቹ የሚያስተላልፉ ሶፍት ዌሮች (keyloggers) ይጠቀሳሉ።

የሌላ ሰው ማንነት ማግኘት ወይም መያዝ ራስን በመደበቅ ወይም ሌላ ሰው ሆኖ በመገኘት (impersonate) ሌሎች በርካታ ወንጀሎችን ለመፈፀም የሚያስችል አደገኛ ዝግጅት ወይም መሰናዳት በመሆኑ በርካታ ሃገሮች ወንጀል አድርገውታል። ስለሆነም የማንነት ስርቆት ዋና አላማ ሌላ ወንጀል ለመፈፀም ሁኔታዎችን ማመቻቸት ሲሆን ለምሳሌ ያህል የሌላ ሰውን ATM መለያ ኮድ (PIN) በእጁ ያስገባ ሰው በያዘው ካርድ የፈለገው ገንዘብ ከባንክ ማውጣት ወይም ማዘወዋወር፣ ያገኘውን ሚስጢራዊ መረጃ ለሶስተኛ ወገን በተለይም ለተደራጁ ወንጀለኞች መሸጥ ይችላል። ይህ ወንጀል በርካታ የአለማችን ሰዎች ሰለባ የሆኑበትና በበርካታ ቢሊዮን የሚቆጠር የገንዘብ ኪሳራ እያደረሰ ያለ ሲሆን በተለይም እንደ ማህበራዊ ሚዲያዎች፣ ኤሌክትሮኒክ ግብይት፣ ኤሌክትሮኒክ የታክስ ስርዓት እና ሌሎች የዕለት ተዕለት እንቅስቃሴዎች በሳይበር ቴክኖሎጂዎች ጥገኛ መሆናቸው የወንጀሉ መስፋፋትና አደገኛነት እንዲጎላ አድርገውታል። በሃገራችንም የተለያዩ ኤሌክትሮኒክ አገልግሎት መስጠት ከመጀመራቸው ጋር ተያይዞ ወንጀሉ እየተስፋፋ መምጣቱ የተለያዩ ማሳያዎች ያሉ ሲሆን የቴክኖሎጂው አጠቃቀም ሲያድግ በተለይም ከኤሌክትሮኒክ ግብይት፣ የኤሌክትሮኒክ መታወቂያ አሰጣጥ፣ ኤሌክትሮኒክ የመንግስት አስተዳደር እና የመሳሰሉ የሃገሪቱ ዕቅዶች በስፋት ተግባራዊ በሚሆንበት ወቅት ወንጀሉ አሳሳቢ መሆኑ አይቀርም። ይህንን ከግምት ውስጥ በማስገባት “የኤሌክትሮኒክ ማንነት ስርቆት” በረቂቅ አዋጁ ሽፋን ካገኙ ወንጀሎች አንዱ ሆኗል።

ንኡስ ክፍል ሦስት

ስለህገ ወጥ የኮምፒዩተር ዳታ ይዘት

ይህ ንኡስ ክፍል የኮምፒዩተር ዳታ ይዘት በራሱ ህገ-ወጥ የሚሆንባቸው ድርጊቶች የሚመለከት ሲሆን የኢንተርኔት (በተለይም ማህበራዊ ሚዲያዎች) መስፋፋትና አለም አቀፍ ተደራሽነት ተከትሎ ትልቅ ስጋት እያስከተሉ ያሉ ወንጀሎች ናቸው፡፡ ኢንተርኔት ፍፁም ያልተገደበ ነፃነት የሚያጎናፅፍ በመሆኑ በሰዎች አዕምሮ ውስጥ ያለን ማንኛውም ሃሳብ ያለምንም ገደብ ለአለም መግለፅና ማሰራጨት ያስችላል፡፡ ስለሆነም ገደብ ካልተበጀለት የኢንተርኔት አጠቃቀም ከሚያስገኘው ዘርፈ ብዙ ቀሜታ በተጨማሪ የህገ-ወጦች መፈልፈያ እንደሚሆንም ግንዛቤ መውሰድ ያስፈልጋል፡፡ ይህም ማለት በኢንተርኔት አማካኝነት የሚሰራጩ ህገ-ወጥ ፅሁፎች፣ ምስሎች፣ ፊልሞች፣ ወዘተ በቀላሉ በማንኛውም ጊዜና ቦታ ተደራሽ ሊሆኑ የሚችሉ በመሆናቸው የሚያስከትሉት ጉዳትም በዚያው መጠን የከፋ ይሆናል፡፡ እነዚህ ወንጀሎች በሃገራችንም በስፋት የሚፈፀሙና በተለይም የኢንተርኔት ይዘት ሬጉላቶሪ አካላት አለመኖር ወይም አለመጠናከር እንዲሁም የሕግ ማዕቀፍ አለመኖር ችግሩ እንዳባባሱት ይታመናል፡፡ የኮምፒዩተር ዳታ ይዘትን የሚመለከቱ ወንጀሎች እጅግ በርካታና እንደየሀገሮች ተጨባጭ ሁኔታና ባህል የተለያዩ ቢሆኑም በዚህ ክፍል በዋናነት በአብዛኞቹ አለም አቀፍ የሳይበር ህጎች የጋራ መግባባት የተደረሰባቸው ብቻ ተመርጠዋል፡፡

አንቀፅ 12- ለአካለ መጠን ባልደረሱ ልጆች ላይ የሚፈፀሙ ፀያፍ ወይም ለመልካም ጠባይ ተቃራኒ የሆኑ ወንጀሎች

የኢንተርኔትንና ተዛማጅ ቴክኖሎጂዎችን መስፋፋትና አለም አቀፍ ተደራሽነት ተከትሎ አካለ መጠን ባልደረሱ ልጆች ላይ የሚፈፀሙ ወንጀሎች እየተበራከቱ መጥተዋል፡፡ ከነዚህም የህፃናት ፖርኖግራፊ በቀዳሚነት የሚጠቀስ ነው፡፡ ይህ ድርጊት የህፃናትን ህይወትና ሞራል እንዲሁም ትውልድን ሊያበላሽ የሚችልና ህፃናትን ለከፍተኛ አደጋ ከሚያጋልጡ ወንጀሎች በቀዳሚነት የሚጠቀሰው የህፃናት ወሲባዊ ጥቃት የሚያባብስ ተግባር ነው፡፡ ከዚህም አልፎ ህፃናትን በማማለል ስለወሲብ የተሳሳተ ግንዛቤ እንዲኖራቸው በማድረግ ወደ ልቅና ህይወታቸውንና ቀጣይ ተስፋቸውን ለከፍተኛ አደጋ የሚያጋልጥ፣ ሕፃናት በወሲብ ላይ ያላቸው አመለካከት የተዛባ እንዲሆንና አለዕድሜያቸው በርካሽ ወሲብ እንዲጠመዱና ቀልባቸው እንዲሳብ የሚያደርግ በመሆኑ በበርካታ ሃገራት ህጎችና አለም አቀፍ ስምምነቶች ልዩ ትኩረት ከሚሰጣቸው ወንጀሎች ቀዳሚው ነው፡፡ የህፃናት ፖርኖግራፊ የሚመለከቱ ምስሎችና

ቪዲዮዎች በተጨባጭ ህፃናት ፆታዊ ግንኙነት ሲፈፅሙ ብቻ ሳይሆን የረቀቁ ቴክኖሎጂዎችን በመጠቀም ሃሰተኛ ምስሎችና ቪዲዮዎችም ይሰራሉ ወይም ይሰራጫሉ።

ይህንን ከግምት ውስጥ በማስገባት በረቂቅ አዋጁ መሰረት በህፃናት ፖርኖግራፊ ወንጀል የሚያስጠይቁ ድርጊቶች በሁለት የተከፈሉ ሲሆን እነዚህም፦

1. ህፃናት ወሲባዊ ድርጊት ሲፈፅሙ የሚያሳይ ስዕላዊ መግለጫ፣ ፖስተር ወይም ቪዲዮ በኮምፒዩተር ስርዓት አማካኝነት ማዘጋጀት፣ ማሰራጨት፣ ማከፋፈል፣ ለሽያጭ ማቅረብ፣ ይዞ መገኘት ወይም ሌሎች ሰዎች እንዲያዩት ማመቻቸት እና
2. በአዋቂዎች የተፈፀመ ወሲባዊ ድርጊትን ለአካለ መጠን ባልደረሱ ህፃናት የተፈፀመ የሚያስመስል ስዕላዊ መግለጫ፣ ፖስተር፣ ቪዲዮ ወይም ኦዲዮ በኮምፒዩተር ስርዓት ወይም በኮምፒዩተር መረብ አማካኝነት ማዘጋጀት፣ ማሰራጨት፣ ማከፋፈል፣ ለሽያጭ ማቅረብ፣ ይዞ መገኘት ወይም ሌሎች ሰዎች እንዲያዩት ማመቻቸት (ይህንን መስራት የሚያስችሉ የተለያዩ ቴክኖሎጂዎች (photo shops) በቀላሉ ከኢንተርኔት ማግኘት ይቻላል) ናቸው።

ከዚህም በተጨማሪ ወሲባዊ ይዘት ያላቸውን ንግግሮችን፣ ስዕሎችን፣የጽሁፍ መልዕክቶችን ወይም ተንቀሳቃሽ ምስሎችን በማሰራጨት አካለ መጠን ያልደረሱ ልጆችን ማነሳሳትና መመልመልን (child grooming) በዚህ አንቀፅ ንኡስ አንቀፅ (2)መሰረት የሚያስቀጣ ወንጀል ሆኗል።

የወንጀሉን አሳሳቢነትና አስከፊነት ግምት ውስጥ በማስገባት ድርጊቱን ከምንጩ መቆጣጠር አስፈላጊ በመሆኑ በዚህ ረቂቅ አዋጅ መሰረት ከማዘጋጀት (production) ጀምሮ በኮምፒዩተር ወይም በዳታ ማከማቻ መሳሪያ (ለምሳሌ-በCD) ያለፈቃድ ይዞ እስከመገኘት ድረስ በወንጀል የሚያስጠይቅ ሲሆን **"ሌሎች ሰዎች እንዲያዩት ማመቻቸት"** የሚለው የህጉ አገላለፅ ደግሞ በኢንተርኔት አማካኝነት የማሰራጨት እና የፖርኖግራፊ ድረ-ገፆችን የመፍጠር (ከ 5 ሚሊዮን በላይ የፖርኖግራፊ ድረ-ገፆች አሉ) ተግባራት ለመከላከል ያለመ ነው።

አንቀፅ 13- በሰዎች ነፃነትና ክብር ላይ የሚፈፀሙ የኮምፒዩተር ወንጀሎች

በኮምፒዩተር ስርዓት አማካኝነት በግለሰቦች ነፃነትና ክብር ላይ ከሚፈፀሙ ወንጀሎች መካከል የስም ማጥፋት ወንጀልና ማስፈራራት/ዛቻ (cyber stalking) በዋናነት ይጠቀሳሉ። የኢንተርኔት

መስፋፋት ሚሊዮኖችም በቀላሉ መድረስ የሚያስችል በመሆኑ ለተለየዩ ህገ-ወጦችም መጠቀሚያ ሆኗል፡፡ በተለይም በመረጃ መረብ አማካኝነት የሚሰራጩ የማስፈራሪያና የዛቻ መልእክቶች ዜጎች ቴክኖሎጂውን ለመጠቀም ያላቸው ፍላጎትና አመኔታ የሚሸረሽር እና ለተለያዩ የስነ ልቦናዊና ማህበራዊ ቀውስ የሚዳርጉ እንዲሁም የተለያዩ ፖለቲካዊና ማህበራዊ ችግሮች የሚያስከትሉ በመሆናቸው ከወዲሁ መፍትሄ ያስፈልጋቸዋል፡፡ የተለያዩ ጥናቶች እንደሚያሳዩትም እስከ የግድያ ዛቻ የሚደርሱ ማስፈራሪያዎች በሰዎች ላይ በተለይም በማህበራዊ ሚዲያዎች አማካኝነት የሚደርስና በመደበኛ ወንጀሎች እንደምንመለከተው የዛቻ ወንጀል አፈጻጸም አይነት ብቻ ሳይሆን መልኩን በመለወጥ ተደጋጋሚ የሆኑ የማይፈለጉ መልእክቶችን በመላክ፣ በማሰራጨት እና የተበዳዩን የኮምፒውተር ኮሚኒኬሽን እያንዳንዷን እንቅስቃሴ በመከታተል(surveillance) ፍርሃትን፣ ድንጋጤን ወይም የስነ ልቦና ጫናን መፍጠር ነው፡፡ ከዚህም ጋር ተያይዞ ሌላው አሳሳቢ ድርጊት የግለሰቦች ወይም የድርጅቶች መልካም ስም በሃስት የማጥፋት ዘመቻ (defamation) የሚመለከት ነው፡፡ የተለያዩ ጥናቶች እንደሚያመለክቱት ወደ 3 ቢሊዮን የሚጠጋው የአለማችን ህዝብ የኢንተርኔት ተጠቃሚ ነው፡፡ ስለሆነም በኢንተርኔት አማካኝነት የሚሰራጩ እንደዚህ አይነት ወንጀሎች በሴኮንዶች በቀላሉ ለ3 ቢሊዮን ሰዎች ሊደርስ የሚችል ሲሆን የሚያስከትለው መዘዝም በዚያው ልክ የከፋ ነው፡፡ በተለይም የድርጊቱ ፈፃሚዎች በቀላሉ ያለመታወቅና ከየትኛውም የአለም ጫፍ ሊነሳ የሚችል በመሆኑ ጉዳዩ በአለም ህብረተሰብ ዘንድ የበለጠ ትኩረት እንዲያገኝ አድርጎታል፡፡

እነዚህ ወንጀሎች በሃገራችንም በስፋት ከሚፈፀሙ የኮምፒውተር ወንጀሎች መካከል ሲሆኑ በተለይም የታዋቂ ሰዎችን ስም ማጥፋት፣ የሌሎችን ሃይማኖት፣ ብሔርና መሰል አቋሞች መሰረት ያደረጉ ዘመቻዎች እየተበራከቱ መጥተዋል፡፡ እንደዚህ አይነት ድርጊት ዜጎች በህገ መንግስቱ የተረጋገጡላቸው መሰረታዊ መብቶች የሚጥስ እንዲሁም ዜጎች በኢንፎርሜሽን ኮምኒዩኬሽን ቴክኖሎጂ አጠቃቀም ላይ ያላቸው አመኔታ የሚሸረሽር በመሆኑ ልዩ ትኩረት የሚሻ ጉዳይ ነው፡፡ ስለሆነም መነሻው ምንም ይሁን በኮምፒዩተር ወይም በኮምፒዩተር መረብ አማካኝነት የሌላ ግለሰብን ክብር የሚነካ፣ የሚያዋርድ፣ የሚያንቋሽሽ፣ የሚያስፈራራ፣ መልካም ስምን የሚያጠፋ ወይም ሌላ ማንኛውም ህገ-ወጥ ድርጊት የሚያሳይ ፅሁፍ፣ ምስል፣ ስዕል፣ ፊልም፣ ንግግር ወይም ሌላ ማንኛውም መረጃ ማዘጋጀት፣ ማሰራጨት እና ማከፋፈል በዚህ አንቀፅ መሰረት በወንጀል የሚያስጠይቅ ተግባር ነው፡፡

አንቀፅ 14- በህዝብ ደህንነት ላይ የሚፈፀሙ የኮምፒዩተር ወንጀሎች

የኢንፎርሜሽን ቴክኖሎጂ በተለይም ደግሞ የኢንተርኔት መስፋፋት ለሃገሪቱ ሁለንተናዊ እንደገት ቁልፍ ሚና እንደሚጫወት የሚያከራክር ጉዳይ ባይሆንም የቴክኖጂው አጠቃቀም ተገቢውን ቁጥጥር ካልተደረገበት ለተለያዩ የጥፋት አላማዎች ማስፈፀሚያ እንደሚውልና ይህም ሃገሪቱ ከቴክኖሎጂው ማግኘት የሚገባትን ጠቀሜታ ከማስቀረቱ ባሻገር የህብረተሰቡን ሰላም እና ደህንነት ጠንቅ እንደሚሆን መገንዘብ ያስፈልጋል፡፡ ለምሳሌ ያህል ኢንተርኔት በተለይም የወጣቱን ቀልብ እየሳቡ ያሉትን ማህበራዊ ሚዲያዎች በአንድ ህብረተሰብ መካከል የተለያዩ አመፆችና የሁከቶች ለማነሳሳት፣ የስነ-ልቦና ጦርነት ለማካሄድ፣ በዜጎች መካከል የፍርሃትና ያለመተማመን ስሜት እንዲፈጠሩ ለማድረግ፣ የተለያዩ የተዛቡ መረጃዎችና ፕሮፓጋንዳዎች ለማሰራጨት እና ተያያዥ ህገወጥ ድርጊቶችን ለማከናወን በስፋት ጥቅም ላይ የሚውሉ ብቻ ሳይሆን ተመራጭ ስትራቴጂ እየሆነ መምጣቱ ይታወቃል፡፡ በሃገራችንም የእነዚህ ቴክኖሎጂዎች ተደራሽነት ተከትሎ በህብረተሰቡ መካከል የፍርሃት ስሜት፣ አመፅ፣ ሁከት ወይም ግጭት እንዲፈጠር የሚያነሳሱ መልዕክቶች በኮምፒውተር ስርዓት ወይም በኢንተርኔት አማካኝነት ማሰራጨትና ለዚህ አላማ ብቻ የሚሰሩ ድረ-ገፆች እየተበራከቱ መጥቷል፡፡ በኢንቴርነት አማካኝነት የሚሰራጩ እነዚህ ህገ-ወጥ መልእክቶች በአንዴ ሚሊዮኖችን የመድረስ ዕድል ስላላቸው የሚያስከትሉት መዘዝ ከፍተኛ መሆኑ በቀላሉ መገንዘብ ያስፈልጋል፡፡ ለዚህም ጠንካራ የህግ ማዕቀፍ አለመኖር የራሱ አስተዋፆ የሚያበረክት መሆኑን በኮምፒዩተር ስርዓት አማካኝነት በህብረተሰቡ መካከል የፍርሃት ስሜት የሚፈጥሩ እንዲሁም አመፅን፣ ሁከትን፣ ወይም ግጭትን እንዲፈጠር የሚያነሳሱ ፅሁፎች፣ ቪዲዮዎች ወይም ንግግሮች ማሰራጨት በዚህ አንቀፅ መሰረት የወንጀል ተጠያቂነት የሚያስከትል ይሆናል፡፡

አንቀፅ 15- የስፓም መልእክቶችን ስለማሰራጨት

ያለፈቃድ በኢሜል አድራሻ አማካኝነት የሚሰራጩ የንግድ ማስታወቂያዎች በእንግሊዘኛው አጠራር ስፓም (spam) በመባል የሚታወቅ ሲሆን እንደዚህ ዓይነቱ መልዕክት እጅግ የተለመደና ብዙ ትኩረት የማይሰጠው ቢሆንም በርካታ ችግሮችና የደህንነት ስጋቶች እንደሚያስከትል የተለያዩ ጥናቶች ያመለክታሉ፡፡ የስፓም መልዕክቶች በዋናነት ያለምንም ወጭ ለሚሊዮኖች በመድረስ ምርቶችና አገልግሎቶችን ለማስተዋወቅ የሚሰራጭ ቢሆንም አብዛኞቹ ህገ ወጥ ይዘት ያላቸው የኮምፒዩተር ዳታዎች እና ጎጂ ፕሮግራሞችም (ቫይረሶችና ዎርሞች) የሚሰራጩት በስፓም መልዕክት አማካኝነት ነው፡፡ ከዚህም አልፎ የስፓም መልዕክት

ማሰራጨት የተለያዩ የፖለቲካ አጀንዳዎችና ፕሮፓጋንዳዎች በአንድ ጊዜ ለሚሊዮኖች ለማድረስ ያገለግላል። የስፓም መልዕክትን ማሰራጨት ከሚያስከትላቸው ጉዳቶች መካከል፦

- የመልዕክቱ ሰለባ የሆኑ የኮምፒዩተር ስርዓቶች ዳታ የማከማቸትና የመተንተን አቅም ያዳክማል፣ አገልግሎቱን እስከ ማደናቀፍና መቋረጥም ሊደርስ ይችላል፤
- በስፓም መልክ ከሚሰራጩ መልዕክቶች ጋር የኮምፒዩተር ስርዓትና ዳታ ሊያወድሙ የሚችሉ የተለያዩ ጎጂ ሶፍትዌሮች ይሰራጫሉ፤
- የስፓም መልዕክቶች ከተለያዩ ድረ-ገፆችና ሰርቨሮች የኢሜል አድራሻዎችን በመሰብሰብና ያለ ተቀባዩ ፈቃድ ወይም ጥያቄ የሚላኩ በመሆናቸው የሰዎች የግል ነፃነት (privacy) ይጥሳሉ።

ያለፈቃድ በኢሜል አድራሻ አማካኝነት በርካታ የንግድ ማስታወቂያዎች ማሰራጨት (ስፓም) በተለያዩ ሃገሮችና አለም አቀፍ ህጎች ልዩ ትኩረት ከተሰጣቸው የሳይበር ጥቃቶች አንዱ ሲሆን በሃገራችንም በተደጋጋሚ ከሚፈፀሙ ጥቃቶች አንዱ ሆኖ ተለይቷል። ከዚህም አልፎ የኢትዮ-ቴሌኮምን ጨምሮ የተለያዩ የሃገሪቱ የኮምፒውተር አድራሻዎች (ID addresses) በአለም አቀፍ የሳይበር ደህንንት ተቋማት ዘንድ እንደስጋት ምንጭ እንዲታዩ (black list እንዲደረጉ) ምክንያት ሆኗል። ስለሆነም ያለፈቃድ በቴሌፎን እና በፖስታ ማስታወቂያ ማሰራጨት እንደማይቻል ሁሉ በኢሜል አድራሻ አማካኝነት ማስታወቂያ ማሰራጨትም በርካታ ስጋቶች የሚያስከትል በመሆኑ በዚህ አንቀፅ መሰረት የሚያስቀጣ ወንጀል ሆኗል። ነገር ግን በአንቀፅ 15 (2) እንደተመለከተው በኢሜል አድራሻ አማካኝነት የንግድ ማስታወቂያዎች ማሰራጨት በወንጀል የማያስጠይቅባቸው ልዩ ሁኔታዎች እንዳሉ መረዳት ይቻላል። እነዚህም፡-

- ከተቀባዩ የተሰጠ ፈቃድ ሲኖር፤
- ማስታወቂያው ደንበኞችን ወይም ተጠቃሚዎችን ከአዳዲስ ምርቶች ወይም አገልግሎቶች ለማስተዋወቅ ያለመ ከሆነ (ለምሳሌ ያህል በሚሊዮኖች የሚቆጠሩ ደንበኞች ወይም የተመዘገቡ ተጠቃሚዎች ያሉት አገልግሎት ሰጪ አስተዳደራዊ ጉዳዮች የሚመለከቱ ማስታወቂያዎች ለማስነገር ወይም አዳዲስ ምርቶችና አገልግሎቶች ለማስተዋወቅ በአንድ ጊዜ ለሁሉም ደንበኞቹ የኢሜል መልዕክት ሊልክ ይችላል። እንደዚህ አይነቱ መልእክት በዕለት ተዕለት የቢዝነስ እንቅስቃሴ የሚከናወን በመሆኑ እንደስፓም መልእክት ተደርጎ መወሰድ የለበትም።)

- የላኪውን ትክክለኛ ማንነት፣ አድራሻ እና የመልእክቱ ተቀባይ ተመሳሳይነት ያላቸው መልዕክቶችን በቀጣይነት ላለመቀበል የሚያስችል ቀላልና ትክክለኛ አማራጭ የያዘ ከሆነ ነው፡፡ ለዚህም እንደምክንያት የተቀመጠው የንግድ ተቋማት ምርቶቻቸውን ለአዳዲስ ተጠቃሚዎች የሚያስተዋውቁበትን መንገድ ለመፍጠር ለማስቻል ሲሆን ተጠቃሚዎችም ቢሆኑ ምርቶችን ወይም አገልግሎቶችን በቀላሉ እንዲተዋወቁ ያስችላል በሚል እሳቤ ነው፡፡ ነገር ግን ተጠቃሚው የሚላክለት መልዕክትን በቀጣይነት መቀበል ካልፈለገ ይህኑ ፍላጎቱን በቀላል መንገድ መተግበር የሚያስችል ቴክኒካዊ የሆነ መንገድ በግልጽ መካተት የሚኖርበት ሲሆን በሌላ አነጋገር ከመልዕክቱ ጋር ተያይዞ መልዕክት ተቀባዩ በቀጣይ ሁኔታ መልዕክቱን መቀበል የሚፈልግ መሆኑን እና አለመሆኑን የሚጠይቅ መጠይቅ እንዲሁም ይህንም ፍላጎቱን በቀላሉ መተግበር የሚያስችል ቴክኒካዊ መንገድ መካተት ይኖርበታል፡፡

አንቀፅ 16- ስለየአገልግሎት ሰጪዎች ተጠያቂነት

በአንቀፅ 2 ንኡስ አንቀፅ (1) ላይ እንደተመለከተው “የዳታ ፕሮሰሲግ አገልግሎት” በኮምፒዩተር ስርዓት አማካኝነት ዳታን የመቀበል፣ የማከማቸት፣ የመተንተን፣ የማሰራጨት፣ የማጓጓዝ ወይም የማስተላለፍ አገልግሎት ሲሆን የኔትዎርክ አገልግሎችንም ይጨምራል፡፡ እነዚህ አገልግሎቶች የሚሰጡ አካላትም አገልግሎት ሰጪዎች ይባላሉ *(አንቀፅ 2(13) ይመልከቱ)፡፡* ለምሳሌ ያህል የቴሌኮም አገልግሎት፣ የኔትዎርክ አገልግሎት፣ የኢንቴርኔት አገልግሎት፣ የዌብሳይት ሆስቲንግ አገልግሎት እና የመሳሰሉ አገልግሎቶችን የሚሰጡ አካላት እንዲሁም ድረ-ገፅ ኦፕሬተሮች፣ በኢንተርኔት አማካኝነት የሚሰጡ የክፍያ፣ የጨረታና መሰል አገልግሎቶችን የሚሰጡ አካላት መጥቀስ ይቻላል፡፡ ስለሆነም በኮምፒውተር ስርዓት አማካኝነት የሚደረጉ ግንኙነቶችና እንቅስቃሴዎች በእነዚህ አገልግሎት ሰጪዎች በኩል ማለፍ የግድ ይሆናል፡፡ በመሆኑም ያላቸው የተጠያቂነት ደረጃ በህግ መወሰን ስላለበት ይህ ድንጋጌ አስፈልጓል፡፡

በተለመደው የህግ አሰራር መሰረት በተለያዩ የህትመት ውጤቶች አማካኝነት ለሚወጡ ህገ ወጥ ይዘቶች ከዋናው ባለቤት ወይም ከደራሲው በተጨማሪ በአሳታሚዎች ዘንድም የህግ ተጠያቂነት እንደሚያስከትል ይታወቃል፡፡ የዚህ መነሻም አሳታሚዎች ስለሚያሳትሙት ነገር ይዘት ጠንቅቀው ያውቃሉ (በሶስተኛ ወገን የተዘጋጀ ቢሆንም) እንዲሁም ከመታተሙ በፊት ይዘቱን የመመርመርና ኢዲት የማድረግ ሃላፊነት ስላላቸው ነው፡፡ በተመሳሳይ መልኩ

አብዛኞቹ የኢንተርኔት ህትመቶች፣ ቪዲዮዎች፣ ንግግሮችና የተለያዩ መልእክቶች የሚሰራጩት በአገልግሎት ሰጪዎች (ለምሳሌ በድረ-ገፆች) አማካኝነት መሆኑን ይታወቃል። ይህም ማለት አገልግሎት ሰጪዎች የአሳታሚዎችን (publishers) ሚና ይጫወታሉ ማለት ነው። ነገር ግን ከመደበኛ አሳታሚዎች በተለየ መልኩ አብዛኞቹ አገልግሎት ሰጪዎች በሶስተኛ ወገኖች (ለምሳሌ የድረ-ገፅ ተጠቃሚዎች) አማካኝነት ለሚሰራጩ ዳታዎች በቀጥታ የመቆጣጠርና ኤዲት የማድረግ ሃላፊነትም ሆነ አቅም የላቸውም። ስለሆነም አገልግሎት ሰጪዎች ደንበኞቻቸው ለሚያሰራጯቸው ህገ-ወጥ ይዘት ያላቸው የኮምፒዩተር ዳታዎች መሰረተ-ልማቱን ከማመቻቸት ውጭ በቀጥታ ተሳታፊ ባለመሆናቸው በመርህ ደረጃ የወንጀል ተጠያቂነት ሊኖራቸው አይገባም። የዚህ መርህ መነሻም አገልግሎት ሰጪዎች ሶስተኛ ወገኖችን በሚያሰረጯቸው ዳታዎች ይዘት ላይ ቀጥተኛ ዕውቀት የላቸውም የሚል ነው። በሌላ አባባል አገልግሎት ሰጪዎች በሚሰራጩ ዳታዎች ይዘት ላይ ቀጥተኛ ዕውቀት ካላቸው ከተጠያቂነት አያመልጡም ማለት ነው። ስለሆነም በአንቀፅ 16 መሰረት አንድ አገልግሎት ሰጪ በሶስተኛ ወገኖች ለሚሰራጩና ህገወጥ ይዘት ያላቸው ዳታዎች በወንጀል ተጠያቂ ሊሆን የሚችልባቸው አጋጣሚዎች የሚከተሉት ናቸው።

- ዳታውን በማሰራጨት፣ በማዘጋጀት ወይም አርትኦት በማድረግ በቀጥታ የተሳተፈ እንደሆነ፦

  አብዛኞቹ አገልግሎት ሰጪዎች የአጠቃቀም ፖሊሲ (terms/conditions of use) አላቸው። በዚህም በሶስተኛ ወገኖች አማካኝነት በሚሰራጩ ዳታዎች ላይ ያላቸው ስልጣንና ሃላፊነት ይገልፃሉ። ለምሳሌ ያህል የተለያዩ የጥናትና ምርምር ውጤቶች የሚያሰራጭ አንድ የድረ-ገፅ ኦፕሬተር በሶስተኛ ወገኖች የሚዘጋጁ ምርቶች ይፋ ከመሆናቸው በፊት የተለያዩ የኢዲቲንግ ስራዎች እንደሚሰራላቸው የሚገልፅ ሲሆን ይህም በሚሰራጩ መልዕክቶች ላይ ቀጥተኛ ተሳትፎ እንዳለው ያሳያል።
- ህገወጥ ዳታ መሆኑን በቀጥታ እያወቀ ዳታውን ለማስወገድ ወይም ተደራሽ እንዳይሆን ለማድረግ ምንም አይነት እርምጃ ያልወሰደ እንደሆነ (ለምሳሌ በስም ማጥፋት ወንጀል ተጠቂ ከሆኑ ሰዎች ሪፖርት ቢቀርብለት)፤
- ህገወጥ ዳታውን እንዲያስወግድ ወይም ተደራሽ እንዳይሆን እንዲያደርግ በሚመለከተው የአስተዳደር አካል (የኢንተርኔት ይዘትን የመቆጣጠር ስልጣን በተሰጠው አካል) ተነግሮት ሳይቀበል የቀረ እንደሆነ ናቸው።

ከእነዚህ መስፈርቶች አንዱ ካልተሟላ ሶስተኛ ወገኖች ለሚያሰራጯቸውና ህገወጥ ይዘት ያላቸውን ዳታዎች አገልግሎት ሰጪዎችን በወንጀል ተጠያቂ ማድረግ ባይቻልም ወንጀሉን ለመመርመር በሚደረገው ጥረት ግን የመተባበርና ተጠርጣሪውን የመለየት እና መሰል ግዴታዎች አለባቸው ግዴታዎቻቸው ካልተወጡም አግባብ ባለው ድንጋጌ ተጠያቂ ይሆናሉ። ለምሳሌ ከሚሰጧቸው አገልግሎቶች ጋር የተያያዙ ወይም በኮምፒውተር ስርዓቶቻቸው አማካኝነት የሚሰራጩ የኮምፒውተር ዳታዎችን ለአንድ አመት ያህል ይዞ የማቆየት (አንቀፅ 23)፣ በመርማሪው አካል ጠለፋ ወይም ክትትል በሚያደርግበት ጊዜ አስፈላጊውን ትብብር የማድረግ (አንቀፅ 24 (6))፣ የሳይበር ጥቃት መድረሱን ሲያውቁ ወይም በሚያስተዳድሯቸው የኮምፒዩተር ስርዓቶች አማካኝነት ማንኛውም የሶስተኛ ወገን ህገወጥ የይዘት ዳታ እየተሰራጨ መሆኑን ሲረዱ ወዲያውኑ ለኤጄንሲው የማሳወቅ እና አስፈላጊውን እርምጃ የመውሰድ (አንቀፅ 26) እንዲሁም የኮምፒውተር ወንጀል የፈፀሙ ደንበኞች ማንነትና ዝርዝር መረጃ ለመርማሪዎች ይፋ የማድረግ (አንቀፅ 30) ግዴታ አለባቸው።

ንኡስ ክፍል አራት

ስለሌሎች ወንጀሎች

አንቀፅ 17- የመተባበር ግዴታን ስለመጣስና የምርመራ ሂደትን ስለማደናቀፍ

የኮምፒውተር ወንጀል ምርመራ በባህሪው በርካታ ሰንሰለት የሚያልፍና የተለያዩ አገልግሎት ሰጪዎች ትብብር የሚጠይቅ ነው። ይህ ድንጋጌም በዚህ አዋጅ መሰረት የኮምፒውተር ዳታን ይዘው እንዲያቆዩ፣ የደህንነት ጥበቃ እንዲያደርጉ፣ ለምርመራ የሚፈለገውን ዳታ ለመርማሪ አካል እንዲሰጡ፣ መርማሪው እንዲተባበሩና መሰል ግዴታ የተጣለባቸው አካላት ግዴታቸው ባልተወጡበት ጊዜ የወንጀል ተጠያቂነት እንዳለባቸው የሚደነግግ ነው። ከዚህም በተጨማሪ መርማሪው አካል በሚያከናውነው የኮምፒውተር ወንጀል የምርመራ ሂደት ሆን ብለው የሚያደናቅፉ ሰዎች ከባድ የወንጀል ተጠያቂነት እንደሚያስከትልባቸው በዚህ አንቀፅ ንኡስ አንቀፅ (2) ላይ ተደንግጓል።

በሌላ ህግ ስለተደነገጉ የወንጀል ድርጊቶች እና ተደራራቢ ወንጀሎች (አንቀፅ 18 እና አንቀፅ 19)

ከላይ በስፋት እንደተዳሰሰው የሳይበር ምህዳር ለአዳዲስ ወንጀሎች መፈጠር ብቻ ሳይሆን ነባር/መደበኛ ወንጀሎችም በአዲስና ውስብስብ በሆነ መንገድ እንዲፈፀሙ አስችሏል፡፡ በዚህ ምክንያትም በኮምፒውተር አማካኝነት በርካታ መደበኛ ወንጀሎች (በዚህ አዋጅ ከተደነገጉት ውጭ) ሊፈፀሙ ይችላሉ፡፡ ስለሆነም የአዋጁ አንቀፅ 18 በዚህ አዋጅ ሽፋን ያላገኙ ነገር ግን በሌላ የወንጀል ህግ የሚያስቀጡ ድርጊቶች በኮምፒውተር አማካኝነት ቢፈፀሙ አግባብ ያላቸው ህጎች ተፈፃሚ እንደሚሆኑ የሚደነግግ ነው፡፡ ከዚህም በተጨማሪ በዚህ አዋጅ የተደነገጉ የወንጀል ድርጊቶች በሌሎች ህጎች የተደነገጉ ወንጀሎች ሊያስከትሉ ይችላሉ፡፡ እንደዚህ አይነት ሁኔታ በሚያጋጥምበት ጊዜ ድርጊቱ በተደራራቢ ወንጀል እንደሚያስቀጣ በአንቀፅ 19 ተደንግጓል፡፡

አንቀፅ 20- በህግ የሰውነት መብት በተሰጠው አካል ላይ የሚጣል ቅጣት

እንደማንኛውም የወንጀል ድርጊት የኮምፒውተር ወንጀልም በግለሰቦች ብቻ ሳይሆን በህግ የሰውነት መብት በተሰጣቸው ድርጅቶችም ይፈፀማል፡፡ በተለይም ከአዕምራዊ ንብረትና ሌሎች እጅግ ሚስጢራዊ የሆኑ የኮምፒውተር ዳታዎች ስርቆት ጋር በተያያዘ ድርጅቶች በስፋት ከሚሳተፉባቸው የወንጀል ድርጊቶች ናቸው፡፡ እነዚህ ሚስጢራዊ የግለሰቦች፣ የድርጅቶች እንዲሁም የመንግስት ተቋማት የኮምፒውተር ዳታዎች ለማግኘትም የተለያዩ የስለላ ቴክኖለጂዎች ይጠቀማሉ እንዲሁም ይህንን ድርጊት የሚያስፈፅሙላቸው ግለሰቦች በተለይም ሃከሮች በመቅጠር ይሰራሉ፡፡ እነዚህ ሁኔታዎች ከግምት ውስጥ በማስገባት በህግ የሰውነት መብት በተሰጣቸው አካላት ላይ የሚጣል የቅጣት መጠን በዚህ አዋጅ አንቀፅ 20 ላይ የተደነገገ ሲሆን የቅጣት መጠኑም በወንጀል ህግ አንቀፅ 90 ላይ ከተቀመጠው የመቀጮ መጠን ከፍ እንዲል ተደርጓል፡፡ ስለመቀጮ አወሳሰን መርሆች የሚደነግገው የወንጀል ህጉ አንቀፅ 90 ተቀጪው ህጋዊ ሰውነት ያለው ድርጅት በሆነ ጊዜ መቀጮው ከብር 100 እስከ ብር 500,000 መሆን እንዳለበት ይደነግጋል፡፡ ነገር ግን በዚህ አዋጅ በግለሰቦች ላይ ከተጣለው የቅጣት መጠን እና የኮምፒውተር ወንጀል ከሚያስከትለው ጉዳት አንፃር የወንጀል ህጉ በድርጅቶች ላይ ያስቀመጠው የመቀጮ መነሻ እጅግ አናሳ በመሆኑ መነሻው ወደ ብር 50,000 ከፍ እንዲል ተደርጓል፡፡ በዚህ መሰረትም በዚህ አዋጅ ለተደነገገው የወንጀል ድርጊት የተጣለው ቅጣት መቀጮ ከሆነ እና ተቀጪው የህግ ሰውነት ያለው ድርጅት ከሆነ መቀጮው ከብር ሃምሳ ሺህ እስከ ብር አምስት መቶ ሺህ ይሆናል (አንቀፅ 20 (1))፡፡ ለወንጀሉ የተጣለው ቅጣት እስራት ከሆነ ደግሞ የዚህ አዋጅ አንቀፅ 20 (2) ተፈፃሚ ይሆናል፡፡ ከዚህም በተጨማሪ በዚህ አዋጅ

መሰረት ለተደነገገው የወንጀል ድርጊት የተጣለው ቅጣት መጠኑ በግልፅ የተቀመጠ መቀጮ ከሆነ በአምስት ተባዝቶ ህጋዊ ሰውነት ባላቸው ድርጅቶች ላይ ተፈፃሚ ይሆናል፡፡

ክፍል ሶስት

የመከላከልና የምርመራ ሂደቶች

የኮምፒውተር ወንጀልን ለመከላከልና ለመመርመር በመደበኛ ህጎች ከተደነገጉት መንገዶች በተጨማሪ በርካታ ቴክኒካዊና ህጋዊ መንገዶች አሉ፡፡ በዚህ ክፍልም የወንጀል ህግ እና ሌሎች አግባብነት ያላቸው ህጎች ድንጋጌዎች በኮምፒውተር ወንጀሎች ላይም እንደአግባብነታቸው ተፈፃሚ እንደሚሆኑ ሳይዘነጋ የኮምፒውተር ወንጀልን ለመመርመርና ለመከላከል የተለየ ጠቀሜታ ያላቸው አዳዲስ ድንጋጌዎች የተካተቱ ሲሆን የዋና ዋናዎቹ ድንጋጌዎች ማብራሪያ እንደሚከተለው ቀርቧል፡፡

አንቀፅ 22- የመመርመር ሥልጣን

በዚህ ኣዋጅ አንቀጽ 22 (1) እንደተመለከተው አቃቤ ህግ እና ፖሊስ እንደማንኛውም መደበኛ ወንጀል የኮምፒውተር ወንጀልም የመመርመር ስልጣን አላቸው፡፡ ነገር ግን አብዛኞቹ የኮምፒውተር ወንጀሎች (በተለይም የኮምፒዩተር ስርዓትና ዳታ ሚስጢራዊነት፣ ተደራሽነትና ተአማኒነት ላይ የሚፈፀሙ ወንጀሎች) በመደበኛው ህግ የማስፈፀም አሰራር መቆጣጠር እጅግ አስቸጋሪ በመሆኑ በተለመደው የፖሊስና የአቃቤ ህግ የወንጀል ምርምራ ሂደት ብቻ የሚፈታ አይደለም፡፡ በተለይም ከምርመራና ማስረጃ ከማሰባሰብ ጋር በተያያዘ በርካታ ፈተናዎች ያሉት በመሆኑ ለዚህ ተብለው የሚቋቋሙ የሳይበር ደህንነት ተቋማት፣ ልዩ የፖሊስና የአቃቤ ሕግ ክፍሎች ያስፈልጋሉ፡፡ የተለያዩ ሃገራት ተሞክሮ እንደሚያሳየውም አብዛኞቹ የህግ አስፈፃሚ አካላት ልዩ የኮምፒውተር ወንጀል ዩኒቶች ያቋቋሙ ናቸው፡፡ በሃገራችንም የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ የሳይበር ወንጀሎችን በመከላከልና በመመርመር ሂደት ለፖሊስና ሌሎች በህግ ስልጣን ለተሰጣቸው አካላት ትብብር የማድረግ፣ ቴክኒካዊ ድጋፍ የመስጠት እንዲሁም በምርመራ ሂደት የተገኙ ቴክኒካዊ መረጃዎች የመተንተንና ማስረጃ የማቅረብ ሃላፊነት ተሰጥቶታል፡፡

አንቀፅ 23- የኮምፒውተር ዳታን ይዞ ስለማቆየት

ለኮምፒውተር ወንጀል ምርመራ እጅግ አስፈላጊ የሆኑ ማስረጃዎች በዲጂታል ወይም ኤሌክትሮኒክ መልክ የሚገኙና ለተለያዩ የደህንነት ስጋቶች በቀላሉ የተጋለጡ ናቸው። ከዚህም በተጨማሪ በኮምፒዩተር ስርዓት አማካኝነት የሚደረጉ ግንኙነቶች በርካታ ሰንሰለቶች የሚያልፉ በመሆናቸው ለኮምፒውተር ወንጀል ምርማራ አስፈላጊ የሆኑ መረጃዎች በተለያዩ አካላት ተበታትነው ይገኛሉ። ለምሳሌ ያህል በተጠርጣሪው የኮምፒዩተር ስርዓት፣ የወንጀል ተጠቂ (target) በሆነ የኮምፒዩተር ስርዓት፣ በኢንተርኔት አገልግሎት ሰጪዎች ወይም በሌሎች ሶስተኛ ወገኖች ማለትም የትምህርት ተቋማት፣ የቢዝነስ ተቋማት፣ የመንግስት ተቋማት እንዲሁም በተለያዩ ሰርቨሮች ሊገኙ ይችላሉ። ስለሆነም በኮምፒውተር ወንጀል የተጠርጣሪን ሰው ለመለየት ግንኙነቱ ባለፈባቸው አካላት ወይም የግንኙነት ሰንሰለቶች በኩል ማለፍ ይጠይቃል ወይም ሰውየው የተጠቀመበትን የኮምፒዩተር ዳታ ትራፊክ መተንተን የግድ ይሆናል። በተለይም በተጠቃሚው ልዩ የኮምፒዩተር አድራሻ (IP adress) ላይ የሚደረገውን ትንተና የወንጀሉን ዱካ ለማግኘት አይነተኛ ሚና ይጫወታል።

ነገር ግን ይህንን ትንተና ለማከናውን በርካታ ፈተናዎች እንዳሉ መዘንጋት የለበትም። ከእነዚህ ፈተናዎችም ቀዳሚው የወንጀሉን ዱካ ለማግኘት እጅግ ጠቃሚ የሆነውን የኮምፒዩተር ዳታ ወዲያውኑ ከኮምፒውተር ስርዓት እንዲጠፋ ወይም እንዲወገድ የሚደረግ መሆኑ ነው። ይህም የሚሆንበት ምክንያት በአንድ በኩል የኮሙኒዩኬሽን ሂደቱ ከተጠናቀቀ (ለምሳሌ፦ የኢሜል መልዕክት ከተላከ፣ ቪዲዮ ዳውንሎድ ከተደረገ ወይም ሌላ የኢንተርኔት አገልግለት ከተጠናቀቀ) በኋላ ይህንን የኮምኒዩኬሽን ሂደት የተከናወነበትን ትራፊክ ዳታ ለተጠቃሚውም ሆነ ለአገልግሎት ሰጪው ምንም አይነት ጠቀሜታ ስለማይኖረው እንዲጠፋ ስለሚደረግ ሲሆን በሌላ በኩል ደግሞ እንደዚህ አይነት የሚሊዮኖች ዳታ ተከማችቶ እንዲቆይ ማድረግ አገልግሎት ሰጪ ድርጅቶችን ከፍተኛ የማከማቸት አቅም ያለው መሳሪያ (storage device) እና ወጭ ስለሚጠይቃቸው ነው።

ከእንደዚህ አይነት ሽክም ለመላቀቅ ያላቸው አማራጭ ታዲያ ዳታዎችን ወይም የዳታ ትራፊክ ወዲያውኑ ማስወገድ ወይም ማጥፋት ይሆናል። ከዚህ በተጨማሪም የኮምፒዩተር መረብ አገልግሎት ተጠቃሚዎች ዳታ የሚያከማቹ አገልግሎት ሰጪዎች አገልግሎቱ ካለቀ በኋላ እንዲያጠፉ በህግ የሚገደዱበት አጋጣሚ አለ (ለምሳሌ የዳታ ጥበቃ/data protection/ ህጎች የግለሰቦችን ዳታ በአገልግሎት ሰጪዎች ተከማችቶ የሚቆይበት የጊዜ ገደብ ያስቀምጣሉ)። አንዳንድ ዳታዎችም በባህሪያቸው ለአጭር ጊዜ ብቻ የሚቆዩ ሊሆኑ ይችላሉ። በሌላ በኩል

ደግሞ በወንጀሉ መፈፀም፣ የወንጀሉ መፈፀም መታወቅ (discovery of the crime)፣ ለመርማሪዎች ሪፖርት በማድረግ እና መደበኛ ምርመራውን በመጀመር መካከል ብዙ ጊዜ መባከኑ የማይቀር ነው። ይህም ማለት ወንጀል መርማሪዎች የወንጀሉ ዱካ የሚያመላክተውን የኮምፒዩተር ዳታ ሳይወገድ ወይም ሳይጠፋ ሊደርሱበት አይችሉም ማለት ነው። ይህም መርማሪዎች የወንጀሉን ዱካ ለማግኘት እና የወንጀለኛው ማንነት ለመለያት በሚያደርጉት ጥረት ትልቅ እንቅፋት ይሆናል።

ስለዚህ እንደዚህ አይነት ችግሮች ለመፍታት ከሚወሰዱ ህጋዊ እርምጃዎች መካከል አገልግሎቱን የሚሰጡ (ዳታው የሚያከማቹ፣ የሚተነትኑ፣ ወ.ዘ.ተ.) አካላት በህጉ እስከተመለከተው የጊዜ ገደብ ድረስ ዳታው ይዘው እንዲያቆዩ ማድረግ አንዱ ነው። በዚህ መሰረትም አገልግሎት ሰጪዎች በኮምፒውተር ስርዓታቸው ወይም ኔትዎርካቸው አማካኝነት የሚሰራጩትን ወይም የሚከማችቱን የኮምፒውተር ዳታዎች ወይም ከሚሰጧቸው አገልግሎቶች ጋር በተያያዘ የሚያገኟቸው ዳታዎች ለአንድ አመት ጊዜ ይዘው የማቆየት እና ይህም ዳታ ህግ ከሚፈቅደው አሰራር ውጭ ለማንኛውም አካል ይፋ ያለማድረግ ሃላፊነት እንዳለባቸው በአንቀፅ 23 ላይ ተደንግጓል።

አንቀፅ 24- የኮምፒውተር ዳታን ስለማሰባሰብ

የኮምፒውተር ወንጀልን ለመከላከል ከሚወሰዱ እርምጃዎች ሌላው በኮምፒዩተር ስርዓት አማካኝነት የሚደረጉ ግንኙነቶች እና የኢንተርኔት እንቅስቃሴዎች በቀጥታ በመጥለፍ የሚከናወን ነው። የሃገራችን የተለያዩ ህጎች ካባድ ወንጀሎችን ለመከላከል የተጠርጣሪዎች የስልክ፣ የሞባይና የኢሜል ግንኙነቶች መጥለፍ ይፈቅዳሉ (ለምሳሌ የፀረ ሽብርተኝነትና የፀረሙስና ህጎች)። ነገር ግን የኮምፒውተር ወንጀል ለመከላከል እነዚህ ህጎች ከሚፈቅዷቸው የጠለፋ አይነቶች ባሻገር የተለያዩ የኮምፒዩተር ዳታዎችን መሰብሰብ ይጠይቃል። ለምሳሌ ያህል ሰዎች በኢንተርኔት አማካኝነት የሚያደርጓቸው እንቅስቃሴዎች (chat, file transfer, share, likes, download, logs, web traffic, instant messaging, site visited, ---) በቀጥታ መከታተል (ህግ በሚፈቅደው መልኩ) ለወንጀል ምርመራ አስፈላጊ የሆኑ ዳታዎች ለማግኘት ያስችላሉ።

በሞዴልነት ከተመረጡትን አለም አቀፍ የኮምፒዩተር ወንጀል ህጎች መረዳት እንደሚቻለው ይህንን ድርጊት በሁለት መንገድ ይከናወናል። የመጀመሪያው በኮምፒዩተር ስርዓት አማካኝነት

የሚደረጉ ግንኙነቶች የሚመለከት **ትራፊክ ዳታ** በቀጥታ መጥለፍ ወይም መከታተል ሲሆን ሁለተኛው መንገድ ደግሞ በኮምፒዩተር ስርዓት አማካኝነት የሚደረጉ ግንኙነቶች ሙሉ **ይዘት** (content) በቀጥታ በመጥለፍ ወይም በመከታተል የሚከናወን ነው። ይህ አካሄድ በተለይም ከፍተኛ ጉዳት ሊያስከትሉ የሚችሉ የሳይበር ጥቃቶችን ለመከላከል፣ ወንጀለኞች የረቀቁ ቴክኖሎጂዎችን በመጠቀም ራሳቸው ለመደበቅ የሚያደርጉትን ሙከራ ለማክሸፍ እና በባህሪያቸው በፍጥነት ሊጠፉ ወይም ሊቀየሩ የሚችሉ ለወንጀል ምርመራ አስፈላጊ የሆኑ መረጃዎችን ለማግኘት እንዲሁም የወንጀሉ ሰንሰለት ወይም ኔትዎርክ ለማወቅ እጅግ ጠቃሚ መንገድ በመሆኑ በሃገራችንም ተግባራዊ ማድረግ ያስፈልጋል። በዚህ መሰረትም የተጠርጣሪዎችን በኮምኒዩኬሽን ሂደት ላይ ያለን የኮምፒዩተር ዳታ፣ የዳታ ፕሮሰሲንግ አገልግሎት ወይም የኢንተርኔት እና ሌሎች መሰል ግንኙነቶችን በቀጥታ መጥለፍ ወይም መከታተል እንደሚቻል አንቀፅ 24 ይደነግጋል።

ነገር ግን በዚህ መንገድ የሚገኙ ዳታዎችና መረጃዎች የግለሰቦችን የግል ነፃነት ሊጎዱ የሚችሉ በመሆናቸው የተፈቀደው አሰራር በዘፈቀደ ተግባራዊ እንዳይደረግ የተለያዩ ገደቦች ያስፈልጉታል። በዚህም መሰረትም መርማሪው አካል የኮምፒውተር ወንጀልን ለመመርመርና ለመከላከል ያለው ፍላጎት ከግለሰቦች ነፃነት ፍላጎት ጋር ሚዛናዊ ለማድረግ የሚያስችሉ የተለያዩ ገደቦች በአንቀፅ 24 ተደንግገዋል። እነዚህም፣

- መርማሪው አካል የተጠርጣሪዎችን በኮምኒዩኬሽን ሂደት ላይ ያለን የኮምፒዩተር ዳታ፣ የዳታ ፕሮሰሲንግ አገልግሎት ወይም የኢንተርኔት እና ሌሎች መሰል ግንኙነቶችን ለመጥለፍ ወይም ለመከታተል በቅድሚያ የፍርድ ቤት ፈቃድ ሊኖረው ይገባል(አንቀፅ 24 (1))፣
- ጠለፋው ወይም ክትትሉ የሚካሄደው የተፈለገው ዳታ በሌላ መንገድ ማግኘት የማይቻል ሲሆን እና ይህም በሚኒስትሩ ሲታመን መሆን አለበት (ይህንን ሁኔታ ባልተሟላበት ጊዜ ፍርድ ቤት ፈቃድ መስጠት አይችልም) (አንቀፅ 24 (2))፣
- በጠለፋው ወይም ክትትሉ ወቅት የተገኙ ዳታዎች ወይም መረጃዎች ለተያዘው ጉዳይ ወይም ለሌላ ወንጀል ምርምራ አስፈላጊ ካልሆኑ ወዲያውኑ መወገድ አለባቸው (አንቀፅ 24 (5))፣ እንዲሁም
- በዚህ ሂደት የሚገኙ ማናቸውም የኮምፒውተር ዳታዎች በሚስጢር መያዝ አለባቸው (አንቀፅ 24 (7))።

እነዚህ ገደቦች እንደተጠበቁ ሆነው አንዳንድ የሳይበር ጥቃቶች ግን ጊዜ የማይሰጡ እንዲሁም በሃገሪቱ ቁልፍ የኢንፎርሜሽን መሰረተ ልማቶች ጉዳት የሚያደርሱ ሊሆኑ ይችላሉ፡፡ በአንቀፅ 2 (10) እንደተመለከተው ቁልፍ መሰረተ ልማቶች የሳይበር ጥቃት ቢደርስባቸው በህዝብ ደህንነት እና በሃገሪቱ ብሄራዊ ደህንነት ላይ ከፍተኛ ጉዳት ሊያስከትሉ የሚችሉ የኮምፒዩተር ስርዓቶች፣ የኮምፒዩተር ኔትዎርኮች ወይም የኮምፒዩተር ዳታዎች ናቸው፡፡ ስለሆነም በእነዚህ መሰረተ ልማቶች የተቃጣ ጥቃት ሲኖር እና ጥቃቱ ለመከላከል ወይም አጥቂዎቹ ለመለየት መደበኛው የህግ ሂደት መከተል የማያስችል አስቸኳይ ሁኔታ ሲያጋጥም መርማሪው አካል ያለፍርድ ቤት ፈቃድ ጠለፋ ወይም ክትትል ሊያካሂድ እንደሚችል በአንቀፅ 24 (3) ተደንግጓል፡፡ ይህም የሆነበት በሁለት ዋና ዋና ምክንያቶች ሲሆኑ እነዚህም፤ የመጀመሪያው ጥቃቱ የተፈፀመው ወይም ሊፈፀም ይችላል ተብሎ የተጠረጠረው በቁልፍ መሰረተ ልማቶች ላይ መሆኑ እና በእነዚህ መሰረተ ልማቶች ላይ የሚደርስ ጥቃት ደግሞ የሚያስከትለው ጉዳት እጅግ አደገኛ በመሆኑ ሲሆን ሁለተኛው ምክንያት ደግሞ መደበኛው የህግ ስነስርዓት ለመከተል (ማለትም ከፍርድ ቤት ፈቃድ በማውጣት) የማያስችል አስቸኳይ ጊዜ ሲኖር ነው፡፡ ነገር ግን በእንደዚህ አይነት ሁኔታም ቢሆን የመርማሪው አካል ስልጣን ሚዛኑ የጠበቀ እንዲሆን ማድረግ አስፈላጊ በመሆኑ ሚኒስትሩ ያለ ፍርድ ቤት ትዕዛዝ ለመጥለፍ ወይም ለመከታተል መነሻ የሆኑትን ምክንያቶች በ48 ሰዓት ውስጥ ለፌዴራል ከፍተኛ ፍርድ ቤት ፕሬዘዳንት ማቅረብ የሚኖርበት ሲሆን ፕሬዚዳንቱም ተገቢ ያሉትን ትዕዛዝ (ማፅደቅ ወይም ውድቅ ማድረግ) ወዲያውኑ መስጠት እንዳለበት ተደንግጓል (አንቀፅ 24 (4))፡፡

አንቀፅ 25- ኮምፒውተርን፣ የኮምፒውተር ስርዓትን ወይም መሰረተ ልማቶችን ከአደጋ ስለመጠበቅ

የኮምፒውተር ወንጀልን ለመከላከል የተጠርጣሪዎችን ግንኙነት እና ዳታ መጥለፍ ወይም ለምርመራ አስፈላጊ የሆኑ የኮምፒውተር ዳታዎች መሰብሰብ ብቻ በቂ አይደለም፡፡ የሳይበር ጥቃቶች አንዴ ከደረሱ (በተለይም በዳታዎችና መሰረተ ልማቶች ላይ) ጥቃቶቹን በቀላሉ ለማስወገድና የተጠቁ ዳታዎች ወይም መሰረተ ልማቶች ወደነበሩበት ለመመለስ ውስብስብ ስራ እና በርካታ ወጪ የሚጠይቅ ሊሆን ይችላል፡፡ ከዚህም በተጨማሪ አብዛኞቹ የሳይበር ጥቃቶች ለበርካታ አመታት ሳይታወቁ ሊቆዩ ይችላሉ፡፡ ለምሳሌ ያህል በኮምፒውተር ስርዓቶች ወይም ኔትዎርኮች ላይ የሚታይ ጉዳት የሚያደርሱ ካልሆነ በስተቀር አብዛኞቹ የኮምፒውተር ዳታዎች

የሚሰርቁ ጥቃቶች፣ የሳይበር ስለላ እና የመሳሰሉ የሳይበር ጥቃቶች በቀላሉ በተጠቃሚው የሚታወቁ አይደሉም።

ስለሆነም የኮምፒውተር ስርዓቶች፣ ኔትወርኮች፣ ዳታዎችና የመሰረተ ልማቶች ደህንነት በየጊዜው በሚመለከታቸው አካላት በዋናነትም በኮምፒውተር ድንገተኛ አደጋ ምላሽ መስጫ ማዕከል አማካኝነት መፈተሽ ይኖርበታል። ይህ አካሄድ የደረሱ ጥቃቶችን ወደሌሎች ሳይዛመቱ ለመቆጣጠር እንዲሁም ተጠቀሚዎች ወይም ዜጎችን አስቀድሞ ለማስጠንቀቅ ያግዛል። ይህንን ተግባራዊ ለማድረግም ኤጀንሲው መርማሪው አካላት ጋር በመተባበር የሳይበር ጥቃት ሰለባ ወይም መነሻ ሊሆኑ እንደሚችሉ በተጠረጠሩ ኮምፒውተሮች፣ የኮምፒውተር ስርዓቶች ወይም መሰረተ ልማቶች ላይ ድንገተኛ ፍተሻ ወይም የዲጂታል ፎረንሲክ ምርመራ ማድረግ እና አስፈላጊ የሆኑ የደህንነት እርምጃዎች መውሰድ እንደሚችል በአንቀፅ 25 ላይ ተደንግጓል።

አንቀፅ 26- ሪፖርት የማድረግ ግዴታ

የተለያዩ ጥናቶች እንደሚያሳዩት የኮምፒውተር ወንጀሎችን ለመከላከልና ለመቆጣጠር የሚደረጉት ስራዎች ውጤታማ እንዳይሆኑ ከሚያደርጉ ጉዳዮች መካከል አብዛኞቹ የወንጀል ድርጊቶች ወይም ጥቃቶች ለሚመለከተው አካል ሪፖርት የማይደረጉ መሆናቸው ነው። በዚህ ምክንያትም የሳይበር ጥቃቶች መፈፀማቸው የሚታወቁት በርካታ ጉዳት ካደረሱ እና ከተስፋፉ በኋላ ነው። ይህም እየደረሱ ያሉ ጥቃቶች ስፋት፣ የጥቃቶቹ ባህሪ፣ አይነትና ምንጭ እንዲሁም የሚያደርሱት ጉዳት እንዳይታወቅ ያደርገዋል። እነዚህ ጉዳዮች በግልፅ ካልታወቁ ደግሞ ውጤታማ የመከላከል፣ የመቆጣጠርና የመርመር ስትራቴጂ ሊነደፍና ተግባራዊ ሊደረግ አይችልም። ይህንን ችግር ለመፍታት ማንኛውም ሰው የኮምፒውተር ወንጀል መፈፀሙ ሲያውቅ ለሚመለከተው አካል ሪፖርት ማድርግ እንዳለበት የሚጠበቅ ቢሆንም በዋናነት ደግሞ አገልግሎት ሰጪዎች የተለያዩ ጥቃቶችና የጥቃት ምልክቶች በፍጥነት የሚደርሳቸው በመሆኑ እንዲሁም በኮምፒውተር ስርዓቶቻቸው አማካኝነት የሚጠራጩ ዳታዎች ማወቅ ስላለባቸው የሳይበር ጥቃት ወይም የኮምፒውተር ወንጀል መፈፀሙ ሲያውቁ ወድያውኑ ለኤጀንሲው ሪፖርት የማድረግና አስፈላጊው እርምጃ የመውሰድ ግዴታ እንዳለባቸው በአንቀፅ 26 ላይ የተደነገገ ሲሆን ይህንን ውጤታማ ለማድረግም ኤጀንሲው የሪፖርቲንግ ስርዓት ማመቻቸት እንዳለበት ተደንግጓል።

ክፍል አራት

የማስረጃና የስነ - ስርዓት ድንጋጌዎች

በመደበኛው የወንጀል ፍትህ አስተዳደር ወንጀለኞችን በህግ ለማስቀጣት ምክንያታዊ ከሆነ ጥርጣሬ በላይ አሳማኝ ማስረጃ ለፍርድ ቤት ማቅረብ የግድ ይሆናል፡፡ በእንደዚህ አይነት ሁኔታ የሚቀርብ ማስረጃ አብዛኛውን ጊዜ በዓይን የሚታይ፣ የሚጨበጥ በመሆኑ ጉዳዩን ለማረጋገጥ ወይም ውድቅ ለማድረግ የሚያዳግት አይደለም፡፡ በአንፃሩ የኮምፒውተር ወንጀል የሚፈፀመው አካላዊ ግዙፍነት በሌለው የሳይበር ምህዳር በመሆኑ ወንጀለኞቹን ለመያዝና በህግ ለመቅጣት የሚያስፈልገው ማስረጃ አካላዊ ግዙፍነት የሌለው (intangible) ማስረጃ ነው፡፡ ስለሆነም የኮምፒውተር ወንጀልን እንደ ሌሎች መደበኛ ወንጀሎች በዓይን ምስክሮች፣ ግዙፍነት ባላቸው ማስረጃዎች ወይም በኤግዚቢት ማስረጃዎች ማረጋገጥ አስቸጋሪ ነው፡፡ ይህንን ወንጀል ለማረጋገጥ የሚያስፈልገው ማስረጃ ኤሌክትሮኒክ (ዲጂታል) ማስረጃ ሲሆን ይህ ማስረጃ በተፈጥሮው የማይጨበጥና ለተለያዩ የደህንነት ስጋቶች በእጅጉ የተጋለጠ ነው፡፡ ይህም ማለት ዲጂታል ማስረጃ በሚለይበት፣ በሚሰበሰብበት፣ በሚከማችበት፣ በሚተነተንበት እንዲሁም ለፍርድ ቤት በሚቀርብበት ወቅት ከጊዜ ብዛት፣ ሆን ተብሎ ወይም በቸልተኝነት ወይም ከማስረጃው (ዳታው) ተፈጥሯዊ ባህርይ የተነሳ በቀላሉ ሊጠፋ፣ ሊበላሽ፣ ሊለወጥ የሚችል ነው፡፡ በመሆኑም ይህ የማስረጃ ዓይነት ከተለመደው የወንጀል ምርመራ ሂደት የተለየ ቴክኖሎጂ፣ ላብራቶሪ፣ የተለያዩ ቴክኒካዊ ዘዴዎችና ሙያዊ ብቃት የሚጠይቅ በመሆኑ የኮምፒውተር ወንጀልን ለመከላከል፣ ለመመመርና ወንጀለኞችን ለፍትህ ለማቅረብ በሚደረገው ጥረት በርካታ ፈተናዎች ያጋጥማሉ፡፡ እነዚህን ችግሮች ለመፍታትም ልማዳዊ ቴክኒኮችን ተፈፃሚ ማድረግ እንደተጠበቀ ሆኖ ከዘርፉ ውስብስብነት ጋር አብረው መራመድ የሚችሉ አዳዲስ እይታዎችና የምርመራ ዘዴዎች ማበጀት ያስፈልጋል፡፡ በኮምፒዩር ወንጀል ምርመራ ወቅት የሚያስፈልጉ ማስረጃዎች በዋናነት ይዘትን የሚመለከቱ ዳታዎች (content related) እና ትራፊክ ዳታ (non-content) የሚመለከቱ የኮምፒዩተር ዳታዎች ተብለው ሊከፈሉ ይችላሉ፡፡

በኢ.ፌ.ዴ.ሪ. የወንጀል ፍትህ ፖሊሲ ላይ እንደተመለከተው እነዚህ አዳዲስ የስነ-ስርዓትና የምርመራ ዜዴዎች በህግ ማስደገፍና ማስተዋወቅ አስፈላጊ በመሆኑ የኮምፒውተር ወንጀልን ለመቆጣጠር፣ ለመመርመርና አጥፊዎች ለማስቀጣት የሚያስችሉ አዳዲስ የስነስርዓት ደንቦች በዚህ ረቂቅ ህግ ተካቷል፡፡ ስለሆነም በዚህ ክፍል የተመለከቱ ድንጋጌዎች ዋና አላማ የህግ

አስፈፃሚዎችና መርማሪዎች የሳይበር ወንጀልን መቆጣጠር፣ መመርመርና አጥፊዎችን ማስቀጣት የሚያስችሏቸው አዳዲስ ስልቶችንና ስርዓቶችን በህግ ማቋቋም ነው። ነገር ግን በኮምፒዩተር ወንጀል ምርመራ ሂደት አዳዲስ የስነ-ስርዓት ደንቦች መከተል አስፈላጊ ቢሆንም በምንም አይነት መልኩ የዜጎችን ሰብአዊ መብቶች እና ነፃነቶች በሚጋፋ መልኩ ተፈፃሚ መሆን የለባቸውም። ስለሆነም በዚህ ረቂቅ አዋጅ መሰረት የሚከናወኑ የምርመራ ሂደቶች ምን ጊዜም ቢሆን በሃገሪቱና በአለም አቀፍ ህጎች የተረጋገጡና የዜጎች ዋስትና የሆኑ ሰብአዊና ዴሞክራሲያዊ መብቶች ባከበረ መልኩ መከናወን ይኖሩባቸዋል።

አንቀፅ 29-የኮምፒዩተር ዳታ ደህንነት ለመጠበቅ ስለሚሰጥ ትእዛዝ

ከላይ በአንቀፅ 24 እንደተመለከትነው የኮምፒውተር ወንጀሎችን ለማስቀጣት የሚያስችሉ ማስረጃዎች በዋናነት ዲጂታል ወይም ኤሌክትሮኒክ ማስረጃዎች ሲሆኑ እነዚህ ማስረጃዎችም በባህሪያቸው በቀላሉ ሊበላሹ፣ ሊቀየሩ ወይም ለተለያዩ የደህንነት ስጋቶች የተጋለጡ በመሆናቸው ማስረጃዎችን ለማሰባሰብ፣ ለመያዝና ለፍርድ ቤት ለማቅረብ በሚደረገው ጥረት አስፈላጊው ጥንቃቄ ማድረግ ያስፈልጋል። ይህ እንደተጠበቀ ሆኖ ለምርምራ እጅግ አስፈላጊ የሆኑ አብዛኞቹ የኮምፒውተር ዳታዎች ደግሞ መደበኛ ምርመራ ከመካሄዱ በፊት በተለያየ ምክንያት ሊጠፉ፣ ሊበላሹ፣ ሊቀየሩ ወይም ለሌላ መሰል የደህንነት አደጋ ሊጋለጡ ይችላሉ። ስለሆነም መደበኛ የምርመራ ሂደት ከመጀመሩ በፊት ለምርመራው የሚያስፈልጉ ዳታዎች እንዳይጠፉ ወይም ይዘታቸውን እንዳይቀይሩ ጥበቃ እንዲደረግላቸው የሚያስችል ዘዴ ማበጀት ያስፈልጋል። ይህንን ዘዴም ዳታውን የያዙ አካላት ለተወሰነ ጊዜ (ከ3 ወራት ላልበለጠ) ሳያጠፉ እንዲያቆዩ እና አስፈላጊውን የደህንነት ጥበቃ እንዲያደርጉ የሚያስገድድ ህግ ሲሆን በተለያዩ ሃገራት የሚሰራበትና በአፍሪካ ህብረት የሳይበር ደህንነት ረቂቅ ቃል ኪዳንም (convention) ልዩ ትኩረት የተሰጠው ጉዳይ ነው።

በአንቀፅ 2(8) ላይ እንደተመለከተው "የኮምፒዩተር ዳታ ደህንነት" ማለት አንድን የኮምፒዩተር ዳታ እንዳይጠፋ፣ እንዳይቀየር፣ ላልተፈቀደለት አካል ተደራሽ እንዳይሆን፣ ሚስጢራዊነቱ እንዳይጋለጥ ወይም ሌላ ማንኛውም ጉዳት እንዳይደርስበት መጠበቅ ነው። ስለሆነም የዚህ ድንጋጌ (አንቀፅ 29) አላማ ለወንጀል ምርመራ ጠቃሚ የሆኑትን የኮምፒዩተር ዳታዎች በመርማሪዎች እጅ ከመግባታቸው በፊት ከጥፋት፣ ከመቀየር ወይም ከሌላ ማንኛውም የደህንነት ስጋት መጠበቅ ነው።

በዚህ መሰረትም አንቀፅ 29(1) የኮምፒውተር ወንጀል ለመመርመር ስልጣን የተሰጠው አካል ለወንጀሉ ምርመራ አላማ አስፈላጊ የሆነን የኮምፒዩተር ዳታ ሊጠፋ ወይም ሊቀየር እንደሚችል በበቂ ምክንያት ሲያምን ዳታውን የያዘ ወይም በቁጥጥር ስር ያደረገን ሰው አስፈላጊው የደህንነት ጥበቃ እንዲያደርግ ሊያዝ እንደሚችል ይደነግጋል፡፡ ይህም ማንኛውም የኮምፒውተር ወንጀል ፈፃሚዎች ማንነት ለመለየት የሚያስችል የኮምፒዩተር ዳታ በተለያዩ አካላት በተለይም የኮምፒዩተር መረብ አማካኝነት አገልግሎት የሚሰጡ አካላት (ለምሳሌ ድረ-ገፅ ኦፕሬተሮች) የሚገኝ በመሆኑና ይህንን የወንጀለኞችን ማንነት መለየት የሚያስችል የኮምፒዩተር ዳታ ካልተገኘ የኮምፒውተር ወንጀልን መቆጣጠር የማይቻል በመሆኑ ነው፡፡ ስለሆነም የእነዚህ አካላት ትብብር የግድ በመሆኑ አንቀፅ 29(1) አስፈልጓል፡፡ አንቀፅ 29(1) ተግባራዊ ለማድረግ የፍርድ ቤት ፈቃድ አያስፈልግም፡፡ ምክንያቱም በአንድ በኩል ድንጋጌው የኮምፒውተርና ወንጀል መፈፀሙን ሲታወቅ ወድያውኑ (Expedited) ተግባራዊ መደረግ ያለበት መሆኑ ሲሆን በሌላ በኩል ደግሞ ተላልፎ የሚሰጥ ወይም ይፋ የሚደረግ ዳታ ባለመኖሩ በሰዎች መብቶችና ነፃነቶች ላይ ስጋት የማያስከትል መሆኑ ነው፡፡ አንቀፅ 29 (2) በመርማሪ አካላት ትእዛዝ የተሰጣቸው ሰዎች የኮምፒዩተር ዳታ ደህንነት ለመጠበቅ ወዲያውኑ አስፈላጊውን እርምጃ መውሰድ እንዳለባቸው የሚያስገድድ ሲሆን ይህም ለወንጀል ምርመራ አስፈላጊ የሆነን ዳታ በቅፅበት የመጥፋት፣ የመበላሸት ወይም የመቀየር ዕድሉ በጣም ሰፊ በመሆኑ ነው፡፡ ይህንን ትእዛዝ የተሰጣቸው አካላት የዳታውን ደህንነት ቢያንስ ለሦስት ወራት ጠብቀው የማቆየት ሃላፊነት ያለባቸው ሲሆን የጊዜ ገደቡ መነሻም በሞዴልነት የተመረጡትን አለም አቀፍ የህግ ማዕቀፎች ነው፡፡ (አብዛኞቹ አለም አቀፍ ህጎች ከ90 ቀናት መሆን እንዳለበት ይደነግጋሉ)

አንቀፅ 30-የኮምፒዩተር ዳታ ለማግኘት ስለሚሰጥ ትእዛዝ

በዚህ ረቂቅ አዋጅ አንቀፅ 29 መሰረት የተከማቸን የኮምፒዩተር ዳታ የደህንነት ጥበቃ ማድረግ እንጂ ለመርማሪዎች እንዴት ተላልፎ እንደሚሰጥ ወይም ይፋ እንደሚደረግ አልተደነገገም፡፡ ስለሆነም የደህንነት ጥበቃ የተደረገላቸው የኮምፒዩተር ዳታዎች መርማሪዎች ፍርድ ቤት በሚወስነው የጊዜ ገደብ ውስጥ ይፋ እንዲደረግላቸው ወይም ተላልፎ እንዲሰጣቸው ወይም አክሰስ እንዲያደርጉ በአንቀፅ 30 መሰረት ፍርድ ቤትን መጠየቅ ይችላሉ፡፡ ነገር ግን መርማሪ አካላት በዚህ ድንጋጌ መሰረት ተላልፎ እንዲሰጣቸው የሚጠይቁት ዳታ በአንቀፅ 29 መሰረት የደህንነት ጥበቃ እንዲደረግለት የታዘዘውን ብቻ ላይሆን ይችላል፡፡ ለምሳሌ በኢንተርኔት

አማካኝነት የተለያዩ አገልግሎቶች የሚሰጡ አካላት የደንበኞቻቸውን መረጃ ለኮምፒውተር ወንጀል ምርመራ አስፈላጊ ሆኖ እስከተገኘ ድረስ አሳልፈው የመስጠት ወይም የመተባበር ግዴታ አለባቸው ማለት ነው፡፡

ስለሆነም ፍርድ ቤት በአንቀፅ 30 መሰረት በማንኛውም ሰው (አገልግሎት ሰጪ ድርጅትን ጨምሮ) ይዞታ ወይም ቁጥጥር ስር ያለውና ለወንጀል ምርምራ አስፈላጊ የሆነውን የኮምፒዩተር ዳታ (ለምሳሌ የተመሰጠሩ ዳታዎች ለመፍታት የሚያስችሉ ፕሮግራሞች፣ ኮዶች፣ ቁልፎች፣ ወዘተ) ለመርማሪው አካል ተላልፈው እንዲሰጡ ወይም ይፋ እንዲደረጉ ትዕዛዝ መስጠት የሚችል ሲሆን “በቁጥጥር ስር” የሚለው አገላለፅ አካላዊ ደራሽነት (physical access) ብቻ ሳይሆን ቨርቹዋል ደራሽነትንም (ለምሳሌ፡- remote online storage system) ያካትታል፡፡ ይህ ድንጋጌ ተግባራዊ ለማድረግ የፍርድ ቤት ፍቃድ ያስፈለገበት ምክንያትም ተላለፎ የሚሰጠውን ዳታ በሰዎች የግል ነፃነት ላይ የሚያስከትለው ችግር እንዳይኖር ለማድረግ የፍርድ ቤት ይሁንታ ማግኘት አስፈላጊ በመሆኑ ነው፡፡

አንቀፅ 31 - ስለደራሽነት፣ መበርበርና ስለመያዝ

በማንኛውም የወንጀል ምርመራ ወቅት ወንጀል የተፈፀመበትን ስፍራ መበርበርና የወንጀል ፍሬዎችን መያዝ (search and seisure) የተለመደ ነው፡፡ በሃገራችንም በስፋት ተግባራዊ ከሚደረጉ የምርመራ ዘዴዎች ቀዳሚው ነው፡፡ ነገር ግን በወንጀለኛ መቅጫ ሥነ-ሥርዓት ሕጋችንና ሌሎች ሥራ ላይ ባሉ ህጎቻችን ያሉትን የብርበራና መያዝ ድንጋጌዎች እንደተጠበቁ ሆነው በዚህ ረቂቅ አዋጅ ከኮምፒውተር ወንጀል ባህሪ ጋር አብረው ሊራመዱ የሚችሉ አዳዲስ የብርበራና መያዝ ቴክኒኮች ማካተተ አስፈላጊ ሆኖ ተገኝቷል፡፡ ለምሳሌ ያህል፡-

- በስራ ላይ ካሉ ህጎች በተለየ መልኩ በዚህ ረቂቅ አዋጅ መሰረት ከቁሳዊ ነገሮች ባሻገር የኮምፒዩተር ኔትዎርኮችና ዳታዎችም ሊበረበሩና ሊያዙ ይችላሉ፤
- የህግ አስፈፃሚ አካላት ወይም መርማሪዎች እንዲበረበር የተፈለገውን ነገር በአካል የት እንዳለ ሳያውቁ ቢቀሩም በኢንተርኔት አማካኝነት መበርበር ይችላሉ፤
- በኮምፒዩተር ወንጀል ምርመራ ወቅት ከርቀት የወንጀለኞችን ማንነት መለየት የሚያስችል ሶፍትዌር (remote forensic software) ያሉ ዘመናዊ የምርመራ ቴክኒኮችን መጠቀም ይቻላል፤

- በኮምፒዩተር ወንጀል ምርመራ ወቅት ተግባራዊ የሚደረገው የብርበራና መያዝ ዘዴ በመደበኛ ወንጀሎች ላይ እንደሚደረገው በተጠርጣሪው ቤት ውስጥ በአካል መግባት ሳያስፈልግ በኮምፒዩተር መረብ አማካኝነት (online-search) ሊከናወን ይችላል።

የኮምፒዩተር ዳታዎችን በማንኛውም ስፍራ ሆነው መጠቀም እንዲቻል ጠቃሚ ዳታዎችን በኢንተርኔት አማካኝነት አክሰስ በሚደረጉ ሰርቨሮች ውስጥ ማስቀመጥ የተለመደ ነው። ይህም ማለት ለማስረጃነት የሚያገለግለውን ዳታ የብርበራ ፈቃድ (search warrant) በወጣበት ስፍራ ወይም መሳሪያ ሳይሆን በሌላ ቦታ ወይም መሳሪያ ሊከማች ይችላል ማለት ነው። ለምሳሌ ያህል እንዲበረበር ፈቃድ የተሰጠው በተጠርጣሪው መኖሪያ ቤት ያለው የኮምፒዩተር ስርዓት ቢሆንና ብርበራው በሚካሄድበት ጊዜ ግን ተፈላጊውን ዳታ ወይም ማስረጃ ያለው የብርበራ ፈቃድ በወጣበት የኮምፒዩተር ስርዓት ሳይሆን ተጠርጣሪው በኢንተርኔት ወይም ሌላ ኔትዎርክ አማካኝነት አክሰስ በሚያደርገው ሰርቨር ሊሆን ይችላል።

ይህም በአንድ በኩል በመርማሪዎች አስቀድሞ ባለመታወቁ ምክንያት የብርበራ ፈቃድ ያልወጣበት ሲሆን በሌላ በኩል ደግሞ ሌላ የፍርድ ቤት ፈቃድ መጠየቅ ጠቃሚውን ማስረጃ እስኪጠፋ ድረስ ቆሞ የመጠበቅ ያህል ይቆጠራል። ስለሆነም ውጤታማ የሆነ የምርመራ ስራ ማከናወን የሚያስችል መንገድ መፍጠር ያስፈልጋል። ሰለሆነም መርማሪዎች እንዲበረበር የተፈለገውን የኮምፒዩተር ዳታ የብርበራ ፈቃድ በወጣበት ሳይሆን ከዚህ ውጪ ባለ የኮምፒዩተር ስርዓት (ሰርቨር) የሚገኝ መሆኑን ካመኑና ይህንን ውጫዊ የኮምፒዩተር ስርዓትም የብርበራ ፈቃድ በወጣበት የኮምፒዩተር ስርዓት አማካኝነት ማግኘት የሚቻል ከሆነ ድጋሚ የፍርድ ቤት ፈቃድ ሳያስፈልግ የብርበራ ስራቸውን ማከናወን ይችላሉ ማለት ነው። (አንቀፅ 31 (2))

የወንጀል መርማሪዎች ብርበራቸውን ሲያጠናቅቁ ከሚወስዱት እርምጃ አንዱ ለማስረጃ አስፈላጊ የሆነውን ኮምፒውተር፣ የኮምፒዩተር ስርዓት፣ የኮምፒዩተር ፕሮግራም፣ የኮምፒዩተር ዳታ፣ የዳታው ይዘት ወይም ትራፊክ ወይም ዳታው የተከማቸበትን መሳሪያ መያዝ ነው። ነገር ግን አንድ አንድ ጊዜ ለማስረጃነት የተፈለገውን ዳታ የተከማቸበትን ሃርድዌር መያዝ አላስፈላጊ ወይም አስቸጋሪ ሆኖ ሊገኝ ይችላል። በእንደዚህ አይነት ሁኔታ የተፈለገው ዳታ እንጂ ዳታውን የተከማቸበት ሃርድዌር ባለመሆኑ የወንጀሉ መርማሪዎች ተፈላጊውን ዳታ ወደ ራሳቸው መሳሪያ ኮፒ በማድረግ ሊይዙ ይችላሉ። ይህን በሚያደርጉበት ወቅት ደግሞ ዋናው ዳታ (orginal data) በተጠርጣሪው የኮምፒዩተር ስርዓት ወይም ሃርድዌር የሚቀር ሲሆን ይህንንም

ዳታ ማጥፋት የግድ ሊሆን ይችላል፤ (ለምሳሌ፦ ዳታው የህፃናት ፖርኖግራፊ ሲሆን)፡፡ ይህንን ተከትሎም መርማሪዎች በእጃቸው ያለውን ዳታ በፍርድ ቤት ዋጋ እንዳያጣ ለማድረግ እና ተአማኒነቱን እንደያዘ ለማቆየት (maintain integrity of copied data) የሚያስችል ቴክኒካዊ እርምጃ እንዲወስዱ (ለምሳሌ ኢንክሪፕት ማድረግ) የሚያስችል የህግ ፈቃድ ያስፈልጋቸዋል፡፡ ስለሆነም ኮፒ የተደረገ ዳታ ተአማኒነቱን የሚያረጋግጥላቸው እርምጃ ከወሰዱ በኋላ መርማሪዎች በዋናው ዳታ (በተጠርጣሪው የኮምፒዩተር ስርዓት ያለው) ላይ የተለያዩ ውሳኔዎች መወሰን ይችላሉ ማለት ነው፡፡ ለምሳሌ በማንኛውም መልኩ በሌሎች ሰዎች አክስስ እንዳይደረግ ማድረግ (encrypt) ይችላሉ፡፡

ከላይ እንደተገለፀው ለኮምፒዩተር ወንጀል ምርመራ አስፈላጊ የሆኑትን ዳታዎች በተለያዩ አካላት ተበታትነው ሊገኙ ይችላሉ፡፡ ስለሆነም መርማሪዎች ተጠርጣሪው ዳታውን ያከማቸበት ሰርቨር በትክክል ቢያወቁም አገልግሎት ሰጪ ድርጅቶች (የሰርቨሩ ባለቤቶች) እጅግ በርካታ የኮምፒዩተር መሳሪያዎችና ሃርድ ዲስኮች የሚጠቀሙ በመሆናቸው ለወንጀል ምርመራ የተፈለገውን ዳታ በትክክል ያለበትን ቦታ ለመለየት ያስቸግራቸዋል፡፡ ወይም ደግሞ ወንጀል መርማሪዎች ዳታው የተከማቸበትን የኮምፒዩተር መሳሪያ (ለምሳሌ ሃርድ ድራይቭ) በትክክል ቢደርሱበትም የደህንነት እርምጃዎች (ለምሳሌ በሚስጢራዊ የይለፍ ቃል፤ ኢንክሪፕሽን) ተፈላጊውን ዳታ እንዳያገኙ እንቅፋት ሊሆንባቸው ይችላል፡፡ እነዚህ ችግሮችም በቀላሉ ለመፍታት በዚህ ረቂቅ ህግ የተወሰደው እርምጃ የኮምፒዩተር ስርዓቱ ሚስጢራዊ ኮዶችና አሰራር የሚያውቅና የሰርቨሩ መሰረተ ልማት ለማስተዳደር ሃላፊነት የወሰደ ሰው (system administrator) የወንጀል መርማሪዎችን የመተባበር ግዴታ እንዲኖረው ማድረግ ነው፡፡ ወይም ደግሞ የተመሰጠሩ ዳታዎች ለመፍታት የሚያስችል የኮምፒዩተር ዳታ (ለምሳሌ ቁልፍ) የያዘ ሰው አሳልፎ እንዲሰጥ ወይም እንዲተባበር ይደረጋል፡፡ ስለሆነም ብርበራ የሚከናወኑበትን የኮምፒዩተር ስርዓት አሰራርን ወይም የኮምፒተር ዳታ ደህንነት ለማስጠበቅ የተወሰዱ እርምጃዎችን የሚያውቅን ሰው ራሱን የሚያስወነጅል እስካልሆነ ድረስ የኮምፒዩተር ወንጀል መርማሪ አካላትን የመተባበር ግዴታ አለበት ማለት ነው፡፡ (አንቀፅ 31 (4))

ነገር ግን ብርበራ በሚካሄድበት ወቅት መርማሪው አካል የብርበራ ፈቃድ ያልወጣላቸው ነገር ግን የዚህን አዋጅ ድንጋጌዎች ወይም ሌሎች ህጎችን የሚፃረሩ የኮምፒዩተር ስርዓት አሰራር ወይም የኮምፒዩተር ዳታ ይዘት ሊያጋጥመው ይችላል፡፡ በእንደዚህ አይነት ሁኔታ የኮምፒውተር ስርዓቱ ወይም የኮምፒውተር ዳታው ጥቅም ላይ እንዳይውል፣ እንዲታገድ

ወይም እንዲዘጋ ለፍርድ ቤት ትዕዛዝ እንዲሰጥለት መርማሪው አካል ጥያቄ ማቅረብ እንደሚችልና ፍርድ ቤቱም ለጉዳዩ ጥያቄ በቀረበለት በ48 ሰዓት ጊዜ ውስጥ አስፈላጊውን ትዕዛዝ መስጠት እንዳለበት ተደንግጓል (አንቀፅ 31 (5))፡፡

ተቀባይነት ስለሚኖራቸው ማስረጃዎች እና ትክክለኛነትን ስለማረጋገጥ (አንቀፅ 32 እና 33)

ከላይ በስፋት እንደተመለከተው የኮምፒውተር ወንጀል ማስረጃዎች በዋናነት በዲጂታል ወይም በኤሌክትሮኒክ መልክ የሚገኙ ዳታዎች ሲሆኑ እነዚህ ዳታዎች ወደ ሰነድ መልክ ተቀይረው ካልቀረቡ በስተቀር መርማሪዎች፣ አቃቤያን ህግ እና ዳኞች በቀላሉ ሊረዷቸው የማይችሉ ሊሆኑ ይችላሉ፡፡ በተለይም የትራፊክ ዳታ በኮምፒውተር ፎረንሲክ ባለሙያዎች ተተርጉሞ የሚቀርብ እንጂ የህግ ባለሙያዎች በቀላሉ የሚረዷቸው አይደሉም፡፡ ስለሆነም በሌሎች አግባብ ያላቸው ህጎች ስለማስረጃ አቀራረብና ተቀባይነት የተደነገጉትን እንደተጠበቁ ሆነው የማንኛውም ኮምፒውተር ዳታ የሚመለከት ሰነድ ወይም የሰነዱ የተረጋገጠ ግልባጭ ወይም የተረጋገጠ የኤሌክትሮኒክስ መዝገብ ወይም ህትመት የኮምፒውተር ወንጀልን ለማስረዳት በማስረጃነት ሊቀርብ እንደሚችልና ተቀባይነትም እንደሚኖረው ተደንግጓል፡፡

ነገር ግን ከማስረጃዎቹ ተቀባይነት ባሻገር የኮምፒውተር ዳታዎች የሚሰበሰቡባቸው መንገዶችም ከተለመደው የማስረጃ አሰባሰብ ዘዴ የተለየ በመሆኑ የተለያዩ አዳዲስ የማስረጃ አሰባሰብና ምርመራ ዘዴዎች በአዋጁ ተካትተዋል፡፡ እነዚህ የኮምፒውተር ወንጀልን ለመመርመርና ተጠርጣሪዎችን ጥፋተኛ ለማሰኘት እጅግ ጠቃሚ የሆኑ የኮምፒውተር ዳታዎች በሃገሪቱ መርማሪ አካላት ብቻ የሚገኙ ሳይሆን ከተለያዩ የውጭ ሃገር መሰል ተቋማት በትብብርና ቅንጅት የሚሰበሰቡ ናቸው፡፡ ይህም ከኮምፒውተር ወንጀል ድንበር የለሽ ባህሪ የሚመነጭ ሲሆን በውጭ ሃገር የምርመራ ተቋማት አማካኝነት የተገኙ ማስረጃዎች በሃገር ውስጥ የኮምፒውተር ወንጀሎችን የፍርድ ሂደት ላይ ተቀባይነት ካላገኙ ወንጀሉ በቀላሉ መከላከልና ወንጀል አድራጊዎችን ወደፍትህ ማቅረብ እጅግ አስቸጋሪ ይሆናል፡፡ ስለሆንም በዚህ አዋጅ የተደነገጉትን የማስረጃ አሰባሰብ መንገዶች እንዲሁም አግባብ ባላቸው ሌሎች ህጎች መሰረት የተሰበሰቡ እና ከውጭ ሀገር የሕግ አስከባሪ አካላት የተገኙ ዲጂታል ወይም ኤሌክትሮኒክ ማስረጃዎች የኮምፒውተር ወንጀሎችን ጉዳይ ለማስረዳት በፍርድ ቤት ተቀባይነት እንደሚኖራቸው በአንቀፅ 32 ላይ ተደንግጓል፡፡

ነገር ግን እነዚህ የኮምፒውተር ዳታዎች በቀላሉ ሊቀየሩ፣ ሊጠፉ፣ ሊዛቡ፣ ወይም ለሌሎች የደህንነት አደጋዎች በቀላሉ የሚጋለጡ በመሆናቸው በማስረጃነት ለፍርድ ቤት በሚቀርቡበት ወቅት እንዳለ መቀበል ሳይሆን ትክክለኛነታቸውን ማረጋገጥ እጅግ አስፈላጊ ይሆናል። ስለሆነም ማስረጃዎቹ የሚያቀርብ አካል የማስረጃዎቹን ተዓማኒነት እና ትክክለኛነት የማስረዳት ኃላፊነት ይኖረዋል (አንቀፅ 33)። ይህም ሲባል አንድ ማስረጃ ማለትም አንድን የተያዘ የኮምፒውተር ዳታ የሚመለከት ሰነድ ከሆነ፣ የሰነዱ የተረጋገጠ ግልባጭ፣ የተረጋገጠ የኤሌክትሮኒክስ መዝገብ ወይም ህትመት ለፍርድ ቤቱ ሲቀርብ ተዓማኒነቱ መረጋገጥ ይኖርበታል። የማስረጃው ተዓማኒነትም ማስረጃው ከተገኘበት ምንጭ፣ ወደ ማስረጃ ከተቀየረበት አግባብ፣ ወዘተ ጋር ተያያዥነት ያለው ነው። በሌላ በኩል የቀረበው ሰነድ ትክክለኛነትም እንዲሁ መረጋገጥ አለበት። በአገራችን ህግ ሰነድ የሚረጋገጥባቸው ሂደቶች በሰነዶች ማረጋገጥና ምዝገባ አዋጅ በዝርዝር ተደንግጎ ይገኛል። ይህ አዋጅ የሰነዶች ትክክለኛነት የሚረጋገጥባቸውን ሂደቶች ያስቀመጠ ሲሆን ከዚህ ውጭ ግን አንድ ሰነድ የኮምፒውተር ዳታን የሚመለከት ሆኖ ከቀረበ ይኸው ሰነድ ወይም የሰነዱ የተረጋገጠ ግልባጭ፣ የተረጋገጠ የኤሌክትሮኒክስ መዝገብ ወይም ህትመት ትክክለኛ መሆኑን ማስረጃውን ያቀረበው አካል ማስረዳት ያለበት ሲሆን እንደነገሩ ሁኔታ ይህንን አዋጅ ጨምሮ በሌሎች ህጎች የተመለከተ የሰነድ ማረጋገጥ ሂደቶችም ተፈፃሚ ሊደረጉ ይችላሉ።

ዋና የኤሌክትሮኒክ ሰነድ (አንቀፅ 34)

የኮምፒውተር ወንጀሎች አፈፃፀም ውስብስብ ከመሆኑ የተነሳ የሚሰበሰቡ ማስረጃዎች እና ማስረጃዎቹ የሚተነተኑበትም አግባብ ውስብስብ ይሆናል። በዚህ ሂደት ውስጥ በአንቀፅ 32 ላይ ተቀባይነት ስለሚኖራቸው ማስረጃዎች የተዘረዘሩ ሲሆን በዋናነት የሚነሳው የኮምፒውተር ወንጀል ማስረጃ የኤሌክትሮኒክ ማስረጃ ይባላል። በማናቸውም ኮምፒውተር ወይም የኮምፒውተር ስርዓት አማካይነት አንድ ዳታ ምክንያታዊ በሆነ ወይም በታወቀ ስርዓት አማካይነት ስርዓቱን ተከትሎ ከተመዘገበ ወይም ክምችት ከተካሄደበት እና ፕሮሰስ ከተደረገ በኋላ የሚገኝ የኤሌክትሮኒስ መዝገብ በማስረጃነት የሚቀርብ ከሆነ እንደዋና ኤሌክትሮኒክስ ሰነድ ይቆጠራል። ምክንያቱም በማስረጃነት የቀረበው ሰነድ የተገኘው አስተማማኝነቱ በተረጋገጠ የኤሌክትሮኒክስ መዝገብ በተመዘገበበት ወይም በተከማቸበት አግባብ እና ስርዓት ስለሆነ ነው። ለምሳሌ አንድ የወንጀል መረጃን የሚመዘግብ የኮምፒውተር ስርዓት ቢኖር እና ስርዓቱን ተከትሎ የሚገኘውን መረጃ ሁሉ የሚመዘግብ ከሆነ እና በኮምፒውተር ስርዓቱ አማካይነት

ፕሮሰስ ተደርጎ እንደ ውጤት ሆኖ የተገኘ አንድ ሰነድ ማስረጃ ከተገኘና ወንጀሉን ለማስረዳት የተገኘውን ማስረጃ ለፍርድ ቤት ማቅረብ አስፈላጊ ቢሆን የቀረበው ማስረጃ እንደዋና ኤሌክትሮኒክ ሰነድ ተደርጎ ይወሰዳል፡፡ ሆኖም አንድ ሰነድ እንደ ዋና የኤሌክትሮኒክ ሰነድ ተደርጎ በማስረጃነት የሚቀርበው በመጀመሪያ ደረጃ የኤሌክትሮኒክ ዳታው የተመዘገበበት ወይም የተከማቸበት ስርዓት አስተማማኝ ሲሆን ነው፡፡ አስተማማኝነቱ ባልተረጋገጠ ወይም በኮምፒውተር ስርዓቱ ላይ ግልፅ ችግር ካለና የምዝገባ ወይም የክምችት ሂደቱ ላይ አሉታዊ ተፅዕኖ ያለው ከሆነ፣ በዚያ መንገድ የተገኘው ማስረጃ እንደ ዋና የኤሌክትሮኒክ ሰነድ ተደርጎ በማስረጃነት ሊቀርብ አይችልም፡፡ ስለሆነም የኮምፒውተር ስርዓቱን በራሱ በመጠቀም የተገኘ ሰነድ አንዱ የኤሌክትሮኒክ ዋና ሰነድ ሲሆን በሌላ በኩል የኮምፒውተር ስርዓቱን ውጤት ሳይጠብቅ በሌላ ማንኛውም ሁኔታ አንድን የኮምፒውተር ዳታ ሲያከማች ወይም ሲመዘግብ በቆየ ኮምፒውተር ወይም የኮምፒውተር ስርዓትን በመጠቀም ወደ ወረቀት ፅሁፍ የተቀየረ ሰነድ እንደ ኤሌክትሮኒክ ዋና ሰነድ ተደርጎ በማስረጃነት ሊቀርብ ይችላል፡፡ ለምሳሌ አንድ የፋክስ ማሽን አንድን ፅሑፍ በመውሰድ በራሱ መንገድ ፕሮሰስ ካደረገ በኋላ በሂደት የሚገኘውን ውጤት ሳይጠበቅ ሌላኛው ተቀባይ በቀጥታ የተላከውን ወይም የተመዘገበውን መረጃ በወረቀት መልክ ወደ ፅሁፍ ተገልብጦ ይቀርብለታል፡፡ በዚህ ሂደት የተገኘው ሰነድ እንደ ዋና የኤሌክትሮኒክ ማስረጃ ተደርጎ ይወሰዳል፡፡ ነገር ግን ሰነዱ ተቀባይነት የሚኖረው የኮምፒውተር ስርዓቱ በተከታታይ ሲሰራ የነበረና ተመሳሳይ ዳታዎችን ፕሮሰስ ሲያደርግ ወይም አስተማማኝነት ባለው መንገድ ሲመዘግብ ወይም ሲያከማች የነበረ ስርዓት ከሆነ ነው፡፡ ሆኖም የኮምፒውተር ስርዓቱ አስተማማኝነት ወይም ስርዓቱ ሲሰራበት የነበረበትን ሂደት ትክክለኛነት ማረጋገጥ ካልተቻለ ወይም በስርዓቱ ትክክለኛነትን ተቃውሞ ከቀረበ እንደነገሩ ሁኔታ፡-

1. የኮምፒውተር ስርዓቱ ወይም ኮምፒውተሩ በራሱ በተግባር ሲሰራ የነበረ እና ይህም ሂደት አስተማማኝ የነበረ መሆኑ፤ ከዚህም በተጨማሪ ምንም እንኳ ማስረጃው በቀረበበት ወቅት የኮምፒውተሩ ወይም የኮምፒውተር ስርዓቱ የተበላሸ ቢሆንም በተግባር ከመበላሹ በፊት ሲሰራ ተመሳሳይ ውጤት ያላቸውን ሰነዶች ወይም ትክክለኛ ኮፒዎች ሲያመርት ወይም ሲያስገኝ የነበረ መሆኑን፣ እንዲሁም ብልሽቱ በአጠቃላይ ኮምፒውተሩ ወይም የኮምፒውተር ስርዓቱ በሚያወጣው፣ በሚያመርተው ወይም በሚያስገኘው ሰነድ እንጅ የኮምፒውተሩን ተመሳሳይ ውጤት የማመንጨት ተግባር

አስተማማኝነት የማያጓድል መሆኑን በማሳየት የኤሌክትሮኒክ መዝገብ ስርዓትን ትክክለኛነት ማረጋገጥ ይቻላል፡፡

2. አንድን ለፍርድ ቤት ወይም ለፍትህ አካላቱ የቀረበን ማስረጃ ማለትም የኤሌክትሮኒክ ማስረጃው እንዲመዘገብ የተደረገው ማስረጃውን ለማቅረብ ከሚፈልገው ሰው በተቃራኒ ባለው ሌላኛው ተከራካሪ ወገን ከሆነ ማለትም ማስረጃው እንዲመዘገብ የተደረገው በከሳሽ አማካይነት ወይም ከሳሽ ሆኖ በቀረበለት ሰው አማካይነት መሆኑን ተከሳሹ ካስረዳና ይኸውን የኤሌክትሮኒክ መዝገብ በማስረጃነት ካቀረበ ቀደም ሲል ይህ ሰነድ የተገኘው በኮምፒውተሩ ወይም በኮምፒውተር ስርዓቱ አማካይነት መሆኑን እና የስርዓቱም ትክክለኛ መሆኑን በዚህ ማስረዳት ይቻላል፡፡ በሌላ በኩል የኤሌክትሮኒክ መዝገቡ የተመዘገበው በተከሳሹ በራሱ ከሆነ፣ ከሳሽ ወገን ማለትም አቃቤ ህግ ይህንኑ የኤሌክትሮኒክ መዝገብ በማስረጃነት ካቀረበው እና በኮምፒውተር ወይም በኤሌክትሮኒክስ መዝገባ ስርዓቱ ላይ ተቃውሞ ከተነሳ የዚህን ስርዓት ትክክለኛነት አቃቤ ህግ ከሚያረጋግጥባቸው መንገዶች አንዱ መዝገቡ የተመዘገበው በራሱ በተከሳሽ መሆኑን በማሳየት ይሆናል ማለት ነው፡፡

3. ከላይ ከተመለከቱ ምክንያቶችና የማስረዳት መንገዶች በተጨማሪ የኤሌክትሮኒክስ መዝገቡ እንዲመዘገብ ወይም እንዲከማች የተደረገው ማስረጃውን ለማቅረብ ከሚፈልገው ሰው ውጭ በሆነ በሌላ ማንኛውም ሰው ወይም ማስረጃውን ማቅረብ በሚፈልገው ሰው ቁጥጥር ውጭ ባለ ሌላ ሰው አማካይነት ከሆነ እና በተለይም መዝገቡ እንዲመዘገብ የተደረገው ኮምፒውተሩ ወይም የኮምፒውተር ስርዓቱ ከተሰራበት ዓላማ አንፃር በመደበኛነት እና በተከታታይነት ሲሰራበት ከነበረው ሁኔታ አይነት ከሆነ፤ ይህንኑ የሚያሳይ ማስረጃ በማቅረብና በማስረዳት አንድን የኤሌክትሮኒክስ መዝገብ ስርዓትን ትክክለኛነት ማረጋገጥ ይቻላል፡፡ በዚህም ሂደት መዝገቡ የተመዘገበበት ሂደት ከተፅዕኖ ነፃ በመሆን እና መደበኛውን ሂደት በተከተለ አኳኋን መሆኑን ማሳየት ይቻላል፡፡

ለፍርድ ቤት ግምት (አንቀፅ 35)

ከላይ በአንቀፅ 32፣ 33 እና 34 ለማብራራት እንደተሞከረው አንድ ማስረጃ ለቀረበው ጉዳይ አግባብነት ያለው ማስረጃ ከሆነ በቀጣይ የሚነሳው የማስረጃው ተቀባይነት መሆኑ ይታወቃል፡፡ የማስረጃውን ተቀባይነት በአግባቡ ለማሳየትም የማስረጃውን ተዓማኒነት እና ትክክለኛነት ማረጋገጥ ተገቢ ነው፡፡ በዚህ ሂደት ውስጥ ማስረጃው የተገኘበትን አግባብ እና ለማስረጃው

ምንጭ የሆነው ኮምፒውተር ወይም የኮምፒውተር ስርዓት አሰራርን መፈተሽ ያስፈልጋል። ሆኖም በሁሉም ጉዳይ ላይ የሙያዊ ትንተና እየሰጡ መሄድ ለፍትህ አካሄድ አስቸጋሪ ከሆነ ፍርድ ቤቶች ህግን፣ ፍሬ ነገርን እና ማስረጃን በማገናዘብ ውሳኔ ከመስጠታቸው በፊት አንድ ማስረጃ ያለውን አግባብነት ከታወቀ ተቀባይነቱን ለመወሰን እንደነገሩ ሁኔታ ኮምፒውተሩ ወይም የኮምፒውተር ስርዓቱ ስራውን የሚያከናውንበትን ሥነ-ሥርዓት፣ ደረጃ እና አሠራር ግምት ውስጥ ማስገባት ይችላል። አንድ የኮምፒውተር ስርዓት ላይ በህገ-ወጥ መንገድ አንድ ሰው ከገባ ወይም ደራሽነትን ከተላለፈ፤ የኮምፒውተር ስርዓቱ የሚሰራበትን ወይም በማን አማካይነት ሲሰራበት የነበረ መሆኑን ግምት ውስጥ በማስገባት ፍርድ ቤቱ በህገ ወጥ መንገድ የኮምውተር ስርዓቱ ተደርሶበታል ወይም አልተደረሰበትም የሚለውን ለመወሰን የሚያስችለውን ማስረጃ ተቀባይነት የኮምፒውተር አሰራሩን ግምት ወስጥ በማስገባት ሊወስን ይችላል።

በሌላ በኩል አንድ የኮምፒውተር ስርዓት ለምሳሌ አንድ የፕሪንተር ማሽን በምን መንገድ፣ አሰራርና ስነ-ስርዓት መሰረት እንደሚሰራ ከታወቀ በሂደቱ የተገኘውን ማስረጃ ተቀባይነት ለመወሰን ተመሳሳይ የሆነው ፕሪንተር የሚሰራበትን ስነ-ስርዓት፣ ደረጃ እና አሰራር በማየት የማስረጃውን ተቀባይነት ግምት መውሰድ ይቻላል። ስለሆነም ፍርድ ቤት ከአንድ ኮምፒውተር የተገኘ ወይም የአንድ ኮምፒውተር ውጤት የሆነ የኤሌክትሮኒክ ማስረጃን ተቀባይነት ለመወሰን ሌላ ተመሳሳይ ኮምፒውተር ስራውን የሚያከናውንበትን ስነ-ስርዓት፣ ደረጃ እና አሰራር በማየት ማስረጃው በተመሳሳይ የኮምፒውተር ስርዓት የአሰራር ስነ-ስርዓት እና ደረጃ የተገኘ እና ተቀባይነት ያለው መሆኑን ግምት መውሰድ ይችላል።

የማስረዳት ሸክም (አንቀፅ 36)

በወንጀል ፍትህ ስርዓት ውስጥ የወንጀል ክስ የማቅረብ ሃላፊነት የመንግስት ሲሆን ከመንግስት አካላት መካከል የአቃቤ ህግ መሆኑን በልዩ ልዩ አዋጆች ተደንግጎ እናገኘዋለን። (አዋጅ ቁጥር 39/85፣ አዋጅ ቁጥር 74/86፣ አዋጅ ቁጥር 691/2003 እና በወንጀል ሥነ-ሥርዓት ሕጎቻችን) ስለሆነም አቃቤ ህግ የሕግ የበላይነት ለማስከበር ሲል ለሚያቀርባቸው ማናቸውም የወንጀል ክሶች ማስረጃዎችን በማቅረብ ክስን እንደክሱ አቀራረብ የማስረዳትና እና በክሱ ዝርዝር ውስጥ የተነሱ ፍሬ ነገሮችን በትክክል በማስረጃ አስደግፎ በበቂ ሁኔታ ማስረዳት ይኖርበታል።

ስለዚህ አቃቤ ህግ በዋናነት የሚጠበቀው ባቀረበው ክስ ላይ የተመለከቱ ፍሬ ነገሮችን በበቂ ሁኔታ በማስረጃ ማረጋገጥ እና እንደክሱ አግባብ ማስረዳት ይኖርበታል። በዚህ ሂደት ውስጥ

በወንጀል ስነ-ስርዓት ሕግ ቁጥር 134 መሰረት ጥፋተኝነቱን ያመነ ማንኛውም ተከሳሽ ወዲያው ጥፋተኛ ሊባል ወይም ማስረጃ ማሰማት አስፈላጊ ከሆነ ማስረጃው እንዲቀርብ ሊደረግ እንደሚችል ተደንግጓል፡፡ ከዚህም በተጨማሪ በወንጀል ስነ-ስርዓት ህግ ቁጥር 133 መሰረት አንድ ተከሳሽ ክዶ ከተከራከረ አቃቤ ህግ ያቀረበውን ክስ በበቂ ሁኔታ ካስረዳ እና ተከሳሹ ካልተከላከለ የጥፋተኛነት ውሳኔ ሊሰጥ ይችላል፡፡ ስለዚህ ለኮምፒውተር ወንጀሎችም ይኸው ድንጋጌ እና የማስረጃ ምዘና ስርዓት ተፈፃሚ ይደረጋል ማለት ነው፡፡

ከኮምፒውተር ወንጀል አፈፃጸም ውስብስብነት የተነሳ ማስረጃን የማግኘት እና ለፍርድ ቤቱ የማቅረብ ሂደት እንቅፋት ሊገጥመው እንደሚችል ይታወቃል፡፡ ከወንጀል ፈፃሚዎቹ የአፈፃፀም ሂደት፤ ከጉዳዩ ውስብስብነት እና ወንጀሉ በአብዛኛው ቀጥታ ንኪኪን መሰረት ባላደረገ መልኩ የሚፈፀም ወንጀል በመሆኑ በክሱ ለተዘረዘሩ ፍሬ ነገሮች በሙሉ ማስረጃዎችን ማቅረብ ያስቸግራል፡፡ በዚህን ጊዜ ምንም እንኳ አቃቤ ህግ ያቀረበውን ክስ አንደ ክሱ አቀራረብ የማስረዳትና በማስረጃ የማረጋገጥ ግዴታ ቢኖረውም በልዩ ሁኔታ (Exception) የማስረዳት ሸክሙ ወደ ተከሳሽ የሚዞርበት አሰራሮች አሉ፡፡ ሆኖም የማስረዳት ሸክምን የማዛወር ሁኔታ እንደ ነገሩ ሁኔታ በህግ (Legal Shifting of Burden of Proof) ወይም በፍርድ ቤት (Shift of Burden of Proof by Court) ሊሆን ይችላል፡፡ ለውስን የወንጀል ጉዳዮች ማለትም እንደ ሙስና፣ ሽብርተኝነት ወዘተ ለመሳሰሉት የወንጀል ጉዳዮች የማሰረዳት ሸክምን የማዛወር ሂደት በህግ ተደንግጎ ይገኛል፡፡ ሆኖም ለሌሎች ወንጀሎች ነገር ግን የወንጀል አፈፃፀም ሂደታቸው ውስብስብ ለሆኑ እንደ ኮምውተር ወንጀል አይነቶች በተቻለ አቅም በመርህ ደረጃ አቃቤ ህግ ያቀረበውን ክስ በሙሉ በማስረጃ እንዲያረጋግጥ፤ በተወሰኑ ሁኔታዎች ደግሞ ፍርድ ቤቱ የማስረዳት ሸክምን ወደ ተከሳሽ እንዲያዛውር የሚያደርግበትን ሁኔታ መቅረፅ ተገቢ ነው፡፡ በዚህም ሂደት በልዩ ሁኔታ አቃቤ ህግ መሠረታዊ ፍሬ ነገሮችን ካስረዳ እና ፍርድ ቤት የማስረዳት ኃላፊነቱን ወደ ተከሳሹ ማዞር አስፈላጊ መሆኑን ካመነ የማስረዳት ሸክም ከአቃቤ ህግ ወደ ተከሳሽ የሚዛወርበት ሁኔታ እንዲፈቀድ የተደረገ ሲሆን በዚህም ወንጀል አድራጊዎች የተሟላ ማስረጃ ባለመቅረቡ ብቻ ከወንጀል ሃላፊነት እንዳያመልጡ የሚደረግበት አሰራር ለመከተል ታሳቢ የተደረገ ነው፡፡ ስለዚህ እንደ ወንጀሉ ውስብስብነት እና ክብደት ፍርድ ቤቱ እየመዘነ የማስረዳት ሸክምን ወደ ተከሳሽ እንዲዛወር እንዲያደርግ በዚህ ህግ ተፈቅዷዋል፡፡

ክፍል አምስት

የኮምፒውተር ወንጀልን የሚከታተሉ ተቋማት

የኮምፒውተር ወንጀል ለመከላከል፣ ለመቆጣጠር፣ ለመመርመርና ወንጀለኞች ወደ ፍትህ ለማቅረብ አዳዲስ ስልቶችና ቴክኒኮች እንዲሁም አዳዲስ አደረጃጀቶች እንደሚያስፈልግ ከላይ በስፋት ተብራርቷል። በዚህ መሰረትም የኮምፒውተር ወንጀልን የመከታተል ስልጣን በዋናነት የፖሊስና የአቃቤ ህግ ቢሆንም እነዚህ አካላት በተለመደው የአሰራር ስርዓት የኮምፒውተር ወንጀልን መከታተል ስለማይችሉ የሰለጠኑ፣ አስፈላጊውን ቴክኖሎጂ የታጠቁ እና ለዚህ ብቻ ተብለው የተደራጁ የስራ ክፍሎች ሊኖሩ እንደሚገባ አያጠያይቅም። ስለሆነም የአቃቤ ህግ ተቋም እና ፖሊስ የኮምፒውተር ወንጀልን የሚከታተሉ ልዩ የስራ ክፍል ማደራጀት እንደሚችሉ በአዋጁ አንቀጽ 37 ተመልክቷል። ከዚህም በተጨማሪ የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ በኮምፒውተር ወንጀል የምርመራ ሂደት የመተባበር እና አስፈላጊውን ቴክኒካል ድጋፍ የማድረግ ሃላፊነት ያለበት በመሆኑ በቀጥታ የኮምፒውተር ስርዓት አማካኝነት (online investigation) የኮምፒውተር ወንጀል ምርመራ የሚካሄድበትን ስርዓት የመዘርጋት እና ሌሎች አስፈላጊ የምርመራ ቴክኖሎጂዎችን እና ዘዴዎችን የማቅረብ ሃላፊነት እንዳለበት በአንቀፅ 38 ተደንግጓል።

ሌላው ከዚህ ጋር ተያይዞ የሚነሳው ሐሳብ የወንጀል ድርጅቱን በመመርመር እና በክስ ሂደት ውስጥ ተሳታፊ የሚሆኑ ልዩ ልዩ አካላት ሚናን እንዴት ማቀናጀት ይቻላል የሚለው ነው። በተለይም ወንጀሉ ከሌሎች ወንጀሎች ጋር እየተደራረበ በሚመጣባቸው ሁኔታዎች ላይ የልዩ ልዩ አካላት ተሳትፎ ከማስፈለጉም በላይ በልዩ ህጎች ለሌሎች አካላት የተሰጡ ሃላፊነቶችን በማክበር ቅንጅታዊ አሰራር እንዲፈጠር ማድረግ ያስፈልጋል። በተለይም ለወንጀሉ ምርመራ እና የክስ ሂደት ውጤታማነት የፌዴራል ፖሊስ፣ የፍትህ ሚኒስቴር፣ የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ እና ሌሎች የሚመለከታቸው አካላት (ማለትም የፌዴራል የስነ ምግባርና የፀረ ሙስና ኮሚሽን፣ የገቢዎችና ጉምሩክ ባለስልጣን፣ የፋይናንስ ደህንነት መረጃ ማዕከል ወዘተ) ተሳትፎ እጅግ ወሳኝ ነው። ስለሆነም በእነዚህ አካላት መካከል የሚኖረውን ተሳትፎ ለማቀናጀት የሚያስችል የአስፈፃሚ ግብረ ሃይል እንዲኖር ማድረግ በእነዚህ አካላት መካከል ቅንጅት እንዲፈጠርና ስኬታማ ስራ ለመስራት ያስችላል። (አንቀፅ 40) ግብረ-ሀይሉ በፍትህ ሚኒስቴር አማካይነት እንዲመራ ሲደረግ በአብዛኛው በደህንነት ተቋማቱ እና በህግ አስከባሪ አካላት መካከል ምክንያታዊ ግንኙነት እንዲኖር እና በጋራ መስራት በሚችሉበት ሁኔታ

የሚፈጠረው ግንኙነት ከፌዴራል መንግስት አማካሪነት እና የህግ የበላይነትን ከማስከበር ሃላፊነት አኳያ የተቃኘ እንዲሆን ለማስቻል ነው፡፡

የኮምፒውተር ወንጀል በባህሪው ድንበር የለሽ እና አለም አቀፍ ይዘት ያለው ስጋት ነው፡፡ ስለሆነም ስጋቱን ለመከላከል አለም አቀፍ ትብብርና ይህንኑ የሚያመቻች የህግ ማዕቀፍ ወይም ስምምነት ይጠይቃል፡፡ በዚህ መሰረትም የፍትህ ሚኒስቴር መረጃ መለዋወጥን፣ በጋራ የምርመራ ስራ ማከናወንን፣ ወንጀለኛ አሳልፎ መስጠትን እና ሌሎች ጉዳዮች ጨምሮ የኮምፒውተር ወንጀል በሚመለከቱ ጉዳዮች ላይ ከሌላ ሀገር አግባብ ያላቸው ተቋማት ጋር በትብብር መስራት እንዳለበት ተመልክቷል (አንቀፅ 41 ንዑስ አንቀፅ 1)፡፡ በተመሳሳይ መልኩ መርማሪ አካላት የኮምፒውተር ወንጀልን ለመከላከል ወይም ለመመርመር አስፈላጊ የሆኑ መረጃዎችና ማስረጃዎች ለማግኘት ተመሳሳይ ተልእኮ ካላቸው የውጭ ሃገር ተቋማት ጋር የመረጃ ልውውጥ ማድረግ እና የተለያዩ ስምምነቶች መፈራረም እንደሚችል በአንቀፅ 41 ንዑስ አንቀፅ (2) የተደነገገ የተደነገገ ሲሆን በዘርፉ በሚደረገው ትብብር ለመረጃ ልውውጥ ሲባል መርማሪ አካል ከሌላ አገር መርማሪ አካል ጋር እና ሌሎቹም ተቋማት እንዲሁ መገናኘት ይችላሉ፡፡

የኮምፒዩተር ስርዓትን ወይም ንብረትን ስለማገድ፣ መውረስ ወይም መዝጋት (አንቀጽ 42)

ወንጀል ፈፃሚዎችን በፍርድ ሂደት ወንጀል መፈፀማቸው ከተረጋገጠ በኋላ እንደ ተሳትፎ ደረጃቸው፣ እንደወንጀሉ ክብደት እና አፈፃፀም ፍርድ ቤት ቅጣት ይወስናል፡፡ ከቅጣት አይነቶች አንዱ ደግሞ የንብረት መውረስ ይሆናል፡፡ የንብረት መውረስ ቅጣት በዋናነት ለወንጀሉ መፈፀሚያ ጥቅም ላይ የዋለን ንብረት ለመያዝ፣ ለሌላ ወንጀል ጥቅም ላይ እንዳይውል ለማድረግ፣ ወንጀል መፈፀሚያ መሣሪያዎችን ለመግዛት፣ ለማቅረብ፣ ወዘተ የሚያስችሉ የገንዘብ ምንጮችን ለማድረቅ እና በህገ ወጥ መንገድ ተገኘን ንብረት ጥቅም ላይ እንዳይውል ለማስቻል ሲሆን በግልፅ በተደነገገ ጊዜ በህጋዊ መንገድም ቢሆን የተገኘ ገንዘብ/ንብረት ለወንጀል ተግባር ድጋፍ እንዳይሰጥበት ለመከላከል የሚደረገውን የመውረስ ትዕዛዝ ያጠቃልላል፡፡ ስለሆነም በኮምፒውተር ወንጀሎች ላይ የእስራት ቅጣትን እና የመቀጮ ቅጣት እንደወንጀሉ ሁኔታ በግልፅ ተደንግጓል፡፡ ከዚህም በተጨማሪ የኮምፒውተር ወንጀልን ለመፈጸም ጥቅም ላይ የዋለን ማንኛውም የኮምፒውተር ስርዓት፣ ዳታ ወይም መሳሪያ እንደነገሩ ሁኔታ ማገድ፣ መውረስ፣ እንዲወገድ ማድረግ ወይም አገልግሎቱ እንዲዘጋ ማድረግ ወንጀሉ በድጋሚ እንዳይፈፀም ወይም ወንጀሉን ለመፈፀም ጥቅም ላይ የዋለ ስርዓት ወይም

መሳሪያ ወይም ዳታ ለሌላ ወንጀል መፈፀሚያ እንዳይውል ማድረግ ተገቢ አስፈላጊ በመሆኑ በተጨማሪ ቅጣትነት ንብረቱ እንዲወረስ ወይም የኮምፒውተር ስርዓት ከሆነ እንዲዘጋ ወይም ጥቅም ላይ የዋለው ዳታ እንዲወገድ ወይም እንደነገሩ ሁኔታ ጥቅም ላይ የዋለ የኮምፒውተር ስርዓት ደህንነቱ እስኪረጋገጥ ወይም ለሌላ ወንጀል መፈፀሚያ ጥቅም ላይ እንዳይውል እስኪደረግ ድረስ ለጊዜው እንዲታገድ ፍርድ ቤት ትዕዛዝ እንዲሰጥበት በዚህ ህግ እንዲደነገግ ተደርጓል፡፡ ይህም ሌሎች ወንጀሎች እንዳይፈጸሙ የሚደረገውን የመከላከል ሂደት የሚያግዝ ይሆናል ማለት ነው፡፡

ከዚህም በተጨማሪ የኮምፒውተር ወንጀሎችን በመፈጸም በቀጥታም ሆነ በተዘዋዋሪ መንገድ የተገኙ ሐብቶች ለሌሎች የኮምፒውተር ወይም ሌሎች ወንጀሎች መፈፀሚያነት እንዳይውሉ ለማድረግ ሲባል በዚህ ህግ መሰረት እንዲወረሱ ተደንግጓል፡፡ ይህን የወንጀል ድርጊት በመፈጸም የሚገኘውን ሐብት ለመቆጣጠር እና በማናቸውም መልክ የሚኖርን የሃብት ምንጭ ማድረቅ አስፈላጊ በመሆኑ ነው፡፡

ማጠቃለያ

ከላይ በዝርዝር ለማቀመጥ እንደተሞከረው የኮምፒውተር ወንጀል የምንለው ኮምፒውተርን ወይም የኮምፒውተር ስርዓቱን መሰረት በማድረግ የሚፈፀም ወንጀል ሲሆን በኮምፒውተሩ ወይም በኮምፒውተር ስርዓቱ ላይ የሚፈፀም ወንጀልን፣ ኮምፒውተሩን ወይም ስርዓቱን እንደመሳሪያ በማድረግ የሚፈፀም ወንጀልን እና ኮምፒውተሩን የማያስፈልጉ ለምሳሌ ለመልካም ጠባይ ጠቃራኒ የሆኑ ነገሮችን ማከማቻ በማድረግ የሚፈጸሙ ወንጀሎች የሚያጠቃልል ነው፡፡ እነዚህ ድርጊቶች በተለይም በአገራችን ቁልፍ መሰረተ ልማቶች ላይ የሚፈፀሙ ከሆኑ የሚፈጥሩት ማህበራዊ፣ ኢኮኖሚያዊ ወዘተ ጉዳቶች ከፍተኛ በመሆናቸው እና በተለይም በሳይበር ምህዳሩ ውስጥ የሚኖሩ ጥቃቶችን ከወዲሁ ለመከላከልና ለመቆጣጠር ልዩ ህግ ማውጣት የግድ የሚያስፈልግ ይሆናል፡፡ ከዚህም በተጨማሪ የሚኒስትሮች ምክር ቤት በ2003 ባጸደቀው የወንጀል ፍትህ ፖሊሲ ገፅ 62 ነጥብ 4.9 ላይ እንደተመለከተው የኮምፒውተር ወንጀሎችን ለመከላከልና ለመቆጣጠር እንዲሁም ወንጀል ሲፈጸም የሚኖሩ የምርመራ፣ የክስና የክርክር እንዲሁም የማስረጃ ምዘና ስርዓቶችን በግልፅ ለመወሰን የሚያስችል እና በሂደቱም የሚኖሩ አደረጃጀቶችንና አሰራሮችን ለመዘርጋት የሚስችል ህግ መውጣት እንዳለበት አቅጣጫ አስቀምጧል፡፡

ስለሆነም የዚህ ህግ መውጣት በአንድ በኩል መንግስትና ህዝብ ከኮምፒውተር/ ከኮምፒውተር ስርዓት አገልግሎት የሚያገኙትን ጥቅም በተቻለ መጠን ያለምንም እንከን ማግኘት እንዲችሉና በተለይም የቁልፍ መሰረተ ልማቶችን ደህንነት በአግባቡ ለማስጠበቅና ይህንኑ ለማረጋገጥ በሌላ በኩል ወንጀለኞች አገልግሎቱን እንደመሳሪያ በመጠቀም በህዝቡ ሰላምና ደህንነት፣ በአገሪቱ ማህበራዊ፣ ኢኮኖሚያዊ ወዘተ እንቅስቃሴዎች እና የልማት ውጥኖች ላይ ጉዳት እንዳያደርሱ አስቀድሞ ለመከላከልና ለመቆጣጠር፣ ጉዳቱንም አድርሰው/ወንጀል ፈፅመው በተገኙት ላይም ተመጣጣኝ ቅጣት ሊያገኙበት የሚችሉበትን ስርዓት ለመዘርጋትና ውጤታማ ስራ ለመስራት በጣም ጠቃሚ ነው፡፡