የኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ
ፌደራል ነጋሪት ጋዜጣ
FEDERAL NEGARIT GAZETTE
OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

ሃያ ሁለተኛ ዓመት ቁጥር ፹፫
አዲስ አበባ ሰኔ ፴ ቀን ፪ሺ፰ ዓ.ም

በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ
የሕዝብ ተወካዮች ምክር ቤት ጠባቂነት የወጣ

22nd Year No. 83
ADDIS ABABA 7th July, 2016

አዋጅ ቁጥር ፱፻፶፰/ ፪ሺ፰

የኮምፒዩተር ወንጀል አዋጅ………………..…ገጽ ፱ሺ፩፻፬

PROCLAMATION No. 958/2016

Computer Crime Proclamation ………Page 9104

ማውጫ

CONTENTS

አዋጅ ቁጥር ፱፻፶፰/ ፪ሺ፰

PROCLAMATION No.958/2016

የኮምፒዩተር ወንጀልን ለመደንገግ የወጣ አዋጅ

A PROCLAMATION TO PROVIDE FOR THE COMPUTER CRIME

የኢንፎርሜሽንና የኮምኒዩኬሽን ቴክኖሎጂ ለሃገሪቱ ኢኮኖሚያዊ፣ ማህበራዊና ፖለቲካዊ እድገት ቁልፍ ሚና የሚጫወት በመሆኑ፤

የኢንፎርሜሽንና የኮምኒዩኬሽን ቴክኖሎጂ አጠቃቀም ተገቢ ጥንቃቄና ጥበቃ ካልተደረገለት የሃገሪቱን ሁለንተናዊ እድገት ሊያደናቅፍ እንዲሁም የዜጎችን የግል ነፃነት አደጋ ላይ ሊጥሉ ለሚችሉ የተለያዩ የኮምፒዩተር ወንጀሎች እና ሌሎች የደህንነት ስጋቶች የተጋለጠ በመሆኑ፤

በሥራ ላይ ያሉ የሀገሪቱ ሕጎች ከአዳዲስ የቴክኖሎጂ ለውጦች ጋር በበቂ ሁኔታ ተጣጥመው የማይሄዱ እና የኮምፒዩተር ወንጀልን ለመከላከል፣ ለመቆጣጠር፣ ለመመርመርና ተጠርጣሪዎችን ወደ ፍትህ ለማቅረብ የሚያስችሉ ባለመሆናቸው፤

WHEREAS, information and communication technology plays a vital role in the economic, social and political development of the country;

WHEREAS, unless appropriate protection and security measures are taken, the utilization of information communication technology is vulnerable to various computer crimes and other security threats that can impede the overall development of the country and endanger individual rights;

WHEREAS, the existing laws are not adequately tuned with the technological changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes;

https://ethiodata.et/

የኮምፒዩተር ወንጀልን ለመከላከል፣ ለመቆጣጠር፣ ለመመርመርና ኤሌክትሮኒክ ማስረጃዎችን ለመሰብሰብ የሚያስችሉ አዳዲስ ስልቶችንና ሥርዓቶችን በሕግ መደንገግ አስፈላጊ ሆኖ በመገኘቱ፤

በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ ህገ መንግስት አንቀጽ ፶፭(፩) መሰረት የሚከተለው ታውጇል፡-

ክፍል አንድ
ጠቅላላ

1. አጭር ርዕስ

ይህ አዋጅ "የኮምፒዩተር ወንጀል አዋጅ ቁጥር ፱፻፶፰/፪ሺ፰" ተብሎ ሊጠቀስ ይችላል፡፡

2. ትርጓሜ

የቃሉ አገባብ ሌላ ትርጉም የሚያሰጠው ካልሆነ በስተቀር በዚህ አዋጅ ውስጥ፤

1/ "የኮምፒዩተር ወንጀል" ማለት፡-

ሀ) በኮምፒዩተር፣ በኮምፒዩተር ስርዓት፣ በኮምፒዩተር ዳታ ወይም ኔትዎርክ ላይ የሚፈፀም ወንጀል፤

ለ) ኮምፒዩተርን፣ የኮምፒዩተር ስርዓትን፣ የኮምፒዩተር ዳታን ወይም ኔትዎርክን በመጠቀም የሚፈፀም መደበኛ ወንጀል፤ ወይም

ሐ) በኮምፒዩተር፣ በኮምፒዩተር ስርዓት ወይም ኔትዎርክ አማካኝነት የሚሰራጭ ህገወጥ የኮምፒዩተር ዳታ ይዘት ነው፤

2/ "የዳታ ፕሮሰሲንግ አገልግሎት" ማለት በኮምፒዩተር ሥርዓት አማካኝነት ዳታን የመቀበል፣ የማከማቸት፣ የመተንተን፣ የማሰራጨት፣ የማጓጓዝ ወይም የማስተላለፍ አገልግሎት ሲሆን የኔትዎርክ አገልግሎችንም ይጨምራል፤

WHEREAS, it has become necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute computer crimes and facilitate the collection of electronic evidences;

NOW, THEREFORE, in accordance with Article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows:

PART ONE
GENERAL

1. Short Title

This Proclamation may be cited as the "Computer Crime Proclamation No.958/2016".

2. Definitions

In this Proclamation unless the context otherwise requires:

1/ "Computer crime" means

a) A crime committed against a computer, computer system, computer data or computer network;

b) A conventional crime committed by means of a computer, computer system, computer data or computer network; or

c) Illegal computer content data disseminated through a computer, computer system, or computer network;

2/ "data processing service" means the service of reception, storage, processing, emission, routing or transmission of data by means of computer system and includes networking services;

https://ethiodata.et/

3/ "ኮምፒዩተር ወይም የኮምፒዩተር ሥርዓት" ማለት በሶፍትዌር እና ማይክሮቺፕ ቴክኖሎጂ ላይ የተመሰረተ የዳታ ፕሮሰሲንግ፣ ክምችት፣ ትንተና፣ ስርጭት፣ ግንኙነት ወይም ሌሎች ሂሳባዊ ወይም አመክንዮአዊ ተግባራትን የሚያከናውን ማንኛውም መሳሪያ ሲሆን የመሳሪያው ተገጣሚ አካልንም ይጨምራል፤

4/ "የኮምፒዩተር ዳታ" ማለት በኮምፒዩተር ሥርዓት አማካኝነት ሊተነተን የሚችል ማንኛውም የይዘት ዳታ፣ የትራፊክ ዳታ፣ የኮምፒዩተር ፕሮግራም ወይም ደንበኞችን የሚመለከት ማንኛውም ኢንፎርሜሽን ነው፤

5/ "የኮምፒዩተር ፕሮግራም" ማለት አንድ የኮምፒዩተር ሥርዓት ተግባሩን እንዲያከናውን ወይም የታሰበውን ውጤት እንዲያስገኝ የሚያስችል በቃላት፣ በኮድ ወይም በዘዴ የሚገለጽ የመመሪያ ወይም የትዕዛዝ ስብስብ ነው፤

6/ "የትራፊክ ዳታ" ማለት በኮምፒዩተር ሥርዓት አማካኝነት የሚደረግን ኮምዩኒኬሽን መነሻ፣ መድረሻ፣ ዑደት፣ ጊዜ፣ ቀን፣ የግንኙነት ቆይታ፣ የዳታው መጠን፣ የአገልግሎት ዓይነት ወይም መሰል የኮምዩኒኬሽን ሰንሰለት የሚያሳይ በኮምፒዩተር ስርዓቱ የሚመነጭ ዳታ ነው፤

7/ "የይዘት ዳታ" ማለት በድምፅ፣ በተንቀሳቃሽ ምስል፣ በስዕል፣ በሂሳባዊ ቀመር ወይም በሌላ ማንኛውም ቅርፅ የሚገኝን የተከማቸ ወይም በስርጭት ሂደት ላይ ያለ ዳታ ወይም የኮምፒዩተር ኮምዩኒኬሽን ምንነት፣ ፍሬ ነገር፣ ትርጉም ወይም መልዕክት የሚያሳይ የኮምፒዩተር ዳታ ነው፤

3/ "computer or computer system" means any software and the microchips technology based data processing, storage, analysis, dissemination and communication device or any device that is capable of performing logical, arithmetic or routing function and includes accessories of that device;

4/ "computer data" means any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system;

5/ "computer program" means a set of instructions or commands expressed in words, codesor schemes which are capable of causing a computer system to perform or achieve a particular task or result;

6/ "traffic data" means any computer generated data relating to a chain of communication by means of a computer system indicating the communication's origin, destination, route, time, date, duration, size or types of underlying service;

7/ "content data" means any computer data found in the form of audio, video, picture, arithmetic formula or any other form that conveys the essence, substance, meaning or purpose of a stored or transmitted computer data or computer communication;

https://ethiodata.et/

8/ “ኔትዎርክ” ማለት ሁለትና ከዚያ በላይ የኮምፒዩተር ሥርዓቶች እርስ በርስ በማስተሳሰር የዳታ ፕሮሰሲንግ አገልግሎት ለመስጠት ወይም ለማግኘት የሚያስችል ሥርዓት ነው፤

9/ “የኮምፒዩተር ዳታ ደህንነት” ማለት የኮምፒዩተር ዳታ እንዳይጠፋ፣ እንዳይቀየር፣ ላልተፈቀደለት አካል ተደራሽ እንዳይሆን፣ ምስጢራዊነቱ እንዳይጋለጥ ወይም ሌላ ማንኛውም ጉዳት እንዳይደርስበት መጠበቅ ነው፤

0/ “ደራሽነት” ማለት ከኮምፒዩተር 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፤

፲፩/ “ቁልፍ መሰረተ ልማት” ማለት በዚህ አዋጅ ከአንቀፅ 3 እስከ 6 የተመለከተው ማናቸውም የወንጀል ድርጊት ቢፈጸምበት በሕዝብ ደኅንነት እና በብሔራዊ ጥቅሞች ላይ ከፍተኛ ጉዳት ሊያደርስ የሚችል የኮምፒዩተር ሥርዓት፣ ኔትወርክ ወይም ዳታ ነው፤

፲፪/ “ጠለፋ” ማለት በኮምዩኒኬሽን ሂደት ላይ ያለን የኮምፒዩተር ዳታ ወይም የዳታ ፕሮሰሲንግ አገልግሎት መከታተል፣ መቅዳት፣ ማዳመጥ፣ መውሰድ፣ ማየት፣ መቆጣጠር ወይም ሌላ ተመሳሳይ ድርጊት ነው፤

፲፫ “አገልግሎት ሰጪ” ማለት በኮምፒዩተር ስርዓት አማካኝነት ቴክኒካዊ የዳታ ፕሮሰሲንግ ወይም የግንኙነት ስርዓት አገልግሎት ወይም ምትክ

8/ “network” means the interconnection of two or more computer systems by which data processing service can be provided or received;

9/ “computer data security” means the protection of a computer data from deleting, changing, and accessing by unauthorized person, compromising its confidentiality or any other damage;

10/ “access” means to communicate with, to enter in, store in, store data in, retrieve, or obtain data from, to view, to receive, move or copy data from a computer system, or otherwise make use of any data processing service thereof;

11/ “critical infrastructure” means a computer system, network or data where any of the crimes stipulated under article 3 to 6 of this proclamation, is committed against it, would have a considerable damage on public safety and the national interest;

12/ “interception” means real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data;

13/ “service provider” means a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system;

መሰረተ ልማት ለተጠቃሚዎች የሚያቀርብ ሰው ነው፤

፲፬/ "ጠቅላይ ዓቃቤ ሕግ" ማለት በህዝብ ተወካዮች ምክር ቤት የተሾመ የፌደራል ጠቅላይ ዓቃቤ ሕግ ኃላፊ ነው፤

፲፭/ "ዓቃቤ ሕግ" ማለት በጠቅላይ ዓቃቤ ሕጉ ተሹሞ በዓቃቤያነ ሕግ መተዳደሪያ ደንብ መሠረት የሚተዳደር የሕግ ባለሙያ፤ ሲሆን ጠቅላይ ዓቃቤ ሕጉንና ምክትል ጠቅላይ ዓቃቤያነ ሕግን ይጨምራል፤

፲፮/ "መርማሪ አካል" ማለት በሕግ የመመርመር ሥልጣን የተሰጠው አካል ነው፤

፲፯/ "ክልል" ማለት በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ ሕገ መንግሥት አንቀጽ ፵፯(፩) የተመለከተዉ ማንኛውም ክልል ሲሆን ለዚህ አዋጅ አፈፃፀም የአዲስ አበባ ከተማ እና የድሬዳዋ ከተማ አስተዳደሮችን ይጨምራል፤

፲፰/ "ፖሊስ" ማለት የፌደራል ፖሊስ ወይም የፌደራል ፖሊስ ሥልጣን በውክልና የተሰጠው የክልል ፖሊስ ነው፤

፲፱/ "ኤጀንሲ" ማለት የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ ነው፤

፳/ "ሰው" ማለት የተፈጥሮ ሰው ወይም በሕግ የሰውነት መብት የተሰጠው አካል ነው፤

፳፩/ ማንኛውም በወንድ ፆታ የተገለጸው ሴትንም ይጨምራል፡፡

14/ "Attorney General" means head of the Federal Attorney General appointed by the House of Peoples Representatives;

15 "Public prosecutor" means lawyer appointed by the Attorney General and administered by public prosecutors administration regulation and included the Attorney General and the deputy attorney generals;

16/ "investigatory organ" mean a person legally invested with the power of investigation;

17/ "regional state" means any state referred to in Article 47(1) of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose this Proclamation it includes Addis Ababa and Dire Dawa city administrations;

18/ "police" mean Federal Police or Regional State Police to whom the power of the Federal Police is delegated;

19/ "Agency" mean Information Network Security Agency;

20/ "person" means a physical or juridical person;

21/ any expression in the masculine gender includes the feminine.

https://ethiodata.et/

ክፍል ሁለት
የኮምፒዩተር ወንጀሎች ንኡስ ክፍል አንድ
በኮምፒዩተር ሥርዓትና በኮምፒዩተር ዳታ ላይ የሚፈፀሙ ወንጀሎች

፫. ሕገ ወጥ ደራሽነት

1/ ማንኛውም ሰው ሆነ ብሎ ያለፈቃድ ወይም ከተሰጠው ፈቃድ ውጪ የኮምፒዩተር ስርዓት፣ የኮምፒዩተር ዳታ ወይም ኔትዎርክ ደራሽነት በከፊልም ሆነ በሙሉ ያገኘ እንደሆነ ከሦስት ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፴ሺ. እስከ ብር ፶ሺ. በሚደርስ መቀጮ ወይም በሁለቱም ይቀጣል፡፡

2/ በዚህ አንቀጽ ንኡስ አንቀጽ (፩) ላይ የተመለከተው የወንጀል ድርጊት የተፈጸመው፣

ሀ) በሕግ የሰውነት መብት ለተሰጠው ተቋም አገልግሎት ብቻ በሚውል የኮምፒዩተር ሥርዓት፣ የኮምፒዩተር ዳታ ወይም ኔትዎርክ ላይ ከሆነ ከሶስት ዓመት እስከ አምስት ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፴ሺ. እስከ ብር ፶ሺ. በሚደርስ መቀጮ ያስቀጣል፣

ለ) በቁልፍ መሠረተ ልማት ላይ ከሆነ ከአምስት ዓመት እስከ አስር ዓመት የሚደርስ ጽኑ እስራት እና ከብር ፶ሺ. እስከ ብር ፩፻ሺ. በሚደርስ መቀጮ ያስቀጣል፡፡

4. ሕገ ወጥ ጠለፋ

1/ ማንኛውም ሰው ሆነ ብሎ ያለፈቃድ ወይም ከተሰጠው ፈቃድ ውጪ ይፋዊ ያልሆነን የኮምፒዩተር ዳታ ወይም የዳታ ፕሮሰሲንግ አገልግሎት የጠለፈ እንደሆነ ከአምስት ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፲ሺ. እስከ ፶ሺ. በሚደርስ መቀጮ ይቀጣል፡፡

2/ በዚህ አንቀጽ ንኡስ አንቀጽ (1) ላይ የተመለከተው የወንጀል ድርጊት የተፈጸመው:-

PART TWO
COMPUTER CRIMES SECTION ONE
CRIMES AGAINST COMPUTER SYSTEM AND COMPUTER DATA

3. Illegal Access

1/ Whosoever, without authorization or in excess of authorization, intentionally secures access to the whole or any part of computer system, computer data or network shall be punishable with simple imprisonment not exceeding three years or fine from Birr 30,000 to 50, 000 or both.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer system, computer data or network that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000;

b) a critical infrastructure, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000.

4. Illegal Interception

1/ Whosoever, without authorization or in excess of authorization, intentionally intercepts non-public computer data or data processing service shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

https://ethiodata.et/

ሀ) በሕግ የሰውነት መብት ለተሰጠው ተቋም አገልግሎት ብቻ በሚውል የኮምፒዩተር ዳታ ወይም የዳታ ፕሮሰሲንግ አገልግሎት ላይ ከሆነ ከአምስት ዓመት እስከ አስር ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፶ሺ. ሺ. እስከ ብር ፩፻ሺ. በሚደርስ መቀጮ ያስቀጣል፤

ለ) በቁልፍ መሠረተ ልማት ላይ ከሆነ ከአስር ዓመት እስከ አስራ አምስት ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፩፻ሺ. እስከ ብር ፪፻ሺ. በሚደርስ መቀጮ ያስቀጣል፡፡

5. <u>በኮምፒዩተር ሥርዓት ላይ ጣልቃ መግባት</u>

1/ ማንኛውም ሰው ሆነ ብሎ ያለፈቃድ ወይም ከተሰጠው ፈቃድ ውጪ የኮምፒዩተር ዳታን በማስገባት፣ በማሰራጨት፣ በማጥፋት ወይም በመለወጥ የኮምፒዩተር ሥርዓትን ወይም ኔትወርክን መደበኛ ተግባር በከፊልም ሆነ ሙሉ በሙሉ ያደናቀፈ፣ ያወከ፣ ያወደመ ወይም እንዲቋረጥ ያደረገ እንደሆነ ከሶስት ዓመት እስከ አምስት ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፶ሺ. በማይበልጥ መቀጮ ይቀጣል፡፡

2/ በዚህ አንቀጽ ንኡስ አንቀጽ (፩) ላይ የተመለከተው የወንጀል ድርጊት የተፈጸመው፣

ሀ) በሕግ የሰውነት መብት ለተሰጠው ተቋም አገልግሎት ብቻ በሚውል የኮምፒዩተር ሥርዓት ላይ ከሆነ ከአምስት ዓመት እስከ አስር ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፶ሺ. እስከ ብር ፩፻ሺ. በሚደርስ መቀጮ ያስቀጣል፤

a) a computer data or data processing service that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000.

b) a critical infrastructure, the punishment shall be rigorous imprisonment from ten years to fifteen years and fine from Birr 100,000 to 200,000.

5. <u>Interference with Computer System</u>

1/ Whosoever, without authorization or in excess of authorization, intentionally hinders,impairs, interrupts or disrupts the proper functioning of the whole or any part of computer system by inputting, transmitting, deleting or altering computer data shall be punishable with rigorous imprisonment from three years to five years and fine not exceeding Birr 50,000.

2/ where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer system that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000;

https://ethiodata.et/

ለ) በቁልፍ መሠረተ ልማት ላይ ከሆነ ከአስር ዓመት እስከ አስራ አምስት ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፩፻ሺ እስከ ብር ፪፻ሺ በሚደርስ መቀጮ ወይም ነገሩ ከባድ በሆነ ጊዜ ከአስራ አምስት ዓመት እስከ ሃያ ዓመት በሚደርስ ፅኑ እስራት እና ከብር ፪፻ሺ እስከ ብር ፭፻ሺ በሚደርስ መቀጮ ያስቀጣል፡፡

6. **<u>በኮምፒዩተር ዳታ ላይ ጉዳት ማድረስ</u>**

1/ ማንኛውም ሰው ሆነ ብሎ ያለፈቃድ ወይም ከተሰጠው ፈቃድ ውጪ የኮምፒዩተር ዳታን የለወጠ፣ ያጠፋ፣ ያፈነ፣ ትርጉም እንዳይኖረው ወይም ጥቅም እንዳይሰጥ ወይም ለሕጋዊ ተጠቃሚዎች ተደራሽ እንዳይሆን ያደረገ እንደሆነ ከሦስት ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፴ሺ በማይበልጥ መቀጮ ይቀጣል፡፡

2/ በዚህ አንቀጽ ንኡስ አንቀፅ (፩) ላይ የተመለከተው የወንጀል ድርጊት የተፈጸመው፣

ሀ) በሕግ የሰውነት መብት ለተሰጠው ተቋም አገልግሎት ብቻ በሚውል የኮምፒዩተር ዳታ ላይ ከሆነ ከሦስት ዓመት እስከ አምስት ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፴ሺ እስከ ብር ፶ሺ በሚደርስ መቀጮ ያስቀጣል፤

ለ) በቁልፍ መሠረተ ልማት ላይ ከሆነ ከአምስት ዓመት እስከ አስር ዓመት የሚደርስ ጽኑ እስራት እና ከብር ፶ሺ እስከ ብር ፩፻ሺ በሚደርስ መቀጮ ያስቀጣል፡፡

7. **<u>ከኮምፒዩተር መሣሪያና ዳታ አጠቃቀም ጋር የተያያዙ ወንጀሎች</u>**

1/ ማንኛውም ሰው በኮምፒዩተር ሥርዓት፣

b) a critical infrastructure, the punishment shall be rigorous imprisonment from ten years to fifteen years and fine from Birr 100,000 to 200,000 or, in serious case, rigorous imprisonment from fifteen years to twentey years and fine from Birr 200,000 to 500,000.

6. **<u>Causing Damage to Computer Data</u>**

1/ Whosoever, without authorization or in excess of authorization, intentionally alters, deletes, suppresses a computer data, renders it meaningless, useless or inaccessible to authorized users shall be punishable with rigorous imprisonment not exceeding three years and fine not exceeding Birr 30,000.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer data that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000;

b) a critical infrastructure, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000.

7. **<u>Criminal Acts Related to Usage of Computer Devices and Data</u>**

1/ Whosoever, knowing that it can cause damage to computer system, computer data or network, intentionally transmits

https://ethiodata.et/

በኮምፒዩተር ዳታ ወይም በኔትዎርክ ላይ
 ት ሊያደርሱ እንደሚችሉ እያወቀ ለዚህ ዓላማ ተብለው የተመረቱ ወይም የተሻሻሉ የኮምፒዩተር ፕሮግራሞችን ሆነ ብሎ በኮምፒዩተር ሥርዓት አማካኝነት ያሰራጨ እንደሆነ ከአምስት ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፴ሺ በማይበልጥ መቀጮ ይቀጣል።

2/ ማንኛውም ሰው በዚህ አዋጅ ከአንቀጽ 3 እስከ 6 የተዘረዘሩትን የወንጀል ድርጊቶች ለማስፈጸሚያ እንደሚውሉ እያወቀ ለዚህ ዓላማ የሚውሉ የኮምፒዩተር መሣሪያዎችን ወይም የኮምፒዩተር ዳታዎችን ሆነ ብሎ ወደ ሀገር ውስጥ ያስገባ፣ ያመረተ፣ ለሽያጭ ያቀረበ፣ ያከፋፈለ ወይም ሌሎች እንዲያገኙት ያመቻቸ እንደሆነ ከአምስት ዓመት በማይበልጥ ጽኑ እስራትና ከብር ፲ሺ እስከ ብር ፶ሺ በሚደርስ መቀጮ ይቀጣል።

3/ ማንኛውም ሰው በዚህ አዋጅ ከአንቀጽ 3 እስከ 6 የተዘረዘሩትን የወንጀል ድርጊቶች ለመፈፀም በማሰብ በዚህ አንቀጽ ንዑስ አንቀጽ (1) ወይም (2) የተመለከቱትን የኮምፒዩተር መሳሪያዎች ወይም ዳታዎች ይዞ የተገኘ እንደሆነ ከሦስት ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፭ሺ እስከ ብር ፴ሺ በሚደርስ መቀጮ ይቀጣል።

4/ ማንኛውም ሰው ሆነ ብሎ ያለፈቃድ ወይም ከተሰጠው ፈቃድ ውጭ የኮምፒዩተር ሥርዓት፣ የኮምፒዩተር ዳታ ወይም ኔትዎርክ ደራሽነት ማግኘት የሚያስችል የኮምፒዩተር ፕሮግራም፣ የምስጢር ኮድ፣ ቁልፍ፣ የይለፍ ቃል ወይም ሌላ መሰል ዳታ ይፋ ያደረገ ወይም ለሌላ ሰው አሳልፎ የሰጠ እንደሆነ ከአምስት ዓመት በማይበልጥ ቀላል እስራት ወይም ነገሩ ከባድ በሆነ ጊዜ እስከ አምስት ዓመት በሚደርስ ጽኑ

any computer program exclusively designed or adapted for this purpose shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 30,000.

2/ Whosoever, knowing that it is to be used for the commission of unlawful act specified under Articles 3 to 6 of this Proclamation, intentionally imports, produces, offers for sale, distributes or makes available any computer device or computer program designed or adapted exclusively for the purpose of committing such crimes shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

3/ Whosoever possesses any computer devices or data specified under sub-article (1) or (2) of this Article with the intention to further the commission of any of the crimes specified under Articles 3 to 6 of this Proclamation shall be punishable with simple imprisonment not exceeding three years or fine from Birr 5,000 to 30, 000.

4/ Whosoever, without authorization or in excess of authorization, intentionally discloses or transfers any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or network shall be punishable with simple imprisonment not exceeding five years or in serious cases with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

https://ethiodata.et/

እስራት እና ከብር ፲ሺ እስከ ብር ፻ሺ ፱ሺ፩፻፲፫ ደርስ መቀጮ ይቀጣል።

5/ በዚህ አንቀጽ ንኡስ አንቀፅ (4) ላይ የተመለከተውን የወንጀል ድርጊት በቸልተኝነት የተፈፀመ እንደሆነ ቅጣቱ ከአንድ ዓመት የማይበልጥ ቀላል እስራት እና ከብር ፲ሺ የማይበልጥ መቀጮ ይሆናል።

8. <u>ከባድ ሁኔታዎች</u>

በዚህ አዋጅ ከአንቀጽ 3 እስከ 6 የተመለከተው ማንኛውም የወንጀል ድርጊት የተፈፀመው፡-

ሀ) ለወታደራዊ ጥቅም ወይም ለዓለም አቀፍ ግንኙነት ሲባል በሚመለከተው አካል ጥብቅ ምስጢር ተብሎ በተሰየመ የኮምፒዩተር ዳታ ወይም ዳታው በሚገኝበት የኮምፒዩተር ሥርዓት ወይም ኔትዎርክ ላይ ከሆነ፣ወይም

ለ) አስቸኳይ ጊዜ አዋጅ በታወጀበት ወይም ሀገሪቱ በአስጊ ሁኔታ ላይ በምትገኝበት ወቅት ከሆነ፣ ቅጣቱ ከአስራ አምስት ዓመት እስከ ሃያ አምስት ዓመት በሚደርስ ጽኑ እስራት ይሆናል፡፡

<u>**ንኡስ ክፍል ሁለት**</u>

<u>**በኮምፒዩተር አማካኝነት የሚፈፀሙ የማጭበርበር፣ የማታለል እና የስርቆት ወንጀሎች**</u>

9. <u>የኮምፒዩተር ዳታን ወደ ሐሰት መለወጥ</u>

ማንኛውም ሰው የሌላውን ሰው መብት ወይም ጥቅም ለመጉዳት ወይም ለራሱ ወይም ለሌላ ሰው ተገቢ ያልሆነ ማናቸውንም መብት ወይም ጥቅም ለማግኘት ወይም ለማስገኘት በማሰብ ሕጋዊ ውጤት ያለውን ወይም ሊኖረው የሚችለውን የኮምፒዩተር ዳታ ወደ ሐሰት የለወጠ ወይም ሐሰተኛ የኮምፒዩተር ዳታ ያዘጋጀ ወይም በዚሁ የተገለገለ እንደሆነ ከሦስት ዓመት በማይበልጥ ቀላል እሥራት እና ከ፴ሺ ብር በማይበልጥ መቀጮ ወይም ወንጀሉ ከባድ በሆነ ጊዜ ከአስር ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፲ሺ

5/ Where the crime stipulated under sub-article (4) of this Article is committed negligently, the punishment shall be simple imprisonment not exceeding one year and fine not exceeding Birr 10,000.

8. <u>Aggravated Cases</u>

Where the crime stipulated under Article 3 to 6 of this Proclamation is committed:

a) against a computer data or a computer system or network which is designated as top secrete by the concerned body for military interest or international relation, or

b) while the country is at a state of emergency or threat,the punishment shall be rigorous imprisonment from fifteen years to twenty five years.

<u>**SECTION TWO**</u>

<u>**COMPUTER RELATED FORGERY, FRAUD AND THEFT**</u>

9. <u>Computer Related Forgery</u>

Whosoever falsifies a computer data, makes false computer data or makes use of such data to injure the rights or interests of another or to procure for himself or for another person any undue right or advantage shall be punishable with simple imprisonment not exceeding three years and fine not exceeding Birr 30,000 or in a serious cases with rigorous imprisonment not exceeding ten years and fine from Birr 10,000 to 100,000.

https://ethiodata.et/

እስከ ብር ፩፻ሺ በሚደርስ መቀጮ ይቀጣል፡፡

፱ሺ፩፻፲፬

፲. በኮምፒዩተር አማካኝነት የሚፈፀም የማታለል ወንጀል

1/ ማንኛውም ሰው አሳሳች የኮምፒዩተር ዳታዎችን በማሰራጨት፣ የራሱን ማንነት ወይም ሁኔታ በመሰወር ወይም መግለጽ የሚገባውን ነገር በመደበቅ ወይም የሌላውን ሰው የተሳሳተ እምነት በመጠቀም፣ ሌላውን ሰው አታልሎ የራሱን ወይም የሶስተኛ ወገንን ማንኛውም ጥቅም የሚጎዳ ድርጊት እንዲፈጽም ያደረገው እንደሆነ ከአምስት ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፶ሺ በማይበልጥ መቀጮ ይቀጣል፡፡

2/ ማንኛውም ሰው በተጭበረበረ መንገድ የማይገባ ጥቅም ለማግኘት ወይም ለሌላ ሰው ለማስገኘት የኮምፒዩተር ዳታን በመለወጥ፣ በማጥፋት ወይም ሌላ ማንኛውም ጉዳት በማድረስ በሌላ ሰው ላይ ኢኮኖሚያዊ ጉዳት ያደረሰ እንደሆነ ከአምስት ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፲ሺ እስከ ብር ፶ሺ በሚደርስ መቀጮ ወይም ወንጀሉ ከባድ በሆነ ጊዜ እስከ አስር ዓመት በሚደርስ ጽኑ እስራት እና ከብር ፲ሺ እስከ ብር ፩፻ሺ በሚደርስ መቀጮ ይቀጣል።

፲፩. የኤሌክትሮኒክ ማንነት ስርቆት

ማንኛውም ሰው በዚህ አዋጅ አንቀጽ ፲ ላይ የተመለከተውን የወንጀል ድርጊት ለመፈፀም በማሰብ ወይም ለሌላ ማንኛውም ዓላማ የሌላን ሰው የኤሌክትሮኒክ ማንነት የሚያረጋግጥ ዳታ ያለባለቤቱ ፈቃድ በኮምፒዩተር ሥርዓት አማካኝነት ያመረተ፣ ያገኘ፣ የሸጠ፣ ይዞ የተገኘ ወይም ለሌላ ሰው ያስተላለፈ እንደሆነ ከአምስት ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፶ሺ በማይበልጥ መቀጮ ይቀጣል፡፡

10. Computer Related Fraud

1/ Whosoever fraudulently causes a person to act in a manner prejudicial to his rights or those of third person by distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal or taking advantage of the person's erroneous beliefs, shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

2/ Whosoever, with fraudulent intent of procuring any benefit for himself or for another person, causes economic loss to another person by any change, deletion or any other damage of computer data shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000 or in serious cases with rigorous imprisonment not exceeding ten years and fine from Birr 10,000 to 100,000.

11. Electronic Identity Theft

Whosoever, with intent to commit criminal act specified under Article 10 of this Proclamation or for any other purpose produces, obtains, sales, possesses or transfers any data identifying electronic identity of another person without authorization of that person shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.

https://ethiodata.et/

ንኡስ ክፍል ሦስት

ስለሕገወጥ የይዘት ዳታ

፲፪. ለአካለ መጠን ባልደረሱ ልጆች ላይ የሚፈፀሙ ፀያፍ ወይም ለመልካም ጠባይ ተቃራኒ የሆኑ ወንጀሎች

፩/ ማንኛውም ሰው፣

ሀ) ለአካለ መጠን ያልደረሰ ልጅ ወሲባዊ ድርጊት በግልጽ ሲፈጽም የሚያሳይ፣ ወይም

ለ) አዋቂ ሰው ለአካለ መጠን ያልደረሰ ልጅ መስሎ ወሲባዊ ድርጊት በግልጽ ሲፈፅም የሚያሳይ፣ ስዕላዊ መግለጫ፣ ፖስተር፣ ቪዲዮ ወይም ምስል የኮምፒዩተር ሥርዓትን በመጠቀም ሆነ ብሎ ያዘጋጀ፣ ያሰራጨ፣ ለሽያጭ ያቀረበ፣ ያከፋፈለ፣ ሌሎች እንዲያገኙት ያመቻቸ ወይም ያለ ፈቃድ ይዞ የተገኘ እንደሆነ ከሦስት ዓመት እስከ አስር ዓመት በሚደርስ ጽኑ እስራት ይቀጣል።

፪/ ማንኛውም ሰው ወሲባዊ ይዘት ያላቸውን ንግግሮችን፣ ስዕሎችን፣ የጽሁፍ መልእክቶችን ወይም ቪዲዮችን በኮምፒዩተር ሥርዓት አማካኝነት በማሰራጨት ወይም በመላክ ለአካለ መጠን ያልደረሰ ልጅን ለወሲባዊ ድርጊት ያነሳሳ ወይም የመለመለ እንደሆነ ከአምስት ዓመት እስከ አስር ዓመት በሚደርስ ጽኑ እስራት ይቀጣል።

፲፫. በሰዎች ነፃነትና ክብር ላይ የሚፈፀሙ ወንጀሎች

ማንኛውም ሰው ሆነ ብሎ፣

፩/ የኮምፒዩተር ሥርዓትን በመጠቀም በሚያሰራጨው

SECTION THREE

ILLEGAL CONTENT DATA

12. Obscene or Indecent Crimes Committed Against Minors

1/ Whosoever intentionally produces, transmits, sales, distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system that depicts:

a) a minor engaged in sexually explicit conduct; or

b) a person appearing to be a minor engaged in sexually explicit conduct; shall be punishable with rigorous imprisonment from three years to ten years.

2/ Whosoever entices or solicits a minor for sexual explicit conduct by transmitting or sending erotic speeches, pictures, text messages or videos through computer system shall be punishable with rigorous imprisonment from five years to ten years.

13. Crimes against Liberty and Reputation of Persons

Whosoever intentionally:

1/ intimidates or threatens another person or his families with serious danger or injury by disseminating any writing, video, audio or any other image through a computer systems shall be punishable, with simple imprisonment not exceeding three years or

https://ethiodata.et/

ጽሁፍ፣ ንግግር፣ ቪዲዮ ወይም ስዕል አማካኝነት በሌላ ሰው ወይም በተጎጂው ቤተሰቦች ላይ ከባድ ጉዳት ወይም አደጋ ለማድረስ በማሰብ

ነፈራራ ወይም የዛተ እንደሆነ ከሦስት ዓመት በማይበልጥ ቀላል እስራት ወይም እንደወንጀሉ ከባድነት ከአምስት ዓመት በማይበልጥ ጽኑ እስራት ይቀጣል፤

፪/ ተጎጂውን ወይም ቤተሰቦቹን የሚመለከት መረጃ ወይም መልእክት በኮምፒዩተር ሥርዓት አማካኝነት በተደጋጋሚ በመላክ፣ በማሰራጨት ወይም የተበዳዩን የኮምፒዩተር ኮምዩኒኬሽን በመከታተል ፍርሃትን፣ ስጋትን ወይም የሥነ-ልቦና ጫናን የፈጠረ እንደሆነ ከአምስት ዓመት በማይበልጥ ቀላል እስራት ወይም እንደወንጀሉ ከባድነት ከአስር ዓመት በማይበልጥ ጽኑ እስራት ይቀጣል፤

፫/ የሌላን ሰው ክብር ወይም መልካም ስም የሚያጎድፍ ጽሁፍ፣ ንግግር፣ ስዕል ወይም ተንቀሳቃሽ ምስል በኮምፒዩተር ሥርዓት አማካኝነት ያሰራጨ እንደሆነ፣ የግል አቤቱታ ሲቀርብበት ከሦስት ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፴ሺ በማይበልጥ መቀጮ ወይም በሁለቱም ይቀጣል፡፡

፲፬. በሕዝብ ደህንነት ላይ የሚፈፀሙ ወንጀሎች

በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ የወንጀል ህግ አንቀፅ ፪፻፶፯ የተደነገገው እንደተጠበቀ ሆኖ በማንኛውም ሰው ሆነ ብሎ በህብረተሰቡ መካከል አመጽ፣ ሁከት ወይም ግጭት እንዲፈጠር የሚያነሳሳ ጽሁፍ፣ ተንቀሳቃሽ ምስል፣ ድምጽ ወይም ማንኛውንም ሌላ ምስል በኮምፒዩተር ሥርዓት አማካኝነት ያሰራጨ እንደሆነ ከሦስት ዓመት በማይበልጥ ጽኑ እስራት ይቀጣል፡፡

፲፭. በኮምፒዩተር ስርዓት አማካኝነት ስለሚሰራጭ ማስታወቂያ

in a serious cases with rigorous imprisonment not exceeding five years.

2/ causes fear, threat or psychological strain on another person by sending or by repeatedly transmitting information about the victim or his families through computer system or by keeping the victim's computer communication under surveillance shall be punishable with simple imprisonment not exceeding five years or in serious case with rigorous imprisonment not exceeding ten years.

3/ disseminates any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of another person shall be punishable, upon complaint, with simple imprisonment not exceeding three years or fine not exceeding Birr 30,000or both.

14. Crimes against Public Security

Without prejudice to the provisions Article 257 of the Criminal Code of the Federal Democratic Republic of Ethiopia, Whosoever intentionally disseminates through a computer system any written, video, audio or any other picture that incitesviolence, chaos or conflict among people shall be punishable with rigorous imprisonment not exceeding three years.

15. Dissemination of Advertisement through computer system

1/ Whosoever, with intent to advertise or sell any product or service, disseminates advertisement messages through e-mail or related computer address without prior consent from the recipient shall be

https://ethiodata.et/

፩/ ማንኛውም ሰው ምርትን ወይም አገልግሎትን ለማስተዋወቅ ወይም ለሽያጭ ለማቅረብ ሆን ብሎ የማስታወቂያ መልዕክቶችን ያለተቀባዩ ፈቃድ በኢ.ሜይል ወይም መሰል የኮምፒዩተር አድራሻ አማካኝነት ያሰራጨ እንደሆነ ከሦስት ዓመት በማይበልጥ ቀላል እስራት እና ከብር ፴ሺ. በማይበልጥ መቀጮ ወይም ወንጀሉ ከባድ በሆነ ጊዜ ከአምስት ዓመት በማይበልጥ ፅኑ እስራት እና ከብር ፶ሺ. በማይበልጥ መቀጮ ይቀጣል፡፡

2/ የዚህ አንቀጽ ንኡስ አንቀጽ (፩) ድንጋጌ ቢኖርም፡-

ሀ) ማስታወቂያው በዋናነት ደንበኞችን ከአዳዲስ ምርቶች ወይም አገልግሎቶች ጋር ለማስተዋወቅ ያለመ ከሆነና ደንበኞቹ ፈቃደኛ ከሆኑ፣ ወይም

ለ) የላኪውን ትክክለኛ ማንነት፣ አድራሻ እና የመልእክቱ ተቀባይ ተመሳሳይነት ያላቸው መልእክቶችን በቀጣይነት ላለመቀበል የሚያስችል ቀላልና ትክክለኛ አማራጭ የያዘ ከሆነ በወንጀል አያስጠይቅም።

፲፮. ስለአገልግሎት ሰጪዎች የወንጀል ተጠያቂነት

ማንኛውም አገልግሎት ሰጪ በሚያስተዳድረው የኮምፒዩተር ሥርዓት አማካኝነት ለተሰራጨ ማንኛውም የሦስተኛ ወገን ሕገወጥ የይዘት ዳታ በሚከተሉት ሁኔታዎች በዚህ አዋጅ ከአንቀጽ ፲፪ እስከ ፲፬ በተመለከቱት ድንጋጌዎች መሠረት በወንጀል ተጠያቂ ይሆናል፤

፩/ ሕገ-ወጥ የይዘት ዳታውን በማሰራጨት ወይም አርትኦት በማድረግ በቀጥታ የተሳተፈ ከሆነ፤

፪/ ሕገ-ወጥ የይዘት ዳታ መሆኑን እንዳወቀ ዳታውን ለማስወገድ ወይም ተደራሽ እንዳይሆን ለማድረግ ወዲያውኑ እርምጃ ያልወሰደ ከሆነ፤ ወይም

punishable with simple imprisonment not exceeding three years and fine not exceeding Birr 30,000. or, in serious case, with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

2/ Notwithstanding the provision of sub-article (1) of this Article, dissemination of commercial advertisement through email account shall not be punishable provided that:

a) the primary purpose of the advertisement is to introduce customers with new products or services and the customers have willing; or

b) the advertisement contains valid identity and address of the sender, and valid and simple way for the recipient to reject or unsubscribe receipt of further advertisement from the same source.

16. Criminal Liability of Service Providers

A service provider shall be criminally liable in accordance with Articles 12 to 14, of this Proclamation for any illegal computer content data disseminated through its computer systems by third parties, if it has:

1/ directly involved in the dissemination or edition of the contentdata;

2/ upon obtaining actual knowledge that the content data is illegal, failed to take any measure to remove or to disable access to the content data; or

3/ failed to take appropriate measure to remove or to disable access to the content data upon obtaining notice from competent administrative authorities.

https://ethiodata.et/

፫/ ሕገ-ወጥ የይዘት ዳታውን እንዲያስወግድ ወይም ተደራሽ እንዳይሆን እንዲያደርግ በሚመለከተው አካል ተነግሮት ተገቢ እርምጃ ሳይወስድ የቀረ ፱ሺ፩፻፲፰ ንደሆነ፡፡

ንኡስ ክፍል አራት
ስለሌሎች ወንጀሎች

፲፯. የመተባበር ግዴታን ስለመጣስና የምርመራ ሂደትን ስለማደናቀፍ

ማንኛውም ሰው፡-

፩/ በዚህ አዋጅ አንቀጽ ፳፬(፪)፣ አንቀፅ ፳፭(፮)፣ አንቀፅ ፴(፪)፣አንቀፅ ፴፩(፪) ወይም አንቀፅ ፴፪(፬) መሰረት የተጣለበትን የመተባበር ግዴታ ያልተወጣ እንደሆነ ከአንድ ዓመት በማይበልጥ ቀላል እስራት ወይም ከብር ፲ሺ በማይበልጥ በመቀጮ ይቀጣል፤

2/ በዚህ አዋጅ መሠረት የሚከናወን የኮምፒዩተር ወንጀል ምርመራ ሂደትን ሆነ ብሎ ያደናቀፈ እንደሆነ ከአምስት ዓመት በማይበልጥ ጽኑ እስራት እና ከብር ፶ሺ በማይበልጥ መቀጮ ይቀጣል።

፲፰. በሌላ ሕግ ስለተደነገገ የወንጀል ድርጊት

በዚህ ክፍል ከተደነገጉት ወንጀሎች ውጭ ሌላ ወንጀል በኮምፒዩተር ሥርዓት አማካይነት የተፈጸመ እንደሆነ አግባብነት ያለው ሕግ ተፈፃሚ ይሆናል፡፡

፲፱. ተደራራቢ ወንጀሎች

በኮምፒዩተር ሥርዓት አማካይነት የሚፈፀም ማናቸውም ዓይነት ወንጀል በልዩ ሕጎች ወይም በወንጀል ሕግ የሚያስቀጣ ሌላ ወንጀል አስከትሎ እንደሆነ፣ ለዚሁ ወንጀል ተገቢነት ያለው ድንጋጌ በተደራቢነት ተፈፃሚ ይሆናል፡፡

፳. በሕግ የሰውነት መብት የተሰጠው አካል ላይ የሚጣል ቅጣት

በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ የወንጀል ሕግ አንቀጽ ፺ (፩)፣ (፫) እና (፬) ላይ የተደነገገው ቢኖርም በዚህ ክፍል የተመለከተውን ወንጀል የፈፀመው በሕግ

SECTION FOUR
OTHER OFFENCES

17. Failure to Cooperate and Hindrance of Investigation

Whosoever:

1/ fails to comply with the obligations provided for under of Article 24(2) Article 25(6), Article 30 (2), Article 31(2) or Article 32 (4) of this Proclamation shall be punishable with simple imprisonment not exceeding one year or fine not exceeding Birr 10,000;

2/ intentionally hinders the investigation process of computer crimes conducted pursuant to this Proclamation shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

18. Criminal Act Stipulated in Other Laws

Where any crime other than those provided for under this Part is committed by means of a computer, the relevant law shall apply.

19. Concurrent Crimes

Where any of the criminal acts provided for under this Part has resulted in the commission of another crime punishable under any special law or criminal code, the relevant provision shall apply concurrently.

20. Penalty Imposed on Juridical Person

Notwithstanding Article 90 (1), (3) and (4) of the Criminal Code of the Federal Democratic Republic of Ethiopia, where any offence stipulated under this Part is committed by juridical person,

1/ the penalty shall be fine from Birr 50,000 to 500,000 for a crime punishable with fine;

https://ethiodata.et/

ሰውነት መብት በተሰጠው አካል ሲሆን፣

፩/ ለወንጀሉ የተጣለው ቅጣት መቀጮ ከሆነ መቀጮው ከብር ፶ሺ እስከ ብር ፫፻ሺ

 ይሆናል፡፡

፪/ ለወንጀሉ የተጣለው ቅጣት የእስራት ቅጣት ከሆነ የቅጣቱ መጠን፡-

ሀ) እስከ ሦስት ዓመት ቀላል እስራት ለሚያስቀጣ ወንጀል እስከ ብር ፶ሺ፣

ለ) እስከ አምስት ዓመት ቀላል እስራት ለሚያስቀጣ ወንጀል እስከ ብር ፩፻ሺ፣

ሐ) እስከ አምስት ዓመት ጽኑ እስራት ለሚያስቀጣ ወንጀል እስከ ብር ፩፻፶ሺ፣

መ) እስከ አስር ዓመት ጽኑ እስራት ለሚያስቀጣ ወንጀል እስከ ብር ፪፻ሺ፣

ሠ) ከአስር ዓመት በላይ ጽኑ እስራት የሚያስቀጣ ወንጀል ሲሆን በዚህ አንቀጽ ንዑስ አንቀጽ (፩) እስከተመለከተው ከፍተኛ መቀጮ መጠን ለመድረስ በሚችል፣ መቀጮ ይቀጣል፡፡

፫/ ለወንጀሉ የተጣለው ቅጣት መቀጮ ሆኖ መጠኑ በግልጽ ከተመላከተ መቀጮው አምስት እጥፍ ይሆናል፡፡

ክፍል ሦስት
የመከላከልና የምርመራ ሂደቶች

፳፩. መርህ

በዚህ ክፍል እና በክፍል አራት ስር የተደነገጉት ስነ ስርዓቶች፣ የምርመራ ሂደቶች እና የማስረጃ ድንጋጌዎች በህገ መንግስቱ እና አገሪቷ ተቀብላ ባፀደቀቻቸው ዓለምአቀፍ ስምምነቶች ጥበቃ ያገኙ ሰብዓዊና ዲሞክራሲያዊ መብቶች ባረጋገጠ መልኩ ተፈፃሚ መሆን አለባቸው፡፡

2/ when the penalty provided for is imprisonment, the penalty shall be:

a) a fine not exceeding 50,000 Birr for a crime punishable with simple imprisonment not exceeding three years,

b) a fine not exceeding 100,000 Birr for a crime punishable with simple imprisonment not exceeding five years,

c) a fine not exceeding 150,000 Birr for a crime punishable with rigorous imprisonment not exceeding five years,

d) a fine not exceeding 200,000 Birr for a crime punishable with rigorous imprisonment not exceeding ten years,

e) a fine of up to the general maximum laid down in sub-article (1) of this Article for a crime punishable with rigorous imprisonment exceeding ten years.

3/ Where fine is expressly provided as punishment for a crime, it shall be five fold.

PART THREE
PREVENTIVE AND INVESTIGATIVE MEASURES

21. Principle

The prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensure protection for human and democratic rights guaranteed under the Constitution of the Federal Democratic Republic of Ethiopia and all international agreements ratified by the country.

22. General

1/ Computer crime prevention and investigation shall be conducted in accordance with the provisions of this Part.

https://ethiodata.et/

፳፪. ጠቅላላ

፩/ የኮምፒዩተር ወንጀልን የመከላከልና የምርመራ ሂደት በዚህ ክፍል ድንጋጌዎች መሰረት ይከናወናል።

፪/ የዚህ ክፍል ድንጋጌዎች እንደተጠበቁ ሆነው በዚህ ህግ በግልፅ ባልተሸፈኑ ጉዳዮች ላይ የወንጀል ሕግ እና ሌሎች አግባብነት ያላቸው የሕግ ድንጋጌዎች በኮምፒዩተር ወንጀሎች ላይም ተፈፃሚ ይሆናሉ።

፳፫. የመመርመር ሥልጣን

፩/ በዚህ አዋጅ የተደነገጉ ወንጀሎችን አቃቤ ሕግ እና ፖሊስ በጋራ የመመርመር ስልጣን አላቸው፤ አቃቤ ሕግም የምርመራ ሂደቱን ይመራል፡፡

፪/ ኤጀንሲው በኮምፒዩተር ወንጀል ምርመራ ሂደት ድጋፍ እንዲያደርግ ሲጠየቅ አስፈላጊውን ቴክኒካዊ ድጋፍ ይሰጣል፣ በምርመራ ሂደት የተገኙ መረጃዎችን ይተነትናል፤ እንዳስፈላጊነቱ ማስረጃዎችን ያቀርባል፡፡

፳፬. የኮምፒዩተር ዳታን ይዞ ስለማቆየት

፩/ በሌሎች ሕጎች የተደነገገው እንደተጠበቀ ሆኖ ማንኛውም አገልግሎት ሰጭ አካል በኮምዩኒኬሽን ሂደት ላይ ያለን የኮምፒዩተር ትራፊክ ዳታ ወይም ከዳታ ፕሮሰሲንግ አገልግሎት ጋር በተያያዘ የሚያገኛቸውን የትራፊክ ዳታዎች ቢያንስ ለአንድ ዓመት ይዞ ማቆየት ይኖርበታል፡፡

፪/ በፍርድ ቤት ትዕዛዝ መሰረት እንዲገለጥ ካልተወሰነ በስተቀር ዳታው በምስጢር መያዝ አለበት፡፡

፳፭. የኮምፒዩተር ዳታን ስለማሰባሰብ

በሌሎች ሕጎች የተደነገጉ ልዩ ሁኔታዎች እንደተጠበቁ ሆነው፣

፩/ የኮምፒዩተር ወንጀልን ለመከላከል እና

2/ Without prejudice the provisions of this Part, for issues not clearly covered in this law,the provisions of the Criminal Code and other relevant laws shall be applicable to computer crimes.

23. Investigative Power

1/ The public prosecutor and police shall have joint power to investigate criminal acts provided for in this Proclamation. And the public prosecutor shall lead the investigation process.

2/ Where requested to support the investigation process, the Agency shall provide technical support, conduct analysis on collected information, and provide evidences if necessary.

24. Retention of Computer Data

1/ Without prejudice to any provision stipulated in other laws, any service provider shall retain the computer traffic data disseminated through its computer systems or traffic data relating to data processing or communication service for one year.

2/ The data shall be kept in secret unless the court orders for disclosure.

25. Real-time Collection of Computer Data

Without prejudice special provisions stipulated under other laws,

1/ to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other

ለምርመራ መነሻ የሚሆኑ መረጃዎችን ማሰባሰብ ተገቢ ሆኖ ሲገኝ የተጠርጣሪዎችን በኮምኒዩኬሽን ሂደት ላይ ያለን የኮምፒዩተር ፱ሺ፩፻፳፩ ታ፣ የዳታ ፕሮሰሲንግ አገልግሎት ወይም የኢንተርኔት እና ሌሎች መሰል ግንኙነቶችን እንዲጠለፍ ወይም ክትትል እንዲደረግበት መርማሪ አካል ለፍርድ ቤት ጥያቄ ሊያቀርብ ይችላል፡፡ ፍርድ ቤቱም ተገቢውን በመወሰን እንዳስፈላጊነቱ ጠለፋው ወይም ክትትል የሚደረግበት ሁኔታ እና ትዕዛዙን የሚያስፈፅመውን አካል ይወስናል፡፡

፪/ የዚህ አንቀጽ ንዑስ አንቀጽ (፩) ድንጋጌ ተፈፃሚ የሚሆነው በሌላ አኳኋን ዳታውን ማሰባሰብ የማይቻል ሲሆን እና ይኸው በጠቅላይ ዓቃቤ ህጉ ተቀባይነት አግኝቶ ሲወሰን ብቻ ይሆናል፡፡

፫/ በዚህ አንቀጽ ንዑስ አንቀጽ (፩) እና (፪) የተደነገገው ቢኖርም በቁልፍ መሰረተ ልማት ላይ ጉዳት ሊያስከትል የሚችል የኮምፒዩተር ወንጀል ስለመፈፀሙ ወይም ሊፈፀም ስለመሆኑ በቂ ጥርጣሬ ሲኖር እና አስቸኳይ ሁኔታ ሲያጋጥም ጠለፋው ወይም ክትትሉ ያለፍርድ ቤት ትዕዛዝ እንዲከናወን ጠቅላይ ዓቃቤ ሕጉ ለመርማሪ አካል ሊፈቅድ ይችላል፡፡

4/ ጠቅላይ ዓቃቤ ሕጉ በዚህ አንቀጽ ንዑስ አንቀጽ (፫) መሰረት ያለፍርድ ቤት ትዕዛዝ ለመጥለፍ ወይም ለመከታተል መነሻ የሆኑትን ምክንያቶች በ፵፰ ሰዓት ውስጥ ለፌደራል ከፍተኛ ፍርድ ቤት ፕሬዚዳንት ማቅረብ አለበት፤ ፕሬዚዳንቱም ተገቢውን ትዕዛዝ ወዲያውኑ መስጠት ይኖርበታል፡፡

፭/ በዚህ አንቀጽ ከንዑስ አንቀጽ (፩) እስከ (፬) መሠረት የሚገኝ ማንኛውም መረጃ ለጉዳዩ አግባብነት ከሌለው በጠቅላይ ዓቃቤ ህጉ ውሳኔ ወዲያውኑ መወገድ አለበት፡፡

related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary.

2/ Sub-article (1) of this Article shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Attorney General.

3/ Notwithstanding the provisions of sub-article (1) and (2) of this Article, the Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed.

4/ The Attorney General shall present the reasons for interception or surveillance without court warrant under sub-article (3) of this Article to the President of the Federal High Court within 48 hours, and the president shall give appropriate order immediately.

5/ Any irrelevant information collected pursuant to sub-articles (1) to (4) of this Article shall be destroyed immediately upon the decision of the Attorney General.

6/ Any service provider shall cooperate when requested to carry on activities specified under sub-articles (1) and (3) of this Article.

https://ethiodata.et/

፮/ ማንኛውም አገልግሎት ሰጭ አካል በዚህ አንቀጽ ንዑስ አንቀጽ (፩) ወይም ንዑስ አንቀጽ (፫) የተደነገገውን ለማካሄድ ሲጠየቅ …ፈላጊውን ትብብር ማድረግ አለበት፡፡

፯/ በዚህ አንቀጽ ንዑስ አንቀጽ (፭) የተደነገገው እንደተጠበቀ ሆኖ በዚህ አንቀጽ መሠረት የሚሰበሰብ ማንኛውም መረጃ በምስጢር መያዝ አለበት፡፡

፳፮. ኮምፒዩተርን፣ የኮምፒዩተር ሥርዓትን ወይም መሠረተ ልማቶችን ከአደጋ ስለመጠበቅ

፩/ የኮምፒዩተር ወንጀል ሊፈፀም እንደሚችል በቂ ጥርጣሬ ሲኖር እና ጥቃቱን ለመከላከልና ለመቆጣጠር፣ ዜጎችን አስቀድሞ ለማስጠንቀቅ፣ የምርመራ ሂደቱን ውጤታማ ለማድረግ ወይም የሚደርሰውን ጉዳት ለመቀነስ ኤጀንሲው ከመርማሪ አካላት ጋር በመተባበር እና ከፍርድ ቤት ፈቃድ በማውጣት የጥቃት ሰለባ ወይም መነሻ ሊሆኑ እንደሚችሉ በተጠረጠሩ ኮምፒውተሮች፣ የኮምፒዩተር ሥርዓቶች ወይም መሠረተ ልማቶች ላይ ድንገተኛ ፍተሻ ወይም የዲጂታል ፎረንሲክ ምርመራ ሊያካሂድ፣ ተስማሚ የሆነ የደህንነት መሳሪያ ወይም አገልግሎት ሊያቀርብ ወይም ሌላ መሰል ማንኛውንም እርምጃ ሊወስድ ይችላል፡፡

፪/ ለዚህ አንቀጽ ንዑስ አንቀጽ (፩) ተፈፃሚነት አስፈላጊ ከሆነ እና ጥያቄ ከቀረበ የሚመለከታቸው አካላት የመተባበር ግዴታ አለባቸው፡፡

፳፯. ሪፖርት የማድረግ ግዴታ

፩/ ማንኛውም አገልግሎት ሰጪ አካል ወይም የመንግስት ተቋም በዚህ አዋጅ የተደነገጉት ወንጀሎች እየተፈጸሙ መሆኑን ያወቀ እንደሆነ ወይም በሚያስተዳድረው የኮምፒዩተር ሥርዓት አማካኝነት ማንኛውም የሦስተኛ ወገን ሕገ ወጥ የይዘት ዳታ እየተሰራጨ መሆኑን ከተረዳ ወዲያውኑ ለኤጀንሲው እና ወንጀሉን በተመለከተ

7/ Without prejudice sub-article (5) of this Article, any information collected in accordance with this Article shall be kept confidential.

26. Protection of Computer, Computer System or Infrastructure from Danger

1/ Where there are reasonable grounds to believe that a computer crimeis to be committed and it is necessary to prevent and control the crime, provide early warning to citizens, to minimize the risks or for effectiveness of the investigation, the Agency, in collaboration with the investigatory organ, and upon court warrant, may conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures that are suspected to be attacked or deemed to be the sources of attack.

2/ For the implementation of the provision of sub-article (1) of this Article,as may be necessary and upon request, concerned organs shall have duty to cooperate.

27. Duty to Report

1/ Any service provider or government organ who has knowledge of the commission of the crimes stipulated in this Proclamation or dissemination of any illegal content data by third parties through the computer system it administers shall immediately notify the Agency, accordingly report to the police about the crime and take appropriate measures.

https://ethiodata.et/

ለፖሊስ ማሳወቅ እና አስፈላጊውን እርምጃ መውሰድ ይኖርበታል፡፡

፪/ ኤጀንሲው ሪፖርት የሚቀርብበትን ፎርም እና ሥርዓት በተመለከተ በመመሪያ ይወስናል፡፡

፳፰. <u>ስለመያዝና በእስር ስለማቆየት</u>

በሌሎች ልዩ ሕጎች የተደነገጉት ሁኔታዎች እንደተጠበቁ ሆነው፣

፩/ በዚህ አዋጅ የተመለከተ የኮምፒዩተር ወንጀል ለመፈጸሙ ወይም እየተፈፀመ ስለመሆኑ በቂ ጥርጣሬ ሲኖር በወንጀል ሕግ ሥነ-ሥርዓት በተደነገገው መሰረት ፖሊስ ተጠርጣሪዎችን ሊይዝ ይችላል፤

፪/ በዚህ አንቀጽ ንዑስ አንቀጽ (፩) መሰረት የተያዘ ሰው ምርመራ ያልተጠናቀቀ እንደሆነ በወንጀል ሕግ ሥነ-ሥርዓት በተደነገገው መሰረት ተጨማሪ የምርመራ ጊዜ ሊሰጥ ይችላል፤ ሆኖም በጠቅላላ የሚሰጠው ተጨማሪ የምርመራ ጊዜ ከአራት ወራት መብለጥ የለበትም፡፡

<u>ክፍል አራት</u>

<u>የማስረጃና የሥነ-ሥርዓት ድንጋጌዎች</u>

፳፱. <u>ጠቅላላ</u>

፩/ የኮምፒዩተር ወንጀል የፍርድ ሂደትና የማስረጃ አሰባሰብ በዚህ ክፍል ድንጋጌዎች መሰረት ይከናወናል።

፪/ የዚህ ክፍል ድንጋጌዎች እንደተጠበቁ ሆነው የወንጀል ሕግ ጠቅላላ ክፍልና የወንጀለኛ መቅጫ ሥነ-ሥርዓት ሕግ ድንጋጌዎች በኮምፒዩተር ወንጀሎች ላይ ተፈፃሚ ይሆናሉ።

፴. <u>የኮምፒዩተር ዳታ ደህንነት ለማስጠበቅ ስለሚሰጥ ትዕዛዝ</u>

፩/ መርማሪው አካል ለኮምፒዩተር ወንጀል ምርመራ ዓላማ አስፈላጊ የሆነን የተወሰነ የኮምፒዩተር ዳታ ሊጠፋ ወይም ሊቀየር

2/ The Agency may issue a directive as to the form and procedures of reporting.

28. <u>Arrest and Detention</u>

With out prejudice the provisions stipulated in special laws,

1/ where there are reasonable grounds to believe that a computer crime is committed or under commission, police may arrest suspects in accordance with the provisions of the Criminal Procedure Code.

2/ Where the investigation on the person arrested pursuant to sub-article (1) of this Article is not completed, remand may be granted in accordance with the provisions of the Criminal Procedure Code; provided, however, the overall remand period may not exceed four months.

<u>PART FOUR</u>

<u>EVIDENTIARY AND PROCEDURAL PROVISIONS</u>

29. <u>General</u>

1/ Computer crime proceedings and collection of evidence shall be conducted in accordance with the provisions of this Part.

2/ Without prejudice to the provisions of this Part, the General Part provisions of the Criminal Code and the Criminal Procedure Code shall be applicable to computer Crimes.

30. <u>Order for Preservation of Computer Data</u>

1/ Where there are reasonable grounds to believe that a computer data required for computer crime investigation is vulnerable to loss or modification, the investigatory organ may order, in writing, a person to preserve the specified data under his control or possession.

https://ethiodata.et/

እንደሚችል በበቂ ምክንያት ሲያምን ዳታውን የያዘ ወይም በቁጥጥር ሥር ያደረገ ሰው አስፈላጊውን የደህንነት ጥበቃ እንዲያደርግ
 በጽሁፍ ሊያዝ ይችላል።

፪/ በዚህ አንቀጽ ንኡስ አንቀጽ (1) መሰረት ትዕዛዝ የተሰጠው ሰው በጽሁፍ የተገለፀውን የኮምፒዩተር ዳታ ደህንነት ለመጠበቅ ወዲያውኑ አስፈላጊውን እርምጃ የመውሰድና ከሦስት ወራት ላልበለጠ ጊዜ ጠብቆ የማቆየት እንዲሁም የተሰጠውን ትዕዛዝ በምስጢር የመያዝ ግዴታ አለበት።

3/ መርማሪው አካል በዚህ አንቀጽ ንዑስ አንቀጽ (2) የተመለከተው የጊዜ ገደብ ሲያበቃ ለተጨማሪ ሦስት ወራት ለአንድ ጊዜ ብቻ እንዲራዘም ትዕዛዝ ሊሰጥ ይችላል።

፴፩. <u>የኮምፒዩተር ዳታ ለማግኘት ስለሚሰጥ ትእዛዝ</u>

1/ በማንኛውም ሰው ይዞታ ወይም ቁጥጥር ሥር ያለ የኮምፒዩተር ዳታ ለኮምፒዩተር ወንጀል ምርመራ አስፈላጊ መሆኑ በበቂ ምክንያት ሲታመን መርማሪው አካል የኮምፒዩተር ዳታውን ለማግኘት ወይም ለማየት ለፍርድ ቤት ማመልከት ይችላል።

2/ ፍርድ ቤቱ የቀረበውን ጥያቄ ካመነበት እና ጉዳዩ የሚመለከተውን ሰው መጥራት ካላስፈለገው ማንኛውም ሰው በእጁ የሚገኘውን የኮምፒዩተር ዳታ ለመርማሪው አካል እንዲሰጥ ወይም እንዲያሳይ ሊያዝ ይችላል።

፴፪. <u>ስለደራሽነት፣ ብርበራ እና መያዝ</u>

1/ ለኮምፒዩተር ወንጀል ምርመራ ዓላማ አስፈላጊ ሆኖ ሲገኝ መርማሪ አካል ከፍርድ ቤት ፈቃድ በማውጣት ማንኛውም የኮምፒዩተር ሥርዓት፣ ኔትዎርክ ወይም የኮምፒዩተር ዳታ ከርቀት ወይም በቦታው በአካል በመገኘት መበርበር ወይም ደራሽነት ማግኘት ይችላል።

2/ መርማሪ አካል በብርበራ እንዲያዝ የተፈለገውን

2/ The person ordered under sub-article (1) of this Article shall immediately take necessary measures to secure the specified computer data and preserve it for three months and keep such order confidential.

3/ The investigatory organ may order only a one-time extension for another three months up on the expiry of the period stipulated under sub-article (2) of this Article.

31. <u>Order for Obtaining of Computer Data</u>

1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data.

2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.

32. <u>Access, Search and Seizure</u>

1/ Where it is necessary for computer crime investigation, the investigatory organ may,upon getting court warrant, search or access physically or virtually any computer system, network or computer data.

2/ Where the investigatory organ reasonably believes that the computer data sought is stored in another computer system and can be obtained by same computer system, the search or access may be extended to that other computer system without requesting separate search warrant.

https://ethiodata.et/

የኮምፒዩተር ዳታ የብርበራ ፈቃድ በወጣበት የኮምፒዩተር ሥርዓት አማካኝነት ሊገኝ በሚችል ሌላ የኮምፒዩተር ሥርዓት ውስጥ የተከማቸ መሆኑን በበቂ ምክንያት ሲያምን ድጋሚ የፍርድ ቤት ፈቃድ ሳይጠይቅ የብርበራ ሥራውን ማከናወን ፱ሺ፩፻፳፭ ይም ደራሽነት ማግኘት ይችላል።

3/ መርማሪ አካል በዚህ አንቀጽ ንኡስ አንቀጽ (1) እና (2) መሰረት የብርበራ ሥራውን ሲያከናውን ከወንጀሉ ጋር ግንኙነት ያለውን፣

ሀ) ማንኛውም የኮምፒዩተር ሥርዓት ወይም ዳታ መያዝ፣

ለ) በብርበራ የተገኘውን የኮምፒዩተር ዳታ ኮፒ ወይም ፎቶ ግራፍ ማስቀረት፣

ሐ) ማንኛውም ቴክኖሎጂ በመጠቀም የዳታውን ደህንነት ማስጠበቅ፣

መ) ብርበራ በተከናወነበት የኮምፒዩተር ሥርዓት ውስጥ የቀረውን ዳታ በምንም መልኩ ተደራሽ እንዳይሆን ማድረግ፣ ወይም

ሠ) የጠፉ ዳታዎችን መልሶ ማግኘት፣ ይችላል።

4/ መርማሪው አካል ብርበራ የሚከናወንበትን የኮምፒዩተር ሥርዓት አሰራርን ወይም የኮምፒዩተር ዳታ ደህንነት ለማስጠበቅ የተወሰዱ እርምጃዎችን በሥራው ምክንያት የሚያውቅ ማንኛውም ሰው የብርበራ ሥራውን ሊያግዝ የሚችል አስፈላጊውን መረጃ ወይም የኮምፒዩተር ዳታ እንዲሰጠው ሊያዝ ይችላል።

5/ መርማሪ አካል ብርበራውን ሲያካሂድ ያገኛቸው ማናቸውም የኮምፒዩተር ሥርዓት አሰራር ወይም የኮምፒዩተር ዳታ የዚህን አዋጅ ድንጋጌዎች ወይም ሌሎች ሕጎችን የሚፃረሩ መሆናቸውን ሲያምን የኮምፒዩተር ሥርዓቱ ወይም የኮምፒዩተር ዳታው ጥቅም ላይ እንዳይውል፣ እንዲታገድ ወይም በተወሰነ መልኩ እንዲገደብ ለፍርድ ቤት ትዕዛዝ እንዲሰጥለት ጥያቄ ሊያቀርብ

3/ In the execution of search under sub-article (1) or (2) of this Article, the investigatory organ may:

a) seize any computer system or computer data;

b) make and retain a copy or photograph data obtained through search;

c) maintain the integrity of the relevant stored data by using any technology;

d) render inaccessible the stored data from the computer system on which search is conducted; or

e) recover deleted data.

4/ In the execution of search, the investigatory organ may order any person who has knowledge in the course of his duty about the functioning of the computer system or network or measures applied to protect the data therein to provide the necessary information or computer data that can facilitate the search or access..

5/ Where the investigatory organ finds the functioning of a computer system or computer data is in violation of the provisions this Proclamation or other relevant laws, it may request the court to order for such computer data or computer system to be rendered inaccessible or restricted or blocked. The court shall give the appropriate order within 48 hours after the request is presented.

6/ Where the search process on juridical person requires the presence of the manager or his agent, the investigatory organ shall take appropriate measure to do so.

https://ethiodata.et/

ይችላል፣ ፍርድ ቤቱም ጉዳዩ በቀረበለት በ፵፰ ሰዓት ጊዜ ውስጥ አስፈላጊውን ትዕዛዝ መስጠት አለበት፡፡

6/ የሕግ ሰውነት ባላቸው አካላት ላይ በሚደረግ ብርበራ የተቋሙ ኃላፊ ወይም ተወካይ መገኘት አስፈላጊ ከሆነ መርማሪው ተገቢውን

፱ሺ፩፻፳፮ ዝፈፀም አለበት፡፡

፴፫. ተቀባይነት ስለሚኖራቸው ማስረጃዎች

1/ በዚህ አዋጅ መሰረት የተያዘን የኮምፒዩተር ዳታ የሚመለከት ሰነድ፣ የሰነዱ የተረጋገጠ ግልባጭ ወይም የተረጋገጠ የኤሌክትሮኒክስ መዝገብ ወይም ህትመት በፍርድ ቤት ለቀረበው የክስ ጉዳይ በማስረጃነት ሊቀርብ ይችላል፣ ተቀባይነትም ይኖረዋል፡፡

2/ በወንጀለኛ መቅጫ ሥነ-ሥርዓት ሕግና በሌሎች አግባብነት ባላቸው ሕጎች መሰረት የሚቀርቡ ማስረጃዎች ተቀባይነት እንደተጠበቀ ሆኖ፡-

ሀ) በዚህ አዋጅ በተመለከቱት መንገዶች የተሰበሰቡ ማስረጃዎች፣ ወይም

ለ) ከውጭ ሀገር አግባብ ባላቸው የሕግ አስከባሪ አካላት የኢትዮጵያ ሕግ በሚፈቅደው መሠረት የተገኙ ዲጂታል ወይም ኤሌክትሮኒክ ማስረጃዎች የኮምፒዩተር ወንጀሎችን ጉዳይ ለማስረዳት በፍርድ ቤት ተቀባይነት ይኖራቸዋል።

፴፬. ትክክለኛነትን ስለማረጋገጥ

በሌሎች ሕጎች የሰነድ ማስረጃ ስለሚረጋገጥበት ሁኔታ የተደነገገው እንደተጠበቀ ሆኖ በዚህ አዋጅ አንቀጽ ፴፫ የተመለከቱ ማስረጃዎችን ለፍርድ ቤት በማስረጃነት የሚያቀርብ ማንኛውም ሰው የማስረጃዎቹን ተአማኒነት እና ትክክለኛነት የማስረዳት ኃላፊነት አለበት፡፡

33. Admissibility of Evidences

1/ Any document or a certified copy of the document or a certified printout of any electronic record relating to computer data seized in accordance with this Proclamation may be produced as evidence during court proceedings and shall be admissible.

2/ Without prejudice to the admissibility of evidences to be produced in accordance with the Criminal Procedure Code and other relevant laws, any digital or electronic evidence:

a) produced in accordance with this Proclamation; or

b) obtainedby appropriate foreign law enforcement bodies in accordance with Ethiopian Law shall be admissible in court of law in relation to computer crimes.

34. Authentication

Without prejudice to the authentication of written documents stipulated in other laws, any person who produces evidences provided under Article 33 of this Proclamation in a court proceeding has the burden to prove its authenticity.

35. Original Electronic Document

1/ Any electronic record which is obtained upon proof of the authenticity of the electronic records system or by which the data was recorded or stored shall be presumed original electronic document.

2/ Without prejudice to sub-article (1) of this Article, the electronic printout which is

https://ethiodata.et/

፴፭. ስለዋና የኤሌክትሮኒክ ሰነድ

1/ አስተማማኝነቱ በተረጋገጠ የኤሌክትሮኒክ ዳታ የተመዘገበበት ወይም የተከማቸበት ሥርዓትን ተከትሎ የተገኘ የኤሌክትሮኒክ መዝገብ የኤሌክትሮኒክ ዋና ሰነድ ይሆናል፡፡

2/ የዚህ አንቀጽ ንዑስ አንቀጽ (1) ድንጋጌ
፱ሺ፩፻፳፯ ንደተጠበቀ ሆኖ በተከታታይ ሲሠራበት በቆየ አስተማማኝነት ባለው ዳታን ሲያከማች ወይም ሲመዘግብ በቆየ ሥርዓት በመጠቀም ወደ ወረቀት ጽሑፍ የተቀየረ ወረቀት የኤሌክትሮኒክ ዋና ማስረጃ ይሆናል፡፡

3/ የኤሌክትሮኒክ መዝገብ ሥርዓትን ትክክለኛነት ለማረጋገጥ ባልተቻለ ጊዜ፣

ሀ) ኮምፒውተሩ ወይም መሣሪያው በተግባር ሲሠራ መቆየቱን፣ ብልሽት ያጋጠመው ቢሆንም የኮምፒውተሩን አስተማማኝነት የማያጓድለው መሆኑን፤

ለ) የኤሌክትሮኒክ መዝገቡ እንዲመዘገብ የተደረገው ማስረጃውን ለማቅረብ ከሚፈልገው ወገን በተቃራኒ ባለው ሌላኛው ተከራካሪ ወገን መሆኑን፣ ወይም

ሐ) የኤሌክትሮኒክ መዝገቡ እንዲመዘገብ ወይም እንዲከማች ያደረገው ሰው ማስረጃውን ለማቅረብ በሚፈልገው ሰው ቁጥጥር ሥር ያለመሆኑና ምዝገባው ወይም ክምችቱ የተለመደውን ሥራ ተከትሎ የተፈፀመ መሆኑን፣ የሚያሳይ ማስረጃ ማቅረብ ይቻላል፡፡

፴፮. ስለፍርድ ቤት ግምት

ፍርድ ቤቱ በዚህ አዋጅ መሠረት የኤሌክትሮኒክ ሰነድ ተቀባይነትን ለመወሰን ተመሳሳይ ኮምፒዩተር ሥራውን የሚያከናውንበትን ሥነ-

obtained using a secured system under regular operation shall be considered original electronic evidence.

3/ Where the authenticity of an electronic record is not proved, any evidence that shows the following fact shall be admissible.

a) the computer system was operating properly or the fact of its not operating properly did not affect the integrity of the electronic record; or

b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the other litigant party seeking to introduce it; or

c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

36. Presumption of Courts

When assessing the admissibility of evidence in accordance with this Proclamation, the court may have regard to the procedure, standard or manner in which a similar computer system is functioning.

37. Burden of proof

1/ Public prosecutor has the burden of proofing material facts regarding the cases brought to the court in accordance with the standards stipulated in law.

https://ethiodata.et/

ሥርዓት፣ ደረጃ እና አሠራር ግምት ውስጥ ማስገባት ይችላል፡፡

፴፯. የማስረዳት ሸክም

1/ ዐቃቤ ሕግ ባቀረበው ክስ ላይ የተመለከተ ፍሬ ነገርን የማስረዳት እና በሕግ በተቀመጠው መመዘኛ መሠረት የማረጋገጥ ኃላፊነት አለበት፡፡

፱ሺ፩፻፳፰

2/ በዚህ አንቀጽ ንዑስ አንቀጽ (1) የተደነገገው ቢኖርም አቃቤ ህግ መሠረታዊ ፍሬ ነገሮችን ካስረዳ እና ፍርድ ቤት የማስረዳት ኃላፊነቱን ወደ ተከሳሹ ማዞር አስፈላጊ መሆኑን ካመነ የማስረዳት ሸክም ወደ ተከሳሽ ሊዞር ይችላል፡፡

ክፍል አምስት
የኮምፒዩተር ወንጀል ጉዳዮችን የሚከታተሉ ተቋማት

፴፰. የኮምፒዩተር ወንጀል የሚከታተል አቃቤ ሕግና ፖሊስ

1/ በሕግ በተሰጠው ሥልጣን መሰረት የኮምፒዩተር ወንጀልን የሚከታተል አቃቤ ሕግ ወይም መርማሪ በዚህ አዋጅ የተደነገጉትን የመፈፀምና የማስፈፀም ኃላፊነት አለበት፡፡

2/ በዚህ አዋጅ ሥልጣን የተሰጠው የአቃቤ ሕግ እና ፖሊስ የኮምፒዩተር ወንጀልን የሚከታተል ልዩ የስራ ክፍል እንደአስፈላጊነቱ ሊያደራጁ ይችላሉ፡፡

፴፱. ስለኤጀንሲው ኃላፊነት

ኤጀንሲው በቀጥታ የኮምፒዩተር ሥርዓት አማካኝነት የኮምፒዩተር ወንጀል ምርመራ የሚካሄድበትን ዘዴዎች እና ሌሎች አስፈላጊ የምርመራ ቴክኖሎጂዎችን የማቅረብ ኃላፊነት አለበት፡፡

፵. የኮምፒዩተር ወንጀል የዳኝነት ሥልጣን

1/ የፌደራል ከፍተኛ ፍርድ ቤት በዚህ አዋጅ በተደነገጉ ወንጀሎች ላይ የመጀመሪያ ደረጃ

2/ Notwithstanding the provisions of sub-article (1) of this Article, upon proof of basic facts of the case by the public prosecutor if the court believes necessary to shift the burden of proofing to the accused, the court may do so.

PART FIVE
INSTITUTIONS THAT FOLLOW UP CASES OF COMPUTER CRIME

38. Public Prosecutor and Police Following up Cases of Computer Crime

1/ A Public prosecutor or investigative officer empowered to follows up computer crime cases in accordance with the powers conferred by law shall have the responsibility to enforce and cause to enforce the provisions of this Proclamation.

2/ The Attorney General and Police empowered in this Proclamation may organize separate specialized task units when necessary to follow up computer crimes.

39. Duty of the Agency

The Agency shall have duty to establish online computer crimes investigation system and provide other necessary investigation technologies.

40. Jurisdiction

1/ The Federal High Court shall have first instance jurisdiction over computer crime stipulated under this Proclamation.

2/ The judicial jurisdictions stipulated under Article 13 and Article 17 (1) (b) of the Federal Democratic Republic of Ethiopia Criminal Code shall include computer crimes.

https://ethiodata.et/

የዳኝነት ሥልጣን ይኖረዋል፡፡

2/ የዳኝነት ሥልጣንን የተመለከቱ በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ የወንጀል ሕግ አንቀጽ ፲፫ እና አንቀጽ ፲፯ ንዑስ አንቀጽ (፩) ፊደል ተራ (ለ) ድንጋጌዎች የኮምፒዩተር ወንጀልንም ያካትታሉ፡፡

፱ሺ፩፻፳፱

፵፩. **አስፈፃሚ ግብረ-ኃይል ስለማቋቋም**

1/ በሌላ ሕግ ለኤጀንሲው የተሰጠው ሀገራዊ የሳይበር ደህንነት ኦፕሬሽንን በበላይነት የመምራትና የማስተባበር ሥልጣኑ እንደተጠበቀ ሆኖ የኮምፒዩተር ወንጀልን ለመከላከልና ለመቆጣጠር የጠቅላይ ዓቃቤ ሕግ፣ የፌደራል ፖሊስ ኮሚሽን እና ሌሎች አግባብነት ያላቸውን አካላት ኃላፊዎችን ያቀፈ ብሔራዊ አስፈፃሚ ግብረ-ኃይል ይዋቀራል፡፡

2/ የጠቅላይ ዓቃቤ ሕግ አስፈፃሚ ግብረ ኃይሉን ያስተባብራል፤ በግብረ ኃይሉ ሊሳተፉ የሚገባቸውን አግባብነት ያላቸው ሌሎች ተቋማትን ይለያል፤ ውክልና እንዲኖራቸው ያደርጋል፡፡

3/ አስፈፃሚ ግብረ ኃይሉ የኮምፒዩተር ወንጀልን ለመከላከልና ለመቆጣጠር የሚያስችሉ የጋራ አገራዊ ምክክሮች እንዲኖሩ ያደርጋል፣ በየጊዜው በሚያጋጥሙ አደጋዎች ላይ ምክረ-ሐሳብ ያቀርባል፣ በየተቋማቱ ሊሰሩ የሚገቡ ጉዳዮችን በመለየት የአጭር እና የረጅም ጊዜ እቅዶችን ይነድፋል፣ እንዲሁም ልዩ ልዩ አካላትን በማስተባበር የተቀናጀ አሰራር እንዲኖር ያደርጋል፡፡

ክፍል ስድስት
ልዩ ልዩ ድንጋጌዎች

41. **Establishment of Executing Task Force**

1/ Without prejudice the power of the Agency to lead national cyber security operation as stipulated in other relevant laws, a National ExecutingTask Force comprising the Federal Attorney General the Federal Police Commission, and other relevant bodies shall be established in order to prevent and control computer crimes.

2/ The Federal Attorney General shall lead the ExecutingTask Force, identify other relevant organizations to be incorporated in the Task Force and ensure their representation.

3/ The Task Force shall,for the prevention and control computer crimes, develop national discussion forum, discuss on occasional dangers materialized and provide recommendation thereof, design short and long term plans to be performed by the respective institutionsas well as put in place synchronized system by coordinating various relevant organs.

PART SIX
MISCELLANEOUS PROVISIONS

42. **International Cooperation**

1/ The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system.

https://ethiodata.et/

፵፪. <u>ዓለም አቀፍ ትብብር</u>

፩/ ጠቅላይ ዓቃቤ ሕግ መረጃ መለዋወጥን፣ በጋራ የምርመራ ሥራ ማከናወንን፣ ወንጀለኛ አሳልፎ መስጠትን እና ሌሎችን ጨምሮ የኮምፒዩተር ወንጀልን በሚመለከቱ ጉዳዮች ላይ ከሌላ ሀገር አግባብ ያለው ባለሥልጣን ጋር በዚህ አዋጅ፣ ኢትዮጵያ ተዋዋይ ወገን

፱ሺ፩፻፴ ነችበት ስምምነት እና የኢትዮጵያ የሕግ ሥርዓት በሚፈቅደው መሠረት በትብብር ይሰራል ወይም ስምምነት ሊፈራረም ይችላል።

፪/ ለዚህ አዋጅ አፈፃፀም ሲባል መርማሪ አካል ተመሳሳይ ተልዕኮ ካለው የሌላ ሀገር መሰል ተቋም ጋር የመረጃ ልውውጥን፣ በሌላ መልኩ የጋራ ትብብርን ሊያደርግ ወይም እንደ አስፈላጊነቱ ስምምነት ሊፈራረም ይችላል፡፡

፫/ በዚህ አንቀጽ መሰረት የተገኘ ማንኛውም መረጃ ወይም ማስረጃ የኮምፒዩተር ወንጀልን ለመከላከል ወይም ለመመርመር ዓላማ ይውላል፡፡

፵፫. <u>የኮምፒዩተር ሥርዓትን ወይም ንብረትን ስለማገድ፣ ስለመውረስ ወይም ስለመዝጋት</u>

1/ ፍርድ ቤት በዚህ አዋጅ መሰረት በጥፋተኛ ላይ ቅጣት ሲወስን ወንጀሉን ለመፈፀም ጥቅም ላይ የዋለ ማንኛውም የኮምፒዩተር ሥርዓት፣ ዳታ ወይም መሳሪያ በመንግስት እንዲታገድ፣ እንዲወረስ፣ እንዲወገድ ወይም የዳታ ፕሮሰሲንግ አገልግሎቱ እንዲዘጋ በተጨማሪነት ሊያዝ ይችላል።

2/ ተከሳሹ በመጨረሻ ውሳኔ መሰረት ጥፋተኝነቱ ከተረጋገጠ ጥፋተኝነቱ በተረጋገጠበት ወንጀል ሥራ በቀጥታ መንገድ ያገኘው ንብረት ወይም ሐብት ይወረሳል፡፡

3/ ለዚህ አንቀጽ አፈፃፀም ሲባል አግባብ ያላቸው ሌሎች ህጎች ተፈፃሚነት ይኖራቸዋል፡፡

2/ For the effective implementation of this Proclamation, the investigatory organ may exchange information with institutions of another country having similar mission, perform joint cooperation in other forms or sign agreement with institutions of another country, when necessary.

3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.

43. <u>Suspension, Confiscation or Blockage of Computer System or Asset</u>

1/ The court, in sentencing an offender under this Proclamation, may give additional order for the suspension, confiscation or removal of any computer system, data or device or blockage of data processing service used in the perpetration of the offence.

2/ The property or proceedings of the accused that he directly acquired through the computer crime for which he has been convicted shall be confiscateif the accused is convicted through a final decision;

3/ Other relevant laws shall be applicable for the implementation of this article.

44. <u>Power to Issue Regulationand Directive</u>

1/ The Council of Ministers may issue regulations necessary for the implementation of this Proclamation.

2/ The Agency may issue directives necessary for the effective implementation of this Proclamation.

https://ethiodata.et/

፵፬. ደንብና መመሪያ የማውጣት ስልጣን

1/ የሚኒስትሮች ምክር ቤት ይህን አዋጅ ለማስፈፀም የሚያስፈልግ ደንብ ሊያወጣ ይችላል፡፡

2/ ኤጀንሲው ይህን አዋጅ ለማስፈፀም የሚያስፈልግ መመሪያ ሊያወጣ ይችላል፡፡

፵፭. ስለተሻሩና ተፈፃሚነት ስለማይኖራቸው ሕጎች

1/ የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ የወንጀል ሕግ አንቀጽ ፯፻፮ እስከ አንቀጽ ፯፻፲፩ የተመለከቱት ድንጋጌዎች እና የቴሌኮም ማጭበርበር ወንጀል አዋጅ ቁጥር ፯፻፷፩/፪ሺ፬ አንቀጽ ፭ በዚህ አዋጅ ተሽረዋል።

2/ የዚህን አዋጅ ድንጋጌዎች የሚቃረን ማናቸውም አዋጅ፣ ደንብ፣ መመሪያ ወይም የአሰራር ልማድ በዚህ አዋጅ በተሸፈኑ ጉዳዮች ላይ ተፈፃሚነት የለውም፡፡

፵፮. አዋጁ የሚጸናበት ጊዜ

ይህ አዋጅ በፌደራል ነጋሪት ጋዜጣ ታትሞ ከወጣበት ቀን ጀምሮ የጸና ይሆናል፡፡

አዲስ አበባ ሰኔ ፴ ቀን ፪ሺ፰ ዓ.ም

ዶ/ር ሙላቱ ተሾመ
የኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ
ሪፐብሊክ ፕሬዚዳንት

45. Repeal and Inapplicable Laws

1/ Articles 706 to 711 of the Criminal Code of the Federal Democratic Republic of Ethiopia and article 5 of Telecom Fraud Offence proclamation no. 761/2012 are hereby repealed.

2/ No proclamation, regulations, directives or practices shall, in so far as they are inconsistent with this Proclamation, be applicable with respect to matters provided for by this Proclamation.

46. Effective Date

This Proclamation shall enter into force on the date of its publication in the Federal Negarit Gazette.

Done at Addis Ababa, this 7th day of July, 2016

MULATU TESHOME (Dr.)
PRESIDENT OF THE FEDERAL DEMOCRATIC
REPUBLIC OF ETHIOPIA

https://ethiodata.et/