



**JAMHUURIYADDA SOMALILAND**  
**Wasaaradda Isgaadhsiinta**  
**& Tiknoolajiyadda**

**XEERKA**  
**AMNIGA TIKNOOLAJIYADDA IYO**  
**DEMBIYADDA TIKNOOLAJIYADDA**  
**CASRIGA AH**

**(CYBERSECURITY AND CYBERCRIME ACT)**

**Xeer Lr. XX/2023**



## TUSMO

CUTUBKA 1-AAD .....	10
QODOBO HORDHACA .....	10
Qodobka 1-aad .....	10
Magaca Xeerka .....	10
Qodobka 2-aad .....	10
Erey-bixin .....	10
Qodobka 3-aad .....	19
Sarraynta Xeerka .....	19
Qodobka 4-aad .....	20
Ujeeddooyinka Xeerka .....	20
Qodobka 5-aad .....	20
Awoodda Garsoorka Xeerka .....	20
CUTUBKA 2-AAD .....	22
HANNAANKA MAAMULKA AMNIGA IYO DEMBIYADA TIKNOOLAJIYADDA CASRIGA AH .....	22
Qodobta 6-aad .....	22
Maamulka Amniga iyo Dembiyada Tiknoolajiyadda Casriga ah .....	22
Qodobka 7-aad .....	22
Masuuliyadda Wasaaradda .....	22
Qodobka 8-aad .....	24
Masuuliyadda Xarunta Amniga Tiknoolajiyada Casriga ah .....	24
CUTUBKA 3-AAD .....	26

ILAALINTA MACLUUMAADKA XASAASIGA AH IYO KAABAYAASHA MACLUUMAADKA XAASAASIGAGA AH.....	26
Qodobta 9-aad.....	26
Xadka ilaalinta macluumaadka iyo kaabayaasha macluumaadka xaasaasiga ah ..	26
Qodobka 10-aad.....	26
Ku dhawaaqidda iyo diiwaan-gelinta macluumaadka xaasaasiga ah.....	26
Qodobka 11-aad.....	28
Ku kaydinta macluumaadka xaasaasiga ah dalka gudahiisa .....	28
Qodobka 12-aad.....	29
Baadhidda kaabaha macluumaadka xaasaasiga ah.....	29
Qodobka 13-aad.....	30
Waajibaadka warbixinta shilalka amni ee ku saabsan kaabaha macluumaadka xaasaasiga ah .....	30
Qodobka 14-aad.....	31
Layliyada amniga Tiknoolajiyadda Casriga ah ee Qaranka.....	31
CUTUBKA 4-AAD.....	33
DHEX-GALKA ISGAADHSIINTA.....	33
Qodobka 15-aad.....	33
Mamnuucida Dhex-galka Isgaadhsiinta.....	33
Qodobka 16-aad.....	34
Awoodda dhex-gelidda shirkadda Isgaadhsiinta.....	34
CUTUBKA 5-AAD.....	35
RUQSAD-SIINTA SHIRKADAHA AMNIGA TIKNOOLAJIYADDA CASRIGA AH	35

Qodobka 17-aad .....	35
Mamnuucidda bixinta adeegyada amniga Tiknoolajiyadda Casriga ah ruqsad la'aan.....	35
Qodobka 18-aad .....	36
Codsiga ruqsadda .....	36
Qodobka 19-aad .....	37
Cusboonaysiinta ruqsadda .....	37
Qodobka 20-aad .....	38
Diidmada bixinta ama cusboonay-siinta ruqsadda .....	38
Qodobka 21-aad .....	40
Muddada ay ruqsaddu shaqaynayso.....	40
Qodobka 22-aad .....	40
Kala noqoshada ama Xayiraada ruqsadda.....	40
CUTUBKA 6-AAD .....	45
KOOXDA GURMADKA SHILALKA AMNIGA TIKNOOLAJIYADDA CASRIGA AH EE QARANKA.....	45
Qodobka 23-aad .....	45
Aas-aasida kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah ee qaranka .....	45
Qodobka 24-aad .....	47
Hanaanka la-socodka iyo gurmada shilalka amniga Tiknoolajiyadda Casriga ah .....	47
Qodonka 25-aad .....	47

Hanaanka digniinta xili-hore .....	47
Qodobka 26-aad .....	48
Awoodda lagu geli karo, baadhi karo, lagula wareegi karo xog.....	48
Qodobka 27-aad .....	49
Carqaladeynta Kooxda Gurmada Shilalka Amniga Tiknoolajiyadda Casriga ah .....	49
Qodobka 28-aad .....	50
Amniga Tiknoolajiyadda Casriga ah ee degdegga ah.....	50
CUTUBKA 7-AAD.....	51
DANBIYADA TIKNOOLAJIYADDA CASRIGA AH .....	51
Qodobka 29-aad .....	51
Gelid aan la ogolayn.....	51
Qodobka 30-aad .....	52
Gelid ujeeddadeedu tahay in la sameeyo dembi .....	52
Qodobka 31-aad .....	52
Faragelin aan la ogolayn .....	52
Qodobka 32-aad .....	54
Jidgooyo elegtiroonig ah.....	54
Qodobka 33-aad .....	56
Haysashada agabka iyo xogta aan la ogolayn.....	56
Qodobka 34-aad .....	57
Bixinta Baasweethka.....	57
Qodobka 35-aad .....	57

Ciqaabaha dembiyada xogta kaabayaasha xaasaasiga ah ee Qaranka .....	57
Qodobka 36-aad .....	58
Basaasida Tiknoolajiyadda Casriga ah .....	58
Qodob 37-aad .....	59
Cabsi-gelinta Tiknoolajiyadda Casriga ah .....	59
Qodobka 38-aad .....	59
Dhibaataynta Tiknoolajiyadda Casriga ah.....	59
Qodobka 39-aad .....	60
Dabagalka Tiknoolajiyadda Casriga ah.....	60
Qodobka 40-aad .....	61
Boobka Tiknoolajiyadda Casriga ah.....	61
Qodobka 41-aad .....	61
Baahinta xog been ah.....	61
Qodobka 42-aad .....	62
Been-abuurka Baraha Bulshada .....	62
Qodobka 43-aad .....	63
Mamnuucidda Muuqallada Qaaqaawan.....	63
Qodobka 44-aad .....	64
Muuqaallada Qaaqaawan ee Carruurta .....	64
Qodobka 45-aad .....	65
Duufsashada carruurta .....	65
Qodobka 46-aad .....	66

Foorjariga Tiknoolajiyadda Casriga ah.....	66
Qodobka 47-aad .....	66
Khayaanada Tiknoolajiyadda Casriga ah.....	66
Qodobka 48-aad .....	67
Argagixisada Tiknoolajiyadda Casriga ah .....	67
Qodobka 49-aad .....	68
Xatooyada Aqoonsiga iyo Iska Dhigista Qof kale.....	68
Qodobka 50-aad .....	68
Dabis .....	68
Qodobka 51-aad .....	69
Hakinta Farriimaha Elektaroonigga ah .....	69
Qodobka 52-aad .....	70
Farriimaha Elektaroonigga ee huriya burbur hantiyeed ama qalalaase.....	70
Qodobka 53-aad .....	70
Faafinta Muuqaallada Dhaqan-xumada Wata .....	70
Qodobka 54-aad .....	71
Faafinta Muuqaallada iyo Sawirada gaarka ah.....	71
Qodobka 55-aad .....	72
Hadalka Nacaybka Xambaarsan.....	72
Qodobka 56-aad .....	73
Hadalka Cunsuriyadda Xanbaarsan.....	73
CUTUBKA 8-AAD .....	74

CADEYNTA ELECTRONIGA AH .....	74
Qodobka 57-aad .....	74
Ogolaanshaha Caddaynta Elektaroonigga ah .....	74
Qodobka 58-aad .....	74
Xaqiijinta cadaymaha xogta Elektaroonigga ah .....	74
CUTUBKA 9-AAD .....	76
AWOODDA BAADHISTA, RAADINTA, GELIDDA, AMA LAWAREEGIDA .....	76
Qodobka 59-aad .....	76
Habraaca Baadhista Elektaroonigga ah .....	76
Qodobka 60-aad .....	77
Raadinta, gelida, ama la wareegista xog elegtaroonig ah .....	77
Qodobka 61-aad .....	79
Raadinta, Galida, iyo la Wareegista Qaldan .....	79
Qodobka 62-aad .....	79
Amarka Tirtiridda .....	79
Qodobka 63-aad .....	80
Caddaynta Elektaroonigga ah ee si Sharci-Darro ah loo helay .....	80
CUTUBKA 10-AAD .....	81
ISKAASHIGA    CAALAMIGA AH EE GACAN KU HAYNTA AMAANKA TIKNOOLAJIYADDA CASRIGA AH .....	81
Qodobka 64-aad .....	81
Tilmaamidda aagagga iskaashiga .....	81



Qodobka 65-aad .....	81
Heshiisyada Calamiga ah .....	81
CUTUBKA 11-AAD .....	83
QODOBO GUUD .....	83
Qodobka 66-aad .....	83
Ciqaabta Guud .....	83
Qodobka 67-aad .....	83
Magdhawga .....	83
Qodobka 68-aad .....	84
Kaalmo .....	84
Qodobka 69-aad .....	84
Racfaan .....	84
Qodobka 70-aad .....	85
Xeer-nidaamiye .....	85
Qodobka 71-aad .....	85
Dhaqan-galka Xeerka .....	85

<p style="text-align: center;"><b>CUTUBKA 1-AAD</b></p> <p style="text-align: center;"><b>QODOBO HORDHAC AH</b></p> <p style="text-align: center;"><b>Qodobka 1-aad</b></p> <p style="text-align: center;"><b>Magaca Xeerka</b></p> <p>1. Xeerkan waxa loogu yeedhayaa Xeerka Amniga Tiknoolajiyadda iyo Dembiyada Tiknoolajiyadda Casriga ah, Xeer Lr. XX/2023.</p> <p style="text-align: center;"><b>Qodobka 2-aad</b></p> <p style="text-align: center;"><b>Erey-bixin</b></p> <p>Ereyadan soo socda ee xeerka ku jira, haddii si ka duwan aanu qodobku u qeexin, waxa ay la micno noqonayaan sidan:</p> <p>1. <b>Adeeg bixiye:</b> waxa loo la jeedaa</p> <p>a) hay'ad dawladded ama mid gaar ah oo siisa adeeg macaamiisheeda iyada oo adeegsanaysa agabka tiknoolajiyadda.</p> <p>b) hay'ad kasta oo kale oo adeegsata ama kaydisa xog kumbiyuutar oo ay leeyihiin macaamiisheedu.</p>	<p style="text-align: center;"><b>CHAPTER 1</b></p> <p style="text-align: center;"><b>PRELIMINARY PROVISIONS</b></p> <p style="text-align: center;"><b>Article 1</b></p> <p style="text-align: center;"><b>Short Title</b></p> <p>1. This Act may be cited as the Cybersecurity and Cybercrimes Act, XX/2023.</p> <p style="text-align: center;"><b>Article 2</b></p> <p style="text-align: center;"><b>Interpretation</b></p> <p>In this Act, unless the context otherwise requires:</p> <p>1. <b>Service provider:</b> means</p> <p>a) a public or private entity that provides to users of its services the means to communicate by use of a computer system; and</p> <p>b) any other entity that processes or stores computer data on behalf of that entity or its users.</p>
--	---

<p>2. <b>Adeegga isgaadhsiinta Elektaroonigga:</b> Waxa loo la jeedaa adeeg kasta oo bixiya awood wax lagu diro, helo, isticmaalo ama lagu kaydiyo xidhiidh elegtarooniya.</p> <p>3. <b>Baasweedh:</b> waxa loo la jeedaa macluumaad kasta oo loo adeegsan karo gelitaanka ama isticmaalka adeegga ama nidaamka kumbuyutarka.</p> <p>4. <b>Amniga Tiknoolajiyadda Casriga ah:</b> Waxa loo la jeedaa xaalad lagaga hortagayo weerarada ku wajahan koombiyuutar si loo ilaaliyo dhawrsoonaanta, sugnaashaha, iyo in la heli karo macluumaad lagu kaydiyey, lagu farsameeyey, ama lagu gudbiyey kombiyuutarkaas.</p> <p>5. <b>Baadhe:</b> waxa loo la jeedaa cid kasta oo lagu qeexay ama lagu ogolaaday waaran maxkamadeed, ama uu codsaday sarkaal booliis ah si uu uga caawiyo raadinta, gelitaanka, ama qabashada xog ama koombiyuutar.</p> <p>6. <b>Boobka Tiknoolajiyadda Casriga ah:</b> waxa loo la jeedaa samaysashada magac elegtaroonig ah oo looga</p>	<p>2. <b>Electronic Communications Service:</b> means any service which provides the ability to send, receive process or store electronic communications.</p> <p>3. <b>Password:</b> means any information that can be utilized to access or make use of a computer service or system.</p> <p>4. <b>Cyber Security:</b> means the state in which a computer is protected from attack for the purpose of ensuring the confidentiality, integrity and availability of information stored in, processed by, or transmitted through the computer.</p> <p>5. <b>Investigator:</b> means any fit and proper individual identified and allowed under the provisions of a search warrant or requested by a police officer to help the officer in the search for, access to, or seizure of a computer.</p> <p>6. <b>Cybersquatting:</b> means acquiring a domain name in bad faith in order to profit, mislead, destroy reputation, or</p>
--	---

<p>danleeyahay in si qaldan looga faa'iidaysto, iyadoo la samaynayo marin habaabin, sumcad dilis, ama laga horjoogsanayo dadka ama shirkadaha samaysashada magac elegtaroonig ah iyada oo la samaysanayo:</p> <p>a) magac ama calaamad ganacsi oo la mid ah ama si uun ugu eeg mid hore shirkadi si sharci ah u diwaan gashatay.</p> <p>b) magac la mid ah ama si uun ugu eg magac qof caan ahi leeyahay.</p> <p>7. <b>Carruur:</b> waxa loo la jeedaa qof ka yar shan iyo toban sano.</p> <p>8. <b>Dabagalka Tiknoolajiyadda Casriga ah:</b> waxa loo la jeedaa ku dhaqanka xasarad ama dabagellida qof kale, koox, ama hay'ad iyadoo la isticmaalayo hab elegtaroonig ah, gaar ahaan internetka.</p> <p>9. <b>Dalka:</b> Waxa loola jeedaa dalka Jamhuuriyadda Somalilayn iyo xafiisyada ama safaaradaha dalka ee ku yaal wadanka dibadadiisa.</p>	<p>prevent another from registering the same, if the domain name is:</p> <p>a) similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of registration,</p> <p>b) identical or in any way similar to the name of a person other than the registrant, in the case of a personal name.</p> <p>7. <b>Child:</b> means a person younger than fifteen years old.</p> <p>8. <b>Cyberstalking:</b> means the practice of stalking another person, group, or organization using electronic means, especially the Internet.</p> <p>9. <b>Country:</b> means the Republic of Somaliland and its representatives in foreign countries.</p>
--	---

<p>10. <b>Dembiyada Tiknoolajiyadda Casriga ah:</b> waxa loo la jeedaa dembiga ka dhaca adeegsiga, ama ka faa'iidaydiga Tiknoolajiyadda Casriga ah oo ku xidhan isgaadhsiinta elegtiroonigga ah ama internetka.</p> <p>11. <b>Dhibaataynta Tiknoolajiyadda Casriga ah:</b> waxa loo la jeedaa adeegsiga Tiknoolajiyadda Casriga ah si loogu dhibaateeyo, lagu cabsi geliyo, ama loogu hanjabo qof kale ama lagu faafiyo war been ah ama xumaan qof ku saabsan.</p> <p>12. <b>Duufsashada carruurta:</b> waxa loo la jeedaa in iyadoo la adeegsanayo hab Kumbuyuutar ama internet, lagu dhiirriyo carruur in ay ku kacaan fal anshax-xumo ah sida galmo.</p> <p>13. <b>Faragelin:</b> waxa loo la jeedaa wax kasta oo wax u dhimaya sirta, helitaanka, ama sugnaanshaha asalka kombiyuutar, barnaamij ama xog elegtiroonig ah.</p> <p>14. <b>Farriin elegtarooniga:</b> waxa loo la jeedaa xog loo abuuray, loo gudbiyey, loo helay, ama loo kaydiyey hab elegtaroonig ah. Xogtaasi oo ah qaab la fahmi karo.</p>	<p>10. <b>Cybercrime:</b> means a crime that takes place in, uses, or benefits from a computer-simulated environment or when connected to or associated with electronic communications or networks such as the internet.</p> <p>11. <b>Cyber harassment:</b> means the use of electronic communication to bully, intimidate, or threaten another person or to spread false or malicious information about someone.</p> <p>12. <b>Child solicitation:</b> means successfully or unsuccessfully encouraging a minor to engage in sexual conduct through the use of a computer system or internet.</p> <p>13. <b>Interference:</b> means any compromise of the confidentiality, availability, or integrity of a computer, or of any program or data.</p> <p>14. <b>Electronic message:</b> means data that was created, transmitted, received, or stored by electronic methods, with any output of the data being in a form that can be comprehended.</p>
--	--

<p>15. <b>Gelid:</b> waxa loo la jeedaa gelid ama in uu qof doono in uu galo barnaamij ama xog ku kaydsan Kumbuyuutar iyo in uu qofku:</p> <p>a) wax ka beddelo, dib u habeeyo ama tirtiro barnaamij, xog ama wax kasta oo la xidhiidha barnaamijkaas ama xogtaas oo ku jirta Kumbuyuutarkaas;</p> <p>b) nuqul ka sameeyo, wareejiyo ama uu u raro barnaamij ama xog:</p> <p>i. kumbuyuutar kale oo aan ahayn kan uu ku jiro; ama</p> <p>ii. meel ka duwan oo ku taal isla Kumbuyuutarka uu ku jiro;</p> <p>c) sababo in laga soo saaro barnaamij ama xog kumbuyuutarkaas ku jirta; ama</p> <p>sababo hab uu u isticmaalo barnaamij kumbuyuutar ama qayb ka mid ah barnaamijkaas si uu u fuliyo hawl.</p> <p>16. <b>Hadal nacayb xambaarsan:</b> waxa loo la jeedaa nooc kasta oo isgaadhsiin elegtiroonig ah, ha ahaato muuqaal, maqal, baahin, ama qoraal, taas oo ku lug leh cadaawad ama kala soocid ku wajahan qof ama kooxo bulsho oo gaar ah oo ku salaysan jinsiyad, isir,</p>	<p>15. <b>Access:</b> means gaining entry into or intent to gain entry by a person to a program or data stored in a computer and the person:</p> <p>a) alters, modifies or erases a program or data or any aspect related to the program or data in the computer;</p> <p>b) copies, transfers or moves a program or data to:</p> <p>i. any computer other than that in which it is stored; or</p> <p>ii. to a different location in the same computer in which it is stored;</p> <p>c) causes it to be output from the computer in which it is held, or uses it by causing the computer to execute a program or is itself a function of the program.</p> <p>16. <b>Hate speech:</b> means any form of communication, whether video, audio, streaming, or written, that involves hostility or segregation directed toward an individual or particular social groups on the basis of race, ethnicity, tribalism, sex, age, disability, color, marital status,</p>
--	---

<p>qabyaalad, lab ama dheddig, da', naafo, midab, xaalad guur, uur, xaalad caafimaad, iyo heerka dhaqaale, dhaqan, diin, caqiido, damiir, ama asal.</p> <p>17. <b>Dhex-galid elegtiroonig ah:</b> waxa loo la jeedaa dhagaysiga, daawashada, duubista ama in la ogaado micnaha iyo ujeedada ku jirta xog elegtiroonig ah oo gaar ah. Eegida, badalida, ama duubista xag gaar ah oo ka timid ama ku socota kombiyuutar iyada oo la isticmaalayo isgaadhsiin elegtiroonig ah.</p> <p>18. <b>Kaabayaasha Macluumaadka xaasaasiga ah:</b> waxa loo la jeedaa kaabaha Tiknoolajiyadda Casriga ah ee loo isticmaalo adeegyo muhiim u ah nabadgelyada bulshada, xasilloonida dhaqaale, amniga qaranka, iyo xasilloonida caalamiga ah.</p> <p>19. <b>Kumbuyuutar:</b> waxa loo la jeedaa agab kasta oo isticmaala barnaamijyo isaga oo adeegsanaya tilmaamo la faray, sida dhiskitoob, laabtoob, taablat moobayl, iwm.</p>	<p>pregnancy, health status, and economic status, culture, religion, belief, conscience, or origin.</p> <p>17. <b>Interception:</b> means listening to, watching, recording, or otherwise learning the content, meaning, or intent of such a function, or monitoring, changing, viewing, or recording non-public transmissions of data to or from a computer over a telecommunication systems.</p> <p>18. <b>Critical Information Infrastructure:</b> means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, and international stability.</p> <p>19. <b>Computer:</b> means any programmable device that runs computer programs in accordance with set of instructions and include desktop, laptop computer, workstation, mobile device, PDA, or similar devices capable of running computer programs.</p>
--	--

<p>20. <b>Macluumaad Xaasaasi ah:</b> waxa loo la jeedaa macluumaad ay Wasaaradda Isgaadhsiintu, iyada oo kaashanaysa hay'addaha kale ee ay khusayso, ku tilmaanto in ay xaasaasi u tahay dhanka nabadgelyada qaranka, dhaqaalaha iyo fayaqabka bulshada Jamhuuriyadda Somaliland.</p> <p>21. <b>Muuqaallo qaaqaawan:</b> waxa loo la jeedaa nooc kasta oo elegtaroonig ah oo muujinaya ama shidaya codad anshax-xumo ama muuqaallo dad qaaqaqaawan iyo wixii lamid ah.</p> <p>22. <b>Muqaalada qaaqaqaawan ee carruurta:</b> waxa loo la jeedaa qaab kasta oo muujinaya ilmo yar oo ku hawlan anshax xumo, sida galmo hadday tahay mid dhab ah ama mid khiyaali ah.</p> <p>23. <b>Qabasho:</b> waxa loo la jeedaa xayiraadda xog, barnaamij kumbuyuutar, ama kumbuyuutar si loo ilaaliyo caddaymaha elegtiroonigga ah ee ku keydsan kumbuyuutar. Samaynta ama haysashada nuqul xog, barnaamij, ama qoraal daabacan.</p>	<p>20. <b>Critical Information:</b> means information that is declared by the Ministry of ICT in coordination with other related agencies to be critical for the purposes of national security or the economic and social wellbeing of the Republic of Somaliland.</p> <p>21. <b>Pornography:</b> means any form of media that shows or plays sounds or images of a person engaging in explicit sexual conduct.</p> <p>22. <b>Child pornography:</b> means any media in which a minor is shown to be engaging in sexually explicit behavior, whether in actuality or fictitiously.</p> <p>23. <b>Seize:</b> means rendering inaccessible data, a computer program, or a computer in order to preserve evidence, making and retaining a copy of data or a computer program, or making and retaining a printout of the output of data or a computer program.</p>
--	--



<p>24. <b>Agab:</b> Waxa ka mid ah—</p> <ul style="list-style-type: none"> <li>a) Qaybaha kumbuyuutarka sida kaaadhadhka garaafigga, walxaha wax lagu kaydiyo iyo boroseesarka.</li> <li>b) Agabka wax lagu kaydiyo sida haadh dhiskiga, mimariyada ama cajaladaha Elektaroonigga ah.</li> <li>c) Agabka loo adeegsado War gelinta kumbuyuutarka sida kiiboodhka, mooska, taraak-baadh, iskaanno iyo kamarooyin.</li> <li>d) Agabka wax soosaarka sida daabace, sawir-muujiyayal iyo</li> <li>e) Agabka loo adeegsado jid-gooyadda farriimaha, hadalka ama isgaadhsiin elektarooniga ah.</li> </ul> <p>25. <b>Qulqulka xogta:</b> waxa loo la jeedaa xog kombiyuutar oo ku saabsan isgaadhsiin elektiroonig ah, taasi oo tilmaamaysa isgaadhsiintu asal ahaan, halka ay u socoto, halka ay marayso, waqtiga, taariikhda, cabbirka, muddada, ama nooca adeegga ay sido.</p>	<p>24. <b>Device:</b> includes—</p> <ul style="list-style-type: none"> <li>a) components of computer systems such as graphic cards, memory chips and processors</li> <li>b) storage components such as hard drives, memory cards, compact discs and tapes.</li> <li>c) input devices such as keyboards, mouse, trackpad, scanner and digital cameras.</li> <li>d) output devices such as printer and screens; and</li> <li>e) an apparatus which can be used to intercept a wire, oral or electronic communications.</li> </ul> <p>25. <b>Traffic data:</b> means computer data pertaining to a communication using a computer system, generated by a computer system that played a role in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or the type of underlying service.</p>
--	---

<p>26. <b>Tiknoolajiyadda Casriga ah:</b> waxa loo la jeedaa adeegsiga deegaan kumbuyuutar abuuray, ama internetka ama jaaddadka kale ee isgaadhsiinta elegtarooniga ah.</p>	<p>26. <b>Cyber:</b> means either a computer-simulated environment or some form of engagement with the wider internet or other forms of electronic communication.</p>
<p>27. <b>Shilka amaanka Tiknoolajiyadda Casriga ah:</b> Waxa loo la jeedaa fal si sharci darro ah khasaare ugu yeelanaya dhawrsoonaanta, sugnaanshaha, iyo in la heli karo macluumaad lagu kaydiyey, lagu farsameeyey, ama lagu gudbiyey kombiyuutarkaas.</p>	<p>27. <b>Cyber Security Incident:</b> means an act or activity on or through a computer or computer system, that jeopardizes or adversely impacts, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system.</p>
<p>28. <b>Waxyaalo ku saabsan takoor iyo shisheeye naceyb:</b> waxa loo la jeedaa maqal iyo muuqaal kasta oo dhiiri galinaya, kobcinaya, abuuraya, kicinaya rabshado ka dhan ah qof ama kooxo oo ku salaysan isir, midab, wadan, beello ama qowmiyad.</p>	<p>28. <b>Racist and xenophobic material:</b> means any visual or aural portrayal of ideas or beliefs that encourages, promotes, or incites violence against any individual or group of individuals on the basis of race, colour, descent, or national or ethnic origin.</p>
<p>29. <b>Wasaaradda:</b> Waxa loo la jeedaa Wasaaradda Isgaadhsiinta iyo Tiknoolajiyadda, Jamhuuriyadda Somalilayn.</p>	<p>29. <b>Ministry:</b> means the Ministry of Information and Communication Technology, the Republic of Somaliland.</p>

<p>30. <b>Shirkadaha</b> <b>Maamula</b>  <b>Kaabayaasha</b> <b>Macluumaadka</b>  <b>Xaasaasiga ah:</b> waxa loo la jeedaa qof ama dhawr-qof oo xakameynaya ama masuul ka ah kaabayaasha xogta ama macluumaadka xaasaasiga ah.</p> <p>31. <b>Xarunta:</b> waxa looga jeedaa Xarunta Amniga Tiknoolajiyadda Casriga ah.</p> <p>32. <b>Xog kumbuyuutar:</b> waxa loo la jeedaa xog ama macluumaad kasta oo uu Kumbuyuutar sameeyn karo.</p>	<p>30. <b>Controller:</b> means a person, either alone or in common with other persons, who controls and is responsible for critical information infrastructure</p> <p>31. <b>Center:</b> means the Cyber Security Center.</p> <p>32. <b>Computer data:</b> means any data or information that can be processed by a computer.</p>
<p style="text-align: center;"><b>Qodobka 3-aad</b></p> <p style="text-align: center;"><b>Sarraynta Xeerka</b></p> <p>1. Si aan ka hor imanayn qodobada Dastuurka dalka, haddii ay dhacdo khilaaf sharci oo u dhexeeya qodobbada xeerkan iyo xeer kale oo la xidhiidha amniga, dembiyada, iyo baadhista dembiyada la xidhiidha Tiknoolajiyadda Casriga ah, tix-gelinta waxa leh ku dhaqanka qodobbada xeerkan.</p>	<p style="text-align: center;"><b>Article 3</b></p> <p style="text-align: center;"><b>Supremacy of Act</b></p> <p>1. Without prejudice to any other Constitutional provisions, whenever there is a contradiction between the provisions of this Act and any other written law governing cyber security, cybercrime, and digital forensics, the provisions of this Act must prevail to the extent of the inconsistency issue.</p>

<p style="text-align: center;"><b>Qodobka 4-aad</b></p> <p style="text-align: center;"><b>Ujeedooyinka Xeerka</b></p> <p>Ujeedooyinka Xeerkani waa:</p> <ol style="list-style-type: none"> <li>a) in la helo sharci lagu maamulo aminga iyo dembiyada Tiknoolajiyadda Casriga ah.</li> <li>b) in la sameeyo qaab-dhismeed ay dawladdu ku sugto amniga Tiknoolajiyidda Casriga ah.</li> <li>c) in la ilaaliyo amniga kaabayaasha macluumaadka xaasaasiga ah ee qaranka.</li> <li>d) in la aas-aaso Kooxda Gurmadka Shilalka Amaanka Tiknoolajiyadda Casriga ah.</li> <li>e) in la dhiso nidaamka Baadhista, Dacwaynta iyo Cigaabta la xidhiidha Dembiyada Tiknoolajiyadda Casriga ah.</li> </ol>	<p style="text-align: center;"><b>Article 4</b></p> <p style="text-align: center;"><b>Objectives of the Act</b></p> <p>Objectives of this Act includes:</p> <ol style="list-style-type: none"> <li>a) to facilitate a law governing cyber security and cyber crimes.</li> <li>b) to facilitate governing cybersceurity.</li> <li>c) to fasilitate securing national critical informaation infrastructures.</li> <li>d) to esatablish nationa Cybersecurity Incident Response Team.</li> <li>e) to facilitate the investigation, prosecution, and punishment of cybercrimes.</li> </ol>
<p style="text-align: center;"><b>Qodobka 5-aad</b></p> <p style="text-align: center;"><b>Awoodda Garsoorka Xeerka</b></p> <ol style="list-style-type: none"> <li>1. Maxkamadaha dalku waxa ay awood u leeyihiin in ay ka gar-</li> </ol>	<p style="text-align: center;"><b>Article 5</b></p> <p style="text-align: center;"><b>Jurisdiction</b></p> <ol style="list-style-type: none"> <li>1. The courts of Somaliland shall have jurisdiction where an act or an</li> </ol>

<p>sooraan fal dembiyeed ama xadgudub sharci oo xeerkani mamnuucay oo:</p> <p>a) lagu galay gudaha Jamhuuriyadda Somaliland</p> <p>b) uu muwaadin u dhashay Jamhuuriyadda Somaliland ku galay dalka dibadiisa, isaga oo ku xadgudbaya xeerarka waddanka uu dembiga ku galay.</p> <p>c) lagu dul galay markab ama diyaarad ka diiwaan gashan dalka;</p> <p>d) fal-danbiyeedka qayb ka mid ah lagu galay dalka Jamhuuriyadda Somaliland; ama</p> <p>e) lagu galay meel ka baxsan Jamhuuriyadda Somaliland oo dhibka ka dhasha faldembiyeed- kaasi saamayn ku yeelanayo dalka.</p>	<p>omission constituting an offence under this Act has been committed:</p> <p>a) in the territory of Somaliland;</p> <p>b) by a national of Somaliland outside the territory of Somaliland, if the person's conduct would also constitute an offence under the law of the country where the offence was committed</p> <p>c) on a ship or aircraft registered in Somaliland;</p> <p>d) in part in Somaliland; or</p> <p>e) outside the territory of Somaliland and where any result of the offence has an effect in the country.</p>
---	---

<p style="text-align: center;"><b>CUTUBKA 2-AAD</b></p> <p style="text-align: center;"><b>HANNAANKA MAAMULKA AMNIGA IYO DEMBIYADA TIKNOOLAJIYADDA CASRIGA AH</b></p> <p style="text-align: center;"><b>Qodobta 6-aad</b></p> <p style="text-align: center;"><b>Maamulka Amniga iyo Dembiyada Tiknoolajiyadda Casriga ah</b></p> <p>1. Wasaaradda Isgaadhsiinta iyo Tiknoolajiyadda JSL ayaa masuul ka noqonaysa Hagidda iyo Maamulka Amniga iyo Dembiyada Tiknoolajiyadda Casriga ee dalka.</p> <p style="text-align: center;"><b>Qodobka 7-aad</b></p> <p style="text-align: center;"><b>Masuuliyadda Wasaaradda</b></p> <p>1. Masuuliyadda Wasaaradda ee la xidhiidha Amniga iyo Dembiyadda Tiknoolajiyadda Casriga ah waxa ka mid ah:</p> <p style="padding-left: 40px;">a) aas-aasida Xarunta Amniga Tiknoolajiyadda Casriga ah.</p>	<p style="text-align: center;"><b>CHAPTER 2</b></p> <p style="text-align: center;"><b>REGULATION OF CYBER SECURITY AND CYBERCRIME SERVICES</b></p> <p style="text-align: center;"><b>Article 6</b></p> <p style="text-align: center;"><b>Regulation of Cybersecurity and Cybercrimes</b></p> <p>1. Ministry of Communication and Technology shall be responsible for the planning of Cyber Security and cybercrimes.</p> <p style="text-align: center;"><b>Article 7</b></p> <p style="text-align: center;"><b>Functions of the Ministry</b></p> <p>1. The functions of the Ministry relating to cybersecurity and cybercrime are to:</p> <p style="padding-left: 40px;">a) establish the Cyber Security Center.</p> <p style="padding-left: 40px;">b) establish the National Cybersecurity Incident Response Team (CIRT).</p>
--	--

<p>b) aas-aasida kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</p> <p>c) soo saarida iyo ansixinta xeer-nidaamiyayaasha, habraacyada iyo xeerka anshaxa amniga iyo baadhista dembiyada Tiknoolajiyadda casriga ah.</p> <p>d) dejinta iyo ansixinta istaraatajiiyadda iyo siyaasadda amniga iyo dembiyada Tiknoolajiyadda Casriga ah.</p> <p>e) soo saarista warbixin guud oo sannadle ah oo la xidhiidha amniga iyo dembiyada Tiknoolajiyadda Casriga ah.</p> <p>f) isku dubaridka iyo la socodka hawlaha la xidhiidha amniga iyo dembiyada Tiknoolajiyadda Casriga ah.</p>	<p>c) issue and approve Cyber Security and cybercrime regulations, guidelines, and codes of conduct.</p> <p>d) issue and approve national cybersecurity and cybercrime policies and strategies.</p> <p>e) disseminate a yearly report on cybersecurity and cybercrimes status of the country.</p> <p>f) coordinate and oversee cyber security activities.</p>
--	---

<p><b>Qodobka 8-aad</b></p>	<p><b>Article 8</b></p>
<p><b>Masuuliyadda Xarunta Amniga Tiknoolajiyada Casriga ah</b></p>	<p><b>Functions of the Cybersecurity Center</b></p>
<p>1. Xaruntu waxa ay u xil saaran tahay:</p> <ul style="list-style-type: none"> <li>a) Diiwaan-gelinta <ul style="list-style-type: none"> <li>i. shirkadaha adeeg bixiyayaasha amniga Tiknoolajiyadda Casriga ah,</li> <li>ii. shirkadaha maamula kaabayaasha macluumaadka xaasaasiga ah.</li> </ul> </li> <li>b) hawlgalinta iyo diyaarinta qorshaha kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</li> <li>c) samaynta hanaanka la socodka iyo gurmada amniga Tiknoolajiyadda Casriga ah.</li> <li>d) samaynta wacyigalinta iyo digniinta xili hore (Early Warning System) ee la</li> </ul>	<ul style="list-style-type: none"> <li>1. The center is responsible for: <ul style="list-style-type: none"> <li>a) the registration of <ul style="list-style-type: none"> <li>i. cyber security services provider companies.</li> <li>ii. companies controlling the national critical information infrastructure.</li> </ul> </li> <li>b) the preparation of the duties and functions of CIRT.</li> <li>c) the establishment of cyber security monitoring and emergence system.</li> <li>d) the establishment of cyber security awareness and early warning system.</li> <li>e) conducting cyber drill exercises.</li> <li>f) providing cyber security trainings and workshops.</li> <li>g) the coordination of incident response teams in the public and private sectors.</li> </ul> </li> </ul>



<p>xidhiidha khataraha amniga Tiknoolajiyadda Casriga ah.</p> <p>e) qabashada layliyo (Cyber drill) la xidhiidha amniga Tiknoolajiyadda Casriga ah.</p> <p>f) bixinta tababarka iyo aqoon is-weydaarsiga la xidhiidha amniga iyo dembiyada Tiknoolajiyadda Casriga ah.</p> <p>g) isku xidhka iyo hoggaaminta kooxaha ka shaqeeya amniga Tiknooliyadda Casriga ah.</p> <p>h) diyaarinta farsamooyin suurto galinaya ilaalinta amniga kaabayaasha macluumaadka xasaasi ah.</p> <p>i) samaynta xidhiidho caalami ah oo ku saabsan sugidda iyo ka hortaga khataraha amniga Tiknoolajiyadda Casriga ah.</p>	<p>h) prepare guidelines and procedures needed for securing the national critical information infrastructure.</p> <p>i) establish international cooperation with foreign states and strengthen partnerships in combatting cyber threats.</p>
--	--

<p style="text-align: center;"><b>CUTUBKA 3-AAD</b></p> <p style="text-align: center;"><b>ILAALINTA MACLUUMAADKA XASAASIGA AH IYO KAABAYAASHA MACLUUMAADKA XAASAASIGAGA AH</b></p> <p style="text-align: center;"><b>Qodobta 9-aad</b></p> <p style="text-align: center;"><b>Xadka Ilaalinta Macluumaadka iyo Kaabayaasha Macluumaadka Xaasaasiga ah</b></p> <p>1. Qodobada Cutubkan waxa lagu dabaqayaa ilaalinta macluumaadka xasaasiga ah, ilaalinta kaabayaasha macluumaadka xaasaasiga ah iyo shirkadaha maamula kaabayaasha macluumaadka xaasaasiga ah.</p> <p style="text-align: center;"><b>Qodobka 10-aad</b></p> <p style="text-align: center;"><b>Ku Dhawaaqidda iyo Diiwaan-gelinta Macluumaadka Xaasaasiga ah</b></p> <p>1. Wasaaraddu iyada oo kaashanaysa hay'adaha ay khusayso ee amniga iyo</p>	<p style="text-align: center;"><b>CHAPTER 3</b></p> <p style="text-align: center;"><b>PROTECTION OF CRITICAL INFORMATION AND CRITICAL INFORMATION INFRASTRUCTURE</b></p> <p style="text-align: center;"><b>Article 9</b></p> <p style="text-align: center;"><b>Scope of Protecting Critical Information and Critical Information Infrastructure</b></p> <p>1. The provisions of this Chapter apply to a critical information, critical information infrastructure, and the controllers of critical information infrastructure.</p> <p style="text-align: center;"><b>Article 10</b></p> <p style="text-align: center;"><b>Declaration of Critical Information</b></p> <p>1. The Ministry in coordination with security agencies for cybersecurity and cybercrimes may by regulation declare information which is of</p>
--	---

<p>dembiyada Tiknoolajiyadda Casriga ah, waxay soo saaraysaa xeer-nidaamiye qeeraxaya shuruudaha iyo halbeega la xidhiidha macluumaadka muhiimka u ah ilaalinta amniga qaranka, dhaqaalaha iyo fayao-qabka bulshada, una aqoonsanaysa iyadoo raacaysa ujeedooyinka Cutubkan inay yihiin macluumaad xasaasi ah.</p> <p>2. Kaabayaasha lagu kaydiyo macluumaad xasaasi ah waxa ay u aqoonsanaysaa in ay yihiin kaabayaasha macluumaadka xasaasiga ah oo u baahan ilaalin gaar ah.</p> <p>3. Wasaaradda ayaa xeer nidaamiye ku soo saaraysa shuruudaha iyo hannaanka diiwaangelinta kaabaha macluumaadka xasaasiga ah.</p> <p>4. Hannaanka beddiladda lahaanshaha kaabayaasha macluumaadka xasaasiga ah waxa qeexi doona xeer nidaamiye.</p>	<p>importance to the protection of national security, economic or social well-being community, to be critical information for the purposes of this Chapter.</p> <p>2. Infrastructure containing critical information shall be declared critical information infrastructure.</p> <p>3. The Ministry may issue a regulation related to the process and requirement for the registration of critical information infrastructure.</p> <p>4. The Ministry may issue a regulation related to the change of ownership of critical information infrastructure.</p>
---	--

<p style="text-align: center;"><b>Qodobka 11-aad</b></p> <p style="text-align: center;"><b>Ku Kaydinta Macluumaadka Xaasaasiga ah Dalka Guddihiisa</b></p>	<p style="text-align: center;"><b>Article 11</b></p> <p style="text-align: center;"><b>Localization of Critical Information</b></p>
<ol style="list-style-type: none"> <li>1. Cid kasta oo maamusha macluumaadka xaasaasiga ah waa in ay ku kaydisaa macluumaadka xaasaasiga ah xarumo-kayd (Data Centers) oo ku yaal dalka guddihiisa.</li> <li>2. Iyada oo aan la eegayn farqadda 1-aad ee qodobkan, Wasaaraddu waxay u ogolaan kartaa in macluumaadka xaasaasiga ah lagu kaydiyo dalka dibadiisa.</li> <li>3. Cidkasta oo si ogolaansho la'aan ah ugu kaydisa macluumaadka xaasaasiga ah xarumo-kayd oo ka baxsan dalka waxay gelayso dembi, waxaanay mutaysanaysan doontaa, ganaax lacageed oo aan ka badnayn <b>Konton Milyan oo SLSH</b> ama xadhiga aan ka badnayn shan sano ama labadaba.</li> </ol>	<ol style="list-style-type: none"> <li>1. A controller of critical information shall keep all critical information on a server or data center located within the Republic of Somaliland.</li> <li>2. Despite sub-article (1), the Ministry may authorize a controller of critical information to externalize the critical information outside the Republic of Somaliland.</li> <li>3. A controller who fails to keep critical information within the republic of Somaliland without authorizations from the Ministry commits an offence and is subject to a maximum fine not exceeding fifty million SLSH or a maximum sentence of a term not exceeding five years, or to both on conviction.</li> </ol>

<p style="text-align: center;"><b>Qodobka 12-aad</b></p> <p style="text-align: center;"><b>Baadhidda Kaabaha Macluumaadka</b> <b>Xaasaasiga ah</b></p> <ol style="list-style-type: none"> <li>1. Wasaaraddu si ay u hubiso ku dhaqanka qodobada cutubkan waa in ay ku samayso shirkaddaha maamula kaabayaasha macluumaadka xaasaasiga ah baadhid madax banaan.</li> <li>2. Hanaanka baadhitaanka ku xusan farqadda 1-aad ee qodobkan waxa qeexi doona xeer nidaamiye.</li> <li>3. Cidda maamusha kaabe macluumaad xaasaasi ah ee ka hor timaada baadhitaanka ku xusan farqadda 1-aad ee qodobkan waxay galaysaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo aan ka badnayn <b>Afartan Milyan oo SLSH</b> ama xadhiga muddo aan ka badnay afar sano ama labadaba.</li> </ol>	<p style="text-align: center;"><b>Article 12</b></p> <p style="text-align: center;"><b>Auditing of Critical Information Infrastructure to Ensure Compliance</b></p> <ol style="list-style-type: none"> <li>1. The Ministry to ensure compliance with the provisions of this chapter shall conduct independent auditing to the controllers of critical information infrastructure.</li> <li>2. The procedure of the independent auditing under sub-article (1) shall be prescribed in a regulation.</li> <li>3. A controller of a critical information infrastructure who violates sub-article (1) commits an offence and is subject to a fine not exceeding forty million SLSH or to imprisonment for a term not exceeding one year or to both, on conviction.</li> </ol>
---	---

<p><b>Qodobka 13-aad</b></p>	<p><b>Article 13</b></p>
<p><b>Waajibaadka Warbixinta Shilalka Amni ee ku saabsan Kaabaha Macluumaadka Xaasaasiga ah</b></p>	<p><b>Duty to Report Cyber Security Incident in Respect of Critical Information Infrastructure</b></p>
<p>1. Shirkaddaha maamula kaabaha macluumaadka xaasaasiga ah waa in ay warbixin u gudbiyaan Wasaaradda marka ay la kulmaan:</p> <p>a) shil amniga (Cyber Incident) Tiknoolajiyadda Casriga ah oo la xidhiidha kaabaha macluumaadka xaasaasiga ah.</p> <p>b) shil amniga Tiknoolajiyadda Casriga ah oo la xidhiidha shabakad ku xidhan ama uu ku jiro kaabe macluumaad oo xasaasi ah.</p> <p>2. Shirkaddaha maamula kaabaha macluumaadka xaasaasiga ah waa in ay Wasaaradda u soo gudbiyaan warbixin saddex biloodle ah oo ku saabsan shilalka iyo khataraha amniga Tiknoolajiyadda Casriga ah.</p> <p>3. Shirkadda maamusha kaabaha macluumaadka xaasaasiga ah ee soo gudbin wayda warbixinta ku xusan</p>	<p>1. A controller of a critical information infrastructure shall report to the Ministry if any of the following incidents occur:</p> <p>a) a cyber security incident involving critical information infrastructure.</p> <p>b) a cyber security incident involving any computer under the control of the controller that is connected to or communicates with the critical information infrastructure.</p> <p>2. The controller of critical information infrastructure shall submit to the Ministry a quarterly cyber security incident and threat report.</p> <p>3. A controller of a critical information infrastructure who contravenes sub-article (1) commits an offence and is subject to a maximum fine of twenty million</p>

<p>farqadda 1-aad ee qodobkan, waxay geleysaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Labaatan Milyan oo SLSH</b> ama xadhiga muddo aan ka badnay laba sano ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 14-aad</b></p> <p style="text-align: center;"><b>Layliyada Amniga Tiknoolajiyadda Casriga ah ee Qaranka</b></p> <ol style="list-style-type: none"> <li>1. Wasaaraddu waa inay qabataa layliyo la xidhiidha amniga Tiknoolajiyadda Casriga ah oo looga jeedo in lagu shirrabo/tijaabiyo feejignaanta iyo diyaar-garowga shirkadaha maamula kaabayaasha macluumaadka xaasaasiga ah, si ay uga jawaabaan khatarta amniga Tiknoolajiyadda Casriga ah.</li> <li>2. Cid kasta oo loo diiwaangeliyo in ay tahay shirkad maamusha kaabe macluumaad xaasaasi ah waa in ay ka qayb gashaa layliyada amniga Tiknoolajiyadda Casriga ah ee ay Wasaaraddu qabanayso.</li> </ol>	<p>SLSH or a maximum sentence of two years or to both, on conviction.</p> <p style="text-align: center;"><b>Article 14</b></p> <p style="text-align: center;"><b>National Cyber Security Exercises</b></p> <ol style="list-style-type: none"> <li>1. The Ministry shall conduct cyber security drill exercises to assess the readiness of controllers of different critical information infrastructure to respond to significant cyber security incidents at the national level.</li> <li>2. A critical information infrastructure controller shall take part in a national cyber security drill exercises under sub-article (1).</li> <li>3. A controller who fails to comply with cyber security drill exercises under sub-article (1) commits an offence and is subject: <ol style="list-style-type: none"> <li>a) to a maximum fine of ten million SLSH.</li> </ol> </li> </ol>
--	---

<p>3. Shirkadda maamusha kaabe macluumaad xaasaasi ah ee ka qaybgeli wayda layliyada ku xusan farqaddaha 1-aad ee qodobkan, waxay gelaysaa dembi, waxaanay mutaysanaysaa:</p> <p>a) ganaax lacageed oo aan ka badnayn <b>Toban Milyan oo SLSH.</b></p> <p>b) haddii uu joogteeyso dembiga, waxay mutaysan doontaa ganaax lacageed oo aan ka badnayd <b>Toban Milyan oo SLSH</b> maalin kasta inta uu dembigu socdo.</p>	<p>b) in the case of a continuing offence, a further fine not exceeding ten million SLSH for every day during which the offence continues.</p>
---	--



<p style="text-align: center;"><b>CUTUBKA 4-AAD</b></p> <p style="text-align: center;"><b>DHEX-GALKA</b></p> <p style="text-align: center;"><b>ISGAADHSIINTA</b></p> <p style="text-align: center;"><b>Qodobka 15-aad</b></p> <p><b>Mamnuucida Dhex-galka Isgaadhsiinta</b></p> <ol style="list-style-type: none"> <li>1. Qofku wuxuu geleyaa dembi haddii uu dhex-gal ku sameeyo, isku dayo in uu dhex-gal ku sameeyo ama ku boorriyo qof kale in uu dhex-gal ku sameeyo isgaadhsiinta cid kale leedahay isaga oo adeegsanaya Tiknoolajiyadda Casriga ah.</li> <li>2. Cidda samaysa dhex-galka ku xusan farqadda 1-aad ee qodobkan, waxay gelayaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo aan ka badnayn <b>Konton Milyan oo SLSH</b> ama xadhig aan badnayn Shan sano ama labadaba.</li> </ol>	<p style="text-align: center;"><b>CHAPTER 4</b></p> <p style="text-align: center;"><b>INTERCEPTION OF</b></p> <p style="text-align: center;"><b>COMMUNICATION</b></p> <p style="text-align: center;"><b>Article 15</b></p> <p><b>Prohibition of Interception of Communication</b></p> <ol style="list-style-type: none"> <li>1. A person commits an offense if he or she intercepts, attempts to intercept, or procures another person to intercept or attempt to intercept any communication.</li> <li>2. A person who violates sub-article (1) commits an offence and is subject to a maximum fine of up to fifty million SLSH or a maximum sentence of ten years or to both, on conviction.</li> </ol>
--	---

<p style="text-align: center;"><b>Qodobka 16-aad</b></p> <p style="text-align: center;"><b>Awoodda Dhex-gelidda Shirkadda</b></p> <p style="text-align: center;"><b>Isgaadhsiinta</b></p>	<p style="text-align: center;"><b>Article 16</b></p> <p style="text-align: center;"><b>Interception Capability of Service</b></p> <p style="text-align: center;"><b>Provider</b></p>
<ol style="list-style-type: none"> <li>1. Marka laga yimaaddo xeerarka kale ee dalka, shirkadda Isgaadhsiinta ahi waa in ay u suurtagalisaa hay'adaha fulinta sharciga in ay dhex-gelid isgaadhsiineed (communication Interception) samayn karaan.</li> <li>2. Hay'addaha fulinta sharcigu waa inay wataan Waaran, si ay u sameeyaan dhex-gelida ku xusan farqadda 1-aad ee qodobkan.</li> <li>3. Wasaaraddu, iyadoo la tashanaysa hay'adaha ay khusayso, waxay soo saaraysaa xeer-nidaamiyayaal ku saabsan qaabka farsamo ee loo suurtagalinayo dhex-gelidda ku xusan farqadda 1-aad ee qodobkan.</li> </ol>	<ol style="list-style-type: none"> <li>1. Regardless of any other written law, an electronic communication service provider shall provide a service that can be intercepted by the law enforcement agencies.</li> <li>2. The law enforcement agencies shall provide a court warrant to conduct the interception under sub-article (1).</li> <li>3. The Ministry may, in consultation with the security agencies, issue regulations related to the manner in which every service provider is to give effect to sub-article (1).</li> </ol>

**CUTUBKA 5-AAD**

**RUQSAD-SIINTA**

**SHIRKADAHA AMNIGA**

**TIKNOOLAJIYADDA CASRIGA**

**AH**

**Qodobka 17-aad**

**Mamnuucidda Bixinta Adeegyada**  
**Amniga Tiknoolajiyadda Casriga ah**  
**Ruqsad-la'aan**

1. Cidna ruqsad la'aan ma:
  - a) gali karto ganacsi ku saabsan bixinta adeegga amniga Tiknoolajiyadda Casriga ah
  - b) samayn karto xayaysiis ku saabsan haysashada ganacsi ruqsad leh oo bixinaya adeega amniga Tiknoolajiyadda Casriga ah.
2. Cidda ruqsad la'aan gasha ganacsi ku saabsan adeegga amniga Tiknoolajiyadda Casriga ah ee ku xusan farqadda 1-aad ee qodobkan, waxay gelayso dembi,

**CHAPTER 5**

**LICENSING OF CYBER**

**SECURITY SERVICE PROVIDER**

**Article 17**

**Prohibition from Providing Cyber**  
**Security Services without License**

1. A person shall not, without a licence:
  - a) engage in the business of providing cyber security services to others for a fee or otherwise, or.
  - b) advertise that the person is in the business of providing a licensable cyber security service.
2. A person who violates sub-article (1) commits an offence and is subject to a maximum fine of up to forty million SLSH or a maximum sentence of four year or to both, on conviction.

waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan **Afartan milyan SL\$** ama xadhig aan ka badnayn Afar sano ama labadaba.

### **Qodobka 18-aad**

#### **Codsiga Ruqsadda**

1. Cidda rabta inay gasho adeeg bixinta amniga Tiknoolajiyadda Casriga ah waa inay Xarunta u gudbisaa codsiga ruqsadda.
2. Xaruntu waxay, Soddon beri gudahood oo ka bilaabanta maalinta la helay codsiga, ku bixinaysaa ama ku diidaysaa codsiga iyadoo raacaysa shuruudaha ay dhigtay.
3. Haddii ay Xaruntu ku guul daraysato inay go'aan ku gaadho muddada ku xusan farqadda 2-aad ee qodobkan, haddii aan si kale oo xeer nidaamiyayaashi xeerkan loo caddayn, codsigaasi sidaasu ansax ku yahay.

### **Article 18**

#### **Application for License**

1. A person who intends to engage cyber security services shall submit an application to the Center.
2. The Center shall grant or reject an application within thirty days of receipt on terms and conditions determined by the Center.
3. Unless otherwise specified, the application will be presumed to have been approved if the Center does not decide within the time frame under sub-article (2).
4. When the Center rejects a license application, it shall notify the applicant and give the reasons of the rejection.
5. The Center may request for further particulars or information in respect of an application under this

<p>4. Xaruntu haddii ay u diiddo codsade ruqsadda ganacsiga amniga Tiknoolajiyadda Casriga ah, waa inay caddaysaa sababaha ay u diiday.</p> <p>5. Xaruntu way codsan kartaa xog dheeriya oo ku saabsan codsiga ku xusan qodobkan.</p> <p>6. Haddii ay Xaruntu codsato xog dheeriya, muddada ku xusan farqada 2-aad ee qodobkani way joogsanaysaa.</p>	<p>article in a prescribed manner and form.</p> <p>6. Where the Center requests additional information, the period under sub-article (2), shall stop running.</p>
<p style="text-align: center;"><b>Qodobka 19-aad</b></p> <p style="text-align: center;"><b>Cusboonaysiinta Ruqsadda</b></p> <p>1. Cidda rabta in loo cusboonaysiiyo ruqsad waa in ay Xarunta u doonataa foomka cusboonaysiinta ruqsadda.</p> <p>2. Xaruntu marka ay hesho codsiga ku xusan farqadda 1-aad ee qodobkan, waa inay soddon beri gudahood ku cusboonaysiisaa ama ku diidaa codsiga.</p>	<p style="text-align: center;"><b>Article 19</b></p> <p style="text-align: center;"><b>Renewal of License</b></p> <p>1. A person may apply to the Center for the renewal of a license in the prescribed manner and form.</p> <p>2. Upon receipt of an application under sub-article (1), the Center may, within thirty days renew or reject the application.</p>

<p style="text-align: center;"><b>Qodobka 20-aad</b></p> <p style="text-align: center;"><b>Diidmada Bixinta ama Cusboonaysiinta Ruqsadda</b></p> <ol style="list-style-type: none"> <li>1. Xaruntu way diidi kartaa in ay ruqsad bixiso ama cusboonaysiiso marka: <ol style="list-style-type: none"> <li>a) ay u aragto in uu codsaduhu yahay mid aan u qalmin /ku habboonayn inuu lahaado ama sii lahaan karo ruqsadda ganacsiga amniga Tiknoolajiyadda Casriga ah.</li> <li>b) ay u aragto inuu masuulka ganacsigu yahay mid aan u qalmin ama qof aan ku habboonayn.</li> <li>c) ay u aragto in bixinta ama cusboonaysiinta ruqsaddu aanay danta dadweynuhu ku jirin ama ay xaasaasi ku tahay amniga qaranka.</li> <li>d) ay aragto in aan uu qofku buuxin karin shuruudaha laga rabo.</li> </ol> </li> <li>2. Qofku wuxuu gelayaa dembi marka isaga oo ruqsad doonaya:</li> </ol>	<p style="text-align: center;"><b>Article 20</b></p> <p style="text-align: center;"><b>Refusal to Grant or Renew License</b></p> <ol style="list-style-type: none"> <li>1. The Center may refuse to grant or renew a license if it determines that: <ol style="list-style-type: none"> <li>a) in the case of an individual, that individual is not fit or proper to hold or continue to hold the license.</li> <li>b) In the case of a corporate entity, the business entity's manager is not a fit or proper person.</li> <li>c) it is not in the public interest to grant or renew the license, or the grant or renewal of the license may jeopardize national security, or</li> <li>d) the applicant did not meet the specified criteria.</li> </ol> </li> <li>2. A person commits an offense if, in applying for a license, he or she: <ol style="list-style-type: none"> <li>a) makes any statement or provides any particulars, information, or document that the person knows to be false or does not believe to be true, or.</li> <li>b) intentionally conceals any material fact or provides information that is misleading in a material particular.</li> </ol> </li> </ol>
--	---

<p>a) uu sheego hadal ama bixiyo xog uu ogyahay in ay tahay been ama rumaysan yahay in aanay run ahayn, ama</p> <p>b) uu si ula kac ah u sheego xog been ama marin habaabin ah.</p> <p>3. Qofka gala fal dembiyeed ku xusan farqadda 2-aad ee qodobkan, wuxuu mutaysan doonaa ganaax lacageed oo ugu badnaan dhan <b>konton milyan oo SLSH</b> ah ama xadhiga aan ka badnayn shan sano ama labadaba.</p> <p>4. Xaruntu si ay go'aan uga gaadho in codsadaha ruqsaddu yahay mid u qalma ama ku haboon ruqsadda, waxay tix galinaysaa arrimahan soo socda:</p> <p>a) in codsaduhu xidhiidh la leeyahay qof ku jira hawlo sharcidarro ah.</p> <p>b) in xidhiidhada ganacsi ee codsaduhu daacaddarro ka muuqato.</p> <p>c) in codsaduhu yahay mid dhimirka ka jiran.</p> <p>d) in codsadaha si sharci ah u kacay/musalafay.</p>	<p>3. A person convicted of an offence under sub-article (2) is subject to a maximum fine of up to fifty million SLSH or a maximum sentence of five year or to both.</p> <p>4. The Center may consider any of the following factors in determining whether a person or an officer of a business entity or the business entity is a fit and proper person:</p> <p>a) that the person or officer associates with a person involved unlawful activity.</p> <p>b) that the person or officer demonstrated dishonesty or a lack of integrity</p> <p>c) that the person or officer has a mental disorder.</p> <p>d) the person or officer is an undischarged bankrupt.</p> <p>e) that the person or officer has had a license revoked previously.</p> <p>f) any other criteria prescribed by the Center.</p> <p>5. Sub-article (4) does not limit the circumstances under which a person or an officer of a business</p>
---	--

<p>e) in codsaduhu yahay mid ay Xaruntu ruqsadda hore ugala noqotay.</p> <p>f) Shuruudaha kale ee ay Xaruntu u jidaysay.</p> <p>5. Arrimaha tixgalinta mudan ee ay Xaruntu ku go'aan qaadanayso in codsaduhu yahay mid u qalma ruqsadda, kuma koobna kaliya kuwa ku xusan farqadda 4-aad.</p>	<p>entity may be deemed unfit and proper by the Center.</p>
<p style="text-align: center;"><b>Qodobka 21-aad</b></p> <p><b>Muddada ay Ruqsaddu Shaqaynayso</b></p> <p>1. Muddada ay ruqsaddu dhaqan-gal ahaanaysaa waa shan sano oo ka bilaabmaysa maalinta la bixiyo ruqdsadda.</p> <p style="text-align: center;"><b>Qodobka 22-aad</b></p> <p><b>Kala Noqoshada ama Xayiraada Ruqsadda</b></p> <p>1. Xaruntu waxa ay la noqon kartaa ruqsadda haddii:</p>	<p style="text-align: center;"><b>Article 21</b></p> <p style="text-align: center;"><b>Validity of License</b></p> <p>1. A license is valid for period of five years starting from the date of its issuance.</p> <p style="text-align: center;"><b>Article 22</b></p> <p style="text-align: center;"><b>Revocation or Suspension of License</b></p> <p>1. The Center may by order revoke any license if the Center is satisfied that:</p> <p>a) the licensee has failed to comply with any license condition imposed by the Center.</p>



<p>a) ruqsad haystuhu ku dhaqmi waayo shuruud kasta oo ay Xaruntu ku soo rogto.</p> <p>b) ruqsadda lagu helay been iyo marin habaabin</p> <p>c) ay bixiso ama cusboonaysiiso ruqsad, ka dibna ay ku baraarugto in ay jiraan duruufo ku qasbilahaa in ay Xaruntu diido bixinta iyo cusboonaysiinta ruqsaddaas.</p> <p>d) uu ruqsad-luhu joojiyay shaqadii ruqsadda uu u qaatay.</p> <p>e) ruqsad-luhu uu ku dhawaaqay in uu musalafay, ama si qasab ah/aan qasab ahayn uu u xaraashay, haddii aanu la midoobin ganacsi kale ama dib u dhis ku samayn ganacsigiisa.</p> <p>f) ruqsad-laha lagu xukumay fal dembiyeed xeerkan ama xeerarka kale ee dalku mamnuuceen.</p> <p>g) ruqsad-luhu uu noqdo mid aan u qalmin kuna haboonayn inuu sii haysto ruqsadda.</p> <p>h) ay danta guud ku jirto.</p>	<p>b) the license was obtained through deception or fraud.</p> <p>c) there are circumstances that would have required to refuse the issuance and renewal of that license.</p> <p>d) the licensee has ceased the business or activities for which the license has been issued for.</p> <p>e) the licensee has been declared bankrupt or entered into compulsory or voluntary liquidation for any reason other than amalgamation or reconstruction.</p> <p>f) the licensee has been convicted of an offense under this Act or any other written law.</p> <p>g) the licensee is no longer fit to hold the license.</p> <p>h) it is in the public interest.</p> <p>2. Subject to sub-article (3), in any case in which the Center realises that there is no sufficient cause for revoking any license, may by order:</p> <p>a) suspend the license for a period not exceeding six months.</p> <p>b) written warning to the licensee.</p>
--	--

<p>2. Iyadoo loo eegayo farqadda 3-aad, Xaruntu marka ay u aragto in aanay jirin sababo keenaya in lala noqdo ruqsadda waxay soo saari kartaa go'aamada, sida:</p> <ul style="list-style-type: none"> <li>a) in ay xayirto ruqsadda muddo aan ka badnayn lix bilood.</li> <li>b) in ay digniin qoraal ah u qorto ruqsadlaha.</li> <li>c) in ay soo rogto go'aamo ay ku xadidayso ruqsadda.</li> </ul> <p>3. Xaruntu ma adeegsan doonto awoodaheeda ku xusan farqaddaha 1-aad iyo 2-aad ee qodobkan ilaa ay fursad 14 maalmood ah siiso ruqsadlaha ama wakiilkiisa si ay hab qoraal ah ama hab kale iskugu difaacaan.</p> <p>4. Marka ay Xaruntu la noqoto ruqsad sida ku xusan farqadda 1-aad ee qodobkan ama go'aan kale ka gaadho sida ku xusan farqadda 2-aad ee qodobkan, waa in ay Xaruntu wargalin qoraal ah u gudbisaa ruqsadlaha.</p>	<ul style="list-style-type: none"> <li>c) impose the license any other restrictions that the Center considers appropriate.</li> </ul> <p>3. The Center shall not exercise its powers under sub-articles (1) or (2) unless the licensee against whom the Center intends to exercise the power has been given a period of not more than fourteen days, for the licensee or his/her agent to defend themselves in written way or another way.</p> <p>4. Where the Center has revoked a licence under sub-article (1) or made any order under sub-article (2), the Center shall serve a written notice to the licensee concerned.</p> <p>5. If a licensee has been convicted of an offence that makes impossible for the licensee to continue his operation, and is against the public interest:</p> <ul style="list-style-type: none"> <li>a) the Center may serve a written notice of immediate suspension of its license, and.</li> <li>b) the licensee shall, upon a notice under sub-article (5)(a),</li> </ul>
---	--

<p>5. Haddii ruqsadle dembi lagu xukumo, dembigaas oo aan suurto gelinayn in uu ruqsadluhu sii wato shaqadiisii, kana hor imanaya danta guud:</p> <p>a) Xaruntu waxa ay wargalin qoraal ah ku siinaysaa ruqsadlaha in ay xayiraad degdeg ah ka saartay ruqsadaas.</p> <p>b) ruqsadlaha marka wargalinta xarafka (a) ee farqaddan ku xusan loo keeno, waa inuu joojiyaa dhammaan shaqooyinka ruqsaddu u ogalaanaysay.</p> <p>6. Ruqsadle ruqsadiisa la xayiray sida ku xusan farqadda 5-aad ee qodobkan, waa inuu afar iyo toban maalmood gudahood u dalbadaa dib u eegis marka Xaruntu ku wargaliso go'aanka xayiraada.</p> <p>7. Xaruntu ka dib marka ay go'aankeeda ku xusan farqadda 6-aad ee qodobkan dib u eegis ku samayso:</p> <p>a) way joojin kartaa ruqsadda gabi ahaanba.</p>	<p>immediately cease functions to which the licence was granted.</p> <p>6. A licensee whose license has been suspended under sub-article (5) may apply to the Center for review of the decision within fourteen days of receiving the notice of suspension.</p> <p>7. Following a review of the decision under sub-article (6), the Center may order to:</p> <p>a) suspend the license in question.</p> <p>b) suspend that licence for a period of no more than six months beginning on the date of immediate suspension, or.</p> <p>c) rescind the license's immediate suspension.</p> <p>8. Where the Center has revoked or suspended a licence the Center shall serve a copy of the order to the licensee.</p> <p>9. An order issued under this article does not take effect until after the fourteen days under sub-article (6).</p>
--	--

<p>b) way xayiri kartaa ruqsadda muddo aan ka badnayn lix bilood oo ka bilaabmaysa maalinta ay soo rogtay xayiraadii degdega ahayd.</p> <p>c) way ka noqon kartaa go'aanka ay xayiraadda ku saartay ruqsadda.</p> <p>8. Marka ay Xaruntu go'aan kala-noqosho ama xayiraad ku soo rogto ruqsad, waa in ay nuqulka go'aankaas siisaa ruqsadlaha.</p> <p>9. Go'aan kasta oo qodobkani xusay wuxuu dhaqan galayaa ka dib afar iyo tobonka maalmood ee ku xusan farqadda 6-aad ee qodobkan.</p>	
--	--

<p style="text-align: center;"><b>CUTUBKA 6-AAD</b></p> <p style="text-align: center;"><b>KOOXDA GURMADKA SHILALKA AMNIGA TIKNOOLAJIYADDA CASRIGA AH EE QARANKA</b></p> <p style="text-align: center;"><b>Qodobka 23-aad</b></p> <p><b>Aas-aasida Kooxda Gurmada Shilalka Amniga Tiknoolajiyadda Casriga ah ee Qaranka</b></p> <ol style="list-style-type: none"> <li>1. Wasaaraddu waa in ay aas-aastaa kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</li> <li>2. Wasaaraddu waa in ay soo saartaa xeer nidaamiyaha ay ku shaqaynayso kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</li> <li>3. Kooxdu waxay masuul ka tahay: <ol style="list-style-type: none"> <li>a) ka jawaabida shilalka amniga Tiknoolajiyadda Casriga ah.</li> <li>b) isku dubaridka gurmada shilalka amniga Tiknoolajiyadda Casriga ah</li> </ol> </li> </ol>	<p style="text-align: center;"><b>CHAPTER 6</b></p> <p style="text-align: center;"><b>NATIONAL CYBERSECURITY INCIDENT RESPONSE TEAM</b></p> <p style="text-align: center;"><b>Article 23</b></p> <p style="text-align: center;"><b>Establishment of the National Cybersecurity Incident Response Team (CIRT)</b></p> <ol style="list-style-type: none"> <li>1. The Ministry shall establish the National Cybersecurity Incident Response Team.</li> <li>2. The Ministry shall issue a regulation for the operations of the National Cybersecurity Incident Response Team.</li> <li>3. The National Cybersecurity Incident Response Team is responsible: <ol style="list-style-type: none"> <li>a) for responding to cybersecurity incidents.</li> <li>b) for coordinating cybersecurity incident responses.</li> </ol> </li> </ol>
--	--

<p>4. Wasaaraddu waa in ay u diyaariso kooxda:</p> <p>a) agabka muhiimka u ah ka jawaabista shilalka amniga Tiknoolajiyadda Casriga ah.</p> <p>b) u fududayso iskaashi ay kooxdu la samayso kooxaha gurmada amniga Tiknoolajiyadda Casriga ah ee dalka dibadiisa.</p> <p>5. Xaruntu waa in ay qorshaysaa hawlaha shaqo ee kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</p> <p>6. Wasaaraddu waa in ay kor meertaa shaqooyinka ay qabanayaan kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah.</p> <p>7. Kooxdu waa in ay diyaarisaa warbixin saddex biloodle ah oo ku saabsan shaqooyinkooda iyaga oo raacaya xeer-nidaamiyaha ku xusan farqadda 2-aad.</p>	<p>4. The Ministry shall ensure that the National Cybersecurity Incident Response Team:</p> <p>a) is equipped with the necessary tools to effectively respond to cybersecurity incidents, and</p> <p>b) facilitate collaborations with Cybersecurity Incident Response Teams of other countries.</p> <p>5. The Center has the authority to plan on the working directives of the National Cybersecurity Incident Response Team.</p> <p>6. The Ministry shall oversee the operation of National Cybersecurity Incident Response Team.</p> <p>7. The National Cybersecurity Incident Response Team shall prepare a quarterly report covering its operations in accordance with the regulation under sub-article (2).</p>
--	--

<p style="text-align: center;"><b>Qodobka 24-aad</b></p> <p style="text-align: center;"><b>Hanaanka La-socodka iyo Gurmada</b> <b>Shilalka Amniga Tiknoolajiyadda</b> <b>Casriga ah</b></p> <ol style="list-style-type: none"> <li>1. Xaruntu waa in ay samaysaa hanaanka la-socodka iyo gurmada amniga Tiknoolajiyadda Casriga ah.</li> <li>2. Xaruntu waa inay fulisaa tallaabooyinka farsamo ee khuseeya xaqiijinta hirgalinta hanaanka la-socodka iyo gurmada amniga Tiknoolajiyadda Casriga ah.</li> <li>3. Iyadoo la hirgalinayo ujeedooyinka farqada 2-aad ee qodobkan, Xaruntu waxay fududaynaysaa samaynta dhex-gelid elegtirooniga ah.</li> </ol>	<p style="text-align: center;"><b>Article 24</b> <b>Cybersecurity Incident Monitoring and Response System</b></p> <ol style="list-style-type: none"> <li>1. The Center may establish a cybersecurity incident monitoring and response system.</li> <li>2. The Center shall implement the relevant technical measures to ensure an effective cybersecurity incident monitoring and response system.</li> <li>3. Implementing the monitoring and incident response under sub-article (2), the Center may facilitate measures to conduct electronic interception.</li> </ol>
<p style="text-align: center;"><b>Qodonka 25-aad</b></p> <p style="text-align: center;"><b>Hanaanka Digniinta Xili-hore</b></p> <ol style="list-style-type: none"> <li>1. Xaruntu waa in ay samaysaa hanaanka digniinta xili-hore ee la</li> </ol>	<p style="text-align: center;"><b>Article 25</b> <b>Early Warning System</b></p> <ol style="list-style-type: none"> <li>1. The Center shall establish an early warning system in respect of risks related to cybersecurity incidents.</li> </ol>

<p>xidhiidha khataraha amniga Tiknoolajiyadda Casriga ah.</p> <p>2. Xaruntu waa in ay fulisaa hanaanka digniinta xili-hore si bulshada loogala taliyo arrimaha amniga Tiknoolajiyadda Casriga ah.</p> <p style="text-align: center;"><b>Qodobka 26-aad</b></p> <p style="text-align: center;"><b>Awoodda lagu Geli-karo, Baadhi-karo, lagula Wareegi-karo Xog</b></p> <p>1. Marka ay kooxda gurmadka shilalka amniga Tiknoolajiyadda Casriga ah ay gudanayso waajibbaadkeeda iyadoo wadata waaran maxkamadeed waxa ay ogaysiis la'aan:</p> <p>a) geli kartaa dhisme iyo agab kasta oo Tiknoolajiyadda Casriga ah,</p> <p>b) baadhi kartaa dhisme iyo agab kasta oo Tiknoolajiyadda Casriga ah,</p> <p>c) baadhi kartaa cid kasta oo dhismaha ku jirta haddii la rumaysan yahay in qofku haysto xog ama agab</p>	<p>2. The Ministry shall implement the early warning system to advise the public on cybersecurity matters.</p> <p style="text-align: center;"><b>Article 26</b></p> <p style="text-align: center;"><b>Power to Access, Search and Seize</b></p> <p>1. When the National Cybersecurity Incident Response Team is performing it's functions, with a warrant and without prior notice may:</p> <p>a) enter any premises or access an information system.</p> <p>b) conduct a search of the premises or that information system.</p> <p>c) search any person on the premises if there is a reasonable suspicion that the person is in possession of a computer, document, or record relevant to an investigation.</p> <p>d) extract information from, or make copies of, any book, document, or record on or in the premises or in</p>
---	--



<p>Tiknoolajiyadda Casriga ah oo saamayn ku yeelan kara baadhista,</p> <p>d) kala bixi kartaa xog ama ka samaysan kartaa nuqul xog ama agab kasta oo Tiknoolajiyadda Casriga ah oo yaal dhismaha saamayna ku yeelan kara baadhista.</p> <p style="text-align: center;"><b>Qodobka 27-aad</b></p> <p style="text-align: center;"><b>Carqaladeynta Kooxda Gurmada Shilalka Amniga Tiknoolajiyadda Casriga ah</b></p> <ol style="list-style-type: none"> <li>1. Cid kasta oo ka horjoogsata kooxda gurmada shilalka amniga Tiknoolajiyadda Casriga ah, gudashada waajibaadkeeda shaqo ee uu waajibiyey xeerkan waxay galaysaa dembi.</li> <li>2. Cidda lagu helo fal-dembiyeedka ku xusay farqadda 1-aad ee qodobkan waxay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Labaatan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan laba oo xadhig ah, ama labadaba.</li> </ol>	<p>the information system that is relevant to an investigation;</p> <p style="text-align: center;"><b>Article 27</b></p> <p style="text-align: center;"><b>Obstruction of National Cybersecurity Incident Response Team</b></p> <ol style="list-style-type: none"> <li>1. A person commits an offence if that person obstructs a member of the National Cybersecurity Incident Response Team from conducting a lawful search or seizure under this Act.</li> <li>2. A person convicted of an offence under sub-article (1) is subject to a maximum fine of up to twenty million SLSH or a maximum sentence of two years, or both.</li> </ol>
--	--

<p style="text-align: center;"><b>Qodobka 28-aad</b></p> <p style="text-align: center;"><b>Amniga Tiknoolajiyadda Casriga ah ee Degdegga ah</b></p> <p>1. Wasaaraddu iyada oo la tashanaysa hay'adaha kale ee ay khusayso, waxa ay soo saari kartaa xeer-nidaamiye la xidhiidha amniga degdega ah ee Tiknoolajiyadda Casriga ah sida ka hortagga, ogaanshaha, ama joojinta khatarta ku wajahan:</p> <ul style="list-style-type: none"> <li>a) kaabayaasha macluumaadka xaasaasiga ah,</li> <li>b) amniga qaranka,</li> <li>c) xidhiidhada caalamiga ah,</li> <li>d) dhaqaalaha,</li> <li>e) kala danbaynta guud</li> </ul> <p>2. Cidda u hoggaansami wayda xeer nidaamiyaha ku xusan farqadda 1-aad ee qodobkan waxay gelaysoa dembi, waxaanay mutaysanayaa ganaax lacageed oo ugu badnaan dhan <b>Toban milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan Hal sano oo xadhig ah , ama labadaba.</p>	<p style="text-align: center;"><b>Article 28</b></p> <p style="text-align: center;"><b>Cybersecurity Emergency Measures and Requirements</b></p> <p>1. The Ministry may, in consultation with other relevant agencies, issue regulations authorising or directing a person or organisation specified in the regulations to take such measures or comply with such requirements where the Ministry considers it necessary for the purposes of preventing, detecting, or countering a threat to:</p> <ul style="list-style-type: none"> <li>a) critical information infrastructure,</li> <li>b) national security,</li> <li>c) international cooperations,</li> <li>d) economy,</li> <li>e) public order</li> </ul> <p>2. A person who fails to take any measure or comply with any requirement directed by regulation under sub-article (1) commits an offence and is subject to a maximum panishment of up to ten million SLSH or a maximum sentence of one year, or both.</p>
--	--

<p style="text-align: center;"><b>CUTUBKA 7-AAD</b></p> <p style="text-align: center;"><b>DANBIYADA</b></p> <p style="text-align: center;"><b>TIKNOOLAJIYADDA CASRIGA</b></p> <p style="text-align: center;"><b>AH</b></p> <p style="text-align: center;"><b>Qodobka 29-aad</b></p> <p style="text-align: center;"><b>Gelid aan la Ogolayn</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah u gasha agabka Tiknoolajiyadda Casriga iyada oo aan u haysan ogolaansho waxa ay galaysaa dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Labaatan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan laba sano oo xadhig ah, ama labadaba.</li> <li>2. Ujeeddada qodobkan, waxba ka badali mayso in galitaanka aan la ogolayn ku kooban yahay xog ama barnaamuj gaar ah (specific data).</li> </ol>	<p style="text-align: center;"><b>CHAPTER 7</b></p> <p style="text-align: center;"><b>CYBERCRIME</b></p> <p style="text-align: center;"><b>Article 29</b></p> <p style="text-align: center;"><b>Unauthorised Access</b></p> <ol style="list-style-type: none"> <li>1. A person who intentionally violates security measures with the intention to conduct an unauthorised access order to gain access to a computer system and causes it to perform a function, whether temporarily or permanently, is guilty of an offense and is subject to a maximum fine of up to twenty million SLSH a maximum sentence of two years in prison, or both.</li> <li>2. For the purposes of this article, it is immaterial that the unauthorised access is not directed at a program or data held in any computer.</li> </ol>
--	---

<p style="text-align: center;"><b>Qodobka 30-aad</b></p> <p style="text-align: center;"><b>Gelid Ujeeddadeedu Tahay in la Sameeyo Dembi</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah u gasha agabka/qorme Tiknoolajiyadda Casriga ah iyada oo aan u haysan ogolaansho ujeeddadiisuna ay tahay in uu sameeyo dembi sida in uu tirtiro ama beddelo xog waxay gelayso dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Soddon milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan Saddex sano oo xadhig ah, ama labadaba.</li> <li>2. Gelitaanka aan la ogolayn ee ku xusan faqrada 1-aad ee qodobkan, waxba ka badali mayso in ujeedadu ku kooban tahay xog ama barnaamuj gaar ah (specific data).</li> </ol>	<p style="text-align: center;"><b>Article 30</b></p> <p style="text-align: center;"><b>Access with Intent to Commit further Offence</b></p> <ol style="list-style-type: none"> <li>1. A person who, uses a computer to carry out any operation with the intent to use it to secure unauthorised access to any program or data that is stored on a computer commits an offence and is subject to maximum fine of up to thirty million SLSH or a maximum sentence of three years and six months in prison, or both.</li> <li>2. For the purposes of this article, it is immaterial that the unauthorised access is not directed at a program or data held in any computer.</li> </ol>
<p style="text-align: center;"><b>Qodobka 31-aad</b></p> <p style="text-align: center;"><b>Faragelin aan la Ogolayn</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah u qaada tallaabo ay ka dhalan karto faragelin aan la</li> </ol>	<p style="text-align: center;"><b>Article 31</b></p> <p style="text-align: center;"><b>Unauthorised Interference</b></p> <ol style="list-style-type: none"> <li>1. A person who intentionally and without authorization takes any action that results in an</li> </ol>

<p>ogolayn oo lagu sameeyo xog elektiroonig ah, waxay gelayso dembi, waxaanu mutaysan doonaa ganaax lacageed oo ugu badnaan dhan <b>kow iyo labaatan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan <b>laba sano oo xadhig ah</b>, ama labadaba.</p> <p>2. Ujeeddada farqadda 1-aad ee qodobkan waxa loola jeedaa falalka sababi kara faragelin aanu awood u lahayn, ama aanu ka haysan ogolaansho ciddii lahayd ama maamulaysey xogta.</p> <p>3. Cidda gasha fal-dembiyeedka ku xusan farqadda 1-aad ee qodobkan, kaas oo</p> <ul style="list-style-type: none"> <li>a) keeni kara khasaare maaliyadeed,</li> <li>b) halis ku ah amniga qaranka,</li> <li>c) u geysta cid kale dhaawac jidheed ama dhimasho,</li> <li>d) u geysta cid kale magac dil,</li> <li>e) halis ku ah badqabka bulshada.</li> </ul> <p>waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Konton</b></p>	<p>unauthorized interference into a computer program, or data commits an offense and is subject to a maximum fine of up to 21 million SLSH, or a maximum sentence of 1 year in prison, or both.</p> <p>2. For the purposes of this article, an interference is unauthorised, if the person whose act causes the interference is not entitled to cause that interference, does not have consent to interfere from a person who is so entitled.</p> <p>3. A person who commits an offence under sub-article (1) which results in a significant</p> <ul style="list-style-type: none"> <li>a) financial loss to any person,</li> <li>b) threatens national security,</li> <li>c) causes physical injury or death to any person, or threatens public health</li> <li>d) or public safety,</li> </ul> <p>is subject to a maximum fine of up to fifty million SLSH, or a maximum sentence of five years in prison, or both.</p>
---	---

<p><b>milyan oo SLSH</b>, ama xukun cigaabeed ugu badnaan dhan shan sano oo xadhig ah, ama labadaba.</p> <p>4. Ujeeddada qodobkan, waxba ka badali mayso in farogalinta aan la ogolayn ku kooban tahay xog ama cid gaar ah.</p> <p>5. Ujeeddada qodobkan, waxba ka badali mayso haddii ujeeddada faragelintu keenayso saamayn joogto ah ama mid ku meel gaadh ah.</p>	<p>4. For the purposes of this article, it makes no difference whether the unauthorized interference is directed at a program or data held in any computer.</p> <p>5. for the purpose of this article, it makes no difference whether an unauthorized interference or any intended impact of it is permanent or temporary.</p>
<p style="text-align: center;"><b>Qodobka 32-aad</b></p> <p style="text-align: center;"><b>Jidgooyo Elektaroonig ah</b></p> <p>1. Cidda si ula kac ah u samaysa fal abuuraya jidgooyo loogu talo galay Tiknoolajiyadda Casriga ah, waxay gelayso dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>laba iyo afartan milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan afar sano oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 32</b></p> <p style="text-align: center;"><b>Unauthorised Interception</b></p> <p>1. A person who intentionally and without authorization does any act that intercepts or causes to be intercepted, directly or indirectly, and causes the transmission of data to or from a computer via a telecommunication system commits an offense and is subject to a maximum fine not exceeding forty two million SLSH or a maximum sentence of four in prison, or both.</p>

<p>2. Cidda gasha fal-dembiyeed sida ku cad farqadda 1-aad ee qodobkan, taas oo</p> <ul style="list-style-type: none"> <li>a) keeni kara khasaare maaliyadeed,</li> <li>b) halis ku ah amniga qaranka,</li> <li>c) u geysta cid kale dhaawac jidheed ama dhimasho,</li> <li>d) u geysta cid kale magac dil,</li> <li>e) halis ku ah badqabka bulshada.</li> </ul> <p>waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>konton milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan shan sano oo xadhig ah oo xadhig ah, ama labadaba.</p> <p>3. Ujeeddada qodobkan, waxba ka badali mayso in jidgooyada loogu talagalay xog ama macluumaad gaar ah (specific data).</p> <p>4. Ujeeddada qodobkan, waxba ka badali mayso haddii ujeeddada jidgooyadu keenayso saamayn joogto ah ama mid ku meel gaadh ah.</p>	<p>2. A person who commits an offence under sub-article (1) that causes significant financial loss, threatens national security, causes physical or psychological injury or death to any person, or threatens public health or public safety is subject to a maximum fine of up to fifty million SLSH or a maximum sentence five years in prison, or both.</p> <p>3. For the purposes of this article, it makes no difference whether the unauthorized interception is not intended at a telecommunication system, or a program or data housed in any specific computer system.</p> <p>4. For the purpose of this article, it makes no difference whether an unauthorised interception or any intended result of it is permanent or temporary.</p>
--	--

<p style="text-align: center;"><b>Qodobka 33-aad</b></p> <p style="text-align: center;"><b>Haysashada Agabka iyo Xogta aan la Ogotayn</b></p>	<p style="text-align: center;"><b>Article 33</b></p> <p style="text-align: center;"><b>Unlawful Possession of Devices or Data</b></p>
<ol style="list-style-type: none"> <li>1. Cidda si ula kac ah u samaysa, uga ganacsata xog, nidaam (system) ama agab oo elektaroonig ah oo lagu gali karo faldembiyeed kasta oo xeerkan ku xusan, waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Lixdan Milyan oo SLSH</b>, ama xukun cigaabeed ugu badnaan dhan lix sano oo xadhig ah, ama labadaba.</li> <li>2. Cidda si sharci darro ah oo u kac ah u hesha ama u haysata xog, nidaam ama agab ku xusan farqadda 1-aad ee qodobkan, waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Todobaatan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan todoba sano oo xadhig ah, ama labadaba.</li> </ol>	<ol style="list-style-type: none"> <li>1. A person who knowingly manufactures, sells, procures for use, imports, exports, distributes, or otherwise makes a computer or other device, designed, or adapted for the purpose of committing an offense under this Act, commits an offense and is subject to a maximum fine of up to Sixty Million SLSH, or a maximum sentence of six years in prison, or both.</li> <li>2. A person who intentionally obtains or is in possession of one or more of the devices listed in sub-article (1) without lawful explanation or justification commits an offense and is subject to a maximum fine of up to Seventy Million SLSH, or a maximum sentence of seven years in prison, or both.</li> </ol>



<p style="text-align: center;"><b>Qodonka 34-aad</b></p> <p style="text-align: center;"><b>Bixinta Baasweedhka</b></p> <p>1. Cidda si ula kac ah u bixisa baasweedh ama hab kasta oo lagu galo agab ama nidaamka Tiknoolajiyadda Casriga ah iyada oo aan ogolaansho u haysan, waxay gelayaas dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Labaatan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan laba sano oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 34</b></p> <p style="text-align: center;"><b>Unauthorised Disclosure of Password</b></p> <p>1. A person who intentionally and without authorization discloses a password, access code, or any other method of getting access to a computer programs or data for any wrongful gain, unlawful purpose, or to occasion any loss, commits an offence and is subject to a maximum fine of up to twenty million, or a maximum sentence of two years in prison, or both</p>
<p style="text-align: center;"><b>Qodobka 35-aad</b></p> <p style="text-align: center;"><b>Cigaabaha Dembiyada Xogta Kaabayaasha Xaasaasiga ah ee Qaranka</b></p> <p>1. Xogta kaabayaasha xaasaasiga ah waxa loo la jeedaa xogta Qaran ee Tiknoolajiyadda Casriga ah ee la xidhiidha amniga qaranka, dhaqaalaha, caafimaadka iyo badqabka bulshada.</p>	<p style="text-align: center;"><b>Article 35</b></p> <p style="text-align: center;"><b>Enhanced Penalty for Offences Involving National Critical Information Infrastructure</b></p> <p>1. Critical Information Infrastructure refers to computer systems, electronic data, devices, networks, programs related to national security, national economic, public health and safety.</p>

<p>2. Marka uu qofku galo mid ka mid ah dembiyada lagu tilmaamay qodobada 30, 31, 32, iyo 33 ee kaabayaasha xogta xaasaasiga ah ee qaranka, qofku wuxuu gelayaa dembi, waxaanu mutaysan doonaa ganaax lacageed oo ugu badnaan dhan <b>Sagaashan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan sagaal sano oo xadhig ah oo xadhig ah, ama labadaba.</p>	<p>2. Where a person commits any of the offenses described in articles 30, 31, 32, and 33 on a critical information infrastructure, that person is subject to a maximum fine of up to ninety million SLSH, or a maximum sentence of nine years in prison, or both.</p>
<p style="text-align: center;"><b>Qodobka 36-aad</b></p> <p><b>Basaasida Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah ugu gudbisa dawlad shisheeye xogta Tiknoolajiyadda Casriga ah ee dalka, si liddi ku ah dalka, waxay galaysaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Boqol iyo Labaatan Milyan oo shilin</b> ama xukun cigaabeed ugu badnaan dhan toban sano oo xadhig ah oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 36</b></p> <p><b>Cyberespionage</b></p> <p>1. A person who unlawfully and intentionally performs, authorizes, or permits another person to transfer critical information with the intent to directly or indirectly benefit a foreign government against the Republic of Somaliland, commits an offense and is subject to a maximum fine of up to one hundred twenty million SLSH, or a maximum sentence of ten years in prison, or both.</p>

<p style="text-align: center;"><b>Qodob 37-aad</b></p> <p style="text-align: center;"><b>Cabsi-gelinta Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah ugu hanjabta in uu gaadhsiinayo qof, shirkad gacansi ama hay'ad dawladeed waxyeelo nafeed ama maaliyadeed iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah waxay gelayaa dembi, waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Labaatan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan laba sano oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 37</b></p> <p style="text-align: center;"><b>Cyberextortion</b></p> <p>1. A person who performs or threatens to perform, through a computer, any of the offences described in this Chapter, for the purpose of gaining any unlawful advantage commits an offence and is subject to a maximum fine of up to twenty five million SLSH or a maximum sentence of two years or both.</p>
<p style="text-align: center;"><b>Qodobka 38-aad</b></p> <p style="text-align: center;"><b>Dhibaataynta Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah u qasabta, cabsi gelisa, dhibaataysa, ama waxyeelo u geysto cid kale iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah, waxay gelayaa dembi waxaaney mutaysan doontaa</p>	<p style="text-align: center;"><b>Article 38</b></p> <p style="text-align: center;"><b>Cyber Harassment (Cyberbullying)</b></p> <p>1. A person who intentionally uses a computer with the intent to coerce, intimidate, harass, or to threaten to cause physical harm to another person, commits an offense and is subject to a maximum fine of up to</p>

<p>ganaax lacageed oo ugu badnaan dhan <b>Saddex iyo Labaatan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan hal sano oo xadhig ah, ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 39-aad</b></p> <p><b>Dabagalka Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah u dabagasha, u dirta farriimo meel ka dhac ah, anshax xumo ah, dhaqan xumo ah ama khatar galinaysa cid kale iyada oo adeegsanaya Tiknoolajiyadda Casriga ah, waxay gelayso dembi waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>kow iyo labaatan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan hal sano oo xadhig ah, ama labadaba.</p>	<p>twenty three million SLSH, or a maximum sentence of two years in prison, or both.</p> <p style="text-align: center;"><b>Article 39</b></p> <p style="text-align: center;"><b>Cyber Stalking</b></p> <p>1. A person who intentionally, maliciously, or repeatedly sends electronic messages that is grossly offensive, pornographic or of an indecent, obscene or causes any such message or matter to be so sent, commits an offense and is subject to a maximum fine of up to twenty one million SLSH or a maximum sentence of two years in prison, or both</p>
--	---

<p style="text-align: center;"><b>Qodobka 40-aad</b></p> <p style="text-align: center;"><b>Boobka Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah u qaadata ama adeegsata magac qof caan ah, magac ganacsi, calaamad ganacsi, magac barta internet (domainname), ama kalmad iyo weedh u diiwaan gashan cid kale, ama uu isticmaasha iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah, waxay gelayso dembi waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Afartan milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan labo sano oo xadhig ah oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 40</b></p> <p style="text-align: center;"><b>Cybersquatting</b></p> <p>1. A person who, without authority or right, intentionally takes or uses a name, business name, trademark, domain name, or other word or phrase registered, owned, or in use by another person on the internet or any other computer network commits an offence and is subject to a maximum a fine of up to forty million SLSH or a maximum sentence of four years in prison, or both</p>
<p style="text-align: center;"><b>Qodobka 41-aad</b></p> <p style="text-align: center;"><b>Baahinta Xog-been ah</b></p> <p>1. Cidda si ula kac ah u daabacda ama u baahisa xog been abuur ah ama marin habaabinsa cid kale iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah, waxay gelayso dembi</p>	<p style="text-align: center;"><b>Article 41</b></p> <p style="text-align: center;"><b>False Publications</b></p> <p>1. A person who intentionally, by using a computer or internet, publishes false, misleading, or fictitious data with the intent that the data be considered or acted</p>

<p>waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Konton milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan shan sano oo xadhig ah, ama labadaba.</p>	<p>upon as authentic, with or without financial gain, using a computer or internet, commits an offense and is subject to a maximum fine of up to fifty five million SLSH, or a maximum sentence of five years in prison, or both.</p>
<p style="text-align: center;"><b>Qodobka 42-aad</b></p> <p style="text-align: center;"><b>Been-abuurka Baraha Bulshada</b></p>	<p style="text-align: center;"><b>Article 42</b></p> <p style="text-align: center;"><b>Publication of False Information</b></p>
<ol style="list-style-type: none"> <li>1. Cidda si ula kac ah ku baahisa baraha bulshada xog been ah, propoganda ah, isku dir bulsho, ka been sheegid xaaladda amaanka qaranka, sumacad dilid iyada oo adeegsanaysa Tiknoolajiyadda Casiga ah waxay gelayso dembi waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Todobaatan Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan todoba sano oo xadhig ah, ama labadaba.</li> <li>2. Cidda leh ama maamusha cinwaan baro bulsho oo ay ku xidhan yihiin in ka badan 5,000 qof (followers) ee</li> </ol>	<ol style="list-style-type: none"> <li>1. A person who intentionally publishes information that is false in print, broadcast, data or over a computer system, that is meant cause or results in unrest, or violence among citizens of the country, or which is likely to discredit the reputation of a person commits an offence and is subject to a maximum fine of up to seventy million SLSH, or a maximum sentence of seven years in prison, or both.</li> <li>2. A person who owns and controls a social media platform with more than 5,000 followers and</li> </ol>

<p>si ula kac ah ugu kacda dembiga ku xusan farqadda 1-aad ee qodobkan, waxay gelaysaa dembi, waxaaney mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Sagaashan Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan saddex sano oo xadhig ah, ama labadaba.</p>	<p>intentionally publishes or circulates the data listed under sub-article (1) commits an offence and is subject to a maximum fine of up to ninety million SLSH, or a maximum sentence of two year in prison, or both.</p>
<p style="text-align: center;"><b>Qodobka 43-aad</b></p> <p><b>Mamnuucidda Muuqallada Qaaqaawan</b></p> <ol style="list-style-type: none"> <li>1. Soo saarista, faafinta ama ka qaybqaadashada soo saarista sawirro ama muuqaalo qaaqaawan iyadoo la adeegsanayo Tiknoolajiyadda Casriga ah way reebbantay.</li> <li>2. Cidda si ula kac ah u gasha fal dembiyeedka lagu xusay farqadda 1-aad ee qodobkan, waxay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Konton Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan shan sano oo xadhig ah, ama labadaba.</li> </ol>	<p style="text-align: center;"><b>Article 43</b></p> <p style="text-align: center;"><b>Prohibition of Pornography</b></p> <ol style="list-style-type: none"> <li>1. Producing or participating in the production of pornography using a computer system is prohibited.</li> <li>2. A person who intentionally commits an offence under sub-article (1) is subject to a maximum fine of up to fifty million SLSH, or a maximum sentence of five years in prison, or both.</li> </ol>

<p style="text-align: center;"><b>Qodobka 44-aad</b></p> <p><b>Muuqaallada Qaaqaawan ee Carruurta</b></p> <p>1. Qodobkani wuxuu qeexayaa reebanaanta:</p> <p style="padding-left: 40px;">a) soo saarista, faafinta ama ka qaybqaadashada samaynta sawirro ama muuqaalo qaaqaawan oo caruureed iyada oo la adeegsanaya Tiknoolajiyadda Casriga ah,</p> <p style="padding-left: 40px;">b) siinta, ku qasbida, u ogolaanshaha caruurta muuqaalo qaaqaawan iyada oo la adeegsanayo Tiknoolajiyadda Casriga ah.</p> <p>2. Cidda gasha dembiyada ku xusan farqadda 1-aad ee qodobkan waxay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Todobaatan milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan todoba sano oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 44</b></p> <p style="text-align: center;"><b>Child Pornography</b></p> <p>1. This article prohibits:</p> <p style="padding-left: 40px;">a) production of child pornography for the goal of distributing it via a computer or on internet device;</p> <p style="padding-left: 40px;">b) selling or making pornography available to a child via a computer, or on internet;</p> <p>2. A person who commits an offense under sub-article (1) is subject to a maximum fine of up to seventy five million or a maximum sentence of seven years in prison, or both.</p>
--	---



<p style="text-align: center;"><b>Qodobka 45-aad</b></p> <p style="text-align: center;"><b>Duufsashada Caruurta</b></p>	<p style="text-align: center;"><b>Article 45</b></p> <p style="text-align: center;"><b>Child Solicitation</b></p>
<ol style="list-style-type: none"> <li>1. Qodobkani wuxuu qeexayaa reebanaanta:               <ol style="list-style-type: none"> <li>a) la kulanka caruurta iyada oo la damacsan yahay in la galo fal dembiyeed iyadoo la adeegsanayo Tiknoolajiyadda Casriga ah,</li> <li>b) la xidhiidhka caruurta iyadoo la adeegsanayo Tiknoolajiyadda Casriga ah si loogu sasabto in uu sameeyo fal dembiyeed galmo,</li> <li>c) la shaqaaleeyo caruurta iyada oo la adeegsanayo Tiknoolajiyadda Casriga ah si uu uga qayb qaato bandhigyo qaaqaawan,</li> </ol> </li> <li>2. Cidda gasha dembiyada ku xusan farqadda 1-aad ee qodobkan, waxay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Konton Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan</li> </ol>	<ol style="list-style-type: none"> <li>1. This article prohibits:               <ol style="list-style-type: none"> <li>a) using of a computer system to meet a child with the intent of committing a sexual offense;</li> <li>b) communicating with a child via a computer system in order to persuade the child to engage in sexual conduct with that person;</li> <li>c) recruiting a child to take part in pornographic performances that will be produced or recorded, with or without the intention of distributing such material via a computer system or over the internet;</li> </ol> </li> <li>2. A person who commits an offence under sub-article (1) is subject to a maximum fine of up to fifty milliom SLSH, or a maximum sentence of five years in prison, or both</li> </ol>

<p>dhan shan sano oo xadhig ah , ama labadaba.</p> <p><b>Qodobka 46-aad</b></p> <p><b>Foorjariga Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah u foorjariyaysa, beddesha ama tirtirta xog iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Afartan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan afar sano oo xadhig ah , ama labadaba.</p>	<p><b>Article 46</b></p> <p><b>Cyber Forgery</b></p> <p>1. A person who intentionally forges, alters or deletes computer data, with the intent that it be considered authentic commits an offence and is subject to a maximum fine of up to forty million SLSH or a maximum sentence of four years in prison, or both.</p>
<p><b>Qodobka 47-aad</b></p> <p><b>Khayaanada Tiknoolajiyadda Casriga ah</b></p> <p>1. Cidda si ula kac ah u maleegta dhagar maaliyadeed ama nafeed iyada oo adeegsanaysa Tiknoolajiyadda Casriga waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed</p>	<p><b>Article 47</b></p> <p><b>Cyber Fraud</b></p> <p>1. A person who intentionally frauds with intention to cause potential prejudice to another person commits an offence and is subject to a maximum fine of up to one hundred million, or a maximum</p>

<p>oo ugu badnaan dhan <b>Boqol Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan toban sano oo xadhig ah , ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 48-aad</b></p> <p style="text-align: center;"><b>Argagixisada Tiknoolajiyadda Casriga ah</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah ku baahisa kuna soo bandhigta, ku dhiirigalisa, ku tababarta, ama ku xidhiidha iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah si loo fuliyo ama fududeeyo falal argagixso waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Boqol iyo Konton Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan shan iyo toban sano oo xadhig ah , ama labadaba.</li> </ol>	<p>sentence of five years in prison, or both.</p> <p style="text-align: center;"><b>Article 48</b></p> <p style="text-align: center;"><b>Cyber Terrorism</b></p> <ol style="list-style-type: none"> <li>1. A person who accesses or causes a computer, computer system, or network to be accessed for the purpose of carrying out a terrorist act commits an offense and is subject to a maximum fine of up to one hundred and fifty million SLSH, or a maximum sentence of fifteen years in prison, or both.</li> </ol>
---	--

<p style="text-align: center;"><b>Qodobka 49-aad</b></p> <p style="text-align: center;"><b>Xatooyada Aqoonsiga iyo Iska Dhigista</b></p> <p style="text-align: center;"><b>Qof kale</b></p> <p>1. Cidda si ula kac ah oo xeeladaysan u xadda ama u adeegsata aqoonsiga, saxeexa, sawirka iyo xog kasta oo lagu aqoonsan karo cid gaar ah iyada oo la adeegsanayo Tiknoolajiyadda Casriga ah waxay gelayaa dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Laba iyo Afartan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan labo sano oo xadhig ah , ama labadaba.</p>	<p style="text-align: center;"><b>Article 49</b></p> <p style="text-align: center;"><b>Identity Theft and Impersonation</b></p> <p>1. A person who, intentionally by using a computer transfers, possesses, or uses, the electronic signature, password or any other unique identification feature of any other person, commits an offence and is subject to a maximum fine of up to forty two million SLSH, or a maximum sentence of four years in prison, or both.</p>
<p style="text-align: center;"><b>Qodobka 50-aad</b></p> <p style="text-align: center;"><b>Dabis</b></p> <p>1. Cidda ula kac ah u sameeysa dabis Elektaroonig ah iyada oo adeegsanaysa Tiknoolajiyadda Casriga ujeeddadeeduna tahay in ay la wareegto mulkiyada xog gaar ah oo ciddi leedahay ah waxay</p>	<p style="text-align: center;"><b>Article 50</b></p> <p style="text-align: center;"><b>Phishing</b></p> <p>1. A person who creates or operates a website or sends a message through a computer system with the intent of inducing a website user or message recipient to disclose personal information for an unlawful purpose or to gain</p>

<p>galaysaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Lixdan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan lix sano oo xadhig ah , ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 51-aad</b></p> <p><b>Hakinta Farriimaha Elektaroonigga ah</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah u hakisa ama u haysata farriin elektaroonig ah sida e-mail, lacag bixinta Elektaroonigga ah ama kaadhka lacagta Elektaroonigga ah, waxay gelayaa dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Labaatan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan labo sano oo xadhig ah, ama labadaba.</li> </ol>	<p>unauthorized access to a computer commits an offense and subjected to a maximum fine of up to sixty five million SLSH, or a maximum sentence of six years in prison, or both.</p> <p style="text-align: center;"><b>Article 51</b></p> <p><b>Withholding Electronic Messages</b></p> <ol style="list-style-type: none"> <li>1. A person who intentionally conceals or retains any electronic mail, message, electronic payment, credit or debit card found by the person or delivered to the person in error and which should have been delivered to another person commits an offense and is subject to a maximum fine of up to twenty million SLSH, or a maximum sentence of two year in prison, or both.</li> </ol>
---	---

<p style="text-align: center;"><b>Qodobka 52-aad</b></p> <p style="text-align: center;"><b>Farriimaha Elektaroonigga ee Huriya Burbur Hantiyeed ama Qalalaase</b></p> <p>1. Cidda si ula kac ah u dirta ama soo bandhigta farriin elektaroonig ah iyada oo ujeeddadeedu tahay burbur hantiyeed, cabsi-galin ama qalalaase amni, waxay gelaysoa dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Laba Boqol oo iylan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan toban sano oo xadhig ah , ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 53-aad</b></p> <p style="text-align: center;"><b>Faafinta Muuqaallada Dhaqan-xumada Wata</b></p> <p>1. Cidda si ula kac ah u soo bandhigta ama u faafisa xubnaha cawrada ah ee jidh-keeda, ama muuqaal dhaqan-xumo muujinaya oo ay ku jiraan samaynta sawirro elektaroonig ah iyada oo la</p>	<p style="text-align: center;"><b>Article 52</b></p> <p style="text-align: center;"><b>Electronic Message that Incites Damage to Property or Violence</b></p> <p>1. A person who discloses an electronic message to a person, group of people, or the general public with the intent to incite property damage or violence against a person or group of people commits an offence and is subjected to a maximum fine of about two hundred million SLSH, or a maximum sentence of ten years in prison, or both.</p> <p style="text-align: center;"><b>Article 53</b></p> <p style="text-align: center;"><b>Wrongful Distribution of Obscene or Intimate Images</b></p> <p>1. A person who transfers, publishes, or disseminates the intimate parts or obscene image of another person, including making a digital depiction available for distribution or downloading through a telecommunications network or any other means of transferring</p>
---	--

<p>adeegsanayo Tiknoolajiyadda Casriga ah waxay gelaysoo dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Toban Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan hal sano oo xadhig ah , ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 54-aad</b></p> <p style="text-align: center;"><b>Faafinta Muuqaallada iyo Sawirada gaarka ah</b></p> <ol style="list-style-type: none"> <li>1. Cidda si ula kac ah oo ogolaansho la'aan ah u faafisa ama u soo bandhigta muuqaallo ama sawiro u gaar ah cid kale iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah waxay gelaysoo dembi, waxa aanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Afartan Milayan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan afar sano oo xadhig ah, ama labadaba.</li> <li>2. Cidda si ula kac ah oo ogolaansho la'aan ah ugala baxda, u faafisa</li> </ol>	<p>data to a computer, commits an offence and is subject to a maximum of up to ten million SLSH, or a maximum sentence of one year in prison, or both.</p> <p style="text-align: center;"><b>Article 54</b></p> <p style="text-align: center;"><b>Dissimination of Personal Photos and Videos</b></p> <ol style="list-style-type: none"> <li>1. A person who intentionally and without permission disseminates or presents videos or photos of another person commits an offense and is subjected to a maximum fine of up to forty million of SLSH or imprisonment for a term not exceeding four years, or both.</li> <li>2. A person who intentionally copies, disseminates or discloses to another person digital information materials commits a crime and will be liable to a maximum fine of sixty million SLSH or a maximum sentence of imprisonment of six years, or both.</li> </ol>
--	--

<p>ama u soo bandhigta xog cid kale oo ku kaydsan agabka Tiknoolajiyadda Casriga ah waxay gelaysoo dembi, waxa aanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Lixdan Milayan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan lix sano oo xadhig ah, ama labadaba.</p> <p style="text-align: center;"><b>Qodobka 55-aad</b></p> <p style="text-align: center;"><b>Hadalka Nacaybka Xambaarsan</b></p> <p>1. Cidda si ula kac ah u baahisa, u adeegsata hadal xambaarsan nacayb, isku dir, kicin bulsho, kala qaybin bulsho, aflagaado ama fuquuq waxay gelaysoo dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Afartan Milyan oo SLSH</b> ama xukun ciqaabeed ugu badnaan dhan afar sano oo xadhig ah ama labadaba.</p>	<p style="text-align: center;"><b>Article 55</b></p> <p style="text-align: center;"><b>Hate Speech</b></p> <p>1. A person who, intentionally broadcasts or uses hate speech to create social incitement, social divisiveness or violence commits an offence and is subject to a maximum fine of up to forty five million SLSH or a maximum sentence of four years in prison, or both.</p>
--	---



<p style="text-align: center;"><b>Qodobka 56-aad</b></p> <p><b>Hadalka Cunsuriyadda Xanbaarsan</b></p> <p>1. Cidda si ula kac ah u baahisa, u soo bandhigta ama ugu kacda hadal xanbaarsan cunsuriyad iyo ajaanib nacayb iyada oo adeegsanaysa Tiknoolajiyadda Casriga ah waxay gelaysaa dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan <b>Shan iyo Labaatan Milyan oo SLSH</b> ama xukun cigaabeed ugu badnaan dhan laba sano oo xadhig ah, ama labadaba.</p>	<p style="text-align: center;"><b>Article 56</b></p> <p><b>Racist or Xenophobic Motivated Insult</b></p> <p>1. A person who insults another person using a computer or computer system on the basis of race, color, nationality, ethnic origin, tribe, or religious affiliation commits an offence and is subject to a maximum fine of up to twenty five million SLSH, or a maximum sentence of two years in prison, or both.</p>
--	---

<p style="text-align: center;"><b>CUTUBKA 8-AAD</b></p> <p style="text-align: center;"><b>CADEYNTA ELECTRONIGA AH</b></p> <p style="text-align: center;"><b>Qodobka 57-aad</b></p> <p style="text-align: center;"><b>Ogolaanshaha Caddaynta</b> <b>Elektaroonigga ah</b></p> <ol style="list-style-type: none"> <li>1. Caddaymaha xogta Elektaroonigga ahi waxay yeelanayaan awood la mid ah caddaymaha xeerarka kale ee dalku qeexeen.</li> <li>2. Cidna ma diidi karto awoodda caddaymaha Elektaroonigga ah ee loo soo ururiyey qaab waafaqsan qodobada xeerkan.</li> <li>3. Cidda looga baahdo xog elektaroonig ah waa in ay u bixisaa xogtaa qaab waafaqsan qodobada xeerkan.</li> </ol> <p style="text-align: center;"><b>Qodobka 58-aad</b></p> <p style="text-align: center;"><b>Xaqiiqinta Cadaymaha Xogta</b> <b>Elektaroonigga ah</b></p> <ol style="list-style-type: none"> <li>1. Baadhitaanada la xidhiidha cadaymaha elektarooniga ah</li> </ol>	<p style="text-align: center;"><b>CHAPTER 8</b></p> <p style="text-align: center;"><b>DIGITAL EVIDENCE</b></p> <p style="text-align: center;"><b>Article 57</b></p> <p style="text-align: center;"><b>Admissibility of Electronic Evidence</b></p> <ol style="list-style-type: none"> <li>1. Digital Evidence shall have the same admissibility as evidence defined by other written laws.</li> <li>2. A person cannot deny the validity of electronic evidence collected in accordance with the provisions of this act.</li> <li>3. A person who is required to provide electronic information must provide the information in accordance with the provisions of this act.</li> </ol> <p style="text-align: center;"><b>Article 58</b></p> <p style="text-align: center;"><b>Using Affidavit as Proof of Certain Facts about Digital Evidence</b></p> <ol style="list-style-type: none"> <li>1. Investigations related to digital evidence shall be conducted by a</li> </ol>
--	--

<p>waxaa samayn kara sarkaal boolis oo aqoon u leh ama cid kale oo si sharci ah loogu igmaday.</p> <p>2. Marka xog elegtirooniga loo adeegsanayo dacwad maxkamdeed, waa in ciddi soo ururiyey ku dhaarataa in ay buuxinayo shuruudaha ku xusan farqada 1-aad ee qodobkan.</p> <p>3. Cidda si ula kac ah uga beensheegta dhaarta ku xusan farqadda 2-aad ee qodobkan waxay gelaysoo dembi waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan kow iyo labaatan milyan oo SLSH ama xukun ciqaabeed ugu badnaan dhan laba sano oo xadhig ah, ama labadaba.</p> <p>4. Maxkamada dalku waxay awood u leedahay in ay cidda cadaymaha elegtirooniga ah soo ururisay u diraan waaran si uu u bixiyo caddayn afka ah marka lagu gudo jiro dacwadda laga garnaqayo.</p>	<p>qualified police officer or other legally authorized person.</p> <p>2. When a digital evidence is used for legal proceedings, the person who collected it must prove by oath that he meets the conditions under sub-article (1) of this article.</p> <p>3. A person who intentionally falsifies the oath referred to in sub-article (2) of this article commits an offence and subjected to a maximum fine up to twenty one million SLSH, or a maximum sentence of two year in prison, or both.</p> <p>4. The court of the country has the power to send warrant to the person who collected the electronic evidence to give oral proof during the proceedings.</p>
---	--

<p style="text-align: center;"><b>CUTUBKA 9-AAD</b></p> <p style="text-align: center;"><b>AWOODDA BAADHISTA, RAADINTA, GELIDDA, AMA LAWAREEGIDA</b></p> <p style="text-align: center;"><b>Qodobka 59-aad</b></p> <p><b>Habraaca Baadhista Elektaroonigga ah</b></p> <ol style="list-style-type: none"> <li>1. Laba iyo toban bilood (12) gudahood oo ka bilaabanta maalinka xeerkaan baarlamaanku ansixiyo, madaxwaynuhuna saxeexo, wasaaraddu iyada oo la kaashanaysa laamaha kale ee xukuumada ee ay khusayso, waa in ay curiso habraaca iyo hagayaasha baadhista caddaymaha elegtarooniga ah.</li> <li>2. Habraac iyo hagayaasha lagu xusay farqadda 1-aad ee qodobkan marka la soo saaro iyo wax kabadal kasta oo lagu sameeyo waa in lagu baahiyaa faafinta rasmiga ah ee dawlada (Gazette).</li> </ol>	<p style="text-align: center;"><b>CHAPTER 9</b></p> <p style="text-align: center;"><b>POWER TO INVESTIGATE, SEARCH, ACCESS OR SEIZE</b></p> <p style="text-align: center;"><b>Article 59</b></p> <p style="text-align: center;"><b>Standard Operating Procedures</b></p> <ol style="list-style-type: none"> <li>1. Within twelve months from the data that this act has been passed by the parliament and signed by the president, the Ministry of ICT, in consultation with the National Police Commander, Attorney General, and the Minister of Justice, must issue Standard Operating Procedures for the investigation of any offence or suspected offence under this Act.</li> <li>2. The Standard Operating Procedures referred to in sub-article (1) and any amendment thereto must be published in the official Gazette.</li> </ol>
--	--

<p style="text-align: center;"><b>Qodobka 60-aad</b></p>	<p style="text-align: center;"><b>Article 60</b></p>
<p style="text-align: center;"><b>Raadinta, Gelida, ama La-wareegista</b></p>	<p style="text-align: center;"><b>Search for, Access to, or Seizure of</b></p>
<p style="text-align: center;"><b>Xog Elektaroonig ah</b></p>	<p style="text-align: center;"><b>Computer Data</b></p>
<ol style="list-style-type: none"> <li>1. Sarkaalka booliiska ah ama cid kale ee loo igmadey in ay baadho xogta Elektaroonigga ah waxay awood u leedahay in ay baadho, gasho, ama la wareegto xog iyo agab kasta oo muhiim u ah baadhis Elektaroonig ah ee xeerkani waajibiyey.</li> <li>2. Marka uu sarkaal boolis ah ama cid kale oo la igmaday gudanayo waajibaadka xeerkani waa in uu waaran maxkamadeed haystaa.</li> <li>3. Waaranka lagu bixiyey hab waafaqasan farqadda 2-aad ee qodobkan waa in lagu cadeeyaa xogta, agabka, ama qof kasta oo baadhista muhiim u ah.</li> <li>4. Waaranka lagu bixiyey hab waafaqasan farqadda 2-aad, wey shaqayn doontaa ilaa amarku fulo ama isla maxkamaddii bixisay buriso.</li> <li>5. Marka laga shakiyo in la tirtiro, burburiyo, ama wax laga badalo cadaynta Elektarooniga ah,</li> </ol>	<ol style="list-style-type: none"> <li>1. In accordance with the provisions of Chapter 9 of this Act, a police officer or a ligally authorised person may search for, access, or seize data, computer program, computer system, and computer data storage medium believed to be help for an offence committed under this act.</li> <li>2. When a police officer or an authorized person is performing in accordance to the provisions of this act shall have a court warrant.</li> <li>3. the warrant under sub-article (2) of this article shall clearly state the data, devices, or names indivituals involved in the investigation.</li> <li>4. A search warrant undert sub-article (2) shall remain valid until executed or cancelled by the issuing court.</li> <li>5. A police officer may, <i>without a search warrant</i>, execute the powers under sub-article (2), if the police officer is, on reasonable grounds</li> </ol>

<p>sarkaalka booliisku wuu fulin karaa awoodaha lagu xusay farqadda 2-aad ee qodobkan isagoon wadan waaran.</p> <p>6. Cidda si ula kac ah u hor istaagta dhaqan galka awoodaha sharci ee lagu xusay qodobkan, waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan Laba iyo Afartan Milyan oo SLSH ama xukun ciqaabeed ugu badnaan dhan labo sano oo xadhig ah , ama labadaba.</p> <p>7. Cidda si qaldan uga fa'iidaysta awoodaha lagu bixiyey qodobkan, waxay gelayso dembi, waxaanay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan Laba iyo afartan milyan oo SLSH ama xukun ciqaabeed ugu badnaan dhan labo sano oo xadhig ah , ama labadaba.</p> <p>8. Haddii mulkiilaha xogta Elektaroonigga ah uu yahay haween, waxa baadhista ku xusan farqadda 1-aad ee qodobkan fulinaysa gabadh sarkaalad ah ama</p>	<p>believes, of the opinion that a sensitive data which is the subject of the search may be destroyed, disposed of, or tampered.</p> <p>6. A person who obstructs the lawful exercise of the powers granted under this article commits an offence and is subject a maximum fine of up to forty two million SLSH, or a maximum sentence of four years in prison, or both.</p> <p>7. A person unlawfully benefits from the provisions under this article commits an offence and is subject to maximum fine of up to forty two million SLSH, or a maximum sentence four years in prison, or both.</p> <p>8. If a computer that need to be searched under this article belongs to a female, the search must be carried out by a female police officer. If a female police officer is not available, the search must be carried out by any female designated by a police authority for that purpose.</p>
---	---

<p>gabadh kale oo maamulka boolisku u igmaday.</p> <p><b>Qodobka 61-aad</b></p> <p><b>Raadinta, Galida, iyo la Wareegista Qaldan</b></p> <p>1. Sarkaalka boolis ama baadhaha si sharciga baal marsan oo badheedh ah u adeegsada awoodaha sharci ee Xeerkani siiyey wuxuu gelayaa dembi waxaanu mutaysan doonaa ganaax lacageed oo ugu badnaan dhan Afartan Milyan oo SLSH ama xukun cigaabeed ugu badnaan dhan afar sano oo xadhig ah, ama labadaba.</p> <p><b>Qodobka 62-aad</b></p> <p><b>Amarka Tirtiridda</b></p> <p>1. Sarkaalka boolisku wuxuu maxkamadda ka codsan karaa in la tirtiro ama burburiyo xogaha eletarooniga ah ee la xidhiidha anshax xumada.</p>	<p><b>Article 61</b></p> <p><b>Wrongful Search, Access, or Seizure</b></p> <p>1. A police officer or an investigator who unlawfully and intentionally acts contrary to the authority of a search warrant issued under this Act or consent granted in terms of this Act commits an offence and is subject to a maximum fine of up to forty million or a maximum sentence of four years in prison, or both.</p> <p><b>Article 62</b></p> <p><b>Deletion Order</b></p> <p>1. A police officer, in writing, may apply to a court for an order that data in a computer which contains pornography or other obscene material be deleted or destroyed.</p>
---	---

<p style="text-align: center;"><b>Qodobka 63-aad</b></p> <p style="text-align: center;"><b>Caddaynta Elektaroonigga ah ee si Sharci-darro ah loo Helay</b></p> <p>1. Caddaymaha Elektaroonigga ah ee loo helay hab ka hor imanaya Xeerkan looma adeegsan doono dacwadaha ay ka garnaqayaan heerarka kala duwan ee maxakamadaha dalku.</p>	<p style="text-align: center;"><b>Article 63</b></p> <p style="text-align: center;"><b>Illegally Intercepted Digital Evidence is not Admissible in Court</b></p> <p>1. Digital evidence obtained by a means in contravention of this Act is shall not be rendered admissible in criminal proceedings.</p>
---	---



<p style="text-align: center;"><b>CUTUBKA 10-AAD</b></p> <p style="text-align: center;"><b>ISKAASHIGA CAALAMIGA AH EE GACAN KU HAYNTA AMAANKA TIKNOOLAJIYADDA CASRIGA AH</b></p> <p style="text-align: center;"><b>Qodobka 64-aad</b></p> <p style="text-align: center;"><b>Tilmaamidda Aagagga Iskaashiga</b></p> <p>1. Wasaaraddu iyada oo ka duulaysa danta qaranka waxa ay qeexaysaa habka ay iskaashi ula yeelanayso shirkadaha ganacsiga, ururrada caalamiga ah iyo hay'adaha dawaliga ee ku hawlan amaanka Tiknoolajiyadda Casriga ah ee heer caalami.</p> <p style="text-align: center;"><b>Qodobka 65-aad</b></p> <p style="text-align: center;"><b>Heshiisyada Calamiga ah</b></p> <p>1. Wasaaraddu iyada oo matalaysa dalka waxay heshiis la geli kartaa</p>	<p style="text-align: center;"><b>CHAPTER 10</b></p> <p style="text-align: center;"><b>INTERNATIONAL COOPERATION IN MAINTAINING CYBER SECURITY</b></p> <p style="text-align: center;"><b>Article 64</b></p> <p style="text-align: center;"><b>Identifying Areas of Co-operation</b></p> <p>1. The Ministry shall identify and ensure areas of cooperation with private, international organizations and other government entities involved in cyber security matters at international level.</p> <p style="text-align: center;"><b>Article 65</b></p> <p style="text-align: center;"><b>International Agreement</b></p> <p>1. The Ministry may on behalf of the country enter into any agreement</p>
---	--

<p>dal shisheeye iyo ha'yad caalamiya ah heshiis, ku saabsan iskaashi la xidhiidha baadhitaanka iyo dembi ku oogidda fal-dembiyeed ku xusan xeerkan</p>	<p>with any foreign State and international body regarding the provision of mutual assistance and cooperation relating to the investigation and prosecution of an offence committed under this Act.</p>
---	---

## CUTUBKA 11-AAD

### QODOBO GUUD

#### Qodobka 66-aad

##### Ciqaabta Guud

1. Qofka gala dembiyada ku xusan xeerkan oo aan layhan ciqaab u gaar ah wuxuu mutaysan doonaa ganaax lacageed oo ugu badnaan dhan **Konton Milyan oo SLSH** ama xukun ciqaabeed ugu badnaan dhan shan sano oo xadhig ah, ama labadaba.
2. Shirkadda gasha dembi Xeerkani qeexay oo aan lahayn ciqaab u gaar ah waxay mutaysan doontaa ganaax lacageed oo ugu badnaan dhan **Boqol Milyan oo SLSH**.

#### Qodobka 67-aad

##### Magdhawga

1. Cidda ay dhibaato gaar ah, mid maaliyadeed, mid sumcadeed, mid

## CHAPTER 11

### GENERAL PROVISIONS

#### Article 66

##### General Penalty

1. A person who commits an offense under this Act for which no penalty is specified is subject to a maximum fine of up to fifty million SLSH, or a maximum sentence of five years, or both.
2. A body corporation that commits an offence under this Act for which no penalty is specified is subject to a maximum fine of up to hundred million SLSH.

#### Article 67

##### Compensation

1. A person who suffers from personal problem such as, financial, reputational, commercial,

<p>ganacsi iyo noockastoo kaleba kasoo gaadho xad-gudub ama dembi ka dhashay adeegsiga Tiknoolajiyadda Casriga ah, ciddaasi waxa uu xaq u leedahay in ay magdhow ka helsho cidda xad-gudubka ama dembiga gaysatay marka ay go'aamiso maxkamad awood u leh.</p> <p style="text-align: center;"><b>Qodobka 68-aad</b></p> <p style="text-align: center;"><b>Kaalmo</b></p> <p>1. Cidda ku gasha dal kale dembiyada ku xusan qodobada xeerkan, maxkamaddaha dalku waxay awood u leeyihiin in ay ka codsadaan dalka fal-dambiyeedu ka dhacay xogta Elektaroonigga ah si loo ilaaliyo, loo helo, loo ururiyo ama loogu sameeyo baadhitaan.</p> <p style="text-align: center;"><b>Qodobka 69-aad</b></p> <p style="text-align: center;"><b>Racfaan</b></p> <p>1. Cid kasta oo ku qanci wayda go'aamada ama amarrada Wasaaradda ama Xaruntu gaadhay</p>	<p>or other types of crimes as a result of a cybercrime has the right to compensation from the person who committed the cybercrime, as determined by a court.</p> <p style="text-align: center;"><b>Article 68</b></p> <p style="text-align: center;"><b>Assistance</b></p> <p>1. If a person commits an offense under this Act by means of or facilitated by a computer within the territory of a foreign state, the court may issue a letter requesting assistance from the foreign state to preserve, obtain, collect, or seize data needed to conduct investigations.</p> <p style="text-align: center;"><b>Article 69</b></p> <p style="text-align: center;"><b>Appeal</b></p> <p>1. Any person aggrieved by any decision or order of the Ministry or the Center made under this Act, may appeal to the Courts of the country as the case may be within</p>
--	--

<p>iyadoo adeegsanaysa qodobada Xeerkan, waxay racfaan u qaadan kartaa maxkamaddaha dalka, soddon maalmood gudohood oo ka bilaabmaysa maalinta xukunku dhaco.</p> <p style="text-align: center;"><b>Qodobka 70-aad</b></p> <p style="text-align: center;"><b>Xeer-nidaamiye</b></p> <p>1. Wasaaraddu waxay curin kartaa xeer-nidaamiyayaal iyadoo raacaysa qodobada Xeerkan.</p> <p style="text-align: center;"><b>Qodobka 71-aad</b></p> <p style="text-align: center;"><b>Dhaqan-galka Xeerka</b></p> <p>1. Xeerkan wuxuu dhaqan galayaa marka ay Golayaasha baarlamaanku ansixiyaan isla markaana uu saxeexo Madaxweynaha JSL, laguna soo saaro faafinta rasmiga.</p>	<p>thirty days from the date of the decision or order.</p> <p style="text-align: center;"><b>Article 70</b></p> <p style="text-align: center;"><b>Regulation</b></p> <p>1. The Ministry may issue regulations for the better carrying out of the provisions of this Act.</p> <p style="text-align: center;"><b>Article 71</b></p> <p style="text-align: center;"><b>Implementation of the Act</b></p> <p>1. This act will come into effect when approved by the Houses of Parliament and signed by the President of the Republic of Somaliland and published in the Official Gazette.</p>
--	---