****

**REPUBLIKAE SHQIPËRISË**

**KUVENDI**

**P R O J E K T L I GJ**

**Nr.\_\_\_\_\_\_\_\_/2023**

**PËR**

**SIGURINË KIBERNETIKE[[1]](#footnote-1)**

Në mbështetje të neneve 78 dhe 83, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave,

**K U V E N D I**

**I REPUBLIKËS SË SHQIPËRISË**

**V E N D O S I:**

**KREU I**

**DISPOZITA TË PËRGJITHSHME**

**Neni 1**

**Qëllimi i ligjit**

Qëllimi i këtij ligji është përcaktimi i kornizës së nevojshme ligjore për sigurinë kibernetike dhe arritja e një niveli të lartë të sigurisë kibernetike, për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë, duke përcaktuar procedurat dhe masat e sigurisë për to.

**Neni 2**

**Objekti i ligjit**

1. Objekti i këtij ligji është të përcaktojë të drejtat dhe detyrimet e subjekteve publike dhe private, të cilët administrojnë infrastruktura të informacionit, rrjetet e komunikimit dhe sistemet e tyre, cenimi apo shkatërrimi i të cilave do të kishte impakt në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
2. Ky ligj gjithashtu përcakton:
3. Autoritetin përgjegjës për Sigurinë Kibernetike në Republikën e Shqipërisë, i cili është edhe pika e vetme e kontaktit për çështje të sigurisë kibernetike;
4. Detyrimin e krijimit të ekipit të përgjigjes ndaj incidenteve të sigurisë kibernetike si CSIRT-in Kombëtar, CERT-in, si dhe CSIRT-et sektoriale;
5. Përcaktimin e autoritetit përgjegjës për hartimin e Strategjisë Kombëtare të Sigurisë Kibernetike, brenda fushës së veprimit të këtij ligji, si dhe institucionet e tjera përgjegjëse të sigurisë dhe mbrojtjes që ndërveprojnë për çështjet e sigurisë kibernetike në vend;

ç) Detyrimin e zbatimit të masave të sigurisë dhe raportimin e incidenteve të sigurisë kibernetike nga ana e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

1. Ky ligj nuk bie në kundërshtim me masat e marra për të mbrojtur funksionet thelbësore të shtetit, në veçanti masat për mbrojtjen e sigurisë kombëtare, duke përfshirë masat për mbrojtjen e informacionit, në rastet kur shpërndarja e tij konsiderohet në kundërshtim me interesat thelbësore të sigurisë dhe rendit publik, në veçanti për qëllimet e hetimit, zbulimit dhe ndjekjes së veprave penale.
2. Detyrimet e parashikuara për CSIRT-in Kombëtar, sipas këtij ligji, zbatohen edhe për raportimet në organizmat përgjegjëse të BE-së, në rastin e antarësimit të Republikës së Shqipërisë në Bashkimin Evropian.

**Neni 3**

**Parime të përgjithshme të sigurisë kibernetike**

1. Përpunimi i të dhënave personale sipas përcaktimeve të këtij ligji kryhet sipas dispozitave të përcaktuara në legjislacionin në fuqi për mbrojtjen e të dhënave personale.
2. Në përputhje me përcaktimet e bëra në këtë ligj, zbatohet për aq sa është e mundur, parimi i neutralitetit të teknologjisë, sipas të cilit individët dhe organizatat janë të lirë për të zgjedhur teknologjinë më të përshtatshme për nevojat e tyre duke mos imponuar dhe as diskriminuar ndonjë lloj të veçantë teknologjie.

**Neni 4**

**Përkufizime**

Në kuptim të këtij ligji, termat e mëposhtëm kanë këto kuptime:

1. “**Autoriteti përgjegjës për Sigurinë Kibernetike”,** është Autoriteti Kombëtar për Sigurinë Kibernetike, institucioni publik përgjegjës për zbatimin dhe mbikëqyrjen e këtij ligji, në vijim Autoriteti.
2. **“CERT”,** është Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike.
3. **“CSIRT Kombëtar”,** është Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike, pranë Autoritetit.
4. “**CSIRT sektorial**”, është personi/ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike, për sektorin përkatës, i vendosur pranë një operatori që administron infrastruktura kritike dhe të rëndësishme të informacionit, ose institucioni përgjegjës të linjës.
5. “**CSIRT qeveritar”,** është CSIRT-i sektorial i cili menaxhon të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit për sektorin qeveritar.
6. **“CSIRT pranë operatorëve”,** është ekipi i përgjigjes ndaj Incidenteve të Sigurisë Kibernetike, pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.
7. “**Certifikatë e sigurisë kibernetike**”, është një dokument i lëshuar nga një organ përkatës, që vërteton se një produkt, shërbim ose proces TIK, është vlerësuar për pajtueshmërinë me kërkesat specifike të sigurisë të përcaktuara në skemën e certifikimit të sigurisë kibernetike.
8. **“ENISA**”, është Agjencia për Sigurinë Kibernetike e Bashkimit Evropian.
9. **“Emergjencë e sigurisë kibernetike”,** është situata gjatë së cilës siguria e informacionit në sistemet e informacionit, ose siguria e rrjeteve të komunikimeve elektronike është cenuar duke vënë në rrezik interesin publik të Republikës së Shqipërisë**.**
10. “**Hapësirë kibernetike**”, është mjedisi digjital i aftë të krijojë, procesojë dhe të shkëmbejë komunikimin elektronik të informacionit të krijuar nga rrjetet dhe sistemet e informacionit edhe pa qenë të lidhur në internet.
11. **“Incident i sigurisë kibernetike”,** është një ngjarje kibernetike gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve, sistemeve të informacionit dhe rrjeteve të komunikimit duke sjell efekte negative në to.
12. **“Infrastrukturë kritike e informacionit**”, është tërësia e rrjeteve dhe sistemeve të informacionit, të zotëruara nga një autoritet publik ose privat, që ofrojnë shërbime, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
13. **“Infrastrukturë e rëndësishme e informacionit”** është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik ose privat, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë ofrimin e shërbimit dhe vazhdimësinë e punës, në rastin e cenimit të sigurisë së informacionit.
14. “**Krizë kibernetike**”, është situata gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është seriozisht e rrezikuar, duke vënë në rrezik interesin publik të Republikës së Shqipërisë.
15. **“Loge”,** mesazh apo e dhënë mbi ngjarje lidhur me sigurinë kibernetike.
16. **“Masat e sigurisë kibernetike”,** nënkuptojnë tërësinë e veprimeve për rritjen e sigurisë së informacionit në sistemet e informacionit dhe disponueshmërinë e besueshmërinë e shërbimeve të rrjeteve të komunikimit në hapësirën kibernetike.
17. **“Motor kërkimi në internet”,** është një shërbim digjital, që në parim lejon përdoruesin të kërkojë në të gjitha faqet e internetit, në një gjuhë të veçantë, për çdo temë, pyetje duke i shprehur ato në formën e një fjale kyçe apo fraze dhe realizon lidhjen ku mund të gjendet informacioni me përmbajtjen e kërkuar.
18. **“Operator i infrastrukturës kritike të informacionit**”, është çdo subjekt publik ose privat, i cili administron infrastrukturën kritike të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.
19. “**Operator i infrastrukturës së rëndësishme të informacionit**”, është çdo subjekt publik ose privat, i cili administron infrastrukturën e rëndësishme të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.
20. “**Ofruesi i shërbimit DNS**”, është një subjekt publik ose privat, i cili ofron shërbime të emërtimit të domain-ve në internet.
21. **“Organizmi i Vlerësimit të Konformitetit**”, është një person fizik ose juridik, kombëtar ose ndërkombëtar, i akredituar nga institucioni përgjegjës për akreditim, për të kryer vlerësimet dhe testimet e konformitetit të produkteve, shërbimeve dhe proceseve TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit.
22. “**Pika e shkëmbimit të internetit (IXP)”**:
23. është një infrastrukturë rrjeti që lejon ndërlidhjen e më shumë se dy sistemeve autonome të pavarura, kryesisht për të lehtësuar shkëmbimin e trafikut të internetit;
24. siguron ndërlidhje vetëm me sistemet autonome;
25. nuk kërkon që trafiku i internetit që kalon midis dy sistemeve autonome pjesëmarrëse, të kalojë përmes një sistemi të tretë autonom dhe nuk cenon ose ndërhyn në një trafik të tillë.
26. **“Produkt TIK**", nënkupton një element ose një grup elementësh të një rrjeti ose sistemi informacioni.
27. **“Proces TIK",** nënkupton një grup aktivitetesh të kryera për të hartuar, zhvilluar, ofruar ose mirëmbajtur një produkt ose shërbim TIK.
28. “**Regjistri i emrave të domein-eve me nivel të lartë”,** është regjistri me emrat e domain-eve të internetit brenda një domaini specifik të nivelit të lartë (TLD), i cili administrohet nga Autoriteti përgjegjës për komunikimet elektronike dhe postare.
29. “**Rrjet dhe sistem i informacionit”** është:
30. Një sistem transmetimi, i bazuar në një infrastrukturë, me aftësi administrimi të centralizuar dhe pajisje kalimi ose rutimi dhe burime të tjera, përfshirë këtu elementët e rrjetit që nuk janë aktivë, të cilët lejojnë bartjen e sinjaleve me tela me: radio; mjete me fibra optike ose mjete të tjera elektromagnetike; rrjetet satelitore; rrjetet e lëvizshme ose fikse (me qark dhe kuti, duke përfshirë internetin); rrjetet mobile; sistemet kabllore elektrike kur përdoren për qëllimin e transmetimit të sinjaleve; rrjetet e përdorura për transmetimet radio dhe televizive; rrjetet e televizionit kabllor, pavarësisht nga lloji i informacionit të transmetuar,
31. çdo pajisje ose grup i pajisjeve të lidhura ose ndërlidhura, një ose disa prej tyre, kryejnë përpunimin automatik të të dhënave digjitale, nëpërmjet një programi;
32. çdo e dhënë elektronike e ruajtur, e përpunuar, e nxjerrë ose e transmetuar me anë të rrjeteve ose pajisjeve të përmendura në germat(a) dhe (b), për qëllim të përdorimit funksionimit, mbrojtjes dhe mirëmbajtjes së tyre.
33. **“Rrezik i sigurisë kibernetike**”, është një rrethanë ose një ngjarje, e identifikueshme me efekt të mundshëm negativ për sigurinë e rrjeteve dhe sistemeve të informacionit.
34. **“Qëndrueshmëria kibernetike”,** i referohet aftësisë së sistemeve të informacionit, për të mbrojtur të dhënat nga sulmet kibernetike, si dhe aftësisë për të rifilluar funksionimin në mënyrë sa më të shpejtë në rast të një sulmi kibernetik.
35. **“Siguria e rrjetit dhe sistemeve të informacionit”,** është aftësia e rrjetit dhe e sistemeve të informacionit për t'i rezistuar, në një nivel të caktuar çdo veprimi që kompromenton disponueshmërinë, vërtetësinë, integritetin dhe konfidencialitetin e të dhënave të ruajtura, të transmetuara ose të përpunuara dhe shërbimeve përkatëse të ofruara përmes këtij rrjeti ose sistemeve të informacionit.
36. “**Siguria kibernetike”,** është tërësia e masave organizative, teknike, ligjore dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.
37. **“Strategjia Kombëtare për Sigurinë Kibernetike”,** është një dokument politikash që përcakton objektiva, plane dhe prioritete strategjike për sigurinë e rrjeteve dhe sistemeve të informacionit dhe krijimin e hapësirave kibernetike të sigurta për shoqërinë, në nivel kombëtar.
38. **“Skema e certifikimit të sigurisë kibernetike**”, është tërësia e rregullave, kërkesave teknike, standardeve dhe procedurave të miratuara nga Autoriteti, që zbatohen për certifikimin ose vlerësimin e konformitetit të produkteve, shërbimeve dhe proceseve TIK.
39. **“Standard**”, është një specifikim teknik, i miratuar nga një organ standardizimi me të cilin pajtueshmëria nuk është e detyrueshme dhe që është një nga sa vijon;
40. **standard ndërkombëtar,** i cili nënkupton një standard të miratuar nga një organ ndërkombëtar standardizimi;
41. **standard evropian,** i cili nënkupton një standard të miratuar nga një organizatë evropiane standardizimi;
42. **standard i harmonizuar**, i cili nënkupton një standard evropian të miratuar në bazë të një kërkese të bërë nga Komisioni Evropian, për zbatimin e legjislacionit të harmonizuar me atë të Bashkimit Evropian;

**ç) standard kombëtar**, i cili nënkupton një standard të miratuar nga një organ kombëtar standardizimi.

1. **“Specifikim teknik”,** nënkupton një dokument i cili përcakton karakteristikat e kërkuara të një produkti si nivelet e cilësisë, performancës dhe sigurisë, duke përfshirë kërkesat e zbatueshme për produktin në lidhje me emrin me të cilin produkti shitet, terminologjinë, simbolet, metodat e testimit, paketimi, shënjimi ose etiketimi dhe procedurat e vlerësimit të konformitetit. Ky term mbulon gjithashtu metodat dhe proceset e prodhimit.
2. **“Sistemi i emrave të domain-eve (DNS)**”, është një sistem që në mënyrë hierarkike shpërndan emërtime në një rrjet që përcjell kërkesat për emrat e domain-eve.
3. **“Subjektet e tjera përgjegjëse në fushën e sigurisë kibernetike”,** janë institucionet eprore ose rregullatore përgjegjëse për fushën e veprimtarisë së sektorëve, sipas të cilëve kategorizohen infrastrukturat kritike dhe të rëndësishme të informacionit.
4. **“Shërbimi digjital”**, nënkupton çdo shërbim të shoqërisë së informacionit, që ofrohet me ose pa pagesë, në distancë, me mjete elektronike dhe me kërkesë individuale të një marrësi të shërbimeve. Për qëllime të këtij përkufizimi:
5. "në distancë" do të thotë që shërbimi ofrohet pa qenë palët të pranishme në të njëjtën kohë;
6. “me mjete elektronike” do të thotë që shërbimi është dërguar fillimisht dhe është marrë në destinacionin e tij me anë të pajisjeve elektronike për përpunimin dhe ruajtjen e të dhënave, dhe që tërësisht transmetohet, përcillet dhe merret nëpërmjet rrejtit, radios, me anë të mjeteve optike ose me mjete të tjera elektromagnetike;
7. “me kërkesë individuale të një marrësi të shërbimeve" do të thotë që shërbimi ofrohet nëpërmjet transmetimit të të dhënave me kërkesë individuale.
8. **“Shërbim TIK",** nënkupton një shërbim që konsiston plotësisht ose kryesisht në transmetimin, ruajtjen, marrjen ose përpunimin e informacionit me anë të rrjetit dhe sistemeve të informacionit.
9. **“Shërbim“*cloud computing***”, është një shërbim digjital që lejon hyrjen në një grup të përshkallëzuar dhe elastik të burimeve të ndara kompjuterike, shërbimeve dhe aplikimeve.
10. “**Treg *on-line*”,** është një ose disa platforma elektronike të cilat u mundësojnë konsumatorëve lidhjen e kontratave elektronike për ofrimin dhe përfitimin e mallrave dhe shërbimeve online.
11. “**Trajtimi i incidentit të sigurisë kibernetike”,** janë të gjitha procedurat e nevojshme për identifikimin, analizimin, frenimin dhe ndërhyrjen në rast të një incidenti të sigurisë kibernetike.

**KREU II**

**ORGANIZIMI INSTITUCIONAL DHE SUBJEKTET PËRGJEGJËSE PËR SIGURINË KIBERNETIKE**

 **Neni 5**

**Strategjia Kombëtare për Sigurinë Kibernetike**

1. Autoriteti është institucioni përgjegjës për koordinimin e punës me institucionet e tjera përgjegjëse për sigurinë kibernetike, për hartimin dhe monitorimin e Strategjisë Kombëtare për Sigurinë Kibernetike.

2. Strategjia Kombëtare e Sigurisë Kibernetike, rishikohet brenda një periudhe 5 vjeçare dhe miratohet me vendim të Këshillit të Ministrave.

3. Strategjia shoqërohet nga plani i veprimit i cili hartohet nga institucionet përgjegjëse të sigurisë të koordinuara nga autoriteti dhe rishikohet të paktën çdo dy vjet.

**Neni 6**

**Autoriteti Përgjegjës për Sigurinë Kibernetike**

1. Autoriteti Kombëtar për Sigurinë Kibernetike është organ rregullator dhe institucion përgjegjës për mbikëqyrjen dhe zbatimin e legjislacionit për sigurinë kibernetike në Republikën e Shqipërisë.
2. Autoriteti është institucion juridik publik, me seli në Tiranë, në varësi të Kryeministrit, i cili financohet nga buxheti i shtetit dhe burime të tjera të ligjshme.
3. Autoriteti në marrëdhënie me palët e treta përfaqësohet nga Drejtori i Përgjithshëm.

4. Marrëdhëniet e punës të Drejtorit të Përgjithshëm, nëpunësve dhe punonjësve administrativë të Autoritetit rregullohen në bazë të dispozitave të ligjit nr.7961, datë 12.7.1995 “Kodi i Punës së Republikës së Shqipërisë”, i ndryshuar.

5. Drejtori i Përgjithshëm dhe nëpunësit e njësive teknike të përmbajtjes së Autoritetit, përveç pagës sipas kategorive të pagës së përcaktuar me vendim të Këshillit të Ministrave, përfitojnë një shtesë për natyrë të veçantë pune, në masën deri në 800 000 (tetëqind mijë) lekë në muaj. Masa e shtesës për natyrë të veçantë pune për secilën kategori përcaktohet me vendim të Këshillit të Ministrave.

6. Organizimi dhe funksionimi i Autoritetit miratohet me vendim të Këshillit të Ministrave.

**Neni 7**

**Emërimi, lirimi ose shkarkimi i Drejtorit të Përgjithshëm**

1. Drejtori i Përgjithshëm i Autoritetit emërohet, lirohet ose shkarkohet nga Kryeministri.

2. Drejtori i Përgjithshëm i Autoritetit duhet të plotësojë kriteret e mëposhtme:

1. Të jetë shtetas shqiptar;
2. Të ketë zotësi të plotë për të vepruar;
3. Të ketë diplomë të nivelit të shtatë të Kornizës Shqiptare të Kualifikimeve, “Master shkencor” apo “Master profesional të përfituar në fund të studimeve të ciklit të dytë me 120 kredite dhe me kohëzgjatje normale 2 vite akademike” ose të baras vlefshme me to, sipas legjislacionit për arsimin e lartë, në fushën e teknologjive të informacionit dhe komunikimit (ICT) apo inxhinieri elektronike;

ç ) Të ketë përvojë pune të paktën 10 vjet në profesion;

1. Të shquhet për aftësi profesionale në fushën e sigurisë;

dh) Ndaj tij të mos jetë marrë masa disiplinore e largimit nga puna, që nuk është shuar sipas legjislacionit në fuqi;

1. Të mos jetë dënuar me vendim gjyqësor të formës së prerë për kryerjen e një vepre penale;

ë) Të mos ketë konflikt interesi në ushtrimin e detyrës.

3. Drejtori i Përgjithshëm i Autoritetit lirohet nga detyra kur:

a) plotësohen kushtet për pensionin e plotë të pleqërisë;

b) deklarohet i paaftë për punë nga komisioni kompetent mjekësor;

c) gjendet në një situatë konflikti të vazhdueshëm të interesit;

ç) jep dorëheqjen nga detyra.

4. Drejtori i Përgjithshëm i Autoritetit shkarkohet nga detyra kur:

a) dënohet me vendim gjyqësor të formës së prerë për kryerjen e një krimi apo për kryerjen e një kundërvajtjeje penale me dashje;

b) nuk përmbushen objektivat strategjikë për shkak të performancës së ulët të tij;

c) kryen shkelje të rënda në detyrë.

**Neni 8**

**Kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike**

1.Autoriteti Kombëtar për Sigurinë Kibernetike në fuksion të përmbushjes së qëllimit të këtij ligji ushtron kompetencat e mëposhtme:

* 1. identifikon dhe klasifikon infrastrukturat kritike dhe të rëndësishme të informacionit;
	2. vepron si pikë qendrore kontakti në nivel kombëtar dhe ndërkombëtar, si dhe koordinon dhe bashkërendon punën me institucionet e tjera në fushën e sigurisë kibernetike për zgjidhjen e incidenteve kibernetike;
	3. vepron në cilësinë e CSIRT-it Kombëtar dhe CERT-it;

ç) përcakton dhe kontrollon implementimin e masave të sigurisë kibernetike, që duhet të aplikohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;

* 1. bashkëpunon dhe shkëmben informacione të rëndësishme me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në lidhje me të dhënat në sisteme, kur ato janë të rrezikuara për shkak të një incidenti kibernetik;

dh)ngre dhe administron qendrën operacionale kombëtare të monitorimit të sigurisë kibernetike.

* 1. asiston operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në zgjidhjen e incidenteve kibernetike;

ë) kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet instalimit të agjenteve, me qëllim evidentimin dhe parandalimin e veprimeve keqdashëse;

* 1. vlerëson dhe analizon nivelin e sigurisë së sistemeve për infrastrukturat kritike dhe të rëndësishme të informacionit, nëpërmjet kontrolleve dhe testimeve simuluese;
	2. regjistron organizmat e vlerësimit të konformitetit për masat e sigurisë kibernetike;

gj) krijon dhe administron regjistrin e dokumentimit të incidenteve të sigurisë kibernetike;

* 1. raporton në mënyrë periodike në lidhje me incidentet kibernetike pranë ENISA dhe organizmave të tjera ndërkombëtare në kuadër të angazhimeve të Shqipërisë, për çështjet e sigurisë kibernetike;
	2. kryen aktivitete ndërgjegjësimi dhe edukimit në fushën e sigurisë kibernetike, për të gjitha grupet e shoqërisë;
	3. vepron si qendër kombëtare ndëruniversitare, për të krijuar dhe ngritur kapacitetet e burimeve njerëzore në fushën e sigurisë kibernetike;
	4. ndërmerr masa të nevojshme, bashkëpunon dhe bashkërendon punën me institucionet përgjegjëse për sigurinë dhe mbrojtjen e fëmijëve dhe të rinjve, për krijimin e një mjedisi *on-line* të sigurt kibernetik në Shqipëri.

**Neni 9**

**Subjektet e tjera përgjegjëse për sigurinë kibernetike**

1. Subjekte të tjera përgjegjëse për sigurinë e rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërisë janë si më poshtë vijon:
	1. Subjektet përgjegjëse të sigurisë dhe mbrojtjes:
2. Ministria përgjegjëse për sektorin e energjisë dhe transportit;
3. Ministria përgjegjëse për rendin dhe sigurinë publike;
4. Ministria përgjegjëse për sektorin e ekonomisë dhe financës;

ç) Ministria përgjegjëse për sektorin e kujdesit shëndetësor;

1. Ministria përgjegjëse për mjedisin dhe mbrojtjen e territorit dhe funksione të tjera të lidhura me të;

 dh) Ministria përgjegjëse për mbrojtjen;

1. Ministria përgjegjëse për bujqësinë dhe funksione të tjera të lidhura me të;

ë) Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI);

1. Institucionet e tjera përgjegjëse për ruajtjen dhe përpunimin e të dhënave qeveritare;

g) Çdo institucion tjetër publik i pavarur që administron infrastruktura të informacionit në kuptim të këtij ligji.

1.2. Subjektet përgjegjëse për ofrimin e shërbimeve të sektorëve sa më poshtë vijon:

1. Subjektet që ofrojnë shërbime në sektorët e energjisë, përfshirë sektorët e energjisë elektrike, gazit naftës dhe energjisë bërthamore;
2. Subjektet që ofrojnë shërbime në sektorët e transportit ajror, detar, hekurudhor, rrugor dhe postar;
3. Subjektet që ofrojnë shërbime në sektorët e ekonomisë, financës, infrastrukturës së tregut financiar, sektorin bankar, fintek, shoqëritë e sigurimeve si dhe sistemet mikrofinanciare;

 ç) Policia e shtetit si subjekt me mision ruajtjen e rendit e të sigurisë
 publike;

d) Subjektet që ofrojnë shërbime në sektorët e kujdesit e ndihmës shëndetësore të të autorizuar dhe të akredituar nga autoritetet përgjegjëse;

 dh) Subjektet që ofrojnë shërbime në sektorët e mjedisit dhe mbrojtjes së
 territorit dhe autoritetet territoriale përgjegjëse për furnizimin dhe
 shpërndarjen e ujit të pijshëm;

e) Subjektet që ofrojnë shërbime në sektorët e infrastrukturës digjitale, telekomunikacionit, si dhe shërbimet digjitale;

ë) Subjektet që ofrojnë shërbime në sektorët për përpunimin dhe transmetimin
 e informacionit të klasifikuar që lidhen me sigurinë publike;

f) Subjektet që ofrojnë shërbime në sektorin akademik.

**Neni 10**

**Identifikimi i operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit**

1. Autoriteti, bashkërendon në vazhdimësi punën me subjektet e tjera përgjegjëse për sigurinë kibernetike, për identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit.
2. Identifikimi i operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, kryhet mbi bazën e një metodologjie, e cila miratohet me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
3. Me hyrjen në fuqi të këtij ligji, dhe çdo dy vjet pas hyrjes së tij në fuqi, pika e vetme kombëtare e kontaktit i dërgon Komisionit Evropian dhe ENISA-s informacionin e nevojshëm për zbatimin e këtij ligji, në veçanti në lidhje me identifikimin e operatorëve të infrastrukturave kritike dhe të infrastrukturave të rëndësishme të informacionit.
4. Lista e infrastrukturave kritike dhe të rëndësishme të informacionit është konfidenciale si dhe përditësohet, të paktën një herë në dy vjet nën drejtimin e Autoritetit dhe miratohet me vendim të Këshillit të Ministrave.

**Neni 11**

**Detyrat dhe përgjegjësitë e CSIRT-it Kombëtar**

1. Autoriteti vepron në cilësinë e CSIRT-it Kombëtar dhe përmbush detyrat dhe përgjegjësitë e mëposhtme:
2. Krijon mjetet e nevojshme për komunikim aktiv me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, me qëllim që të sigurohet vazhdimësia e veprimtarisë së tyre në çdo kohë dhe pa ndërprerje.
3. Ndërvepron me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, nëpërmjet platformave të dedikuara për shpërndarje të informacionit dhe raportimin e incidenteve kibernetike për menaxhimin dhe trajtimin e tyre.
4. Monitoron, analizon dhe menaxhon kërcënimet kibernetike, vulnerabilitetet dhe incidentet në nivel kombëtar dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit.

ç) Monitoron rrjetet dhe sistemet e informacionit në infrastrukturat e tyre, kritike dhe të rëndësishme të informacionit mbi incidente të sigurisë kibernetike apo sulme të mundshme kibernetike.

1. Trajton incidentet kibernetike dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligj zbatuese në rast se konstaton ekzistencën e një krim kibernetikë.

dh) Paralajmëron, njofton dhe shpërndan informacion pranë infrastrukturave kritike dhe të rëndësishme të informacionit si dhe subjkteve përgjegjëse, në lidhje me rreziqet e mundshme, vulnerabilitetet dhe incidentet kibernetike.

1. Mbledh dhe analizon të dhënat nëpërmjet hetimit digjital dhe ofron analizë dinamike të riskut dhe të incidentit, si dhe kryen ndërgjegjësimin për situatën aktuale të sigurisë kibernetike.

ë) Siguron ruajtjen e logeve për një periudhë të përcakuar sipas procedurës së caktuar në rregulloren e miratuar nga Drejtori i Pergjithshëm.

1. Ofron sipas kërkesës së operatorëve skanime proaktive të rrjeteve dhe sistemeve të informacionit me qëllim identifikimin e vulnerabiliteteve, me impakt të lartë të mundshëm.
2. Vlerëson kur infrastruktura është në një situatë me risk të lartë dhe kryen veprime reaktive, pas ndodhjes së incidentit kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionuari për më shumë se 4 orë.

gj) Kontrollon implementimin e masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

1. Ndërhyn pranë çdo infrastrukture për të mbështetur në mënyrë aktive zgjidhjen e incidenteve.
2. Analizon dhe përgatit masa të natyrës së veçantë sipas incidentit kibernetik dhe i komunikon ato tek CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.
3. Përgatit udhëzues dhe rregullore për të harmonizuar dhe përmirësuar procedurat e menaxhimit të incitendeve kibernetike, të cilat miratohen nga Drejtori i Përgjithshëm.
4. Mban regjistrin elektronik të pikave të kontaktit me të dhënat e përcaktuara në shkronjën “f”, pika 1, të nenit 13 dhe në nenin 15 të këtij ligji.
5. Simulon rrjetet dhe sistemet e operatorëve për të gjetur pikat e dobëta të infrastrukturës dhe shërbimeve të tyre.
6. Analizon incidentin për të gjetur shkakun e tij si edhe koordinon aktivitetin me operatorët, CSIRT-et sektoriale, institucionet ndrkombëtare dhe qeveritare kur e shikon të arsyeshme;
7. Siguron personel të dedikuar për të siguruar disponueshmërinë në çdo kohë.
8. CSIRT-i Kombëtar bën pjesë në rrjetin e CSIRT-eve ndërkombëtarë dhe ofron asistencë të përbashkët të bazuar në kapacitetet dhe kompetencat e tij, për anëtarët pjesë e këtij rrjeti sipas kërkesës.

nj)Raporton pranë Komisionit Evropian dhe ENISA, një herë në vit llojet e
 incidenteve të ndodhura në Republikën e Shqipërisë.

**Neni 12**

**CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.**

Organizimi dhe funksionimi i CSIRT-eve sektoriale, dhe CSIRT-eve pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit përcaktohet me Vendim të Këshillit të Ministrave.

**Neni 13**

**Detyrat e CSIRT-it sektorial**

Subjektet përgjegjëse për ofrimin e shërbimeve sipas përcaktimeve të bëra në nenin 9 të këtij ligji, duhet të kenë në strukturën e vet CSIRT-in sektorial, përgjegjës për incidentet e sigurisë kibernetike sipas fushës së përgjegjësisë së tyre, i cili:

* + - 1. bashkëpunon me Autoritetin për identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit në Republikën e Shqipërisë.
			2. bashkërendon punën me CSIRT-in kombëtar për rritjen e nivelit të sigurisë kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit që administrojnë operatorët përkatës sipas fushës së tyre të veprimtarisë.
			3. mban përgjegjësi për raportimin e incidenteve kibernetike të ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit që ata dhe operatorët administrojnë sipas fushës së veprimtarisë së tyre.

ç) ruan loge për një periudhë të përcaktuar sipas procedurës së caktuar me rregulloren e miratuar nga Drejtori i Përgjithshëm.

* + - 1. koordinon me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit për mbrojtjen nga incidentet e sigurisë kibernetike të sistemeve dhe rrjeteve që ato administrojnë.

dh)njofton CSIRT-in kombëtar menjëherë pasi identifikon incidentin, si dhe e njofton këtë të fundit në rast të zgjidhjes së shpejtë të incidentit të ndodhur në infrastrukturat që administrojnë.

* + - 1. sipas rastit, siguron ndihmë për operatorët e infrastrukturave të informacionit si dhe ju vë në dispozicion informacionin e nevojshëm që mund të lehtësojë trajtimin efektiv të incidentit.

ë) siguron rritje të kapaciteteve të stafit dhe nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë.

* + - 1. cakton pikën e kontaktit, e raporton pranë CSIRT- it Kombëtar, si dhe lajmëron për çdo ndryshim të ndodhur brenda 7 ditëve kalendarike.

**Neni 14**

**Detyrat e CSIRT-it pranë operatorëve të infrastrukturave kritike të informacionit dhe të rëndësishme të informacionit**

1. Ekipi përgjegjës (CSIRT) për operatorin kryen këto detyra:
	1. Monitoron rrjetet dhe sistemet e informacionit në infrastrukturën e tyre kritike ose të rëndësishme të informacionit mbi incidente të sigurisë kibernetike apo sulme të mundshme kibernetike.
	2. Identifikon dhe kategorizon incidentin, si dhe vlerëson shtrirjen dhe dëmin e shkaktuar prej tij.
	3. Trajton incidentin dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese në rast se konstaton mundësinë e ekzistencës së një krim kibernetik.

ç) Parandalon incidente të ngjashme në te ardhmen duke marrë masa parandaluese.

* 1. Përgatit dhe dërgon pranë CSIRT -it kombëtar raportet e incidenteve sipas formatit dhe afateve të miratuara nga Autoriteti.

dh) Ruan loge për një periudhë të përcakuar sipas procedurës së caktuar në rregulloren e miratuar nga Drejtori i Përgjithshëm.

* 1. Mban dhe ruan kronologjinë e të gjitha provave të incidentit në përputhje me dispozitat e këtij ligji dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale.

ë) Siguron staf të mjaftueshëm dhe të kualifikuar për të mundesuar disponueshmërinë në çdo kohë per menaxhimin e incidenteve kibernetike

* 1. Raporton pranë CSIRT–it kombëtar dhe CSIRT-it sektorial çdo incident të sigurisë kibernetike të ndodhur në infrastrukturat e tyre, i cili përcakton impaktin e incidentit të sigurisë kibernetike.
1. Operatori i infrastrukturës kritike të informacionit ngre në strukturën e vet CSIRT-in, ekipin përgjegjës për incidentet e sigurisë kibernetike, që për shkak të rëndësisë të ketë një ekip me të paktën 3 (tre) persona, ku njëri prej tyre të jetë i trajnuar për qeverisje të sigurisë kibernetike.

**Neni 15**

**Pikat e kontaktit**

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit caktojnë pikat e kontaktit, sipas përcaktimeve në këtë ligj. Në të dhënat për pikat e kontaktit për personat juridikë publikë dhe privatë përfshihen: emri, adresa e selisë, numri i identifikimit (NIPT) të personit juridik ose numri i ngjashëm, i caktuar jashtë vendit, dhe të dhënat e personit të kontaktit që është i autorizuar të veprojë në emër të tij.
2. Pikat e kontaktit, raportohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, pranë CSIRT-it kombëtar dhe CSIRT-it sektorial, brenda 15 ditëve pas hyrjes në fuqi të listës së infrastrukturave kritike dhe të rëndësishme të informacionit, të miratuar me Vendim të Këshillit të Ministrave.
3. Çdo ndryshim në të dhënat e pikave të kontaktit i komunikohen zyrtarisht CSIRT-it kombëtar dhe CSIRT-it sektorial, nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit brenda 7 ditëve kalendarike.

**KREU III**

**ADMINISTRIMI I SIGURISË KIBERNETIKE**

**Neni 16**

**Masat e sigurisë kibernetike**

1. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit janë të detyruar të zbatojnë masat e sigurisë, si dhe të dokumentojnë zbatimin e tyre sipas përcaktimeve të bëra në këtë ligj.
2. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit përdorin produkte të certifikuara gjatë ngritjes së infrastrukturave të tyre të informacionit.
3. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit me qëllim garantimin e vazhdimësisë së shërbimeve, implementojnë masa për të arritur një nivel të lartë të sigurisë kibernetike në infrastrukturat e tyre.
4. Masat e sigurisë kibernetike klasifikohen në masa organizative dhe masa teknike, për menaxhimin e riskut dhe përshtaten nga autoriteti duke marrë në konsideratë zhvillimet e fundit teknologjike.
5. Masat e sigurisë kibernetike kanë për qëllim parandalimin dhe minimizimin e efektit të incidentit në sigurinë e rrjeteve dhe sistemeve të informacionit.
6. Përmbajtja dhe mënyra e dokumentimit të masave organizative dhe teknike të sigurisë kibernetike përcaktohen me rregullore që miratohet me urdhër të Drejtorit të Përgjithshëm të Autoritetit.

**Neni 17**

**Masat për menaxhimin e riskut për operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit**

1. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit implementojnë masa teknike dhe organizative për menaxhimin e riskut, të cilat përfshijnë masa që kanë për qëllim;
2. Përcaktimin e riskut të incidentit;
3. Parandalimin, zbulimin dhe menaxhimin e incidentit;
4. Minimizimin e efektit të incidentit;
5. Gjatë implementimit të masave organizative dhe teknike për menaxhimin e riskut operatorët marrin në konsideratë veçanërisht:
	1. Sigurinë e sistemeve dhe shërbimeve;
	2. Menaxhimin e incidentit;
	3. Menaxhimin e vazhdimësisë së shërbimit;

ç) Monitorimin, auditimin dhe testimin;

d) Përputhshmërinë e standardeve ndërkombëtare.

**Neni 18**

**Masat e sigurisë kibernetike në rast kërcënimi ose incidenti të sigurisë kibernetike**

* 1. Në rast të një incidenti kibernetik apo kërcënimi të mundshëm, aplikohen masat e sigurisë kibernetike të kategorizuara si më poshtë:
	2. Masa paralajmëruese;
	3. Kundërmasat;
	4. Masa mbrojtëse të natyrës së përgjithshme.
	5. Masat paralajmeruese, janë masa me karakter rekomandues të hartuara nga Autoriteti në rastet e një kërcënimi të ndodhur, të cila vendosen në dispozicion të operatorëve për t’u implementuar menjëherë.
	6. Kundërmasat ndërmerren nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, për incidentin e ndodhur në infrastrukturat e tyre. Personi përgjegjës në cilësinë e pikës së kontaktit informon menjëherë Autoritetin për zbatimin e kundërmasave dhe rezultatin e tyre. Kundermasat hartohen rast pas rasti në varësi të natyrës së incidentit të ndodhur.
	7. Masat mbrojtëse të natyrës së përgjithshme, hartohen nga Autoriteti dhe zbatohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

**Neni 19**

**Rreziqet e sigurisë kibernetike dhe raportimi i incidenteve të sigurisë kibernetike**

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, marrin masa për të parandaluar dhe minimizuar ndikimin e rreziqeve dhe incidenteve të sigurisë kibernetike në infrastrukturat e tyre të informacionit.
2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit bashkëpunojnë me CSIRT-in kombëtar dhe CSIRT-in sektorial në të gjitha fazat e një incidenti kibernetik të ndodhur në infrastrukturat e tyre të informacionit.
3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, raportojnë të gjitha llojet e incidenteve të sigurisë kibernetike pranë CSIRT-it kombëtar dhe CSIRT-it sektorial, brenda 4 orëve, nga koha e ndodhjes së incidentit.
4. Për të përcaktuar rëndësinë e ndikimit të një incidenti kibernetik, vlerësohen parametrat e mëposhtëm:
5. numri i përdoruesve të prekur nga ndërprerja e shërbimit;
6. kohëzgjatja e incidentit;
7. shtrirja gjeografike në lidhje me zonën e prekur nga incidenti;

ç) shkalla e ndërprerjes së funksionimit të shërbimit;

d) shtrirja e ndikimit në aktivitetet ekonomike dhe shoqërore.

1. Autoriteti vendos në dispozicion të organizmave ndërkombëtare në fushën e sigurisë kibernetike, të dhënat e administruara në lidhje me incidentet e sigurisë kibernetike, me qëllim trajtimin dhe zgjidhjen e tyre. Komunikimi dhe shkëmbimi i të dhënave sipas përcaktimeve kësaj pike mbështetet në marrëveshje bashkëpunimi ose konfidencialiteti, në përputhje me kuadrin ligjor për mbrojtjen e të dhënave personale.
2. Llojet dhe kategoritë e incidenteve të sigurisë kibernetike, të cilat prekin sistemet dhe rrjetet e informacionit, formatin, elementët e raportimit, afatet e raportimit dhe mënyrën e dokumentimit të incidenteve kibernetike, përcaktohen me rregullore të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoriteti.

**Neni 20**

**Njoftimi vullnetar i incidenteve të sigurisë kibernetike**

1. Përveç operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, raportojnë vullnetarisht edhe subjekte të tjera, për të cilat incidentet kibernetike të ndodhura shkaktojnë ndikim të rëndësishëm në vazhdimësinë e shërbimeve që ato ofrojnë.
2. CSIRT-i kombëtar shqyrton raportimet e bëra dhe në varësi të tyre zbaton procedurën e përmendur në pikën 4 të nenit 19 këtij ligji.
3. Raportimet vullnetare shqyrtohen nga Autoriteti, vetëm pasi është vlerësuar që këto raportime nuk ndikojnë në trajtimin e detyrueshëm të raportimeve të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.
4. Raportimi vullnetar nuk krijon pasoja apo detyrime, për subjektin raportues, nëse ai nuk do të kishte bërë një raportim të tillë.

**Neni 21**

**Informimi i publikut mbi incidentet kibernetike**

* + 1. CSIRT-i kombëtar informon publikun me transparencë për incidentet e ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, kur ky informim është i nevojshëm, duke ruajtur konfidencialitetin e të dhënave të incidentit.
		2. Informimi i publikut mbështetet në një procedurë komunikimi të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.
		3. Nëse një incident kibernetik i raportuar, prek një ose më shumë shtete të tjera, CSIRT–i kombëtar informon shtetet e prekura, në përputhje me dispozitat e këtij ligji dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale.

**Neni 22**

**Kufizimi i të dhënave dhe ruajtja e konfidencialitetit**

1. Nëpunësit e Autoritetit që marrin pjesë në zgjidhjen e incidentit kibernetik, janë të detyruar të ruajnë konfidencialitetin e plotë, për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së tij.
2. Konfidencialiteti i të dhënave ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin, përveç rasteve të parashikuara ndryshe në ligj.
3. Konfidencialiteti i të dhënave të incidentit kibernetik trajtohet sipas legjislacionit në fuqi për mbrojtjen e të dhënave personale.

**Neni 23**

**Kriza kibernetike**

* + 1. Gjendja e krizës kibernetike shpallet me vendim të Këshillit të Ministrave, me propozimin e Kryeministrit. Vendimi për shpalljen e gjendjes së krizës kibernetike njoftohet në media.
		2. Kur është e pamundur të shmanget një kërcënim ndaj sigurisë së informacionit në sistemet e informacionit, sigurisë së shërbimeve ose sigurisë dhe integritetit të rrjeteve të komunikimit elektronik, Autoriteti në koordinim me institucionet e tjera përgjegjëse të sigurisë dhe mbrojtjes, sipas pikës 1.1, të nenit 9, të këtij ligji, i propozon menjëherë Kryeministrit shpalljen e gjendjes së krizës kibernetike dhe masat emergjente për zgjidhjen e situatës.
		3. Gjendja e krizës kibernetike shpallet për një periudhë kohore deri në shtatë ditë. Kjo periudhe mund të zgjatet në mënyrë të përsëritur, në varësi të kompleksitetit të situatës kibernetike, me miratim të Kryeministrit. Periudha maksimale e shpalljes së gjendjes së krizës kibernetike nuk duhet të kalojë 30 ditë.
		4. Gjatë periudhës së gjendjes së krizës kibernetike, Drejtori i Përgjithshëm i Autoritetit, informon Kryeministrin në lidhje me ecurinë dhe zgjidhjen e kësaj gjendjeje, si dhe për kërcënimet reale të mundshme.
		5. Gjatë gjendjes së krizës kibernetike, Autoriteti ka të drejtë të nxjerrë vendime me karakter të përgjithshëm ose të marrë masa mbrojtëse të natyrës së përgjithshme dhe kundërmasa.
		6. Kundërmasat e nxjerra nga Autoriteti para vendosjes së gjendjes së krizës kibernetike mbeten në fuqi për aq kohë sa këto kundërmasa nuk bien në kundërshtim me masat emergjente të deklaruara nga Këshilli i Ministrave.
		7. Autoriteti koordinon veprimet e të gjitha strukturave përgjegjëse për zgjidhjen e gjendjes së krizës kibernetike.
		8. Procedurat për identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike përcaktohen me vendim të Këshillit të Ministrive

**Neni 24**

**Ekipi përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike – CERT**

1. Në rastet e emergjencave dhe krizës së sigurisë kibernetike, Autoriteti në bashkëpunim me subjektet e tjera përgjegjëse sipas përcaktimeve të këtij ligji, ngre një strukturë *ad-hoc*, të quajtur “ekipi i përgjegjës për menaxhimin e emergjencës kibernetike – CERT”.
2. Me qëllim trajtimin në kohë dhe me efiçencë të incidenteve dhe kërcënimeve gjatë krizës kibernetike përfshihen ekspertët më të mirë të fushës.
3. CERT-i, përbëhet nga 10 ekspertë, të cilët thirren nga Autoriteti për hartimin e planit të masave të emergjencës, menaxhimin dhe zgjidhjen emergjencave dhe krizës kibernetike.
4. Ngritja, mënyra e organizimit dhe funksionimit, të CERT-it përcaktohen me vendim të Këshillit të Ministrave.

**KREU IV**

**MBIKQYRJA DHE ZBATIMI I MASAVE TË SIGURISË KIBERNETIKE**

**Neni 25**

**Mbikëqyrja dhe zbatimi i masave te sigurise kibernetike**

* + 1. Autoriteti kontrollon implementimin e masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.
		2. Autoriteti në funksion të ushtrimit të veprimtarisë mbikëqyrese, ushtron këto kompetenca:
	1. mbikëqyr operatorët nëpërmjet inspektimeve dhe kontrolleve periodike, si dhe sa herë e gjykon të arsyeshme;
	2. zhvillon kontrolle me grupe ad-hoc, në rastet e një incidenti kibernetik të ndodhur, ose në rastet e shkeljeve të mundshme të këtij ligji;
	3. zhvillon skanime të rrjeteve dhe sistemeve të operatoreve, për efekt të kontrollit të masave të sigurisë në lidhje me vulnerabilitete të mundshme, duke siguruar transparencë të procesit dhe garantuar konfidencialitetin e informacionit.

ç) kërkon informacionin e nevojshëm për vlerësimin e nivelit të sigurisë së rrjeteve dhe sistemeve të informacionit, për të aksesuar masat e menaxhimit të riskut të ndërmarra nga operatorët.

d) akseson të dhëna, dokumente dhe informacionin e nevojshëm për të kryer funksionin e tij mbikëqyrës ndaj operatorëve;

dh) verifikon evidencat e dokumentuara mbi zbatimin efektiv të politikave të sigurisë kibernetike.

**Neni 26**

**Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit**

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre të informacionit pranë Autoritetit.
2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikëqyrës, i ofrojnë CSIRT-it kombëtar akses të drejtpërdrejtë në ambientet e infrastrukturave dhe sistemet e tyre të informacionit, të cilat janë të lidhura me shërbimet e ofruara prej tyre.
3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, janë të detyruar të zbatojnë rekomandimet dhe masat korrigjuese të lëna nga Autoriteti, si dhe të raportojnë mbi implementimin e tyre.
4. Për impelementimin efektiv të masave të sigurisë kibernetike, operatorët paraqesin pranë Autoritetit raportin e testimit, vleresimit dhe konformitetit, nga një Organizëm i Vlerësimit të Konformitetit, të paktën një herë në 2 vjet.
5. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, janë të detyruar të bashkëpunojnë me Autoritetin në kuadër të realizimit të funksioneve mbikëqyrëse të përcaktuara në këtë ligj.

**KREU V**

**BASHKËPUNIMI**

**Neni 27**

**Bashkëpunimi në nivel kombëtar**

* + 1. Autoriteti koordinon veprimtarinë e tij me institucionet e sigurisë dhe të mbrojtjes si dhe bashkëpunon me subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë ligj.
		2. CSIRT-et pranë operatorëve, CSIRT-et sektoriale kanë detyrimin për të bashkëpunuar në çdo kohë me CSIRT-i Kombëtar dhe Autoritetin, në përmbushje të detyrimeve dhe përgjegjësive që rrjedhin nga ky ligj.
		3. Në përputhje me pikën 1 të këtij neni Autoriteti:
1. bashkëpunon ngushtë me Policinë e Shtetit në rastet kur nga informacioni i siguruar për efekt të këtij ligji, dyshon për elementë të krimit kibernetik.
2. bashkëpunon me institucionin përgjegjës për sigurinë e informacionit të klasifikuar, në rastet kur merr dijeni, mbi kërcënime të mundshme në rrjetet e klasifikuara, të infrastrukturave të informacionit, objekt i këtij ligji.

**Neni 28**

**Bashkëpunimi ndërkombëtar**

1. Autoriteti bashkëpunon me autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.
2. Në kuadër të përmbushjes së angazhimeve, në terma të sigurisë kibernetike si vend anëtar i Aleancës Euro-Atlantike (NATO) dhe Organizata për Sigurimin dhe Bashkëpunimin në Evropë (OSBE), Autoriteti koordinon dhe bashkërendon punën midis këtyre organizmave dhe institucioneve kombëtare.
3. Autoriteti merr pjesë në aktivitetet e grupit të bashkëpunimit të përbërë nga përfaqësues të Shteteve Anëtare të Bashkimit Evropian, Komisionit Evropian dhe Agjencisë së Bashkimit Evropian për Rrjetin dhe Sigurinë e Informacionit (ENISA).
4. Autoriteti merr pjesë në forumet ndërkombëtare për çështje të sigurisë kibernetike dhe bashkëpunon me to, për rritjen e sigurisë kibernetike në vend.

**KREU VI**

**CERTIFIKIMI I SIGURISË KIBERNETIKE**

**Neni 29**

**Përgatitja, rishikimi dhe miratimi i një skeme kombëtare të certifikimit të sigurisë kibernetike**

1. Autoriteti përgatit skemën kombëtare të certifikimit të sigurisë kibernetike në përputhje me skemat e miratuara të Bashkimit Evropian për Certifikimin e Sigurisë Kibernetike.
2. Për përgatitjen e skemës kombëtare të certifikimit të sigurisë kibernetike, Autoriteti konsultohet me grupet e interesit, nëpërmjet një procesi konsultimi formal, të hapur, transparent dhe gjithëpërfshirës.

Të paktën çdo pesë vjet, Autoriteti vlerëson skemat e miratuara të certifikimit të sigurisë kibernetike, duke marrë në konsideratë sugjerimet e palëve të interesuara.

Autoriteti mban faqen e internetit të dedikuar, për të publikuar skemat kombëtare të certifikimit të sigurisë kibernetike, certifikatat e sigurisë kibernetike, si dhe informacion në lidhje me skemat që nuk janë më të vlefshme apo të revokuara.

Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit përdorin produkte, shërbime dhe procese të veçanta TIK, të zhvilluara nga vetë operatorët ose të ofruara nga palë të treta, të certifikuara sipas Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike ose një skemë Evropiane të Certifikimit të Sigurisë Kibernetike.

Me qëllim rritjen e nivelit të sigurisë kibernetike në infrastrukturat e informacionit, Autoriteti inkurajon operatorët për përdorimin e identifikimin elektronik dhe shërbimeve të besuara të kualifikuara, sipas kuadrit ligjor në fuqi për to.

1. Një vit pas hyrjes në fuqi të skemës së certifikimit të sigurisë kibernetike, Autoriteti publikon listën e organizmave të vlerësimit të konformitetit të akredituar, sipas skemës së certifikimit të sigurisë kibernetike.

**Neni 30**

**Miratimi i skemave, niveleve dhe organizmave përgjegjëse për certifikimin e sigurisë kibernetike**

Përcaktohen me vendim të Këshillit të Ministrave:

* + - 1. Skema Kombëtare e certifikimit të sigurisë kibernetike, e cila eshte në përputhje me Skemat Certifikimit të miratuara nga Bashkimi Evropian;
			2. Nivelet e sigurisë së skemës kombëtare të certifikimit të sigurisë kibernetike për produktet, shërbimet dhe proceset e TIK.
			3. Organet përgjegjëse për akreditimin, certifikimin dhe vlerësimin e konformitetit të sigurisë kibernetike sipas skemës së Certifikimit të Sigurisë Kibernetike.

**KREU VII**

**MASAT ADMINISTRATIVE**

**Neni 31**

**Masat korrigjuese**

1. Kur Autoriteti konstaton mangësi në implementimin e masave të sigurisë, në zbatim të këtij ligji, përcakton një afat të arsyeshëm, brenda të cilit operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit, marrin masat korrigjuese përkatëse.

2. Kostot lidhur me zbatimin e masave korrigjuese mbulohen nga operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit.

3. Operatorët janë të detyruar të njoftojnë autoritetin, për marrjen e masave korrigjuese brenda afatit të përcaktuar dhe të paraqesin provat që vërtetojnë këtë fakt.

**Neni 32**

**Kundërvajtjet administrative**

1. Në kuptim të këtij ligji përbëjnë kundërvajtje administrative shkeljet e mëposhtme:
2. mosraportimi pranë CSIRT–it kombëtar dhe CSIRT-it sektorial, të incidentit të sigurisë kibernetike të ndodhur në infrastruktura, sipas përcaktimit në shkronjën “f”, të nenit 14, dhe pikës 3, të nenit 19 të këtij ligji;
3. mosraportimi pranë Autoritetit të pikës së kontaktit apo i përditësimeve të tyre, sipas përcaktimeve në pikat 2 dhe 3, të nenit 15, të këtij ligji;
4. mospërmbushja e detyrimeve të caktuara nga Autoriteti, në zbatim të pikës 1 të nenit 22 të këtij ligji;

ç) mospërmbushja e detyrimeve nga ana e operatorëve sipas përcaktimeve në nenin 26 të këtij ligji;

1. mospërmbushja e detyrimeve nga ana e operatorëve në zbatim të pikës 3, të nenit 31, të këtij ligji.

**Neni 33**

**Sanksionet administrative**

1. Kur Autoriteti konstaton shkeljen e dispozitave, të cilat përbëjnë kundërvajtje administrative, sipas nenit 32, të këtij ligji, vendos dënimin me gjobë si më poshtë:
	1. nga 1 000 000 deri në 10 000 000 lekë, në rast të shkeljeve administrative të përcaktuara në shkronjat “a” dhe “ç” të pikës 1 të nenit 32 të këtij ligji;
	2. nga 200 000 deri në 400 000 lekë, në rast të shkeljeve administrative të përcaktuara në shkronjën “b”dhe “c” të pikës 1 të nenit 32 të këtij ligji;
	3. nga 400 000 lekë deri në 1 000 000 lekë, në rast të shkeljeve administrative të përcaktuar në shkronjën “d” të pikës 1 të nenit 32 të këtij ligji.
2. Të ardhurat e siguruara nga kundërvajtjet administrative derdhen 100 për qind në buxhetin e shtetit.

**Neni 34**

**Pezullimi i ushtrimit të aktivitetit**

Kur Autoritetit konstaton shkelje të përsëritura në përmbushje të detyrimeve të përcaktuara në këtë ligj, nga operatori i infrastrukturave të informacionit, ndaj të cilit rezulton se janë marrë më shumë se 3 (tre) masa administrative të njëpasnjëshme, për mospërmbushjen e detyrimeve që rrjedhin nga ky ligj, Autoriteti vendos pezullimin e ushtrimit të aktivitetit të tij, deri në një afat të papërcaktuar.

**Neni 35**

**Ankimi administrativ**

Procedurat e konstatimit, shqyrtimit, ankimit dhe ekzekutimit të kundërvajtjeve administrative janë ato të parashikuara në ligjin për kundërvajtjet administrative.

**KREU VIII**

**DISPOZITA TË FUNDIT**

**Neni 36**

**Njoftimi i Komisionit Evropian për skemat e certifikimit të sigurisë kibernetike**

Me anëtarësimin në Bashkimin Evropian të Republikës së Shqipërisë, Autoriteti do të njoftojë Komisionin Evropian për çdo skemë të certifikimit të sigurisë kibernetike, për organet e vlerësimit të konformitetit që janë akredituar, si dhe për çdo ndryshim të mëvonshëm.

**Neni 37**

**Aktet nënligjore**

1. Ngarkohet Këshilli i Ministrave, që brenda 6 muajve nga hyrja në fuqi e këtij ligji të nxjerrë aktet nënligjore në zbatim të pikës 4 të nenit 10, nenit 12, pikës 8 të nenit 23, pikës 4 të neni 24 dhe nenit 30, të këtij ligji.
2. Ngarkohet Drejtori i Përgjithshëm i Autoritetit që brenda 6 muajve nga hyrja në fuqi e këtij ligji të nxjerrë aktet nënligjore përkatëse në zbatim të shkronjave “ë” dhe “j” të nenit 11, pikës 6, të nenit 16 dhe pikës 6 të nenit 19, të këtij ligji.
3. Aktet nënligjore të miratuara në zbatim te ligjit nr.2/2017, “Për sigurinë kibernetike”, do të zbatohen edhe pas shfuqizimit të tij, me përjashtim të rasteve kur bien në kundërshtim me dispozitat e këtij ligji, deri në miratimin e akteve nënligjore në zbatim te këtij ligji.

**Neni 38**

**Shfuqizime**

Ligji nr.2/2017, “Për sigurinë kibernetike”, shfuqizohet.

**Neni 39**

**Dispozitat kalimtare**

1. Subjektet përgjegjëse në fushën e sigurisë kibernetike janë të detyruar të harmonizojnë veprimtarinë e tyre me parashikimet e këtij ligji brenda 24 muajve nga data e hyrjes në fuqi e këtij ligji.
2. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike vazhdon të ushtrojë veprimtarinë e tij, pa ndërprerje, si institucioni përgjegjës në fushën e sigurisë kibernetike në përputhje me dispozitat e këtij ligji.

**Neni 40**

**Hyrja në fuqi**

Ky ligj hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

**KRYETARI**

 **LINDITA NIKOLLA**

1. Ky ligj është përafruar plotësisht me Direktivën (BE) 2016/1148 e Parlamentit Evropian dhe Këshillit e datës 6 korrik 2016 “Në lidhje me masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkimin Evropian”, CELEX 32016L1148, Fletorja Zyrtare e Bashkimit Evropian, Seria L, nr.194, datë 19.7.2016, faqe. 1-30 dhe pjesërisht i përafruar me Direktivën (BE) nr.2022/2555 të Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022 “Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, duke ndryshuar Rregulloren (BE) nr.910/2014 dhe Direktivën (BE) nr. 2018/1972, dhe duke shfuqizuar Direktivën (BE) nr. 2016/1148 (NIS 2)”, Fletorja Zyrtare e Bashkimit Evropian, Seria L, nr.333, datë 27.12.2022, faqe 80-152. [↑](#footnote-ref-1)