**RELACION**

**PËR**

**PROJEKTLIGJIN “PËR SIGURINË KIBERNETIKE”**

1. **QËLLIMI I PROJEKTAKTIT DHE OBJEKTIVAT QË SYNOHEN TË ARRIHEN**

Qëllimi i këtij projektligji është përcaktimi i kornizës së nevojshme ligjore për sigurinë kibernetike, me qëllim arritjen e një niveli të lartë të sigurisë kibernetike në nivel kombëtar, duke përcaktuar në mënyrë të qartë procedurat dhe masat e sigurisë.

Ky projektligj ka si objekt përcaktimin e të drejtave dhe detyrimeve të 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 vend.

Gjithashtu, projektligji përcakton në mënyrë të qartë Autoritetin përgjegjës për Sigurinë Kibernetike në Republikën e Shqipërisë, caktimin e pikës së vetme të kontaktit, CSIRT-in Kombëtar, CERT-in, si dhe CSIRT-et sektoriale.

1. **VLERËSIMI I PROJEKTAKTIT NË RAPORT ME PROGRAMIN POLITIK TË KËSHILLIT TË MINISTRAVE, ME PROGRAMIN ANALITIK TË AKTEVE DHE DOKUMENTE TË TJERA POLITIKE**

Projektligji i propozuar për miratim është në përputhje të plotë me rendin juridik të brendshëm dhe me legjislacionin ndërkombëtar. Ky projektligj është përfshirë në Planin Kombëtar për Integrimin Evropian 2023-2025 (PKIE), miratuar me vendimin nr.122, datë 1.3.2023, të Këshillit të Ministrave.

1. **ARGUMENTIMI I PROJEKTAKTIT LIDHUR ME PËRPARËSITË, PROBLEMATIKAT, EFEKTET E PRITSHME**

Rrjetet dhe sistemet e informacionit luajnë një rol të rëndësishëm në shoqërinë shqiptare. Siguria dhe besueshmëria e tyre është po aq e rëndësishme sa edhe vetë ekzistenca e këtyre rrjeteve dhe sistemeve. Shkalla, shpeshtësia dhe ndikimi i incidenteve të sigurisë janë në rritje dhe përfaqësojnë një shqetësim dhe kërcënim serioz për funksionimin e rrjeteve dhe sistemeve të informacionit, gjithashtu edhe të vetë funksionimit të shtetit.Sisteme të tilla mund të bëhen gjithashtu një objektiv për veprime që synojnë të dëmtojnë ose prishin funksionimin e sistemeve.

Kapacitetet e deritanishme nuk janë të mjaftueshme për të garantuar një nivel të lartë sigurie në rrjetet dhe sistemet e informacionit. Përgatitja e përgjigjeve ndaj sulmeve apo incidenteve kibernetike nuk mjafton në nivelin që ato paraqiten, dhe kjo çon në domosdoshmërinë e ngritjes së kapaciteteve të reja teknike dhe ligjore.

Për një përgjigje sa më efektive ndaj sfidave të sigurisë së rrjeteve dhe sistemeve të informacionit është e nevojshme një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, që do të përfshinte krijimin e kapaciteteve minimale por njëkohësisht të larta dhe të mjaftueshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.

Në krahasim me kuadrin ligjor aktual projektligji sjell risi lidhur me:

- Parashikime të qarta ligjore lidhur me subjektet përgjegjëse të sigurisë kibernetike dhe detyrat përkatëse të tyre (Autoritetin Kombëtar Përgjegjës për Sigurinë Kibernetike, CSIRT-in kombëtar, CSIRT sektoriale, CSIRT pranë operatorëve të infrastrukturave të informacionit).

- Ngritjen e një strukture që bën monitorimin e sigurisë në nivel kombëtar – SOC Kombëtar .

- Parashikimi i ngritjes së një strukture për trajtimin e situatave emergjente dhe gjendjes së krizës kibernetike – CERT.

- Garantimi i sigurisë kibernetike përmes rregullimit të certifikimit të sigurisë kibernetike në përputhje me skemat e certifikimit të Bashkimit Evropian si dhe procedurat e lidhura me to.

- Parashikime të qarta ligjore lidhur me administrimin e sigurisë kibernetike: forcimin e masave të sigurisë kibernetike, rritja e mbikëqyrjes në kuadër të zbatimit të tyre, masat për menaxhimin e riskut, raportimet e incidenteve, raportimet vullnetare.

- Rritja e bashkëpunimit kombëtar dhe ndërkombëtar për forcimin e sigurisë kibernetike në vend dhe përmbushjen e detyrimeve ndërkombëtare në këtë fushë.

- Transpozimin e plotë të Direktivës NIS1 si dhe përfshirja e disa elementeve të Direktivës NIS2, duke përmbushur objektivin e përafrimit të legjislacionit vendas me atë të BE-së në kuadër të Planit Kombëtar të Integrimit Evropian të Republikës së Shqipërisë (2023-2025).

Lidhur me sfidat e këtij projektligji shihet si i tillë angazhimi i qeverisë në forcimin dhe garantimin e një niveli të lartë të sigurisë kibernetike në vend duke fuqizuar mjetet teknologjike dhe juridike.

Sfidë tjetër e këtij projektligji mbetet anëtarësimi i Republikës së Shqipërisë në Bashkimin Evropian. Kjo lidhet me faktin se disa nene të Direktivës (BE) 2016/1148 të 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”, aplikohen vetëm për vendet anëtare të Bashkimit Evropian.

1. **VLERËSIMI I LIGJSHMËRISË, KUSHTETUTSHMËRISË DHE HARMONIZIMI ME LEGJISLACIONIN NË FUQI VENDAS E NDËRKOMBËTAR**

Projektligji është në harmoni me legjislacionin vendas në fuqi. Gjithashtu, ky projektligj nuk bie në kundërshtim me Kushtetutën dhe me marrëveshjet ndërkombëtare të ratifikuara nga Republika e Shqipërisë.

1. **VLERËSIMI I SHKALLËS SË PËRAFRIMIT ME ACQUIS COMMUNAUTAIRE (PËR PROJEKTAKTET NORMATIVE)**

Projektligji është hartuar duke përafruar plotësisht Direktivën (BE) 2016/1148 të 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”, Fletorja Zyrtare e Bashkimit Evropian, Seria L, nr.194, datë 19.07.2016, faqe. 1-30.

Gjithashtu, me hyrjen në fuqi të Direktivës (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, u pa e nevojshme përfshirja e disa elementëve të kësaj Direktive, me qëllim përditësimin dhe plotësimin e legjislacionit në fushën e sigurisë kibernetike duke ndjekur qasjen e Bashkimit Evropian.

Shkalla e përafrimit: *e plotë* me Direktivën NIS 1 dhe *e pjesshme* me Direktivën NIS 2.

1. **PËRMBLEDHJE SHPJEGUESE E PËRMBAJTJES SË PROJEKTAKTIT**

Projektligji ka në përmbajtje tetë krerë dhe dyzetë nene përkatësisht si më poshtë:

* Në **kreun I** përcaktohen dispozitat e përgjithshme.

Nenet 1dhe 2 të projektligjit përcaktojnë qëllimin dhe objektin e ligjit.

Neni 3 përmban një dispozitë lidhur me parimet e përgjithshme të sigurisë kibernetike, përkatësisht parimin për përpunimin e të dhënave personale dhe parimin e neutralitetit të teknologjisë.

Në nenin 4 jepen përkufizimet e projektligjit.

* Në **kreun II** parashikohet organizimi institucional dhe subjektet përgjegjëse për sigurinë kibernetike.

Neni 5, përcakton Strategjinë Kombëtare për Sigurinë Kibernetike.

Neni 6, parashikon Autoritetin Përgjegjës për Sigurinë Kibernetike.

Neni 7, përcakton kriteret e emërimit të Drejtorit të Përgjithshëm dhe rastet e lirimit dhe shkarkimit të tij. Emërimi, lirimi dhe shkarkimi i Drejtorit të Përgjithshëm bëhet nga Kryeministri.

Neni 8, përcakton kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike.

Neni 9, përcakton subjektet e tjera përgjegjëse për sigurinë kibernetike (sipas sektorëve përkatës).

Neni 10, përcakton identifikimin e operatorëve të infrastrukturave kritike të informacionit dhe operatorëve të infrastrukturave të rëndësishme të informacionit, autoritetet përkatëse për identifikimin e tyre si dhe afatet e përditësimit të listave të këtyre operatorëve.

Neni 11, përcakton detyrat dhe përgjegjësitë e CSIRT-it Kombëtar.

Neni 12, përcakton CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.

Neni 13, përcakton detyrat e CSIRT-it sektorial, ndërsa neni 14 përcakton detyrat e CSIRT-it pranë operatorëve të infrastrukturave kritike të informacionit dhe operatorëve të infrastrukturave të rëndësishme të informacionit, duke përcaktuar gjithashtu ngritjen në strukturën e vet nga operatori i infrastrukturës kritike të informacionit CSIRT-in, ekipin përgjegjës për incidentet e sigurisë kibernetike, që për shkak të rëndësisë duhet 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, parashikon caktimin e pikave të kontaktit pranë të gjithë operatorëve të infrastrukturave kritike të informacionit dhe operatorëve të infrastrukturave të rëndësishme të informacionit, si dhe raportimin e tyre pranë CSIRT-it kombëtar sipas përcaktimeve të bëra në projektligj.

* Në **kreun III** trajtohet administrimi i sigurisë kibernetike.

Nenet 16 dhe 17 trajtojnë përcaktimin e masave të sigurisë kibernetike, nivelet e tyre, institucionin përgjegjës për miratimin dhe auditimin e zbatimit të këtyre masave, si dhe masat e ndërmarra nga operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit për menaxhimin e riskut.

Neni 18 parashikon masat e sigurisë kibernetike që merren në rast kërcënimi apo incidenti të sigurisë kibernetike, përkatësisht masa paralajmëruese, kundërmasa dhe masa mbrojtëse të natyrës së përgjithshme.

Neni 19 përcakton detyrimin e raportimit në rast të incidentit kibernetik nga ana e infrastrukturave të informacionit, afatin kohor për raportim, parametrat që duhet të merren parasysh për përcaktimin e rëndësisë së incidentit, si dhe rastin kur të dhënat e administruara në lidhje me incidentet kibernetike vendosen në dispozicion të organizmave ndërkombëtare në fushën e sigurisë kibernetike.

Neni 20, trajton rekomandime në lidhje me subjekte të tjerë të cilët nuk janë objekt i këtij ligji, por që zotërojnë rrjete dhe sisteme të cilat mund të jenë objekt sulmesh apo incidentesh kibernetike, ku në këtë rast mund t’i raportojnë këto incidente tek Autoriteti.

Neni 21 përcakton rastet e informimit të publikut mbi incidentet kibernetike.

Neni 22 përcakton mënyrën e trajtimit të të dhënave të përpunuara gjatë procedurës së zgjidhjes së incidentit kibernetik.

Neni 23 përcakton gjendjen e krizës kibernetike, mënyrën dhe afatet e shpalljes së saj, si dhe detyrat e autoriteteve përgjegjëse për menaxhimin e saj.

Neni 24 përcakton ekipin e përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike – CERT-in, grup ad hoc të ngritur nga Autoriteti në bashkëpunim me institucionet përkatëse për rastet e emergjencave dhe krizës së sigurisë kibernetike.

* **Kreu IV** trajton mbikëqyrjen dhe zbatimin e masave të sigurisë nga operatorët e infrastrukturave të informacionit.

Neni 25 parashikon autoritetin mbikëqyrës për kontrollimin e implementimit të masave të sigurisë kibernetike të aplikuara nga operatorët e infrastrukturave të informacionit, si dhe kompetencat në funksion të ushtrimit të veprimtarisë së tij mbikëqyrëse.

Neni 26 parashikon detyrimet e operatorëve të infrastrukturave kritike të informacionit dhe operatorëve të infrastrukturave të rëndësishme të informacionit lidhur me raportimet për infrastrukturat e tyre, aktivitetin mbikëqyrës të CSIRT-it Kombëtar, zbatimit të rekomandimeve dhe masave korrigjuese të lëna nga Autoriteti, paraqitjen e raportit të testimit dhe konformitetit si dhe bashkëpunimit me Autoritetin.

* **Kreu V** trajton bashkëpunimin.

Në nenet 27 dhe 28 të këtij kreu, parashikohet bashkëpunimi në nivel kombëtar dhe në nivel ndërkombëtar, përkatësisht koordinimi i veprimtarisë së Autoritetit me institucionet e sigurisë dhe të mbrojtjes, bashkëpunimi me subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë projektligj, bashkëpunimi me autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.

* **Kreu V**I trajton certifikimin e sigurisë kibernetike.

Në nenet 29 dhe 30 të këtij kreu, parashikohet përgatitja, rishikimi, miratimi i një skeme kombëtare të certifikimit të sigurisë kibernetike, si dhe miratimi me vendim të Këshillit të Ministrave të skemave, niveleve dhe organizmave përgjegjës për certifikimin e sigurisë kibernetike.

* **Kreu VII** përcakton masat administrative.

Në nenet 31, 32 dhe 33 të këtij kreu, parashikohen masat korrigjuese të cilat jepen nga Autoriteti kur konstaton mangësi në zbatimin e masave të sigurisë, kundërvajtjet administrative, si dhe sanksionet administrative kur kemi shkelje të dispozitave që përbëjnë kundërvajtje administrative.

Neni 34 parashikon pezullimin e ushtrimit të aktivitetit të operatorëve të infrastrukturave të informacionit në rastet kur konstaton se ndaj operatorit janë marrë më shumë se 3 (tre) masa administrative të njëpasnjëshme për mos përmbushje të detyrimeve të përcaktuara në këtë projektligj.

Neni 35 përcakton procedurën e konstatimit, shqyrtimit, ankimit dhe ekzekutimit të kundërvajtjeve administrative.

* **Kreu VIII** përcakton dispozitat e fundit.

Neni 36, përcakton njoftimin e Komisionit Evropian për skemat e certifikimit të sigurisë kibernetike

Neni 37, parashikon nxjerrjen e akteve nënligjore dhe afatet e nxjerrjes së tyre.

Neni 38, përcakton dispozitën e shfuqizimit.

Neni 39, përcakton dispozitat kalimtare.

Neni 40, parashikon hyrjen në fuqi të projektligjit.

1. **INSTITUCIONET DHE ORGANET QË NGARKOHEN PËR ZBATIMIN E KËTIJ PROJEKTAKTI**

Për zbatimin e këtij ligji ngarkohen Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, operatorët e infrastrukturave kritike dhe operatorët e infrastrukturave të rëndësishme të informacionit.

1. **PERSONAT DHE INSTITUCIONET QË KANË KONTRIBUAR NË HARTIMIN E PROJEKTAKTIT**

Projektligji është hartuar nga Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK).

1. **RAPORTI I VLERËSIMIT TË TË ARDHURAVE DHE SHPENZIMEVE BUXHETORE**

Miratimi i këtij projektligji sjell efekte financiare për buxhetin e shtetit duke qenë se ky ligj parashikon ngritjen e Qendrës Kombëtare të Sigurisë Kibernetike, ngritjen dhe implementimin e standardeve, si dhe trajnime të vazhdueshme të stafit të Autoritetit me qëllim rritjen e kapaciteteve.

Gjithashtu, ky projektligj sjell efekte financiare për OIKI dhe OIRI lidhur me investimet që duhet të bëjnë forcimin e masave të sigurisë për mbrojtjen e sistemeve dhe rrjeteve të tyre të informacionit. Gjithësesi një parashikim i tillë nuk mund të shprehet në vlerë monetare pasi duhet të bëhet nga vetë infrastrukturat.