RAPORT INDIVIDUAL I KONSULTIMIT PUBLIK

për projektligjin:

“Për disa shtesa dhe ndryshime në ligjin nr. 25/2024 “Për sigurinë kibernetike””.

1. Titulli i projektaktit

Për disa shtesa dhe ndryshime në ligjin nr. 25/2024 “Për sigurinë kibernetike”.

Qëllimi i projektligjit “Për disa shtesa dhe ndryshime në ligjin nr.25/2024 “Për sigurinë kibernetike” është përmirësimi dhe plotësimi i kuadrit ligjor ekzistues në fushën e sigurisë kibernetike, me qëllim rritjen e nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, forcimin e kapaciteteve institucionale për reagimin ndaj incidenteve të sigurisë kibernetike, si dhe përafrimin e mëtejshëm të legjislacionit kombëtar me standardet dhe praktikat e Bashkimit Evropian.

Në funksion të këtij qëllimi, projektligji synon forcimin e rolit, kompetencave dhe përgjegjësive të Autoritetit Kombëtar për Sigurinë Kibernetike në drejtim të koordinimit, mbikëqyrjes dhe reagimit ndaj incidenteve kibernetike, si dhe përmirësimin e organizimit dhe funksionimit të CSIRT-eve sektoriale, duke synuar njëkohësisht forcimin e bashkëpunimit dhe koordinimit ndërinstitucional në nivel kombëtar. Gjithashtu, parashikohet krijimi dhe zbatimi i mekanizmave të rinj të monitorimit dhe vlerësimit të përputhshmërisë, përmes detyrimit të vetëdeklarimit të masave të sigurisë kibernetike dhe raportimit të rregullt nga operatorët e infrastrukturave të informacionit, si dhe rregullimi i procedurave për deklarimin e hostimit dhe administrimin e sistemeve, rrjeteve dhe infrastrukturave të informacionit.

Projektligji synon gjithashtu krijimin e Grupit Ndërinstitucional të Inteligjencës Kibernetike me qëllim shkëmbimin e informacionit dhe forcimin e bashkëpunimit strategjik ndërinstitucional si dhe përmirësimi i mekanizmave të kontrollit dhe rritja e efektivitetit të masave administrative dhe sanksioneve në rast të mosrespektimit të detyrimeve ligjore.

2. **Kohëzgjatja e konsultimeve**

Specifikoni kohëzgjatjen e përgjithshme të konsultimeve publike sa i përket ditëve të punës, përfshirë datën e hapjes dhe mbylljes së konsultimeve publike; nëse kohëzgjatja ishte më e shkurtër se 20 ditë pune e paraparë me ligj, jepni arsye për shkurtimin e kohëzgjatjes.

Kohëzgjatja e konsultimit publik për këtë akt ishte 20 ditë pune nga data e shpalljes së njoftimit në Regjistrin Elektronik për Njoftimet dhe Konsultimet Publike, bazuar në ligjin 146/2014 "Për njoftimin dhe konsultimin publik.
Projektligji për disa shtesa dhe ndryshime në ligjin nr. 25/2024 "Për sigurinë kibernetike" si dhe relacioni shoqërues u publikuan në linkun, ëëë.konsultimipublik.gov.al .

Publikimi u bë në datë 23.6.2026 dhe nëpërmjet një njoftimi të publikuar online në RENJK, të gjitha palët e interesuara ishin të ftuar për të paraqitur komentet dhe rekomandimet e tyre për projektaktin, në adresën e koordinatorit për njoftimin dhe konsultimin publik: ilir.dhimitri@aksk.gov.al, endeida.vasi@aksk.gov.al.

Data e mbylljes së procesit të konsultimit ishte 21.7.2026.

Projektligji regjistroi 870 shikime në RENJKP, por nuk pati komente.

3. **Metoda e konsultimit**

Listoni të gjitha metodat e konsultimit të përdorura, të tilla si konsultimet elektronike (Regjistri Elektronik, posta elektronike, faqet e internetit, etj.), Takimet publike, seancat e organeve këshilluese…, dhe siguroni informacione për afatin kohor, kohëzgjatjen dhe afatet e tyre. Shpjegoni se si u shpërnda informacioni mbi konsultimet e hapura, si u ftuan palët e interesuara të kontribuojnë. Përfshini gjithashtu aktivitete nga konsultimet paraprake nëse janë organizuar të tilla).

Projektligji, në zbatim të ligjit 146/2014, i është nënshtruar procesit të konsultimit publik, nëpërmjet publikimit të tij në portalin "Regjistri elektronik për Njoftimet dhe Konsultimet Publike", nga data 23.6.2026 deri në datën 21.7.2026.

Gjithashtu, më datë 27.7.2026, Autoriteti organizoi në ambientet e tij takime konsultative me grupet e interesit të prekura nga ky projektligj. Pjesëmarrësit në këto takime u njoftuan paraprakisht nga Autoriteti përmes shkresave zyrtare dhe postës elektronike. Gjatë këtyre takimeve u prezantuan risitë kryesore të projektligjit dhe u ftuan përfaqësuesit e grupeve të interesit të shprehnin komentet dhe sugjerimet e tyre.

Në këto takime kishte përfaqësues nga institucionet shtetërore, operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe sektorit bankar. Numri total i pjesëmarrësve në këto takime ishte 75 persona.

4. **Palët e interesit të përfshira**

Listoni të gjithë palët e interesuara, qoftë organizata apo individë, të cilët kanë dhënë komente/kontribut në konsultimet publike përmes metodave të ndryshme të konsultimit, gjatë gjithë procesit të hartimit.
Përmendni gjithashtu numrin dhe strukturën e palëve të interesuara që morën pjesë në takime publike ose seanca të organeve këshilluese.
Specifikoni palët e interesuara që morën pjesë në grupin e punës për hartimin e aktit.

Projektligji është hartuar nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK).

Komente dhe sugjerime për projektligjin, janë paraqitur nga subjektet e mëposhtme:

- Abissnet sh.a, me shkresen nr. 3017 prot., datë 27.7.2026, protokolluar me tonën me nr.1514 prot., datë 29.7.2026;
- Vodafone Albania sh.a, me shkresën nr. 1495 prot., datë 21.7.2026;
- Dhoma Amerikane e Tregtisë, me shkresën nr. 76 prot., datë 24.7.2026, protokolluar me tonën nr. 1526 prot., datë 31.7.2026;
- Shoqata Shqiptare e Bankave, me email të datës 20.7.2026;
- Shoqata e Investitorëve të Huaj në Shqipëri, me email të datës 23.7.2026;
- One Albania, me email të datës 21.7.2026.

5. **Pasqyra e komenteve të pranuara me arsyetimin e komenteve të pranuara/ refuzuara**

Gruponi komentet/ propozimet e pranuara sipas çështjes që ato ngritën;
Gruponi komente të ngjashme së bashku dhe renditni palët e interesuara që i ngritën ato;
Shpjegoni cili ishte vendimi i marrë dhe sqaroni shkurtimisht arsyet për të.

Gjatë procesit të konsultimit u administruan 63 komente/sugjerime, nga të cilat 45 komente u refuzuan, 5 komente u pranuan plotësisht, ndërsa 13 komente u pranuan pjesërisht.

27 komente – u refuzuan, pasi çështjet e ngritura gjejnë rregullim në kuadrin ligjor dhe nënligjor në fuqi, në metodologjitë dhe procedurat përkatëse, ose parashikohet të trajtohen në aktet nënligjore të projektligjit, për rrjedhojë, nuk është vlerësuar e nevojshme përfshirja e tyre në tekstin e projektligjit.
10 komente – u refuzuan, pasi propozimet e paraqitura prekin ndarjen e kompetencave dhe përgjegjësive ndërmjet institucioneve ose modelin institucional të përcaktuar nga kuadri ligjor në fuqi dhe nga projektligji.

4 komente – u refuzuan, pasi propozimet e paraqitura kërkojnë ndërhyrje në çështje që tejkalojnë objektin dhe fushën e rregullimit të projektligjit, përfshirë ndryshime në legjislacionin sektorial.
4 komente – u refuzuan, pasi propozimet e paraqitura nuk rezultojnë të imponuara nga acquis-i përkatës i Bashkimit Evropian dhe qasja e parashikuar në projektligj vlerësohet e pajtueshme me kuadrin evropian, përfshirë mundësinë e miratimit të masave kombëtare shtesë për garantimin e një niveli më të lartë të sigurisë kibernetike.

Komentet dhe sugjerimet pasqyrohen në tabelën më poshtë:

Çështja e adresuar	**Komenti**	**Palët e interesuara**	**Vendimi**	**Justifikimi**
Riformulimi CSIRT sektorial	**Pika 5** të riformulohet: "CSIRT sektorial është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike për sektorin përkatës, i ngritur pranë autoritetit rregullator ose institucionit kompetent sektorial. Për sektorin bankar, CSIRT-i sektorial ngrihet pranë institucionit përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe vepron mbi	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Formulimi i propozuar në projektligj synon të përcaktojë kuadrin institucional për ngritjen dhe funksionimin e CSIRT-eve sektoriale, në përputhje me arkitekturën kombëtare të sigurisë kibernetike dhe ndarjen e përgjegjësive ndërmjet AKSK-së dhe institucioneve kompetente sektoriale. Në përputhje me nenin 15, pika 5, të ligjit nr. 25/2024 "Për sigurinë kibernetike", mënyra e ngritjes së CSIRT-eve sektoriale do të përcaktohet me vendim të Këshillit të Ministrave. Për rrjedhojë, elementet e detajuara lidhur me organizimin, kanalet e komunikimit, procedurat e bashkëpunimit dhe mekanizmat e raportimit

	bazën e një protokolli të miratuar ndërinstitucional. Protokolli përcakton kompetencat, kanalet e komunikimit, afatet, konfidencialitetin dhe shkëmbimin e informacionit, si dhe krijon një pikë të vetme hyrëse ose mekanizëm të integruar raportimi, me qëllim shmangien e paraqitjes së përsëritur të të njëjtit informacion nga operatori.” **ARSYETIM** - Formulimi aktual lejon disa modele organizative njëkohësisht dhe mund të krijojë paqartësi mbi përgjegjësinë, kanalin e raportimit dhe autoritetin udhëheqës. Për bankat, një			do të rregullohen në aktin nënligjor përkatës. Për sektorin bankar, përfshirja e institucionit përgjegjës për licencimin dhe mbikëqyrjen e bankave në ngritjen e CSIRT-it sektorial synon të garantojë koordinim efektiv, duke marrë në konsideratë specifikat e këtij sektori dhe kompetencat e posaçme mbikëqyrëse. Gjithashtu, Direktiva (BE) 2022/2555 (NIS2) nuk përcakton një model unik organizativ për CSIRT-et sektoriale, por u lë shteteve fleksibilitetin për të përcaktuar strukturën më të përshtatshme kombëtare. Për këto arsye, formulimi aktual konsiderohet i përshtatshëm, pasi përcakton përgjegjësitë institucionale, ndërsa detajet procedurale do të adresohen në aktin nënligjor sipas nenit 15, pika 5, të ligjit nr. 25/2024.

	mekanizëm i integruar raportimi ul paraqitjen e përsëritur të të njëjtit informacion dhe ruan kompetencat e mbikëqyrësit financiar, pa cenuar rolin koordinues kombëtar. Për subjektet financiare merret në konsideratë edhe kuadri sektorial për reziliencën operacionale digjitale, përfshirë parimin lex specialis të parashikuar nga neni 4 i NIS2, me qëllim shmangien e mbivendosjes së kërkesave ekuivalente për menaxhimin e riskut TIK, raportimin dhe mbikëqyrjen. **Referenca NIS2: nenet 4, 8, 10, 12, 13 dhe 23**.			

Vetëdeklarimi nuk duhet të zëvendësoj auditin	**Në pikën 60**, pas fjalës "monitorimi" të shtohet: "i bazuar në risk, proporcional dhe jo-zëvendësues i auditimit ose vlerësimit formal të konformitetit". **ARSYETIM -** NIS2 kërkon masa dhe mbikëqyrje proporcionale me riskun. Vetëdeklarimi duhet të shërbejë si instrument paraprak dhe jo si bazë automatike për konstatim shkeljeje pa verifikim, të drejtë sqarimi dhe vlerësim të kontekstit. **Referenca NIS2: nenet 21, 32 dhe 33.**	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Vetëdeklarimi i masave të sigurisë kibernetike është konceptuar në projektligj si një instrument paraprak identifikimi, vlerësimi dhe monitorimi të nivelit të zbatimit të kërkesave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Qëllimi i këtij mekanizmi nuk është zëvendësimi i proceseve të auditimit, vlerësimit të konformitetit apo kontrolleve të tjera të sigurisë, por krijimi i një pasqyre të unifikuar dhe të përditësuar mbi nivelin e përputhshmërisë dhe ekspozimit ndaj rreziqeve kibernetike në nivel kombëtar. Shtimi i formulimit "i bazuar në risk, proporcional dhe jo-zëvendësues i auditimit ose vlerësimit formal të konformitetit" nuk konsiderohet i nevojshëm, pasi këto parime janë tashmë të përfshira në mënyrën e konceptimit dhe zbatimit të mekanizmave të mbikëqyrjes sipas ligjit nr. 25/2024 "Për sigurinë kibernetike".

				Gjithashtu, vetëdeklarimi nuk përbën në vetvete bazë automatike për konstatimin e një shkeljeje administrative. Konstatimi i shkeljeve dhe marrja e masave administrative bëhet në përputhje me procedurat e parashikuara në ligj, duke respektuar parimet e procesit të rregullt administrativ, proporcionalitetit, vlerësimit të rrethanave konkrete dhe të drejtës së subjektit për t'u shprehur. Në këtë kuptim, mekanizmi i vetëdeklarimit është një mjet për rritjen e transparencës, përmirësimin e analizës së riskut dhe orientimin e masave mbikëqyrëse, në përputhje me qasjen e bazuar në risk të kërkuar nga Direktiva (BE) 2022/2555 (NIS2).
Sigurimi i konfidencialitetit për informacionin e mbledhur gjatë vetҫdeklarimit	**Në pikën 4**, togfjalëshi i ri të plotësohet: "japin informacionin e nevojshëm, të përshtatshëm dhe proporcional me qëllimin e identifikimit, mbi bazën e një	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Detyrimi i operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për të dhënë informacion pranë Autoritetit gjatë procesit të identifikimit synon garantimin e një procesi të unifikuar, objektiv dhe të bazuar në kritere të përcaktuara për identifikimin dhe

	kërkese të arsyetuar me shkrim. Informacioni që përmban sekret bankar, të dhëna personale ose informacion tregtar konfidencial kërkohet dhe përpunohet vetëm kur është i nevojshëm për ushtrimin e kompetencës ligjore, në masën proporcionale me qëllimin dhe me masa të posaçme për konfidencialitetin, sigurinë, kufizimin e aksesit dhe afatin e ruajtjes.” **ARSYETIM** - NIS2 lejon mbledhjen e informacionit për identifikimin dhe mbikëqyrjen e subjekteve, por kompetencat duhet të ushtrohen në mënyrë proporcionale			klasifikimin e subjekteve që kanë ndikim në sigurinë kibernetike kombëtare. Informacioni i kërkuar nga Autoriteti nuk përcaktohet në mënyrë të pakufizuar apo sipas vlerësimit diskrecionar të tij, por bazohet në metodologjinë për identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, të miratuar me vendim të Këshillit të Ministrave, e cila përcakton kriteret, elementet e vlerësimit dhe të dhënat e nevojshme për këtë proces. Për rrjedhojë, kërkimi i informacionit realizohet vetëm për qëllime të identifikimit dhe klasifikimit sipas kompetencave ligjore të Autoritetit dhe në përputhje me parimet e nevojshmërisë dhe proporcionalitetit. Detyrimet për ruajtjen e konfidencialitetit, mbrojtjen e të dhënave personale dhe informacionit me natyrë tregtare ose të mbrojtur garantohen nga kuadri ligjor në fuqi. Për këto arsye, nuk vlerësohet e nevojshme

	dhe me masa mbrojtëse për informacionin konfidencial. Kërkesa e arsyetuar krijon gjurmë auditimi dhe kufizon ekspozimin e panevojshëm të arkitekturës bankare. **Referenca NIS2: nenet 3, 27, 32 dhe 33.**			shtimi i kërkesave të propozuara, pasi kuadri ekzistues ligjor dhe metodologjia e miratuar sigurojnë që procesi i mbledhjes së informacionit të jetë i bazuar në kritere të përcaktuara dhe jo në kërkesa të pakufizuara nga Autoriteti.
Identifikimi i operatorëve te infrastrukturave të informacionit	**Në fund të pikës 5** të shtohet: "Operatori njoftohet për përfshirjen, ndryshimin ose heqjen nga lista dhe i jepet mundësia të paraqesë të dhëna sqaruese përpara vendimmarrjes përfundimtare, përveç rasteve urgjente të arsyetuara." **ARSYETIM -** Kjo rrit sigurinë juridike dhe saktësinë e klasifikimit, pa penguar	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Lista e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit miratohet me vendim të Këshillit të Ministrave, bazuar në kriteret dhe metodologjinë e përcaktuar në kuadrin ligjor dhe nënligjor përkatës. Procesi i identifikimit dhe klasifikimit të operatorëve është një kompetencë publike që lidhet drejtpërdrejt me garantimin e sigurisë kibernetike kombëtare. Parashikimi i një procedure të detyrueshme konsultimi individual përpara çdo përfshirjeje, ndryshimi ose heqjeje nga lista mund të ndikojë në efikasitetin e procesit dhe

	kompetencën shtetërore për identifikimin e subjekteve. **Referenca NIS2: nenet 2, 3 dhe 32.**			në aftësinë e autoriteteve për të reaguar ndaj ndryshimeve të shpejta të riskut kibernetik dhe varësive kritike. Megjithatë, operatorët kanë të drejtën të paraqesin të dhëna, dokumente dhe qëndrime gjatë proceseve të identifikimit dhe mbikëqyrjes, sipas procedurave të përcaktuara në aktet nënligjore dhe legjislacionin përkatës. Për rrjedhojë, formulimi aktual konsiderohet i përshtatshëm, pasi garanton fleksibilitetin e nevojshëm institucional dhe siguron identifikim të përditësuar të subjekteve që kanë ndikim në sigurinë kibernetike kombëtare.
Sygjerim per riformulim e kryerjes së simulimeve në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësish	**Shkronja "ll" të riformulohet:** "Kryen simulime, përfshirë shfrytëzimin e kontrolluar të vulnerabilitetete ve, mbi bazën e një vlerësimi të dokumentuar të riskut dhe, për aq sa është e mundur, në	AAB (SHOQATA SHQIPTARE E BANKAVE)	Pranuar pjesërisht	Kompetenca e Autoritetit për kryerjen e simulimeve në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit është parashikuar edhe në ligjin nr. 25/2024 "Për sigurinë kibernetike", i cili i njeh Autoritetit kompetencën për të kryer vlerësime dhe veprime kontrolli me qëllim identifikimin e dobësive dhe rritjen e nivelit të sigurisë

me të informacionit	koordinim dhe planifikim paraprak me operatorin. Përpara fillimit të simulimit miratohet një plan testimi, i cili përcakton objektin dhe kufijtë e testimit, afatin, sistemet e përfshira dhe të përjashtuara, rregullat e angazhimit, kushtet e pezullimit ose ndalimit, personat përgjegjës, trajtimin e të dhënave, ruajtjen e provave dhe procedurën e rikthimit të shërbimit. Për subjektet e sektorit bankar, simulimi koordinohet edhe me institucionin përgjegjës për licencimin dhe mbikëqyrjen e bankave, kur mund të ndikojë në sistemet kritike,			kibernetike të operatorëve. Ndryshimi i propozuar në projektligj synon vetëm të qartësojë dhe operacionalizojë këtë kompetencë ekzistuese, duke parashikuar kryerjen e simulimeve mbi bazën e vulnerabiliteteve të evidentuara nëpërmjet skanimeve proaktive dhe me njoftim paraprak të operatorëve përkatës. Detajimi i elementeve teknike dhe procedurale të simulimit, përfshirë objektin e testimit, rregullat e angazhimit, masat e sigurisë dhe mënyrën e dokumentimit të procesit, nuk është e nevojshme të përcaktohet në nivel ligjor, pasi këto çështje do të rregullohen në procedurën përkatëse të miratuar nga Autoriteti. Gjithashtu, ushtrimi i kësaj kompetence do të kryhet në përputhje me parimet e proporcionalitetit dhe qasjes së bazuar në risk, duke marrë në konsideratë natyrën dhe rëndësinë e infrastrukturave të vlerësuara, përfshirë specifikat e sektorëve me kritikalitet të lartë, si sektori financiar.

	shërbimet financiare, sistemet e pagesave ose vazhdimësinë e shërbimit. Në raste të jashtëzakonsh me dhe urgjente, shmangia nga koordinimi ose planifikimi paraprak duhet të jetë e arsyetuar, e dokumentuar dhe e kufizuar në masën strikt të nevojshme. Procedura përcakton përgjegjësinë për dëmet ose ndërprerjet e shkaktuara nga tejkalimi i objektit të miratuar të testimit, si dhe mënyrën e dokumentimit, raportimit dhe rikuperimit të tyre.” **ARSYETIM -** NIS2 u jep autoriteteve kompetenca inspektimi dhe testimi, por kërkon që masat			Duke marrë në konsideratë shqetësimet e ngritura nga operatorët lidhur me ndikimin e mundshëm operacional të këtyre veprimeve dhe nevojën për garantimin e vazhdimësisë së shërbimeve, dispozita është riformuluar me qëllim forcimin e elementit të koordinimit paraprak me operatorët. Në këtë kuadër, është shtuar parashikimi që realizimi i simulimeve do të kryhet pas **dakordësimit paraprak me operatorët për fashat orare të zhvillimit të tyre**, duke synuar që procesi të realizohet në mënyrë të kontrolluar dhe me ndikim minimal në funksionimin e rrjeteve dhe sistemeve të informacionit.

	mbikëqyrëse të jenë efektive, proporcionale dhe të marrin parasysh riskun. Vetëm "njoftimi paraprak" nuk mjafton për testime që mund të ndikojnë sisteme kritike bankare. **Referenca NIS2: nenet 21, 32 dhe 33.**			
Mbi marrjen e atributeve të Policisë Gjyqësore	Në shkronjën "nj" të shtohet: "Mbledhja dhe ruajtja e provave kryhet duke respektuar zinxhirin e ruajtjes, integritetin e provës, ndarjen e roleve dhe kufizimin e kopjimit në atë që është e nevojshme për hetimin. Informacioni që përmban sekret bankar, të dhëna personale ose	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Pas konsultimeve të zhvilluara dhe vlerësimit të çështjes, është dakordësuar që parashikimi për ushtrimin e atributeve të Policisë Gjyqësore të hiqet nga projektligji. Ky ndryshim synon të shmangë çdo paqartësi në lidhje me kompetencat institucionale dhe ndarjen e përgjegjësive ndërmjet institucioneve përkatëse.

	informacion tregtar konfidencial përpunohet vetëm në masën e nevojshme dhe proporcionale me qëllimin, me masa të posaçme për konfidencialitetin dhe kufizimin e aksesit. Aksesi në prova regjistrohet dhe auditohet, ndërsa afati i ruajtjes dhe asgjësimi i sigurt i kopjeve përcaktohen në përputhje me qëllimin e procedurës dhe legjislacionin në fuqi.” ARSYETIM - NIS2 kërkon bashkëpunim me autoritetet dhe ruajtje të sigurt të informacionit, por nuk zëvendëson garancitë procedurale dhe konfidencialitetin.Ky formulim ul			

	riskun e ekspozimit të të dhënave të klientëve dhe provave. Referenca NIS2: nenet 10, 14, 23 dhe 35.			
CSIRT-i sektorial për sektorin bankar vepron si pikë sektoriale koordinimi	**Pika 1 e nenit 15** Të shtohet një fjali e dytë: "Për sektorin bankar, CSIRT-i sektorial vepron si pikë sektoriale koordinimi. Raportimi nga operatori kryhet përmes një pike të vetme hyrëse ose një mekanizmi të integruar raportimi, i cili mundëson përcjelljen automatike dhe të sigurt të informacionit ndërmjet CSIRT-it sektorial, CSIRT-it Kombëtar dhe autoriteteve të tjera kompetente, pa	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Raportimi i incidenteve për subjektet e sektorit bankar rregullohet nga kuadri ligjor dhe rregullator sektorial në fuqi. Në përputhje me nenin 30 të rregullores "Për qëndrueshmërinë operacionale digjitale", të miratuar me Vendimin nr. 30, datë 1.7.2026 të Këshillit Mbikëqyrës të Bankës së Shqipërisë, subjektet financiare raportojnë incidentet madhore të lidhura me TIK pranë Bankës së Shqipërisë, sipas kërkesave të përcaktuara në këtë rregullore. Pa cenuar detyrimet e raportimit sipas kuadrit rregullator sektorial, subjektet financiare vijojnë të përmbushin detyrimet për njoftimin dhe raportimin pranë autoritetit përgjegjës për sigurinë kibernetike dhe strukturave përkatëse, sipas përcaktimeve të ligjit nr. 25/2024 "Për sigurinë kibernetike".

	kërkuar nga operatori paraqitjen e përsëritur të të njëjtit informacion dhe pa cenuar afatet ligjore ose kompetencat institucionale.” **ARSYETIM** - Synohet shmangia e paraqitjes së përsëritur të të njëjtit informacion dhe vendosja e një mekanizmi të integruar ndërinstitucional. Për subjektet financiare duhet të merret në konsideratë kuadri sektorial për raportimin dhe menaxhimin e incidenteve TIK, duke zbatuar parimin lex specialis për kërkesat ekuivalente ose më të forta dhe duke ruajtur njëkohësisht koordinimin kombëtar të			Për rrjedhojë, krijimi i një mekanizmi të ri të integruar raportimi në dispozitat për CSIRT-et sektoriale nuk konsiderohet i nevojshëm, pasi mund të krijojë mbivendosje me mekanizmat ekzistues të raportimit dhe me kompetencat e autoriteteve sektoriale. Formulimi aktual garanton koordinimin ndërinstitucional, duke respektuar njëkohësisht kuadrin e posaçëm rregullator për sektorin bankar.

	sigurisë kibernetike. **Referenca NIS2: nenet 4, 8, 10, 12 dhe 23.**			
Mbi ndryshimin e afateve të raportimit të incidentit kibernetik	**Shkronja "dh" e nenit 16** Të riformulohet: "dh) njofton, pa vonesë të pajustifikuar, CSIRT-in Kombëtar dhe pikën e kontaktit të operatorit, pasi disponon informacion të mjaftueshëm që krijon bindje të arsyeshme për ekzistencën e incidentit. Njoftimi fillestar mund të plotësohet në faza, në përputhje me afatet dhe kriteret e përcaktuara në ligj dhe aktet nënligjore. Njoftimi për zgjidhjen e shpejtë kryhet vetëm kur incidenti plotëson	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Formulimi i propozuar nuk ndryshon afatet apo detyrimin ekzistues për raportimin e incidenteve. Ky parashikim është tashmë i përcaktuar në nenin 16, shkronja "dh", të ligjit nr. 25/2024 "Për sigurinë kibernetike", ku operatorët kanë detyrimin të njoftojnë CSIRT-in Kombëtar menjëherë pasi identifikojnë incidentin, si dhe në rast të zgjidhjes së shpejtë të tij. Termi "menjëherë" lidhet me momentin e identifikimit të incidentit dhe nuk nënkupton raportim përpara disponimit të informacionit të nevojshëm. Për rrjedhojë, nuk vlerësohet e nevojshme ndryshimi i formulimit aktual.

	kriteret e raportueshmëri së.” **ARSYETIM** - Termi “menjëherë” është absolut dhe mund të krijojë përgjegjësi edhe kur faktet nuk janë verifikuar. NIS2 përdor mekanizëm me faza dhe afate nga momenti i marrjes dijeni për incidentin e rëndësishëm. **Referenca NIS2: neni 23**.			
Mbi raportimin e incidenteve të sigurisë kibernetike pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial	**Në pikën 3 të nenit 17** Në shkronjën “ë”, fjalët “çdo incident” të zëvendësohen me “çdo incident të rëndësishëm sipas kritereve të përcaktuara në ligj dhe aktet nënligjore”. Për sektorin bankar, raportimi kryhet përmes një pike të vetme hyrëse	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Dispozita e propozuar synon të garantojë raportimin në kohë të incidenteve të sigurisë kibernetike pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial, me qëllim mundësimin e një reagimi të koordinuar, shkëmbimit të informacionit dhe marrjes së masave të nevojshme për parandalimin, menaxhimin dhe rikuperimin nga incidentet. Përcaktimi i kategorive të incidenteve që i nënshtrohen raportimit, si dhe kriteret për vlerësimin

	ose një mekanizmi të integruar sektorial dhe kombëtar, i cili garanton përcjelljen automatike dhe të sigurt të informacionit tek autoritetet kompetente, pa kërkuar paraqitjen e përsëritur të të njëjtit informacion nga operatori. **ARSYETIM -** NIS2 vendos detyrim raportimi për incidentet e rëndësishme, jo për çdo ngjarje apo tentativë. Raportimi i pakufizuar krijon volum joproporcional dhe mund të largojë burimet nga reagimi real. **Referenca NIS2: neni 23, pikat 1-4.**			e rëndësisë së tyre, rregullohen në aktet nënligjore përkatëse dhe procedurat e raportimit të miratuara nga Autoriteti, në përputhje me kuadrin ligjor në fuqi. Për këtë arsye, nuk vlerësohet e nevojshme që dispozita ligjore të kufizojë detyrimin e raportimit vetëm për "incidentet e rëndësishme".
Mbi masat për bllokimin	**Në pikën 3 të nenit 17**	AAB (SHOQATA	Pranuar pjesërisht	Pranohet shtimi i togfjalëshit “kur është teknikisht e zbatueshme”,

, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabil iteteve	Shkronja "g" të riformulohet: "vlerësojnë dhe, kur është teknikisht e zbatueshme dhe proporcionale me riskun, zbatojnë masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e IOC-ve, IOA-ve dhe vulnerabilitete ve të komunikuara nga Autoriteti. Komunikimi duhet të përmbajë burimin, nivelin e besueshmërisë, ashpërsinë, sistemet e prekura, afatin e rekomanduar dhe masat alternative. Operatori mund të zbatojë masa kompensuese kur masa e kërkuar krijon risk më të lartë operacional, cenon disponueshmër	SHQIP TARE E BANK AVE)		pasi garanton që masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve të komunikuara nga Autoriteti të zbatohen duke marrë në konsideratë mundësitë teknike dhe specifikat e infrastrukturave të administruara nga operatorët. Pjesa tjetër e propozimit nuk pranohet, pasi kërkesat e detajuara lidhur me përmbajtjen e komunikimeve të Autoritetit, masat kompensuese, procedurat e dokumentimit dhe afatet specifike të zbatimit janë elemente me natyrë teknike dhe operacionale, të cilat mund të përcaktohen në procedura të brendëshme të Autoritetit dhe nuk është e nevojshme të përfshihen në nivel ligjor. Për rrjedhojë, dispozita do të riformulohet duke përfshirë vetëm elementin "kur është teknikisht e zbatueshme", duke ruajtur detyrimin e operatorëve për marrjen e masave të nevojshme për adresimin e treguesve të kompromet imit,

	inë ose bie ndesh me detyrime të tjera rregullatore, duke e dokumentuar dhe njoftuar Autoritetin. Në rast të një kërcënimi kritik, aktiv dhe të konfirmuar, Autoriteti mund të përcaktojë një afat të detyrueshëm për vlerësimin dhe zbatimin e masës ose të një mase kompensuese me efekt ekuivalent, duke marrë në konsideratë ndikimin e mundshëm në disponueshmërinë dhe vazhdimësinë e shërbimit.” **ARSYETIM -** NIS2 kërkon masa teknike, operacionale dhe organizative të përshtatshme e proporcionale. Një detyrim			treguesve të sulmeve dhe vulnerabiliteteve të identifikuara.

	automatik për çdo IOC/IOA/vulnerabilitet, pa vlerësim të besueshmërisë dhe impaktit, mund të shkaktojë bllokime të gabuara ose ndërprerje shërbimi. **Referenca NIS2: neni 21, pikat 1-3.**			

Kriteret, procedurat dhe kërkesat teknike për regjistrimin e organeve të vlerësimit të konformitetit	**Në nenin 20...** Të shtohet: "Kriteret bazohen në kompetencë, pavarësi, paanshmëri, akreditim dhe shmangie të konfliktit të interesit; ato i nënshtrohen konsultimit publik me grupet e interesit dhe njohin akreditimet/certifikimet ekuivalente evropiane." **ARSYETIM -** Kjo shmang varësinë e tepërt nga një regjistrim administrativ dhe ruan besueshmërinë e vlerësimeve. NIS2 mbështet standarde dhe skema evropiane, ndërsa mbikëqyrja duhet të jetë e parashikueshme dhe proporcionale. **Referenca**	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Dispozita e propozuar në projektligj ka karakter autorizues dhe synon të krijojë bazën ligjore për miratimin e aktit nënligjor që do të përcaktojë procedurat dhe kriteret për autorizimin e organeve të vlerësimit të konformitetit për vlerësimin e masave të sigurise kibenretike.. Kriteret për autorizimin e këtyre organeve do të hartohen duke marrë në konsideratë praktikat më të mira të vendeve të Bashkimit Evropian, standardet dhe kërkesat ndërkombëtare të zbatueshme, si dhe parimet e kompetencës teknike, pavarësisë dhe paanshmërisë së organeve të vlerësimit të konformitetit. Përfshirja e elementeve të detajuara të propozuara në nivel ligjor nuk vlerësohet e nevojshme, pasi këto çështje do të trajtohen në aktin nënligjor përkatës, i cili do të përcaktojë në mënyrë të hollësishme kriteret, procedurat dhe kërkesat teknike për regjistrimin e organeve të vlerësimit të konformitetit. Për rrjedhojë, formulimi aktual konsiderohet i përshtatshëm, pasi siguron bazën e nevojshme ligjore për nxjerrjen e aktit nënligjor dhe lejon

	NIS2: nenet 24, 25 dhe 32.			përshtatjen e tij me zhvillimet dhe praktikat më të mira evropiane në këtë fushë.
Mbi mundësinë e operatorëve të infrastrukturave të informacionit për korrigjimin e vetdeklarimit	Në nenin 20/1 të shtohen pikat 4-6: "4. Vetëdeklarimi kufizohet në informacionin e nevojshëm dhe proporcional me riskun dhe mund të përmbushet, tërësisht ose pjesërisht, përmes raporteve ekzistuese të auditimit, vlerësimeve të mbikëqyrësit sektorial ose certifikimeve të njohura. 5. Përpara konstatimit të pasaktësisë ose paplotësisë, Autoriteti njofton operatorin dhe i jep një afat të arsyeshëm për paraqitjen e sqarimeve ose korrigjimin e informacionit. Kjo procedurë	AAB (SHOQATA SHQIPTARE E BANKAVE)	Pranuar pjesërisht	Është marrë në konsideratë propozimi lidhur me nevojën për t'i dhënë operatorit mundësinë për të plotësuar ose korrigjuar informacionin e paraqitur në kuadër të vetëdeklarimit. Për këtë qëllim, në projektligj është reflektuar parashikimi se, në rast të konstatimit të mosdorëzimit të informacionit ose të paraqitjes së informacionit të paplotë në vetëdeklarimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, Autoriteti i njofton këta të fundit dhe u jep një afat të arsyeshëm për paraqitjen e informacionit, sqarimeve ose korrigjimin e informacionit. Pjesa tjetër e propozimit nuk është reflektuar, pasi vlerësohet se çështjet e ngritura rregullohen nga kuadri ligjor në fuqi ose do të trajtohen në aktet nënligjore përkatëse.

	nuk zbatohet kur ka indicie të arsyeshme për deklarim të rremë me dashje, fshehje të qëllimshme ose rrezik të menjëhershëm për sigurinë e sistemeve dhe shërbimeve. 6. Autoriteti garanton klasifikimin e informacionit, kufizimin e aksesit sipas parimit të nevojës për njohje dhe privilegjit minimal, regjistrimin dhe auditimin e aksesit, ruajtjen vetëm për periudhën e nevojshme, mbrojtjen gjatë transmetimit dhe ruajtjes, si dhe asgjësimin e sigurt pas përfundimit të afatit të ruajtjes.” **ARSYETIM -** NIS2 kërkon mbikëqyrje të bazuar në risk dhe lejon kërkesa për			

	informacion/evidencë. Ajo nuk kërkon një vetëdeklarim të pakufizuar dhe as dublim të auditimeve sektoriale. Për bankat, njohja e evidencave ekzistuese ul barrën pa cenuar sigurinë. **Referenca NIS2: nenet 21, 32 dhe 33.**			
Mbi mundësinë e operatorëve të infrastrukturave të informacionit për korrigjimin e vetdeklarimit	Neni 20/2, pika 1 të riformulohet: "Operatorët deklarojnë informacion të nivelit të lartë, të nevojshëm për vlerësimin e riskut dhe mbikëqyrjen, për sistemet që mbështesin shërbimet kritike ose të rëndësishme. Deklarimi nuk përfshin konfigurime të detajuara, kredenciale, topologji të plota, adresa teknike, dobësi të paadresuara	AAB (SHOQATA SHQIPTARE E BANKAVE)	Pranuar pjesërisht	Është marrë në konsideratë propozimi lidhur me nevojën për t'i dhënë operatorit mundësinë për të plotësuar ose korrigjuar informacionin e paraqitur në kuadër të vetëdeklarimit. Për këtë qëllim, në projektligj është reflektuar parashikimi se, në rast të konstatimit të mosdorëzimit të informacionit ose të paraqitjes së informacionit të paplotë në vetëdeklarimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, Autoriteti i njofton këta të fundit dhe u jep një afat të arsyeshëm për paraqitjen

	apo të dhëna klientësh, përveçse kur kërkohen në mënyrë të arsyetuar për një procedurë konkrete mbikëqyrëse dhe me masa të posaçme konfidencialitet i. Autoriteti dokumenton qëllimin e kërkesës dhe përpunimit, kategoritë e personave që do të kenë akses, mënyrën e transmetimit, afatin e ruajtjes dhe procedurën e asgjësimit të sigurt të informacionit. Kur është e mundur, informacioni paraqitet në formë të agreguar, të anonimizuar ose me nivel të reduktuar detaji.” **ARSYETIM -** Inventari i centralizuar me detaje të hostimit dhe arkitekturës			e informacionit, sqarimeve ose korrigjimin e informacionit. Pjesa tjetër e propozimit nuk është reflektuar, pasi vlerësohet se çështjet e ngritura rregullohen nga kuadri ligjor në fuqi ose do të trajtohen në aktet nënligjore përkatëse.

	mund të krijojë një objektiv me risk të lartë. NIS2 kërkon menaxhim të riskut të zinxhirit të furnizimit dhe mundëson informacion mbikëqyrës, por kërkesa duhet të jetë proporcionale dhe e siguruar. **Referenca NIS2: nenet 21(2)(d), 27, 32 dhe 33.**			
Koordinim ndërmjet autoritetesve kompetente	Në nenin 20/2 të shtohet: "Për subjektet e sektorit bankar, forma dhe përmbajtja koordinohen me institucionin përgjegjës për licencimin dhe mbikëqyrjen e bankave, duke shmangur raportimin e dyfishtë dhe duke njohur raportimet ekuivalente rregullatore." **ARSYETIM** - NIS2 lejon	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Koordinimi me autoritetet sektoriale, përfshirë institucionin përgjegjës për licencimin dhe mbikëqyrjen e bankave, do të garantohet nëpërmjet mekanizmave institucionalë dhe akteve nënligjore përkatëse. Forma dhe përmbajtja e vetëdeklarimit do të përcaktohen nga Autoriteti, duke marrë në konsideratë specifikat sektoriale dhe kërkesat ekzistuese rregullatore. Përfshirja e një parashikimi të posaçëm për sektorin bankar në nivel ligjor nuk konsiderohet e nevojshme, pasi këto

	koordinim ndërmjet autoriteteve kompetente; shmangia e dublimit është veçanërisht e rëndësishme për sektorët financiarë me mbikëqyrje të specializuar. **Referenca NIS2: nenet 4, 8, 13 dhe 32.**			çështje janë të natyrës procedurale dhe teknike.
Grupi i Bashkepunimit per Inteligjencen Kiberneti ke	**Pas nenit 33 shtohet neni 33/1** Të shtohen pikat 4 dhe 5: "4. Shkëmbimi i informacionit respekton parimin e nevojës për njohje, klasifikimin, konfidencialitetin dhe mbrojtjen e burimit**.** Informacioni që përmban sekret bankar, të dhëna personale ose informacion tregtar konfidencial ndahet vetëm kur është i	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Mbrojtja e informacionit konfidencial, kufizimi i aksesit dhe shkëmbimi i informacionit në përputhje me kompetencat ligjore garantohen nga kuadri ligjor në fuqi. Përcaktimi i mekanizmave konkretë për klasifikimin, trajtimin e informacionit dhe mënyrën e bashkëpunimit me strukturat sektoriale, përfshirë sektorin bankar, është çështje procedurale që do të rregullohet në aktet nënligjore për organizimin dhe funksionimin e Grupit të Bashkepunimit per Inteligjencen Kibernetike.

	nevojshëm për ushtrimin e kompetencës ligjore, në masën proporcionale me qëllimin dhe me masa të posaçme për sigurinë, kufizimin e aksesit dhe afatin e ruajtjes. Informacioni i identifikueshëm i një operatori privat ndahet vetëm kur është i domosdoshëm dhe, kur është e mundur, pas konsultimit me operatorin. 5. Grupi vendos mekanizma për marrjen e kontributit sektorial nga CSIRT-i i sektorit bankar dhe për shpërndarjen e paralajmërimeve të anonimizuara e të zbatueshme.” **ARSYETIM** - NIS2 promovon shkëmbimin e			

	informacionit dhe koordinimin, por kërkon mbrojtjen e informacionit konfidencial dhe interesave tregtare. Përfshirja e kanalit sektorial u jep bankave informacion veprues pa ekspozim të panevojshëm. **Referenca NIS2: nenet 10, 14, 27 dhe 29.**			
Akreditimi i organeve të vlerësimit të konformitetit (OVK)	**Neni 12** **Në pikën 5 të nenit 39** Të riformulohet: "të akredituara nga institucioni kombëtar i akreditimit ose nga një organ akreditimi i njohur në kuadër të marrëveshjeve evropiane/ndër kombëtare dhe, kur kërkohet nga	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Ndryshimi i propozuar synon të saktësojë kompetencën e Autoritetit Kombëtar për Sigurinë Kibernetike në lidhje me organet e vlerësimit të konformitetit (OVK) që do të veprojnë sipas skemës kombëtare të certifikimit të sigurisë kibernetike, duke përcaktuar rolin e Autoritetit në autorizimin e këtyre organeve. Akreditimi i OVK-ve nuk është kompetencë e Autoritetit Kombëtar për Sigurinë Kibernetike, por realizohet nga organi

	skema, të autorizuara nga autoriteti përgjegjës”. **ARSYETIM -** Autorizimi administrativ nuk duhet të zëvendësojë akreditimin teknik dhe pavarësinë e organit të vlerësimit. Mbajtja e të dy elementeve rrit njohjen reciproke dhe shmang kufizimin e panevojshëm të tregut. **Referenca NIS2: nenet 24 dhe 25; lidhur me përdorimin e skemave evropiane të certifikimit.**			përgjegjës për akreditimin, sipas kuadrit ligjor në fuqi. Kërkesa që OVK-të të jenë të akredituara është një nga kriteret që buron nga vetë skema e certifikimit dhe standardet përkatëse. Për rrjedhojë, dispozita nuk synon zëvendësimin e akreditimit me autorizimin administrativ, por përcaktimin e kompetencës së Autoritetit për autorizimin e OVK-ve në kuadër të skemës kombëtare të certifikimit të sigurisë kibernetike. Elementet dhe kriteret që duhet të përmbushin këto organe do të përcaktohen nga skema.
Përcaktimi i kategorive të produkteve, shërbimeve ose proceseve TIK kritike	**Në nenin 41** Pika 3 të riformulohet duke zëvendësuar detyrimin në nivel operatori me detyrim të synuar: “Këshilli i	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Përcaktimi i detyrimit në nivel operatori dhe jo vetëm në nivel produkti, shërbimi ose procesi TIK është i nevojshëm për të garantuar një qasje të bazuar në risk, duke marrë në konsideratë rëndësinë, ndikimin dhe kritikalitetin e shërbimeve që ofrohen nga operatori.

për të cilat kërkohet certifikim sipas skemës komëtare të certifikimit të sigurisë kibernetike	Ministrave mund të përcaktojë kategori të produkteve, shërbimeve ose proceseve TIK kritike për të cilat kërkohet certifikim, bazuar në një vlerësim të dokumentuar të riskut dhe ndikimit, disponueshmërinë e skemave dhe produkteve të certifikuara, proporcionalitetin e kostos dhe ekzistencën e masave alternative ekuivalente. Përpara vendimit konsultohen operatorët dhe autoritetet sektoriale. Lejohen masa kompensuese dhe periudha realiste tranzitore kur certifikimi nuk është i disponueshëm ose do të cenonte			Produktet, shërbimet ose proceset TIK nuk mund të vlerësohen të shkëputura nga konteksti operacional ku përdoren, pasi i njëjti element teknologjik mund të paraqesë nivele të ndryshme risku në varësi të funksionit që mbështet dhe ndikimit të mundshëm në ofrimin e shërbimeve kritike ose të rëndësishme. Formulimi i propozuar në projektligj është në përputhje me qasjen e parashikuar në nenin 24 të Direktivës (BE) 2022/2555 (NIS2), e cila u lejon Shteteve Anëtare të kërkojnë që kategori të caktuara të subjekteve thelbësore dhe të rëndësishme të përdorin produkte TIK, shërbime TIK dhe procese TIK të certifikuara sipas skemave evropiane të certifikimit të sigurisë kibernetike. Përcaktimi me vendim të Këshillit të Ministrave i operatorëve që do t'i nënshtrohen këtij detyrimi është i nevojshëm për të siguruar një zbatim të bazuar në risk dhe proporcional, pasi niveli i ekspozimit dhe ndikimit nuk lidhet vetëm me produktin ose shërbimin TIK në mënyrë të izoluar, por edhe me

	vazhdimësinë e shërbimit.” **ARSYETIM -** NIS2 lejon që përdorimi i produkteve/shërbimeve të certifikuara të bëhet i detyrueshëm, por pas vlerësimit të riskut dhe kur është e nevojshme për të siguruar nivel të mjaftueshëm sigurie. Detyrimi i përgjithshëm në nivel operatori do të ishte më i gjerë se nevoja e Direktivës. **Referenca NIS2: nenet 24 dhe 25.**			subjektin që e përdor atë, funksionin që mbështet dhe rëndësinë e shërbimit të ofruar.
Kriteret për autorizimin e organeve të vlerësimit të konformitetit	**Pika 2 e nenit 42** Të shtohet: “Kriteret duhet të jenë objektive, transparente, jodiskriminues e dhe të bazuara në akreditim;	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Kriteret për autorizimin e organeve të vlerësimit të konformitetit përbëjnë pjesë të skemës kombëtare të certifikimit të sigurisë kibernetike dhe përcaktohen në përputhje me kërkesat dhe standardet e kësaj skeme. Gjithashtu, parashikimi që procedurat dhe kriteret

	refuzimi, pezullimi ose heqja e autorizimit arsyetohet dhe i nënshtrohet ankimit. Njihen organet ekuivalente të akredituara sipas skemave evropiane.” **ARSYETIM -** Kjo ruan konkurrencën, pavarësinë teknike dhe sigurinë juridike, ndërsa mbështet njohjen e skemave evropiane. **Referenca NIS2: nenet 24 dhe 25.**			për autorizimin të miratohen me vendim të Këshillit të Ministrave është hequr nga projektligji gjatë procesit të rishikimit. Për rrjedhojë, propozimi i paraqitur nuk gjen më objekt rregullimi në dispozitën përkatëse.
Kundravajtjet administrative	**Në nenin 44** Shkronjat “b”, “g” dhe “gj” të plotësohen si vijon: “Kundërvajtja konstatohet kur mosdhënia e informacionit, mosraportimi ose paraqitja e informacionit të pasaktë apo të paplotë është materiale, e	AAB (SHOQATA SHQIPTARE E BANKAVE)	Pranuar	Sugjerimi është marrë në konsideratë dhe është reflektuar në projektligj, duke parashikuar se, në rastet e mosdhënies së informacionit, mosraportimit ose paraqitjes së informacionit të paplotë, Autoriteti njofton paraprakisht operatorin dhe i jep një afat të arsyeshëm për paraqitjen e informacionit, sqarimeve ose

	pajustifikuar dhe vazhdon pas njoftimit me shkrim të operatorit dhe përfundimit të një afati të arsyeshëm për sqarim ose korrigjim. Kërkesa për njoftim dhe korrigjim paraprak nuk zbatohet në rast të deklarimit të rremë me dashje, fshehjes së qëllimshme ose rrezikut të menjëhershëm për sigurinë.” **ARSYETIM -** NIS2 kërkon masa zbatuese efektive, proporcionale dhe bindëse. Jo çdo pasaktësi administrative duhet të trajtohet njësoj me fshehjen e qëllimshme ose shkeljen materiale. **Referenca NIS2: nenet 32, 33 dhe 34.**			korrigjimin e tyre, përpara marrjes së masave administrative, sipas rasteve të parashikuara në projektligj.

Zbatimi i masave korrigjuese nga ana e operatorët e infrastrukturave të informacionit	**Në nenin 44** Shkronja "h" të riformulohet: "mosvlerësimi ose moszbatimi, pa arsyetim të dokumentuar, i masave të komunikuara nga Autoriteti, kur ato janë të zbatueshme, proporcionale dhe të shoqëruara me informacion të mjaftueshëm teknik; nuk përbën shkelje zbatimi i masave kompensuese me efekt ekuivalent." **ARSYETIM -** Kjo lidh kundërvajtjen me formulimin e propozuar në nenin 17 dhe parandalon penalizimin automatik kur udhëzimi do të rrisë riskun operacional ose nuk është i aplikueshëm. **Referenca NIS2: nenet 21, 32 dhe 33.**	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Masat e komunikuara nga Autoriteti bazohen në vlerësimin e riskut, analizën teknike dhe kompetencat e përcaktuara në ligjin nr. 25/2024 "Për sigurinë kibernetike", me qëllim parandalimin ose minimizimin e ndikimit të kërcënimeve dhe incidenteve kibernetike. Operatorët kanë detyrimin të zbatojnë këto masa, ndërsa vlerësimi i rrethanave konkrete dhe proporcionalitetit të çdo shkeljeje bëhet në kuadër të procedurës administrative dhe në përputhje me metodologjinë për vendosjen e masave administrative. Për rrjedhojë, nuk vlerësohet e nevojshme të parashikohen në nivel ligjor përjashtime apo masa kompensuese, pasi këto çështje trajtohen rast pas rasti gjatë ushtrimit të kompetencave mbikëqyrëse të Autoritetit.

Individualizimi i masës së gjobës	**Pika 1 e nenit 45** Pa cenuar nivelet monetare të gjobave të parashikuara në projektligj, në nenin 45 të shtohet një pikë me këtë përmbajtje: "Gjatë përcaktimit të masës konkrete të gjobës, Autoriteti merr në konsideratë natyrën, rëndësinë dhe kohëzgjatjen e shkeljes, shkallën e fajit, përsëritjen, pasojat reale ose potenciale, numrin e përdoruesve të prekur, masat e marra për parandalimin ose kufizimin e dëmit, bashkëpunimin e operatorit, korrigjimin vullnetar të shkeljes dhe çdo rrethanë tjetër	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Kriteret për individualizimin e masës së gjobës janë tashmë të përcaktuara në metodologjinë për vendosjen e masave administrative, e cila zbatohet nga Autoriteti gjatë shqyrtimit të çdo rasti konkret. Në këtë kuadër, merren në konsideratë natyra, rëndësia dhe pasojat e shkeljes, si edhe rrethanat lehtësuese ose rënduese, duke garantuar respektimin e parimeve të proporcionalitetit dhe individualizimit të masës administrative.

	lehtësuese ose rënduese. Vendimi për përcaktimin e masës së gjobës arsyeton zbatimin e këtyre kritereve.” **ARSYETIM** - Individualizimi i masës administrative siguron që gjoba të jetë efektive, proporcionale dhe bindëse dhe shmang trajtimin e njëjtë të pasaktësive administrative, sjelljeve të pakujdesshme dhe fshehjes së qëllimshme. **Referenca NIS2: nenet 32-34.**			
Aktet nënligjore	**Në Aneksin I** Të shtohen pikat 4-6: “4. Projekt-aktet nënligjore që prekin operatorët privatë i nënshtrohen konsultimit publik jo më	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Projektligji përcakton vetëm autorizimet ligjore për nxjerrjen e akteve nënligjore, ndërsa procedura e hartimit dhe miratimit të tyre rregullohet nga legjislacioni horizontal në fuqi për procesin e hartimit të akteve normative, konsultimin

	pak se 30 ditë dhe shoqërohen me vlerësim të ndikimit rregullator, kostos së përputhshmërisë, riskut operacional dhe përputhshmërisë me NIS2. 5. Për aktet që prekin sektorin bankar merret mendimi i institucionit përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe i grupeve përfaqësuese të sektorit. 6. Detyrimet e reja zbatohen pas përfundimit të një periudhe tranzitore të përshtatshme, të përcaktuar në aktin përkatës sipas kompleksitetit dhe ndikimit të kërkesës. Periudha tranzitore nuk duhet të jetë më e shkurtër se: a) 3 muaj për			publik dhe vlerësimin e ndikimit rregullator. Gjithashtu, konsultimi me institucionet dhe grupet e interesit, si dhe përcaktimi i afateve të zbatimit apo periudhave tranzitore, vlerësohen rast pas rasti gjatë hartimit të secilit akt nënligjor, në varësi të natyrës dhe kompleksitetit të masave që do të miratohen.

	kërkesa kryesisht dokumentare ose procedurale; b) 6 muaj për procese të reja raportimi, vetëdeklarimi ose organizimi; c) 12 muaj kur kërkohen ndryshime të konsiderueshme teknike, kontraktuale, infrastrukturore ose certifikuese. Afate më të shkurtra mund të përcaktohen vetëm për raste urgjente, mbi bazën e një vlerësimi të dokumentuar të riskut dhe me masa për ruajtjen e vazhdimësisë së shërbimit.” **ARSYETIM** - Pjesa më e madhe e barrës konkrete do të përcaktohet me akte nënligjore. Konsultimi, vlerësimi i impaktit dhe periudha tranzitore			

	sigurojnë proporcionalitet, zbatueshmëri dhe shmangie të ndërprerjeve në sektorin bankar. **Referenca NIS2: nenet 7, 21, 24, 25 dhe 32.**			

Aktet nenligjor	Të shtohet një dispozitë kalimtare: "Detyrimet që kërkojnë nxjerrjen e akteve nënligjore, miratimin e formateve ose specifikimeve teknike, zhvillimin e platformave, ndryshime teknike, organizative ose kontraktuale, fillojnë të zbatohen pas hyrjes në fuqi të aktit përkatës dhe përfundimit të periudhës tranzitore të përcaktuar në nenin 18. Pa përfundimin e periudhës tranzitore, moszbatimi i kërkesave që varen nga këto akte, platforma ose specifikime teknike nuk përbën kundërvajtje administrative." **ARSYETIM -** Hyrja formale në fuqi pas 15	AAB (SHOQATA SHQIPTARE E BANKAVE)	Refuzuar	Projektligji parashikon afate të qarta për nxjerrjen e akteve nënligjore, ndërsa detyrimet që varen prej tyre bëhen të zbatueshme vetëm pas hyrjes në fuqi të akteve përkatëse. Për më tepër, vetë dispozita e nenit 41, pika 4, parashikon që vendimi i Këshillit të Ministrave, i cili miraton listën e operatorëve për të cilët zbatohet detyrimi i certifikimit, përcakton edhe periudhën e zbatimit të këtij detyrimi, bazuar në vlerësimin e riskut, ndikimit dhe konsultimet me operatorët. Për rrjedhojë, nuk vlerësohet e nevojshme shtimi i një dispozite të veçantë kalimtare, pasi afatet e zbatimit janë tashmë të garantuara nga vetë projektligji dhe aktet nënligjore të nxjerra në zbatim të tij.

	ditësh nuk duhet të krijojë detyrime të pazbatueshme përpara se të ekzistojnë formatet, kriteret dhe procedurat. Një tranzicion i qartë ruan sigurinë juridike dhe vazhdimësinë e shërbimeve. **Referenca NIS2: nenet 21, 23 dhe 32; parimi i proporcionalitetit.**			
Mbi mbivendosjen e kompetencave te AKSK dhe AKEP	Mbi propozimin për të shtuar në nenin 17, pika 3 "CSIRT-i pranë operatorëve kryen këto detyra", gërma (g) me përmbajtjen "zbatojnë masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të komprometimit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve	ONE	Refuzuar	Komenti nuk pranohet, pasi dispozita e propozuar nuk krijon mbivendosje kompetencash me AKEP-in dhe nuk ndërhyn në kompetencat e tij të parashikuara nga Ligji nr. 54/2024 "Për komunikimet elektronike". Masat e parashikuara në këtë dispozitë i drejtohen sipërmarrësve të komunikimeve elektronike në cilësinë e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, me qëllim mbrojtjen e rrjeteve, sistemeve, platformave, pajisjeve, aplikacioneve

	të komunikuara nga Autoriteti, në rrjetet, sistemet, platformat, pajisjet, aplikacionet dhe shërbimet TIK që administrohen prej tyre, me qëllim mbrojtjen e infrastrukturave të tyre nga kërcënimet ose incidentet e sigurisë kibernetike” ONE Albania vlerëson se kompetenca e propozuar krijon mbivendosje me kompetencat që aktualisht ushtron AKEP ndaj sipërmarrësve të komunikimeve elektronike sipas Ligjit nr. 54/2024 "Për komunikimet elektronike". Në sektorin e komunikimeve elektronike, masat teknike për mbrojtjen e rrjeteve dhe shërbimeve,			dhe shërbimeve TIK që ata administrojnë vetë. Këto masa nuk lidhen me detyrimet që AKEP u vendos sipërmarrësve të komunikimeve elektronike në kuadër të menaxhimit të kërcënimeve ndaj përdoruesve apo palëve të treta, sipas kuadrit rregullator sektorial për komunikimet elektronike. Përkundrazi, ndërhyrja e AKSK-së ka si objekt sigurinë kibernetike të infrastrukturave që administrohen nga vetë operatorët, për të garantuar mbrojtjen e tyre nga kërcënimet dhe incidentet kibernetike. Në këtë kuptim, kompetencat e AKSK-së dhe AKEP-it kanë qëllime dhe fusha zbatimi të ndryshme: AKEP ushtron kompetencat e tij rregullatore në sektorin e komunikimeve elektronike, ndërsa AKSK vepron në funksion të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, sipas Ligjit nr. 25/2024 “Për sigurinë kibernetike”. Për rrjedhojë, dispozita nuk krijon dyzim kompetencash, por garanton zbatimin e detyrimeve të operatorëve për mbrojtjen e

	përfshirë menaxhimin e incidenteve, vulnerabiliteteve dhe implementimin e masave të sigurisë, monitorohen dhe mbikëqyren nga AKEP, si autoriteti sektorial kompetent. Vendosja e një detyrimi paralel nga AKSK për të komunikuar dhe urdhëruar zbatimin e masave teknike mbi të njëjtin subjekt mund të sjellë mbivendosje kompetencash ndërmjet dy autoriteteve, rrezik për udhëzime kontradiktore ose jo të koordinuara si dhe paqartësi për sipërmarrësit e komunikimeve elektronike apo autoritetin përgjegjës për mbikëqyrjen dhe zbatimin e masave.			infrastrukturave të tyre dhe mbetet e pandryshuar.

	Për të garantuar sigurinë juridike dhe një model të qartë kuadri rregullator, propozojmë që kjo dispozitë të parashikojë se komunikimi dhe koordinimi i këtyre masave ndaj operatorëve të komunikimeve elektronike të realizohet nëpërmjet autoritetit sektorial kompetent (AKEP), në përputhje me kompetencat e përcaktuara në legjislacionin sektorial, ose të sqarojë rolin e AKEP në këtë proçes.			
Kryerja e simulimeve ne rrjete dhe sisitemet e operatorëve te infrastrukturave të informacionit	Mbi propozimin për të ndryshuar përmbajtjen e tekstit në nenin 13, shkronjë (ll) si vijon “Kryen simulime në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit,	ONE	Pranuar pjesërisht	Dispozita e propozuar nuk synon krijimin e një kompetence të re për Autoritetin Kombëtar për Sigurinë Kibernetike, por qartëson mënyrën e ushtrimit të funksioneve ekzistuese të Autoritetit, në cilësinë e CSIRT-it Kombëtar, për identifikimin, vlerësimin dhe adresimin e cenueshmërive që mund të

	duke shfrytëzuar vulnerabilitetet e evidentuara nëpërmjet skanimeve proaktive sipas shkronjës “g” të këtij neni, duke njoftuar paraprakisht operatorët. Procedura e simulimit miratohet me urdhër të drejtorit të përgjithshëm të Autoritetit” Dispozita e re e propozuar, i njeh Autoritetit kompetencën për të kryer simulime duke shfrytëzuar vulnerabilitete të identifikuara në sistemet dhe rrjetet e operatorëve. Kjo është një kompetencë e re, e cila nuk është e parashikuar në ligjin aktual nr.25/2024. Nga pikëpamja teknike, One Albania vlerëson se shfrytëzimi aktiv (exploitation) i			cenojnë sigurinë dhe qëndrueshmërinë e rrjeteve dhe sistemeve të informacionit të infrastrukturave kritike dhe të rëndësishme të informacionit. Kryerja e simulimeve të sigurisë kibernetike përbën një instrument teknik të vlerësimit të ekspozimit dhe nivelit të mbrojtjes së sistemeve dhe nuk nënkupton ndërhyrje të pakufizuar në mjediset operative të operatorëve. Ushtrimi i kësaj kompetence do të realizohet në mënyrë të kontrolluar, mbi bazën e vulnerabiliteteve të evidentuara paraprakisht dhe në përputhje me procedurën e miratuar nga Autoriteti. Megjithatë, duke marrë në konsideratë nevojën për garantimin e parimit të proporcionalitetit, koordinimit institucional dhe minimizimit të çdo ndikimi të mundshëm në vazhdimësinë e shërbimeve të operatorëve, pranohet pjesërisht sugjerimi për rregullimin më të qartë të procesit të njoftimit paraprak dhe koordinimit me operatorin. Për këtë qëllim, dispozita riformulohet duke përcaktuar detyrimin e Autoritetit për të njoftuar

	vulnerabiliteteve në mjediset operative (production environment) mund të shkaktojë ndërprerje të papritura të shërbimeve, degradim të performancës së rrjetit, ndikim mbi vazhdimësinë e shërbimeve elektronike si dhe pasoja për abonentët dhe infrastrukturën kritike. Për më tepër, nenet 32 dhe 33 të Direktivës (EU) 2022/2555 (NIS2), të cilat përcaktojnë kompetencat mbikëqyrëse të autoriteteve kombëtare, nuk parashikojnë kompetencën për të kryer shfrytëzim aktiv "exploitation" ose simulime aktive në rrjetet e operatorëve. Në këto kushte, ne propozojmë heqjen e kësaj kompetence nga			paraprakisht operatorin për zhvillimin e simulimit, brenda afateve të përcaktuara në procedurën përkatëse, duke marrë në konsideratë specifikat teknike të sektorit dhe garantimin e vijueshmërisë së shërbimeve kritike. Ndërkohë, kërkesa për heqjen e kompetencës nuk pranohet, pasi simulimet përbëjnë një masë të nevojshme për verifikimin e nivelit të sigurisë kibernetike dhe rritjen e rezistencës së infrastrukturave kritike dhe të rëndësishme të informacionit, në funksion të mbrojtjes së interesit publik. Gjithashtu, fakti që Direktiva (BE) 2022/2555 (NIS2) nuk parashikon shprehimisht një mekanizëm të tillë nuk kufizon mundësinë e shteteve për të miratuar masa kombëtare shtesë, në përputhje me nenin 5 të saj, me qëllim garantimin e një niveli më të lartë të sigurisë kibernetike.

	projektligji. Alternativisht nëse kjo klauzolë ruhet, të parashikohet shprehimisht se procedurat, kufizimet, rastet e aplikimit, garancitë teknike dhe koordinimi me operatorin do të rregullohen me akt nënligjor të veçantë, duke marrë në konsideratë specifikat e sektorit të komunikimeve elektronike. Gjithashtu duhet të përcaktohet se çdo simulim zhvillohet vetëm pas koordinimit me operatorin dhe në kushte që garantojnë mosndërprerjen e shërbimeve.			
Ngritja e CSIRT-eve sektorial	Mbi propozimin për ndryshimin e përkufizimit në nenin 5, pika (5), me përmbajtje "CSIRT sektorial" është ekipi i përgjigjes ndaj incidenteve të sigurisë	ONE	Refuzuar	Komenti nuk pranohet, pasi dispozitat e propozuara përcaktojnë qartë modelin institucional të ngritjes dhe funksionimit të individualizimin e masës së gjobës, në përputhje me përgjegjësitë e institucioneve përkatëse sipas sektorëve.

	kibernetike për sektorin përkatës, sipas përcaktimeve në anekset e këtij ligji, i ngritur nga Autoriteti Kombëtar për Sigurinë Kibernetike, institucioni përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe operatori qeveritar që menaxhon infrastruktura qeveritare dhe funksionon pranë ministrive përgjegjëse, institucionit rregullator për bankat, autoritetit apo operatorit qeveritar që menaxhon infrastrukturat qeveritare" si dhe ndryshimin e propozuar në nenin 15, pika 1 "Autoritetit Kombëtar për Sigurinë Kibernetike, institucioni përgjegjës për licencimin dhe mbikëqyrjen e			Për sektorin e komunikimeve elektronike, funksionet e CSIRT-it sektorial do të ushtrohen në përputhje me përcaktimet e ligjit dhe aktet zbatuese përkatëse, duke garantuar koordinimin me CSIRT-in Kombëtar dhe shmangien e çdo dublikimi në procesin e raportimit dhe menaxhimit të incidenteve. Detyrimi i operatorëve për raportimin e incidenteve pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial nuk përbën raportim të dyfishtë për të njëjtin qëllim, por siguron një mekanizëm të koordinuar ndërmjet nivelit kombëtar dhe atij sektorial, duke mundësuar si menaxhimin operacional të incidenteve në sektorin përkatës, ashtu edhe analizën dhe koordinimin kombëtar të kërcënimeve kibernetike. Gjithashtu, marrëdhëniet ndërmjet CSIRT-it Kombëtar dhe CSIRT-eve sektoriale, përfshirë shkëmbimin e informacionit dhe koordinimin e veprimeve, do të përcaktohen në aktet zbatuese në zbatim të Ligjit nr. 25/2024 "Për sigurinë kibernetike".

	bankave dhe operatori qeveritar që menaxhon infrastruktura qeveritare, ngrenë në strukturën e tyre CSIRT-et sektoriale përgjegjës për incidentet e sigurisë kibernetike” Ndryshimi i propozuar sqaron institucionet që krijojnë CSIRT-et sektoriale, por formulimi aktual mbetet i paqartë për sektorin e komunikimeve elektronike. Nga dispozita nuk rezulton qartë nëse CSIRT-i sektorial për komunikimet elektronike do të ngrihet pranë AKEP apo operatorët do të raportojnë vetëm pranë AKSK edhe në rolin e CIRT sektorial. Kjo paqartësi është veçanërisht e			

	rëndësishme pasi projektligji parashikon detyrime raportimi ndaj CSIRT-it sektorial dhe CSIRT-it kombëtar. Në mungesë të një përcaktimi të qartë do të përballeshim me situata të raportimeve të dyfishta, procedurave të ndryshme për të njëjtin incident dhe rritjes së barrës administrative për operatorët. Prandaj, propozojmë që projektligji të përcaktojë shprehimisht: · cili institucion ushtron funksionin e CSIRT-it sektorial për komunikimet elektronike; · marrëdhënien ndërmjet CSIRT-it sektorial dhe CSIRT-it Kombëtar;			

	· mënyrën e koordinimit dhe shkëmbimit të informacionit, në mënyrë që operatorët të mos kenë detyrime të dyfishta raportimi.			
Vetëdeklarimin e mënyrës së hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit	Mbi propozimin për të shtuar nenin 20/2 me përmbajtje "**1.** Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të deklarojnë pranë Autoriteti mënyrën e hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit, duke përfshirë: a) identifikimin e subjektit hostues ose administratorit të infrastrukturës teknologjike; b) llojin e hostimit dhe vendndodhjen e infrastrukturës; ç) masat teknike dhe organizative të zbatuara për	ONE	Refuzuar	Komenti nuk pranohet, pasi detyrimi për vetëdeklarimin e mënyrës së hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit është një mekanizëm i nevojshëm për ushtrimin efektiv të funksioneve të Autoritetit Kombëtar për Sigurinë Kibernetike. Ky detyrim nuk synon krijimin e një procesi të ri auditimi apo mbledhjen e informacionit të panevojshëm teknik, por krijimin e një pasqyre kombëtare mbi ekspozimin kibernetik të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, përfshirë varësitë nga ofruesit e shërbimeve të hostimit, cloud-it dhe virtualizimit. Fakti që Direktiva (BE) 2022/2555 (NIS2) nuk parashikon shprehimisht një detyrim të tillë nuk pengon miratimin e masave kombëtare shtesë, në përputhje me nenin 5 të

	sistemet e hostuara; d) përdorimin e shërbimeve cloud, virtualizimit. 2. Mënyra, forma, përmbajtja dhe procedurat e vetëdeklarimit përcaktohen me urdhër të drejtorit të përgjithshëm të Autoriteti.”. Projektligji parashikon një detyrim të ri për deklarimin pranë Autoritetit të mënyrës së hostimit, administrimit dhe përdorimit të shërbimeve cloud. Nga analizimi jonë, vërejmë se ky detyrim nuk rezulton të jetë kërkesë e Direktivës NIS2. Neni 21 i Direktivës[1] për cakton masat e menaxhimit të riskut që duhet të zbatojnë subjektet, por nuk kërkon raportim			saj, me qëllim garantimin e një niveli më të lartë të sigurisë kibernetike. Informacioni i kërkuar do të kufizohet në të dhënat e nevojshme për qëllime të mbikëqyrjes dhe vlerësimit të riskut kibernetik dhe do të trajtohet në përputhje me kërkesat ligjore për mbrojtjen e informacionit dhe konfidencialitetin. Për rrjedhojë, dispozita nuk krijon një barrë të panevojshme për operatorët, por siguron një instrument të domosdoshëm për identifikimin e varësive kritike teknologjike dhe menaxhimin e rreziqeve që lidhen me to. Për këto arsye, komenti nuk pranohet dhe dispozita mbetet e pandryshuar për çka kërkohet.

	sistematik të arkitekturës së hostimit apo të infrastrukturës cloud. Gjithashtu, analiza krahasimore e legjislacionit të shteteve që kanë transpozuar NIS2[2] (tabela bashkengjitur) nuk evidenton vendosjen e një detyrimi të tillë shtesë. Publikimi apo deklarimi i detajuar i mënyrës së hostimit, vendndodhjes së infrastrukturës apo përdorimit të cloud mund të përmbajë informacion me ndjeshmëri të lartë për sigurinë e operatorëve, për më tepër mbetet e paqartë deri në cfarë niveli detajimi do të kërkohet ky deklarim. Lidhur me këtë pikë, ONE Albania propozon rishikimin e nevojës për këtë			

	dispozitë. Alter nativisht, nëse kjo klauzolë ruhet, atëherë formulimi i klauzolës duhet të jetë i tillë që të parashikojë kufizimin e informacionit që deklarohet vetëm në rastet kur Autoriteti e kërkon për një qëllim konkret mbikëqyrës, bazuar në një analizë risku si dhe garantimin se informacioni i kërkuar do të jetë proporcional me objektivin e sigurisë kibernetike dhe në përputhje me parimin e minimizimit të të dhënave.			
Koordinimi ndërmjet CSIRT-it Kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit (veçanëri	Nenet 13, 15, 16, 17 dhe 23 Nga këndvështrimi i operatorëve të infrastrukturave kritike të informacionit, do të ishte e dobishme të qartësohej më tej mënyra e bashkëveprimit	Shoqata e Investitorëve të Huaj në Shqipëri (FIAA)	Refuzuar	Kuadri i propozuar ligjor parashikon një arkitekturë të koordinuar të menaxhimit të incidenteve kibernetike, ku CSIRT-i Kombëtar, CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve kanë role dhe përgjegjësi të ndryshme, por plotësuese. Ndarja e përgjegjësive ndërmjet këtyre strukturave nuk përbën një rregullim të

sht nenet 13, 15, 16, 17 dhe 23)	ndërmjet CSIRT-it Kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit, veçanërisht në lidhje me: • detyrimet e raportimit; dhe • përgjegjësitë dhe veprimet e secilës strukturë gjatë trajtimit të incidenteve të sigurisë kibernetike. Për operatorët që ushtrojnë veprimtarinë në sektorë të rregulluar, si sektori i energjisë, është e rëndësishme të shmanget krijimi i detyrimeve raportuese të mbivendosura ose të dyfishta. Operatorët u nënshtrohen tashmë detyrimeve të raportimit ndaj disa autoriteteve, përfshirë Autoritetin Kombëtar për Sigurinë Kibernetike dhe autoritetin			ri të krijuar nga ndryshimet e propozuara, por është e parashikuar tashmë në ligjin nr. 25/2024 "Për sigurinë kibernetike", i cili përcakton funksionet, kompetencat dhe mënyrën e bashkëveprimit të Autoritetit Kombëtar për Sigurinë Kibernetike, CSIRT-it Kombëtar, CSIRT-eve sektoriale dhe detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit. CSIRT-i Kombëtar, si strukturë përgjegjëse për koordinimin në nivel kombëtar dhe menaxhimin e incidenteve me ndikim të gjerë, nuk zëvendëson rolin e CSIRT-eve sektoriale, të cilat, në përputhje me parashikimet e ligjit nr. 25/2024, kanë funksionin e sigurimit të ekspertizës specifike sektoriale dhe të mbështetjes teknike për operatorët e sektorëve përkatës. Gjithashtu, detyrimi i operatorëve për raportimin e incidenteve pranë Autoritetit Kombëtar për Sigurinë Kibernetike është një detyrim i përcaktuar shprehimisht në ligjin nr. 25/2024 dhe përbën një element thelbësor të mekanizmit kombëtar të mbikëqyrjes, vlerësimit të rrezikut dhe koordinimit të

	rregullator të sektorit përkatës, si Enti Rregullator i Energjisë – ERE. Ndërkohë, projektligji parashikon në disa dispozita raportimin e incidenteve si pranë CSIRT-it Kombëtar, ashtu edhe pranë CSIRT-it sektorial. Për këtë arsye, me qëllim qartësimin e detyrimeve të operatorëve dhe shmangien e një barre administrative të panevojshme, sugjerojmë që në ligj ose në aktet nënligjore në zbatim të tij të përcaktohen qartë: • përgjegjësit ë përkatëse të CSIRT-it Kombëtar dhe CSIRT-it sektorial; • nëse raportimi pranë njërës strukturë konsiderohet se përmbush edhe			reagimit ndaj incidenteve kibernetike. Për sa i përket sugjerimit për krijimin e një pike të vetme raportimi vetëm pranë AKSK-së, vlerësohet se një ndryshim i tillë nuk është i nevojshëm, pasi kuadri ligjor në fuqi tashmë përcakton rolet dhe përgjegjësitë përkatëse të strukturave të ndryshme të reagimit. Funksionimi i CSIRT-eve sektoriale synon të sigurojë një reagim të specializuar sipas natyrës së sektorit, ndërsa AKSK ruan rolin e autoritetit kompetent kombëtar për koordinimin, mbikëqyrjen dhe menaxhimin e incidenteve me rëndësi kombëtare. Sa i përket bashkëpunimit me autoritetet rregullatore sektoriale, përfshirë Entin Rregullator të Energjisë (ERE), ai do të realizohet nëpërmjet mekanizmave institucionalë të koordinimit, duke respektuar kompetencat ligjore të përcaktuara për secilin institucion dhe pa krijuar mbivendosje të funksioneve të tyre.

	detyrimin e raportimit pranë strukturës tjetër, ose nëse do të krijohet një mekanizëm i përbashkët apo i koordinuar raportimi; dhe • mënyra e koordinimit me autoritetet rregullatore të sektorëve ku ekzistojnë tashmë detyrime të posaçme raportimi, përfshirë sektorin e energjisë. Në këtë kuadër, mund të merret në konsideratë që Autoriteti Kombëtar për Sigurinë Kibernetike të jetë pika qendrore e raportimit për operatorët e sektorit të energjisë dhe që informacioni përkatës t'i përcillet ERE-s dhe institucioneve të tjera kompetente nëpërmjet mekanizmave të koordinuar			

	ndërinstitucional ë.			
Skanimet proaktive, simulimet dhe kompetencat mbikëqyrëse (Neni 13)	(Neni 13) Ndërsa mbështesim objektivin e forcimit të sigurisë dhe rezistencës kibernetike, ndryshimi i propozuar në nenin 13 i njeh Autoritetit një kompetencë të rëndësishme për kryerjen e simulimeve në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit, duke shfrytëzuar vulnerabilitetet e evidentuara nëpërmjet skanimeve proaktive. Duke pasur parasysh ndikimin që aktivitete të tilla mund të kenë mbi funksionimin, vazhdimësinë dhe sigurinë e sistemeve të operatorëve, sugjerojmë që skanimet	Shoqata e Investitorëve të Huaj në Shqipëri (FIAA)	Pranuar pjesërisht	Kompetenca e parashikuar në nenin 13, shkronja "ll", synon t'i mundësojë Autoritetit Kombëtar për Sigurinë Kibernetike ushtrimin efektiv të funksioneve të tij mbikëqyrëse dhe parandaluese, nëpërmjet identifikimit, vlerësimit dhe adresimit proaktiv të cenueshmërive në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit. Duke marrë në konsideratë shqetësimet e ngritura nga operatorët lidhur me ndikimin e mundshëm operacional të këtyre veprimeve dhe nevojën për garantimin e vazhdimësisë së shërbimeve, dispozita është riformuluar me qëllim forcimin e elementit të koordinimit paraprak me operatorët. Në këtë kuadër, është shtuar parashikimi që realizimi i simulimeve do të kryhet pas **dakordësimit paraprak me operatorët për fashat orare të zhvillimit të tyre**, duke synuar që procesi të realizohet në mënyrë të kontrolluar dhe me ndikim minimal në funksionimin e rrjeteve dhe sistemeve të informacionit.

	proaktive dhe simulimet në rrjetet dhe sistemet e operatorit të kryhen vetëm me dakordësinë paraprake dhe në koordinim aktiv me operatorin, në bazë të një plani testimi të dokumentuar dhe të dakordësuar ndërmjet palëve. Operatori duhet të ruajë përgjegjësinë për kryerjen e testimit, ndërsa Autoriteti mund të marrë pjesë, ta mbikëqyrë ose ta ndjekë atë për qëllime mbikëqyrëse. Një qasje e tillë do të siguronte një ekuilibër të përshtatshëm ndërmjet ushtrimit të kompetencave mbikëqyrëse të Autoritetit dhe kërkesave operacionale dhe të sigurisë të operatorëve të infrastrukturave kritike.			Ky ndryshim nuk cenon kompetencën e Autoritetit për kryerjen e simulimeve si pjesë e funksioneve të tij mbikëqyrëse dhe parandaluese në fushën e sigurisë kibernetike, por synon të garantojë një qasje të koordinuar me operatorët dhe të marrë në konsideratë specifikat teknike dhe operacionale të infrastrukturave përkatëse.

Vetëdeklarimi i masave të sigurisë kibernetike dhe vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit (Nenet 20/1 dhe 20/2)	Neni 20/2 përcakton kategoritë e informacionit që operatorët duhet të deklarojnë pranë Autoritetit në lidhje me mënyrën e hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit. Megjithatë, pika 2 e këtij neni parashikon se "mënyra, forma, përmbajtja dhe procedurat e vetëdeklarimit" përcaktohen me urdhër të drejtorit të përgjithshëm të Autoritetit. Referimi te "përmbajtja" e vetëdeklarimit është i gjerë dhe mund të interpretohet se i mundëson aktit nënligjor të kërkojë kategori të tjera informacioni, përveç atyre të përcaktuara shprehimisht në pikën 1 të nenit 20/2.	Shoqata e Investitorëve të Huaj në Shqipëri (FIAA)	Pranuar pjesërisht	Qëllimi i dispozitave të reja për vetëdeklarimin është krijimi i një mekanizmi të unifikuar raportimi, i cili do t'i mundësojë Autoritetit Kombëtar për Sigurinë Kibernetike krijimin e një panorame të përgjithshme në nivel kombëtar mbi nivelin e sigurisë kibernetike, ekspozimin ndaj rreziqeve dhe masat e zbatuara nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Përcaktimi që "mënyra, forma, përmbajtja dhe procedurat" e vetëdeklarimit rregullohen me urdhër të drejtorit të përgjithshëm të Autoritetit nuk nënkupton zgjerim të pakufizuar të detyrimeve të operatorëve, por garanton fleksibilitetin e nevojshëm administrativ dhe teknik për përshtatjen e kërkesave të deklarimit me zhvillimet teknologjike dhe praktikat ndërkombëtare të sigurisë kibernetike. Kufizimi i kompetencës rregulluese vetëm në elementët formalë të paraqitjes së informacionit do të mund të pengonte aftësinë e Autoritetit për të mbledhur informacionin minimal të nevojshëm për ushtrimin e funksioneve të tij ligjore.

	Për këtë arsye, sugjerojmë të qartësohet nëse urdhri i drejtorit të përgjithshëm do të përcaktojë vetëm mënyrën e paraqitjes, formën, nivelin e detajimit dhe procedurën për deklarimin e informacionit të renditur në nenin 20/2, apo nëse nëpërmjet këtij urdhri mund të kërkohen edhe kategori shtesë informacioni nga operatorët. Gjithashtu, shkronja "a" e pikës 1 të nenit 20/2 kërkon identifikimin e "subjektit hostues ose administratorit të infrastrukturës teknologjike". Ndërsa identifikimi i subjektit hostues mund të jetë i nevojshëm për ushtrimin e funksioneve mbikëqyrëse të Autoritetit, informacioni për administratorin e infrastrukturës			Për sa i përket identifikimit të subjektit hostues ose administratorit të infrastrukturës teknologjike, ky informacion është i domosdoshëm për të kuptuar arkitekturën operative të sistemeve, varësitë teknologjike dhe subjektet përgjegjëse për administrimin e komponentëve kritikë. Ky informacion nuk synon marrjen e të dhënave operative të panevojshme apo të detajuara, por identifikimin e përgjegjësive institucionale dhe teknike në zinxhirin e furnizimit dhe administrimit të sistemeve. Duke marrë në konsideratë rëndësinë e garantimit të mbrojtjes së informacionit të administruar nga Autoriteti gjatë ushtrimit të funksioneve të tij ligjore, në projektligj është shtuar një dispozitë e posaçme që parashikon detyrimin për ruajtjen e konfidencialitetit të informacionit të marrë gjatë proceseve të kontrollit, mbikëqyrjes dhe vlerësimit të sigurisë kibernetike. Ky parashikim synon të garantojë që informacioni i siguruar nga operatorët e infrastrukturave kritike dhe

	teknologjike mund të përbëjë informacion të ndjeshëm nga pikëpamja operacionale dhe e sigurisë kibernetike, veçanërisht kur lidhet me administrimin e sistemeve dhe infrastrukturave kritike. Për këtë arsye, sugjerojmë të qartësohet se çfarë informacioni kërkohet konkretisht për identifikimin e administratorit të infrastrukturës teknologjike dhe në çfarë niveli detajimi duhet të paraqitet ky informacion, me qëllim shmangien e deklarimit të informacionit operacional të ndjeshëm përtej atij që është i nevojshëm për ushtrimin e funksioneve të Autoritetit.			të rëndësishme të informacionit, përfshirë të dhënat mbi organizimin, arkitekturën teknologjike dhe masat e sigurisë të zbatuara, të trajtohet në përputhje me kërkesat ligjore për mbrojtjen e informacionit sensitiv dhe të përdoret vetëm për qëllimet e ushtrimit të kompetencave të Autoritetit në fushën e sigurisë kibernetike. Në këtë kuadër, vlerësohet se shqetësimi i ngritur lidhur me garantimin e konfidencialitetit është adresuar nëpërmjet plotësimit të kuadrit ligjor, pa cenuar nevojën e Autoritetit për të administruar informacionin e nevojshëm për përmbushjen e funksioneve të tij mbikëqyrëse.
Mbivendosja e detyrimev	Mbivendosja e detyrimeve të vetëdeklarimit	Abissnet	Refuzuar	AKSK vlerëson shqetësimin e ngritur nga subjekti lidhur me

e të vetëdeklarimit	Ligji nr. 54/2024 “Për komunikimet elektronike në Republikën e Shqipërisë” i njeh AKEP-it një rol thelbësor sektorial. Neni 54, pika 1, detyron ofruesit e rrjeteve dhe shërbimeve publike të marrin masa teknike dhe organizative të përshtatshme e proporcionale. Pika 3 e të njëjtit nen kërkon që incidenti kibernetik që ka ndikuar në funksionimin e rrjeteve, sistemeve ose shërbimeve t’i njoftohet pa vonesë si AKEP-it, ashtu edhe autoritetit përgjegjës për sigurinë kibernetike. Neni 56 i jep AKEP-it kompetencën për të mbikëqyrur nenin 54, për të detajuar masat teknike dhe organizative, për të hetuar mospërputhjet			shmangien e barrës administrative dhe nevojën për koordinim ndërinstitucional. Megjithatë, propozimi që vetëdeklarimet dhe raportimet të depozitohen vetëm pranë AKSK-së, ndërsa informacioni t'i transmetohet më pas AKEP-it, nuk mund të merret në konsideratë. Ligji nr. 25/2024 "Për sigurinë kibernetike" dhe ligji nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë" rregullojnë fusha të ndryshme të mbikëqyrjes dhe u atribuojnë kompetenca të pavarura autoriteteve përkatëse. AKSK ushtron funksionet e autoritetit kombëtar për sigurinë kibernetike dhe mbikëqyr përmbushjen e detyrimeve të operatorëve sipas legjislacionit të sigurisë kibernetike, ndërsa AKEP ushtron kompetencat sektoriale në fushën e rrjeteve dhe shërbimeve të komunikimeve elektronike, në zbatim të legjislacionit të posaçëm. Për rrjedhojë, detyrimet e raportimit dhe vetëdeklarimit që burojnë nga këto dy kuadro ligjore nuk janë të njëjta dhe nuk kanë të njëjtin objekt apo qëllim mbikëqyrës. Edhe

	dhe për të kërkuar informacion, politika të dokumentuara dhe auditime sigurie. Në zbatim të këtyre dispozitave, me vendimin e Këshillit Drejtues nr. 8, datë 13.3.2026, AKEP-i ka miratuar rregulloren "Mbi masat organizative dhe teknike për garantimin e sigurisë së rrjeteve dhe shërbimeve të komunikimeve elektronike". Neni 10 i saj kërkon paraqitjen pranë AKEP-it, brenda muajit shkurt të çdo viti, të një raporti gjithëpërfshirës mbi masat e sigurisë. Shtojca 3 parashikon që përmbushja e kërkesave përkatëse të bëhet nëpërmjet një vetëdeklarimi			kur një pjesë e informacionit teknik mund të jetë i ngjashëm, ai administrohet për qëllime të ndryshme, në funksion të ushtrimit të kompetencave të veçanta të secilit autoritet. Projektligji nuk synon të ndryshojë ose të kufizojë kompetencat e autoriteteve të tjera të përcaktuara me ligje të veçanta, as të ndërhyjë në procedurat e raportimit të parashikuara nga legjislacioni sektorial. Çdo ndryshim në këtë drejtim do të kërkonte ndërhyrje në ligjin nr. 54/2024 dhe aktet nënligjore të nxjerra në zbatim të tij, çka tejkalon objektin e këtij projektligji. Gjithsesi, AKSK mbetet e angazhuar për të forcuar bashkëpunimin dhe shkëmbimin institucional të informacionit me autoritetet sektoriale, me qëllim lehtësimin e proceseve administrative për operatorët, në masën që kjo është e mundur brenda kuadrit ligjor në fuqi, pa cenuar kompetencat e përcaktuara me ligj për secilin institucion.

	formal. Neni 11 kërkon njoftimin fillestar pranë AKEP-it brenda 24 orëve për incidentet me ndikim të mesëm ose të lartë, depozitimin e shtojcave brenda 72 orëve dhe raportimin përfundimtar brenda 30 ditëve. Për rrjedhojë, operatori që është njëkohësisht sipërmarrës i komunikimeve elektronike dhe OIKI përballet me dy regjime që mbështeten në një masë të konsiderueshme në të njëjtin informacion teknik: Pranë AKSK-së, raportim i të gjitha incidenteve brenda katër orëve, përditësim 72-orësh dhe raport përfundimtar brenda një muaji. Pranë AKEP-it, raportim brenda 24 orëve për			

	incidentet me ndikim të mesëm ose të lartë, plotësim 72-orësh dhe raport përfundimtar brenda 30 ditëve. Pranë AKSK-së, vetëdeklarim për masat teknike, organizative dhe operacionale sipas nenit 20/1 të propozuar. Pranë AKEP-it, raport vjetor dhe vetëdeklarim formal sipas nenit 10 dhe shtojcës 3 të rregullores. Konstatimi nuk është se AKEP-i nuk ka kompetencë në fushën e sigurisë së rrjeteve të komunikimeve elektronike. Një kompetencë e tillë parashikohet shprehimisht nga neni 56 i ligjit nr. 54/2024. Çështja që kërkon ndërhyrje ligjore është kufiri dhe mënyra e ushtrimit të kësaj kompetence. Kërkimi nga operatori i një			

	deklarate të dytë përgjithshme mbi të njëjtat masa kibernetike mund të tejkalojë masën e nevojshme për ushtrimin e mbikëqyrjes sektoriale, kur informacioni mund t'i transmetohet AKEP-it drejtpërdrejt nga AKSK-ja. Dy deklarata formale nuk janë thjesht dy kopje dokumentesh që përsërisin njëra-tjetrën. Formularët e miratuar aktualisht nga AKSK-ja dhe AKEP-i përdorin terminologji të ndryshme, pasqyrojnë momente të ndryshme kohore, vendosin kritere jo të njëjta për kualifikimin e incidenteve dhe kërkojnë nivele të ndryshme informacioni. Për rrjedhojë, operatori mund të përballet me			

	pretendimin se një deklaratë është e paplotë ose e pasaktë jo për shkak të fshehjes së informacionit, por për shkak të mospërputhjes ndërmjet dy taksonomive administrative. Për më tepër, depozitimi i informacionit teknik të ndjeshëm në dy sistemeveçanta rrit rrezikun e mospërputhjes së versionit që konsiderohet burimi zyrtar i të dhënave. Zgjidhja e propozuar nuk synon kufizimin e aksesit të AKEP-it në informacion. Në vlerësimin tonë do të ishte e përshtatshme që AKSK-ja të shërbente si pika e vetme e depozitimit të vetëdeklarimeve të përgjithshme të sigurisë kibernetike dhe e			

	njoftimit fillestar të incidenteve, ndërsa informacioni me rëndësi sektoriale t'i transmetohet AKEP-it automatikisht dhe në mënyrë të sigurt.			
Raportimi i incidenteve dhe problematika e afateve	Raportimi i incidenteve dhe problematika e afateve Kuadri aktual ligjor parashikon raportimin e incidenteve kibernetike njëkohësisht pranë disa institucioneve. Për një OIKI që është njëkohësisht sipërmarrës i komunikimeve elektronike, i njëjti incident duhet të raportohet pranë CSIRT-it Kombëtar, CSIRT-it sektorial dhe AKEP-it, ndërsa, kur preken të dhëna personale, mund të lindë edhe detyrimi për njoftimin e	Abissnet	Refuzuar	Lidhur me propozimin për krijimin e një mekanizmi të vetëm raportimi pranë AKSK-së dhe transmetimin automatik të informacionit tek autoritetet sektoriale, vlerësojmë se kjo çështje kërkon një trajtim të koordinuar ndërinstitucional dhe teknik. Detyrimet e parashikuara në ligjin nr. 25/2024 për raportimin e incidenteve janë hartuar në përputhje me kërkesat e Direktivës (BE) 2022/2555 (NIS 2), e cila synon sigurimin e një reagimi të shpejtë ndaj incidenteve që mund të ndikojnë në funksionimin e shërbimeve kritike. Afati prej katër orësh i parashikuar në ligj synon sigurimin e një njoftimi fillestar të shpejtë dhe jo paraqitjen e një raportimi të plotë teknik në momentin fillestar të incidentit. Informacioni mund të plotësohet dhe përditësohet në fazat pasuese, në

	Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale. Në bazë të shkronjës "ë" të pikës 3 të nenit 17 dhe pikës 3 të nenit 23 të ligjit nr. 25/2024 "Për sigurinë kibernetike", operatorët raportojnë pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial çdo lloj incidenti të sigurisë kibernetike, brenda katër orëve nga momenti i identifikimit. Për incidentet e rëndësishme, informacioni përditësohet brenda 72 orëve dhe shoqërohet me një vlerësim fillestar të ashpërsisë, ndikimit dhe, kur janë të disponueshëm, treguesve të kompromitimit. Sipas pikës 5 të			përputhje me zhvillimin e analizës teknike të incidentit. Sa i përket propozimit për zgjatjen e këtij afati në 24 orë, vlerësohet se çështja duhet të analizohet në raport me nevojën për reagim të hershëm kombëtar dhe standardet e përcaktuara në NIS 2, duke mbajtur parasysh natyrën e veçantë të operatorëve të infrastrukturave kritike. Në lidhje me mundësinë e korrigjimit të informacionit fillestar, AKSK vlerëson se raportimi fillestar i bazuar në informacionin e disponueshëm në momentin e identifikimit të incidentit nuk duhet të konsiderohet si deklarim i pasaktë, për sa kohë që operatori vepron në mirëbesim dhe përditëson informacionin sipas kërkesave ligjore.

	nenit 23, raporti përfundimtar i dorëzohet CSIRT-it Kombëtar brenda një muaji pas njoftimit fillestar. Neni 7 i projektligjit, i cili riformulon shkronjën "ë" të pikës 3 të nenit 17 të ligjit nr. 25/2024, e ruan informacionin paralel pranë të CSIRT-ve dhe i shton atij detyrimin për bashkëpunim, shkëmbim të informacionit dhe koordinim të veprimeve. Paralelisht, pika 3 e nenit 54 të ligjit nr. 54/2024, datë 30.5.2024, "Për komunikimet elektronike në Republikën e Shqipërisë", kërkon që ofruesit e rrjeteve publike ose të shërbimeve të komunikimeve elektronike të disponueshme për publikun të njoftojnë pa			

	vonesë si AKEP-in, ashtu edhe autoritetin përgjegjës për sigurinë kibernetike, për incidentet që kanë ndikuar në funksionimin e rrjeteve, sistemeve ose shërbimeve. Pika 5 e po këtij neni i ngarkon më pas vetë AKEP-it detyrimin për të informuar autoritetin përgjegjës për sigurinë kibernetike për incidentet e marra. Kjo strukturë është konkretizuar më tej nga rregullorja "Mbi masat organizative dhe teknike për garantimin e sigurisë së rrjeteve dhe shërbimeve të komunikimeve elektronike". Sipas nenit 8, pika 1, të saj, incidentet me ndikim "të mesëm" ose "të			

	lartë” u njoftohen AKEP-it dhe AKSK-së. Neni 11 kërkon njoftimin fillestar elektronik pranë AKEP-it brenda 24 orëve nga evidentimi i incidentit, depozitimin e shtojcave 1 dhe 2 brenda 72 orëve dhe përditësimin përfundimtar të tyre brenda 30 ditëve kalendarike nga evidentimi. Neni 9, pika 1, shkronja “a”, parashikon ndërkohë që AKEP-i informon pa vonesë autoritetin kombëtar të sigurisë kibernetike për incidentet që mund të kenë ndikim të rëndësishëm. Për pasojë, regjimet nuk ndryshojnë vetëm për nga autoriteti marrës. Ligji nr. 25/2024 përfshin “të			

	gjithë llojet” e incidenteve dhe vendos afatin prej katër orësh, ndërsa rregullorja e AKEP-it e lidh raportimin formal me klasifikimin e ndikimit si “i mesëm” ose “i lartë” dhe parashikon afat 24-orësh. Edhe afati përfundimtar nuk është identik; “30 ditë nga evidentimi” dhe “një muaj pas njoftimit” ndryshojnë si në kohëzgjatje, ashtu edhe në ditën e fillimit të llogaritjes. Për më tepër, konceptet “incident i rëndësishëm”, “incident me ndikim të mesëm ose të lartë” dhe “incident që ka ndikuar në funksionimin e rrjetit ose shërbimit” nuk janë të lidhura shprehimisht nëpërmjet kritereve të			

	përbashkëta të ekuivalencës. Këto dallime kanë pasoja të drejtpërdrejta praktike. Në orët e para të një incidenti, operatori zakonisht disponon të dhëna paraprake, mund të jetë identifikuar sistemi i prekur, por jo shkaku rrënjësor, mund të jetë konstatuar një ndërprerje, por jo numri përfundimtar i përdoruesve të prekur, ose një ngjarje e vlerësuar fillimisht si me ndikim të kufizuar mund të riklasifikohet pas analizimit të regjistrave teknikë (logs). Dorëzimi i disa formularëve, në kohë të ndryshme dhe me taksonomi jo plotësisht të harmonizuara, krijon rrezikun e mospërputhjes formale ndërmjet			

	versioneve, megjithëse secili version mund të ketë qenë i saktë sipas informacionit të disponueshëm në momentin përkatës. Çështja merr rëndësi të veçantë për shkak të pasojave sanksionuese. Shkronja “a” e nenit 44 të ligjit nr. 25/2024 e cilëson kundërvajtje administrative mosraportimin sipas nenit 17, pika 3, shkronja “ë”, dhe nenit 23, pika 3. Neni 16 i projektligjit ruan për këtë kundërvajtje gjobën nga 1 000 000 deri në 10 000 000 lekë. Neni 12 i rregullores së AKEP-it i referon shkeljet te neni 184 i ligjit nr. 54/2024. Meqenëse mosnjoftimi sipas nenit 54, pika 3, nuk është individualizuar			

	shprehimisht ndër rastet e gjobave me përqindje, lind edhe nevoja për të saktësuar nëse dhe në çfarë kushtesh mund të zbatohet klauzola e përgjithshme e nenit 184, pika 1, shkronja “ç”, e cila parashikon gjobë 500 000 lekë për shkeljet e tjera të ligjit. Pa koordinim normativ, i njëjti mosraportim ose vonesë mund të bëhet objekt vlerësimi në dy procedura administrative të ndryshme. Standardi i Direktivës NIS 2 Neni 23 i Direktivës (BE) 2022/2555, datë 14.12.2022 (“NIS 2”) e lidh raportimin e detyrueshëm me incidentet që kanë ndikim të rëndësishëm në ofrimin e shërbimeve. Sekuenca përbëhet nga një			

	paralajmërim i hershëm brenda 24 orëve, një njoftim më i plotë brenda 72 orëve dhe një raport përfundimtar jo më vonë se një muaj pas njoftimit 72-orësh. Vetë direktiva sqaron se akti i njoftimit nuk duhet ta vendosë subjektin njoftues përpara një përgjegjësie të shtuar. Konsiderata (102) e NIS 2 shpjegon se paralajmërimi i hershëm duhet të përmbajë vetëm informacionin e domosdoshëm për të vënë CSIRT-in në dijeni dhe për t'i mundësuar subjektit të kërkojë ndihmë. Detyrimet e raportimit nuk duhet të devijojnë burimet njerëzore dhe teknike nga trajtimi i			

	incidentit, i cili duhet të mbetet përparësia e tyre. Konsiderata (106) rekomandon përdorimin e mjeteve teknike, si një pikë e vetme hyrëse, formularë elektronikë dhe platforma të dedikuara, pikërisht për të thjeshtuar raportimin dhe për të ulur barrën administrative. Në të njëjtën frymë, neni 21 i NIS 2 kërkon që masat e sigurisë të jenë të përshtatshme dhe proporcionale, duke marrë parasysh ekspozimin ndaj riskut, madhësinë e subjektit, probabilitetin dhe ashpërsinë e incidentit, ndikimin e tij shoqëror dhe ekonomik, si dhe koston e zbatimit. Abissnet mbështet nevojën e			

	AKSK-së për të marrë dijeni në kohë reale për ngjarjet që mund të cenojnë sigurinë kibernetike kombëtare. Për këtë arsye, sugjerohet të shqyrtohet rishikimi i afatit prej katër orësh, duke e përcaktuar në 24 orë. Për të dhënat që nuk mund të verifikohen brenda këtij afati propozohet të lejohet shënimi "në verifikim". Gjithashtu, propozohet të përcaktohet se momenti i fillimit të afatit nuk është çdo alarm automatik i prodhuar nga një sistem monitorimi, por momenti kur struktura përgjegjëse e operatorit, pas një vlerësimi paraprak të arsyeshëm, ka siguri të mjaftueshme se ka ndodhur një incident.			

	Përditësimi, korrigjimi ose riklasifikimi i informacionit fillestar, i kryer në mirëbesim dhe mbi bazën e të dhënave të reja, nuk duhet të konsiderohet raportim i pasaktë ose i paplotë. Përgjegjësia duhet të lindë vetëm kur provohet se operatori ka paraqitur me dashje informacion të rremë, ka fshehur të dhëna materiale që i dispononte në momentin e raportimit ose ka refuzuar të përditësojë një ndryshim thelbësor pasi ka marrë dijeni për të. Do të ishte e përshtatshme që detyrimi për raportimin e plotë dhe pasojat sanksionuese të lidheshin kryesisht me incidentet e			

	rëndësishme, sipas kritereve të nenit 26, pika 4, të ligjit nr. 25/2024 dhe parametrave të nenit 23, pika 4. Në të njëjtën frymë, propozohet që klasifikimi “i mesëm” ose “i lartë” i shtojcës 2 të rregullores së AKEP-it të lidhet me kategorinë ligjore të “incidentit të rëndësishëm” përmes një tabele të përbashkët ekuivalence, të miratuar nga AKSK-ja në bashkëpunim me AKEP-in. Në këtë mënyrë, operatori nuk do të përballet me dy vlerësime të ndryshme të rëndësisë së së njëjtës ngjarje. Propozohet që raportimi të kryhet nëpërmjet një pike të vetme elektronike të administruar nga AKSK-ja, në cilësinë e autoritetit			

	kombëtar dhe të CSIRT-it Kombëtar. Me regjistrimin e sinjalizimit, sistemi të gjenerojë automatikisht një identifikues unik të incidentit dhe një vulë kohore. I njëjti identifikues të përdoret për njoftimin 72-orësh, raportin përfundimtar, kërkesat për informacion shtesë dhe komunikimet ndërinstitucionale. Për incidentet që prekin rrjete ose shërbime publike të komunikimeve elektronike, sugjerohet që platforma t'ia vendosë informacionin automatikisht në dispozicion AKEP-it dhe CSIRT-it sektorial, sipas të drejtave të aksesit. Dorëzimi në platformën e AKSK-së të konsiderohet			

	juridikisht si përmbushje e njëkohshme e detyrimit të njoftimit sipas neneve 17 dhe 23 të ligjit nr. 25/2024, nenit 54, pika 3, të ligjit nr. 54/2024 dhe neneve 8 e 11 të rregullores së AKEP-it. Ky mekanizëm nuk cenon kompetencën sektoriale të AKEP-it. Ai eliminon vetëm dorëzimin e përsëritur të të njëjtit informacion. AKEP-i ta ruajë të drejtën për të kërkuar të dhëna plotësuese, kur ato janë specifike për funksionimin, vazhdimësinë ose cilësinë e rrjeteve dhe shërbimeve të komunikimeve elektronike, por këto kërkesa të administrohen në të njëjtën dosje elektronike të incidentit.			

	Propozimi për një linjë të vetme raportimi Në plan normativ, Abissnet propozon që projektligji të plotësohet me një dispozitë koordinuese që: E zgjat afatin e raportimit nga katër orë në 24 orë. Përcakton se korrigjimi në mirëbesim i të dhënave paraprake nuk përbën shkelje administrative. I jep raportimit pranë AKSK-së efektin juridik të njoftimit të njëkohshëm të CSIRT-it sektorial dhe AKEP-it. Parashikon miratimin e një akti të përbashkët AKSK–AKEP për afatet, formularët, shkëmbimin automatik të të dhënave, nivelet e aksesit dhe ruajtjen e			

	konfidencialitetit. Një zgjidhje e tillë nuk dobëson mbikëqyrjen e AKSK-së ose të AKEP-it. Përkundrazi, ajo krijon një burim unik zyrtar të të dhënave teknike, shmang versionet kontradiktore, shpejton shkëmbimin institucional dhe lejon që burimet njerëzore të operatorit të përqendrohen në kufizimin e pasojave dhe rikuperimin pas incidentit.			
Simulimet aktive në rrjetet dhe sistemet e operatorëve	Abissnet mbështet forcimin e kapaciteteve të AKSK-së për identifikimin dhe verifikimin e vulnerabiliteteve në infrastrukturat kritike dhe të rëndësishme të informacionit. Megjithatë,	Abissnet	Pranuar pjesërisht	AKSK vlerëson komentet e paraqitura nga operatorët lidhur me nevojën për garantimin e proporcionalitetit, sigurisë procedurale dhe minimizimit të ndikimit operacional gjatë realizimit të simulimeve aktive të sigurisë kibernetike. Sqarojmë se dispozita e propozuar nuk krijon një kompetencë të re për Autoritetin Kombëtar për Sigurinë Kibernetike, por qartëson mënyrën e ushtrimit të një kompetence

	ndryshimi i propozuar në nenin 13, shkronja “ll”, të ligjit nr. 25/2024, nuk përbën vetëm një saktësim të kompetencës ekzistuese për kryerjen e simulimeve. **5.1. Pamjaftueshmëria e rregullimit** Projektligji përcakton vetëm dy elemente, njoftimin paraprak të operatorit dhe miratimin e procedurës me urdhër të drejtorit të përgjithshëm të AKSK-së. Projektligji krijon një mospërputhje të brendshme në nivelin e garancive. Për skanimin proaktiv, i cili është veprimi më pak ndërhyrës, neni 13, shkronja “g”, kërkon që operatori të njihet paraprakisht me			që buron nga roli i AKSK-së si autoritet kombëtar kompetent dhe CSIRT Kombëtar, në zbatim të ligjit nr. 25/2024 “Për sigurinë kibernetike”. Simulimet e sigurisë kibernetike përbëjnë një instrument teknik dhe parandalues për identifikimin e cenueshmërive dhe vlerësimin e nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit. Kjo kompetencë nuk nënkupton akses të pakufizuar në sistemet e operatorëve, por ushtrohet në mënyrë të kontrolluar, mbi bazën e cenueshmërive të evidentuara dhe në përputhje me procedurat e përcaktuara. Duke marrë në konsideratë shqetësimet e operatorëve lidhur me vazhdimësinë e shërbimeve dhe ndikimin e mundshëm operacional, dispozita është riformuluar duke parashikuar koordinimin paraprak me operatorët për përcaktimin e fashave orare të zhvillimit të simulimeve, me qëllim që këto veprime të kryhen në mënyrë të kontrolluar dhe me ndikim minimal në funksionimin e rrjeteve dhe sistemeve të informacionit.

	të gjitha elementet teknike dhe ligjore të skanimit. Për simulimin që shfrytëzon aktivisht vulnerabilitetin, projektligji kërkon vetëm "njoftim paraprak". Po kështu, neni 31, pika 5 e ligjit nr. 25/2024 e kushtëzon aksesin e drejtpërdrejtë të CSIRT-it Kombëtar në sistemet e operatorit me respektimin e procedurave të sigurisë së këtij të fundit, ndërsa dispozita e propozuar nuk përmban ndonjë referim të tillë. Do të ishte e përshtatshme që një kompetencë më ndërhyrëse të mos shoqërohej me garanci më të dobëta se skanimi që i paraprin asaj. **5.2. Testimi aktiv dhe aksesi në të dhëna**			Procedurat e hollësishme për realizimin e simulimeve, përfshirë kriteret e përzgjedhjes, objektin e testimit, mënyrën e njoftimit, dokumentimin dhe masat mbrojtëse, do të përcaktohen në aktin nënligjor përkatës. Ky ndryshim synon të forcojë qartësinë dhe zbatueshmërinë e dispozitës, duke garantuar një balancim ndërmjet nevojës së AKSK-së për ushtrimin e funksioneve të tij mbikëqyrëse dhe nevojës për ruajtjen e stabilitetit operacional të operatorëve, në përputhje me kërkesat e Direktivës (BE) 2022/2555 (NIS2).

	Nëse shfrytëzimi i vulnerabilitetit krijon mundësinë e aksesit në regjistra, kredenciale, komunikime, të dhëna të trafikut ose të dhëna personale, simulimi nuk mbetet më një veprim thjesht teknik. Ai përfshin përpunim ose akses në të dhëna dhe duhet t'u nënshtrohet neneve 35 dhe 36 të Kushtetutës, ligjit nr. 124/2024, datë 19.12.2024 "Për mbrojtjen e të dhënave personale", si dhe kërkesave të nenit 31, pika 5, të ligjit nr. 25/2024. Vlerësohet e nevojshme që, përpara testimit, të përcaktohet nëse objektivi mund të arrihet pa aksesuar të dhëna reale, duke përdorur mjedise të			

	izoluara dhe llogari testuese. Propozohet që testimi në sistemet e prodhimit dhe aksesi në të dhëna reale të lejohen vetëm kur janë të domosdoshme për një objektiv të dokumentuar dhe kur një metodë më pak ndërhyrëse nuk jep rezultate të barasvlershme. Për çdo simulim propozohet të përcaktohen paraprakisht kategoritë e të dhënave që mund të aksesohen, qëllimi i aksesit, personat e autorizuar, afati i ruajtjes, mënyra e dokumentimit dhe fshirjes, si dhe teknikat që ndalohen shprehimisht. Të dhënat që nuk lidhen me objektivin e testimit nuk duhet të kopjohen, ruhen ose përdoren në			

	procesin mbikëqyrës. Ky standard mbështetet edhe nga vendimi nr. 44, datë 29.7.2025 i Gjykatës Kushtetuese. Ndonëse vendimi lidhet me sekuestrimin e një telefoni në kuadër të një procedimi penal, Gjykata konstatoi cenimin e fshehtësisë së korrespondencës dhe të mbrojtjes së të dhënave për informacionet që nuk kishin lidhje me objektin e hetimit. Gjykata urdhëroi shkatërrimin e kopjeve të parëndësishme dhe vendosjen nën kontroll gjyqësor të të dhënave që mund të ruheshin. Parimisht, vendimi tregon se aksesi në një mjedis digjital nuk mund të shndërrohet në akses të			

	pakufizuar në të gjithë përmbajtjen që gjendet në të dhe se kufizimi sipas qëllimit duhet të shoqërohet me garanci procedurale konkrete. Në të njëjtën linjë, GJEDNJ-ja, në çështjen Société Colas Est dhe të tjerë kundër Francës, nr. 37971/97, datë 16.4.2002, ka pranuar se mbrojtja e nenit 8 të KEDNJ-së shtrihet edhe mbi selinë dhe mjediset e veprimtarisë së një shoqërie tregtare dhe se kompetencat e gjera të kontrollit administrativ, kur nuk shoqërohen me kufij dhe garanci të mjaftueshme, mund të përbëjnë ndërhyrje joproporcionale. Edhe… pse vendimi lidhej me kontrolle fizike, standardi është i zbatueshëm, për			

	analogji, ndaj një ndërhyrjeje aktive në mjedisin digjital të një operatori. **5.3. Akti administrativ individual dhe e drejta e ankimit** Si rregull, do të ishte e përshtatshme që akti t'i njoftohej operatorit jo më pak se 10 ditë pune përpara testimit, në koherencë me afatin e kontrollit të parashikuar nga neni 30 i ligjit nr. 25/2024. Përjashtimi nga ky afat mund të justifikohet vetëm nga një rrezik kritik dhe i menjëhershëm, i dokumentuar posaçërisht në akt. Propozohet që operatorit t'i njihet e drejta të paraqesë kundërshtim teknik ose juridik për objektin, kohën ose mënyrën e testimit.			

	Paraqitja e një kundërshtimi të arsyetuar nuk duhet të konsiderohet refuzim bashkëpunimi sipas nenit 31, pika 9, dhe nuk duhet të sjellë sanksionim. Kundërshtimi nuk është i nevojshëm të pezullojë automatikisht të gjithë veprimtarinë mbikëqyrëse, por do të ishte e përshtatshme të pezullonte teknikën konkrete të kontestuar për pretendimet, mbi shkaqe të arsyeshme, rrezik për ndërprerje të shërbimit, humbje të të dhënave ose pasoja të pakthyeshme. Në kontekstin e projektligjit, nëse mosbashkëpunimi me simulimin mund të sjellë përgjegjësi administrative,			

	operatori duhet të ketë mundësi reale të kundërshtojë paraprakisht ligjshmërinë dhe proporcionalitetin e aktit që urdhëron testimin. **5.4. Përgjegjësia për dëmin e shkaktuar nga simulimi** Shfrytëzimi aktiv i një vulnerabiliteti mund të shkaktojë ndërprerje të shërbimit, korruptim ose humbje të të dhënave, ndryshim të konfigurimeve, aktivizim të mekanizmave automatikë të mbrojtjes ose pasoja ndaj sistemeve të ndërlidhura dhe palëve të treta. Projektligji nuk përcakton se kush mban përgjegjësi kur këto pasoja shkaktohen nga vetë simulimi.			

	Ligji nr. 8510, datë 15.7.1999 "Për përgjegjësinë jashtëkontraktore të organeve të administratës shtetërore", i ndryshuar, dhe Kodi Civil përmbajnë bazën e përgjithshme për kërkimin e shpërblimit të dëmit. Megjithatë, natyra e posaçme dhe rreziku i testimit aktiv kërkojnë një dispozitë të shprehur në ligjin nr. 25/2024. Propozohet të përcaktohet se AKSK-ja përgjigjet për dëmin pasuror dhe jopasuror që ka lidhje shkakësore me veprimet të kryera jashtë fushës së miratuar, me mosrespektimin e protokollit, me vazhdimin e testit pas plotësimit të kushteve të ndërprerjes ose			

	me shkeljen e standardit profesional të kujdesit. Njoftimi paraprak dhe bashkëpunimi i operatorit nuk duhet të interpretohen si marrje përsipër e rrezikut ose si heqje dorë nga e drejta për shpërblim. Kur AKSK-ja përdor testues të jashtëm, vlerësohet se përgjegjësia ndaj operatorit nuk duhet të zhvendoset te kontraktori. Do të ishte e përshtatshme që Autoriteti të mbetej përgjegjës për veprimtarinë e kryer në ushtrim të kompetencës publike, pa cenuar të drejtën e tij të regresit ndaj testuesit. Pas simulimit, propozohet të hartohet një procesverbal teknik, i aksesueshëm edhe nga			

	operatori, ku të pasqyrohen veprimet e kryera, koha, sistemet e prekura, të dhënat e aksesuara, devijimet nga plani dhe çdo efekt i padëshiruar. Ky dokumentim është i nevojshëm si për të ndarë pasojat e vulnerabilitetit ekzistues nga dëmi i shkaktuar prej veprimeve të testuesit, ashtu edhe për ushtrimin efektiv të së drejtës për dëmshpërblim. **5.5. Vlerësimi sipas NIS 2 dhe DORA-s** Nuk rezulton se Direktiva (BE) 2022/2555, NIS 2, ndalon testimin aktiv ose u ndalon shteteve të parashikojnë mjete mbikëqyrëse më të forta. Për këtë arsye, nuk mund të pohohet një papajtueshmëri			

	formale vetëm sepse projektligji lejon shfrytëzimin e vulnerabiliteteve. Çështja kryesore në raport me standardin e NIS 2 lidhet me garancitë procedurale. Nenet 32, pika 2, shkronja "d", dhe 33, pika 2, shkronja "c", e lidhin kryerjen e skanimeve të sigurisë me kritere objektive, jodiskriminuese, të drejta dhe transparente të vlerësimit të rrezikut dhe, kur është e nevojshme, me bashkëpunimin e subjektit. NIS 2 kërkon gjithashtu minimizimin e ndikimit të mbikëqyrjes mbi veprimtarinë e subjektit. Projektligji shqiptar autorizon një teknikë më ndërhyrëse se skanimi, por nuk përcakton as			

	kriteret e vlerësimit të rrezikut dhe as mënyrën e bashkëpunimit gjatë ekzekutimit. Kjo paraqet pikën më të rëndësishme që kërkon harmonizim me standardin e garancive të NIS 2. DORA, Rregullorja (BE) 2022/2554, është një akt sektorial për qëndrueshmërinë operacionale digjitale të sektorit financiar dhe nuk zbatohet drejtpërdrejt si standard i përgjithshëm për çdo OIKI të sektorit të komunikimeve elektronike. Për këtë arsye, nuk identifikohet një konflikt i drejtpërdrejtë juridik ndërmjet projektligjit dhe DORA-s. Megjithatë, nenet 26–27 të DORA-s dhe Rregullorja e Deleguar (BE)			

	2025/1190 tregojnë se testimi aktiv në sisteme prodhimi shoqërohet domosdoshmëris ht me përcaktim paraprak të fushës, vlerësim dhe menaxhim të rrezikut, testues të kualifikuar e të siguruar dhe mundësi ndërprerjeje kur lind rrezik për të dhënat, asetet ose vazhdimësinë e shërbimit. Ky standard është i vlefshëm si model krahasues, por jo si burim i një papajtueshmërie të drejtpërdrejtë. **5.6. Propozimi për riformulimin e dispozitës** Abissnet propozon që neni 13, shkronja "ll", të mos kufizohet në parashikimin e njoftimit paraprak dhe të urdhrit të drejtorit të përgjithshëm.			

	Dispozita duhet të parashikojë shprehimisht se simulimet që përfshijnë shfrytëzimin aktiv të vulnerabiliteteve kryhen vetëm mbi bazën e një vlerësimi të dokumentuar të rrezikut dhe të një akti administrativ individual të arsyetuar, sipas metodologjisë së miratuar me vendim të Këshillit të Ministrave në zbatim të nenit 9, shkronja “e”. Propozohet gjithashtu që, në të njëjtën dispozitë ose në një nen të posaçëm, të garantohet e drejta e operatorit për të kërkuar pezullimin e teknikave që paraqesin rrezik të rëndë e të pakthyeshëm. Do të ishte e përshtatshme të përcaktohej se kundërshtimi i			

	arsyetuar nuk përbën mungesë bashkëpunimi. Po ashtu, sugjerohet të rregullohet shprehimisht përgjegjësia për dëmin e shkaktuar nga testimi jashtë fushës së miratuar ose në kundërshtim me standardin profesional dhe masat e sigurisë.			
Ndalimi i ndërshkimit të dyfishtë	Projektligji propozon gjobë fikse prej **5 000 000 lekësh** për mosdorëzimin në afat të vetëdeklarimit sipas nenit 20/1 dhe gjobë fikse prej **3 000 000 lekësh** për deklarim të pasaktë, të paplotë ose të papërditësuar, si dhe për mosdeklarimin sipas nenit 20/2. Paralelisht, neni 184, pika 1, shkronja "a", nënndarja "xii" e ligjit nr. 54/2024 parashikon gjobë deri në **3 për**	Abissnet	Refuzuar	AKSK vlerëson rëndësinë e garantimit të proporcionalitetit në zbatimin e masave administrative dhe nevojën për shmangien e mbivendosjes së panevojshme të detyrimeve për subjektet e rregulluara. Në këtë drejtim, duhet theksuar se ligji nr. 25/2024 "Për sigurinë kibernetike", i cili ka për qëllim përafrimin e legjislacionit kombëtar me Direktivën (BE) 2022/2555 (NIS 2), përcakton detyrimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për zbatimin e masave teknike, organizative dhe operacionale për menaxhimin e riskut të

	qind të të ardhurave vjetore të vitit të fundit financiar, por jo më shumë se **100 000 000 lekë**, për mosmarrjen e masave teknike, organizative dhe proporcionale sipas nenit 54. Shkronja "ç" e së njëjtës dispozitë parashikon gjobë fikse prej **500 000 lekësh** për shkelje të tjera të dispozitave të vetë ligjit që nuk janë listuar posaçërisht. **Ndalimi i ndëshkimit të dyfishtë** **4.1. Standardet kushtetuese dhe konventore** Neni 34 i Kushtetutës garanton se askush nuk mund të dënohet më shumë se një herë për të njëjtën vepër dhe as të gjykohet përsëri, përveç rigjykimit të vendosur nga një gjykatë më e lartë sipas ligjit.			sigurisë kibernetike, me qëllim rritjen e nivelit të mbrojtjes dhe qëndrueshmërisë së sistemeve, rrjeteve dhe shërbimeve që ata administrojnë. Ndërkohë, vetë Direktiva (BE) 2022/2555 ka parashikuar ndryshime të rëndësishme në raport me kuadrin rregullator të komunikimeve elektronike, duke shfuqizuar nenet 40 dhe 41 të Direktivës (BE) 2018/1972 të Parlamentit Evropian dhe Këshillit, datë 11 dhjetor 2018, "Për krijimin e Kodit Evropian të Komunikimeve Elektronike". Ky ndryshim reflekton nevojën për një qasje të unifikuar dhe të koordinuar në trajtimin e kërkesave për sigurinë e rrjeteve dhe sistemeve të informacionit. Për rrjedhojë, vlerësohet se harmonizimi i mëtejshëm i kuadrit kombëtar për komunikimet elektronike me ndryshimet e sjella nga kuadri evropian është një proces i nevojshëm, i cili duhet të realizohet në bashkëpunim ndërmjet autoriteteve përgjegjëse dhe subjekteve të sektorit. Ky harmonizim do të mundësojë një ndarje më të qartë të kompetencave ndërmjet autoriteteve, duke shmangur vendosjen e

	Në lidhje me personat juridikë, neni 16, pika 2 e Kushtetutës parashikon se të drejtat dhe detyrimet kushtetuese vlejnë edhe për ta, për aq sa pajtohen me natyrën dhe qëllimin e tyre. Garancia plotësohet nga neni 4 i Protokollit nr. 7 të Konventës Evropiane për të Drejtat e Njeriut. Sipas standardit të Gjykatës Evropiane për të Drejtat e Njeriut, emërtimi i një mase si "gjobë administrative" nuk e përjashton atë automatikisht nga nocioni autonom i procedurës penale. Në çështjen Engel dhe të tjerë kundër Holandës, datë 8.6.1976, GJEDNJ-ja përcaktoi tri kritere vlerësimi: klasifikimin e			detyrimeve të dyfishta për sipërmarrësit e komunikimeve elektronike lidhur me zbatimin dhe raportimin e masave të sigurisë për rrjetet dhe sistemet e tyre. Në këtë kuadër, rregullimi i mëtejshëm i legjislacionit të komunikimeve elektronike do të kontribuojë jo vetëm në shmangien e përsëritjes së kërkesave administrative, por edhe në parandalimin e situatave ku i njëjti subjekt mund të përballet me masa administrative ose gjoba të dyfishta për shkak të zbatimit paralel të detyrimeve që burojnë nga kuadro të ndryshme rregullatore për të njëjtin objekt mbrojtjeje.

	shkeljes në të drejtën kombëtare, natyrën e shkeljes, si edhe natyrën dhe rëndësinë e sanksionit. Dy kriteret e fundit janë alternative dhe mund të mjaftojnë edhe kur ligji kombëtar e klasifikon procedurën si administrative. Në çështjen Öztürk kundër Gjermanisë, datë 21.2.1984, Gjykata sqaroi se zhvendosja e një shkeljeje nga fusha penale në atë administrative nuk mund të përdoret për t'i hequr subjektit garancitë materiale të Konventës. Në çështjen Sergey Zolotukhin kundër Rusisë, datë 10.2.2009, GJEDNJ-ja e lidhi elementin idem me identitetin ose ngjashmërinë			

	thelbësore të fakteve materiale, jo vetëm me emërtimin juridik të shkeljes. Ndërsa në çështjen A dhe B kundër Norvegjisë, datë 15.11.2016, Gjykata pranoi se dy procedura mund të bashkëekzistojnë vetëm kur janë pjesë e një regjimi të strukturuar, ndjekin qëllime plotësuese, janë të parashikueshme, zhvillohen në lidhje të ngushtë kohore dhe materiale, shmangin përsëritjen e mbledhjes së provave dhe garantojnë që barra e përgjithshme ndëshkuese të mbetet proporcionale. Edhe jurisprudenca kushtetuese shqiptare mbështet të njëjtat fakte. Në			

	vendimin nr. 5, datë 8.3.2005, Gjykata Kushtetuese ka vlerësuar se parimi nuk lidhet thjesht me zbatimin dy herë të së njëjtës normë, por me ndalimin e një procedimi ose dënimi të dytë për të njëjtin veprim, sjellje ose fakt. **Garancia është konsideruar relevante edhe për përgjegjësinë kundërvajtëse.** Në vendimin nr. 10, datë 2.4.2009, Gjykata ritheksoi rëndësinë e identitetit të faktit dhe të ekzistencës së një vendimi përfundimtar. Edhe vendimi nr. 00-2025-1417, datë 23.9.2025 i Kolegjit Penal të Gjykatës së Lartë, e trajton vendimin përfundimtar për të njëjtin fakt penal si pengesë			

	procedurale që duhet verifikuar kryesisht. Ky vendim nuk zgjidh drejtpërdrejt një konflikt ndërmjet dy autoriteteve administrative, por është relevant për standardin kombëtar të identitetit faktik dhe efektin pengues të vendimmarrjes përfundimtare. Duhet bërë një dallim i rëndësishëm. Vetë ekzistenca e dy autoriteteve ose e dy detyrimeve nuk përbën automatikisht shkelje të parimit **ne bis in idem**. Dy deklarime të dorëzuara në data ose pranë autoriteteve të ndryshme mund të trajtohen formalisht si dy veprime të veçanta. Pikërisht për këtë arsye, megjithatë, do të ishte e			

	arsyeshme që ligji të shmangte krijimin e dy detyrimeve me të njëjtin objekt. **Operatori nuk duhet të ekspozohet ndaj dy gjobave për dy veprime formalisht të ndryshme, por të kryera vetëm nga kërkesa e panevojshme për të deklaruar dy herë të njëjtin informacion teknik.** Rreziku i drejtpërdrejtë i ndëshkimit të dyfishtë shfaqet kur e njëjta mangësi teknike, i njëjti incident ose i njëjti mosveprim raportohet, përdoret nga dy autoritete si bazë materiale për dy procedura ndëshkuese. Në këto raste, parimi i përgjithshëm i bashkëpunimit ndërinstitucional ndërmjet dy autoriteteve nuk është i			

	mjaftueshëm. Vlerësohet e nevojshme të parashikohen rregulla të shprehura për autoritetin që drejton procedurën, shkëmbimin e provave, efektin e vendimit të parë dhe llogaritjen e barrës së përgjithshme ndëshkuese. **4.2. Standardet orientuese të Bashkimit Evropian** Edhe pse Karta e të Drejtave Themelore të Bashkimit Evropian nuk zbatohet në Shqipëri në të njëjtën mënyrë si në një shtet anëtar, nenet 50 dhe 52 të saj dhe jurisprudenca e Gjykatës së Drejtësisë përbëjnë standarde të rëndësishme orientuese për afrimin e legjislacionit. Në çështjen bpost, C-117/20,			

	vendim i datës 22.3.2022, Gjykata e Drejtësisë vlerësoi një situatë ku i njëjti subjekt ishte proceduar nga autoriteti sektorial postar dhe autoriteti i konkurrencës. Ajo kërkoi që mundësia e dy procedurave të mbështetet në rregulla të qarta të parashikueshme, që procedurat të koordinohen dhe që barra e përgjithshme të mos tejkalojë atë që është e domosdoshme. Në çështjen Engie România, C-205/23, vendim i datës 30.1.2025, Gjykata e Drejtësisë trajtoi në mënyrë edhe më të afërt ndërhyrjen e një autoriteti të mbrojtjes së konsumatorit dhe të rregullatorit të energjisë ndaj së njëjtës sjellje.			

	Gjykata kërkoi rregulla të qarta që lejojnë parashikimin e procedurave të dyfishta, koordinim ndërmjet autoriteteve, afërsi kohore të procedurave dhe proporcionalitet të të gjitha sanksioneve të vendosura. Veçanërisht domethënës është neni 35, pika 2, e Direktivës (BE) 2022/2555, datë 14.12.2022 ("NIS 2"). Kur autoriteti i mbrojtjes së të dhënave ka vendosur një gjobë sipas GDPR-së për të njëjtën sjellje, autoriteti i sigurisë kibernetike nuk vendos një gjobë të dytë administrative sipas NIS 2. Megjithatë, masat korrigjuese jondëshkuese mbeten të mundshme. Ky			

	është një model i drejtpërdrejtë i legjislativit për ndarjen ndërmjet korrigjimit dhe mangësisë dhe dyfishimit të ndështkimit. **4.3. Propozimet për koordinimin ndërmjet AKSK-së dhe AKEP-it** Në funksion të një kuadri të unifikuar dhe të zbatueshëm, Abissnet propozon të merret në konsideratë: • Vetëdeklarimet sipas neneve 20/1 dhe 20/2 të depozitohen vetëm pranë AKSK-së. AKEP-i të marrë nga AKSK-ja informacionin që është i nevojshëm për mbikëqyrjen e rrjeteve			

	dhe shërbimeve të komunikimeve elektronike. • Dorëzimi pranë AKSK-së të konsiderohet përmbushje e çdo detyrimi me të njëjtin objekt raportimi ose vetëdeklarimi që mbështetet në të njëjtat të dhëna. AKEP-i të ruajë të drejtën për të kërkuar vetëm informacion shtesë dhe që nuk ndodhet në deklarimin e administruar nga AKSK-ja.			

	• Të krijohet një portal i vetëm për njoftimin e incidenteve. Njoftimi brenda katër orëve pranë AKSK-së t'i transmetohet automatikisht AKEP-it dhe të konsiderohet njoftim i njëkohshëm për efekt të nenit 54, pika 3, të ligjit nr. 54/2024. • Të përcaktohet shprehimisht se për të njëjtin veprim ose mosveprim, të mbështetur në të			

	njëjtat fakte materiale dhe ndaj të njëjtit operator, AKSK-ja dhe AKEP-i nuk vendosin dy gjoba me natyrë ndëshkuese.			
Regjimi i gjobave	**Individualizimi i gjobës** Abissnet, në cilësinë e operatorit të infrastrukturës kritike të informacionit, mbështet vendosjen e një regjimi sanksionues efektiv për shkeljet që cenojnë sigurinë dhe qëndrueshmërinë e infrastrukturave kritike. Megjithatë, efektiviteti i këtij regjimi nuk mund të matet vetëm nga niveli i lartë i gjobave.	Abissnet	Pranuar	Janë rishikuar dhe reflektuar në projektligj ndryshimet përkatëse lidhur me parashikimet për kundërvajtjet administrative dhe masat e gjobave.

	Një sanksion administrativ është efektiv kur është njëkohësisht i individualizuar sipas rrethanave të shkeljes dhe në përpjesëtim të drejtë me rëndësinë e tij. Në këtë këndvështrim, vlerësohet se ndryshimet e propozuara në nenet 15 dhe 16 të projektligjit kërkojnë rishikim. Projektligji rrit nga **200 000–400 000 lekë** në **2 000 000–4 000 000 lekë** gjobat për shkeljet e nenit 44, shkronjat “b”, “ç”, “ç” dhe “e”. Gjithashtu, rrit nga **400 000–1 000 000 lekë** në **4 000 000–10 000 000 lekë** gjobën për mospërmbushjen e masave korrigjuese dhe përfshin në të njëjtin interval shkeljen e të njëjtës shkronjë “h”. Projektligji			

	vendos gjithashtu gjobë fikse prej **5 000 000 lekësh** për mosdorëzimin në afat të vetëdeklarimit. Po ashtu, vendos gjobë fikse prej **3 000 000 lekësh** për paraqitjen e të dhënave të pasakta, të paplota ose të papërditësuara dhe për mosdeklarimin e mënyrës së hostimit dhe administrimit të sistemeve. Relacioni i projektligjit e shpjegon këtë ndërhyrje me nevojën e përgjithshme për forcimin e zbatueshmërisë së ligjit, por nuk paraqet të dhëna mbi numrin dhe natyrën e shkeljeve të konstatuara, dëmet e shkaktuara, pamjaftueshmëri në e masave ekzistuese, praktikat krahasuese apo ndikimin			

	ekonomik të rritjes së gjobave mbi kategoritë e ndryshme të operatorëve. **Një rritje dhjetëfish e kufirit minimal të disa gjobave kërkon një arsyetim të posaçëm dhe një analizë të dokumentuar të nevojës, përshatshmërisë dhe ndikimit të masës.** Neni 10 i ligjit nr. 10 279, datë 20.5.2010 "Për kundërvajtjet administrative", lejon që gjoba të përcaktohet si shumë fikse ose ndërmjet një kufiri minimal dhe maksimal. Për rrjedhojë, shuma fikse nuk është, në vetvete, e ndaluar. Megjithatë, lejimi formal i saj nga ligji i përgjithshëm nuk e përjashton kontrollin e parimit kushtetues të proporcionalitetit dhe nuk e bën shumën fikse të			

	përshtatshme për çdo lloj kundërvajtjeje. Gjobat e propozuara prej **5 000 000** dhe **3 000 000 lekësh** janë fikse dhe nuk lejojnë dallimin ndërmjet një mangësie formale të korrigjueshme dhe një deklarimi të rremë të kryer me dashje, ndërmjet një vonese të shkurtër pa pasoja dhe një mosdeklarimi të zgjatur, ose ndërmjet një pasaktësie pa ndikim dhe fshehjes së një rreziku material. Shkeljet e propozuara në shkronjat "f", "g" dhe "gj" përfshijnë një spektër tepër të gjerë situatash faktike. Mosdorëzimi në afat mund të përbëhet nga një vonesë e shkurtër, e korrigjuar			

	vullnetarisht dhe pa asnjë ndikim në mbikëqyrjen e ushtruar nga Autoriteti, por mund të përbëhet edhe nga një refuzim i qëllimshëm dhe i vazhdueshëm për të bashkëpunuar me Autoritetin. Po kështu, një deklaratë "e pasaktë, e paplotë ose e papërditësuar" mund të përmbajë një gabim material në një fushë dytësore, por mund edhe të fshehë vendndodhjen reale të sistemeve, përdorimin e një ofruesi cloud ose mungesën e një mase kritike sigurie. Trajtimi i këtyre situatave me të njëjtën gjobë prej **3 000 000** ose **5 000 000 lekësh** e kufizon ndjeshëm mundësinë e Autoritetit për të dalluar shkallën			

	e rrezikshmërisë, formën e fajit, kohëzgjatjen, pasojat dhe sjelljen e operatorit pas konstatimit. Për shkeljet me gjobë fikse, metodologjia e parashikuar nga neni 45, pika 2, praktikisht nuk mund të individualizojë masën e dënimit, sepse Autoriteti nuk ka asnjë hapësirë për të lëvizur ndërmjet një minimumi dhe maksimumi. Kjo nuk duket plotësisht në harmoni as me metodologjinë e publikuar nga AKSK-ja, sipas së cilës gjoba duhet të jetë në përpjesëtim me natyrën, rrethanat, pasojat dhe nivelin e përgjegjësisë së subjektit, duke u përzgjedhur masa që cenon në pak të drejtat dhe interesat e ligjshme të operatorit.			

	Regjimi i gjobave duhet të vlerësohet në dritën e neneve 4, 11, 17, 41 dhe 42 të Kushtetutës. Gjoba prek drejtpërdrejt pasurinë dhe ushtrimin e veprimtarisë ekonomike të operatorëve. Për këtë arsye, kufizimi duhet të mbështetet në një normë të qartë, të ndjekë një interes publik legjitim dhe të mos vendosë mbi operatorin një barrë më të rëndë se ajo që është e nevojshme për arritjen e qëllimit. Një regjim i tillë kërkon vlerësim të kujdesshëm në raport me nenin 17 të Kushtetutës dhe nenin 12 të ligjit nr. 44/2015 "Kodi i Procedurave Administrative i Republikës së Shqipërisë", të cilat kërkojnë që kufizimi			

	administrativ të jetë i përshtatshëm, e nevojshme dhe në përpjesëtim me qëllimin e ligjshëm. Neni 18 i Kodit kërkon gjithashtu që procedura administrative të zhvillohet në mënyrë sa më efikase dhe me barrën më të vogël të nevojshme për subjektin. Në vendimin nr. 33, datë 8.6.2016, Gjykata Kushtetuese ka ndërtuar një standard veçanërisht të rëndësishëm për kontrollin e gjobave administrative. Në paragrafët 31–32, Gjykata kërkon që të vlerësohet nëse objektivi publik është mjaftueshëm i rëndësishëm, nëse masa ka lidhje të arsyeshme me objektivin, nëse			

	është e përshtatshme dhe e domosdoshme dhe, së fundi, nëse ekzistojnë mjete më pak të dëmshme për arritjen e të njëjtit qëllim. Proporcionaliteti nuk përmbushet vetëm duke deklaruar rëndësinë e interesit publik, por kërkohet një baraspeshë konkrete ndërmjet interesit të përgjithshëm dhe barrës që i vendoset subjektit. Në të njëjtin vendim, Gjykata evidentoi mungesën e një studimi paraprak, të analizës kosto–përfitim dhe të referencave konkrete në praktikat evropiane si mangësi në justifikimin e ashpërsisë të penaliteteve. Në paragrafin 63–68, ajo vlerësoi			

	se kombinimi i gjobave fikse, rritjes së ndjeshme të tyre dhe mungesës së individualizimit mund ta zhvendosë masën përtej logjikës normale të një sanksioni administrativ dhe të vendosë një barrë të tepruar mbi veprimtarinë ekonomike dhe pronën. Ky vendim nuk nënkupton se çdo gjobë fikse ose çdo rritje e gjobave është automatikisht antikushtetuese. Ai kërkon, megjithatë, që rritja të mbështetet në një nevojë të provuar dhe që struktura e sanksionit të lejojë dallimin ndërmjet shkeljeve me rëndësi dhe pasoja thelbësisht të ndryshme. Këto kërkesa marrin rëndësi të posaçme kur			

	kufiri minimal rritet dhjetëfish dhe kur për shkelje të formuluara gjerësisht vendoset një shumë e vetme e padryshueshme. Edhe jurisprudenca e Gjykatës së Drejtësisë së Bashkimit Evropian ofron një analogji të drejtpërdrejtë. Në çështjen **C-210/10, Urbán**, vendim i datës 9.2.2012, GJED-ja vlerësoi si joproporcional një sistem që vendoste të njëjtën gjobë fikse për shkelje me natyrë dhe rëndësi të ndryshme. Rasti konkret lidhej me mungesën e një të dhëne në vetëm një nga pesëmbëdhjetë dokumentet e kontrolluara, kur informacioni mund të verifikohej nga një dokument tjetër dhe nuk ekzistonte			

	mundësi abuzimi. Gjykata theksoi se një mangësi e tillë nuk mund të trajtohej njësoj si shkeljet që pengonin realisht kontrollin. Në çështjen **C-384/17, Link Logistik N&N**, vendim i datës 4.10.2018, GJED-ja ritheksoi se rëndësia e sanksionit duhet t'i përgjigjet rëndësisë së shkeljes dhe se në caktimin e gjobës duhet të merren parasysh rrethanat individuale të rastit. Neni 4 i ligjit nr. 10 279, datë 20.5.2010, e përkufizon kundërvajtjen administrative si shkelje "me faj" të dispozitave ligjore ose nënligjore. Për rrjedhojë, përgjegjësia sipas neneve 44 dhe 45 të ligjit nr. 25/2024 nuk			

	mund të jetë automatike dhe nuk mund të mbështetet vetëm në konstatimin objektiv se një fushë e vetëdeklarimit ishte e paplotë ose se informacioni u përditësua pas afatit. Në kuadër të procedurës administrative kërkohet të provohen sjellja konkrete e operatorit, mundësia reale për përmbushjen e detyrimit, si edhe faji në formën e dashjes ose pakujdesisë. Paaqartësia e formularit, ndryshimi i menjëhershëm i një konfigurimi teknik, pamundësia objektive, forca madhore ose mbështetja e arsyeshme në informacionin e një ofruesi të jashtëm janë rrethana që kërkojnë të			

	shqyrtohen përpara vendosjes së përgjegjësisë. Barra e provës për kundërvajtjen i takon organit administrativ, sipas nenit 26, pika 3, të ligjit nr. 10 279/2010. Krahas faktit, propozohet që dispozita të përmbajë një prag të rëndësisë materiale. Për qëllimet e nenit 44, një e dhënë duhet të konsiderohet materialisht e pasaktë, e paplotë ose e papërditësuar vetëm kur mangësia është e aftë të ndikojë në: • Vlerësimin e riskut ose të përputhshmërisë së operatorit. • Identifikimin e sistemeve, hostimit, administrimit ose varësive kritike. • Ushtrimin efektiv të			

	mbikëqyrjes nga Autoriteti. • Parandalimin, trajtimin ose kufizimin e pasojave të një incidenti kibernetik. Një gabim shkrimi, një pasaktësi dytësore ose një e dhënë e korrigjuar menjëherë, pa ndikim në vlerësimin e riskut dhe pa synim fshehjeje, nuk duhet të barazohet me paraqitjen me dashje ose me pakujdesi të rëndë të një informacioni të rremë. Vetë Direktiva NIS 2 i cilëson si shkelje serioze dhënien e informacionit të rremë ose me pasaktësi thelbësore dhe jo çdo pasaktësi të parëndësishme. Ligji nr. 25/2024 përmban tashmë, në nenin 43, një logjikë të shkallëzuar kur konstatohen mangësi në			

	zbatimin e masave të sigurisë. AKSK-ja përcakton një afat të arsyeshëm për korrigjimin e tyre. Vetëm mospërmbushja e masës korrigjuese brenda afatit të arsyeshëm mund të sanksionohet me gjobë sipas nenit 44, shkronja "dh". Prandaj, do të ishte më koherente që një mangësi teknike t'i nënshtrohej fillimisht korrigjimit, ndërsa një gabim formal në vetëdeklarim të aktivizonte menjëherë dhe në mënyrë automatike një gjobë fikse prej **3 000 000** ose **5 000 000 lekësh**. Vetë ligji nr. 25/2024 ndjek aktualisht një model më të individualizuar. Neni 43 parashikon, si rregull, lënien e një afati të arsyeshëm për			

	korrigjimin e mangësive, ndërsa neni 45 përdor intervale gjobash dhe parashikon një metodologji për përcaktimin e masës konkrete. Në këtë kontekst, vlerësohet se nuk do të ishte e nevojshme që shkeljet e reja, të cilat në një pjesë të tyre mund të jenë thjesht formale, të trajtohen me një standard më të rëndë se shkeljet ekzistuese të ligjit. Nenet 32 dhe 34 të Direktivës (BE) 2022/2555 – NIS 2 kërkojnë që masat mbikëqyrëse dhe gjobat të jenë efektive, proporcionale dhe bindëse, duke u marrë parasysh rrethanat e çdo rasti. Neni 32, pika 4, parashikon shprehimisht paralajmërime, udhëzime			

	detyruese dhe urdhra për korrigjimin e mangësive brenda një afati. Pika 7 kërkon vlerësimin e rëndësisë dhe kohëzgjatjes së shkeljes, dëmit material ose jomaterial, dashjes ose pakujdesisë, shkeljeve të mëparshme, masave zbutëse dhe shkallës së bashkëpunimit. Pika 8 kërkon arsyetim të hollësishëm, komunikimin e gjetjeve paraprake dhe një afat të arsyeshëm për paraqitjen e komenteve. Në përputhje me këtë standard, për shkeljet e para, formale, jomateriale dhe pa risk të menjëhershëm për sigurinë kibernetike propozohet të parashikohet paralajmërimi me shkrim dhe			

	afati i arsyeshëm i korrigjimit. Gjobitja e drejtpërdrejtë do të ishte e përshtatshme të rezervohej për rastet e mëposhtme: refuzimin e qëllimshëm për të deklaruar ose bashkëpunuar; paraqitjen me dashje ose me pakujdesi të rëndë të informacionit të rremë; fshehjen e një dobësie, varësie ose konfigurimi kritik; pengimin e kontrollit ose moszbatimin e një urdhri korrigjues; shkeljet e përsëritura; shkeljet që kanë shkaktuar ose janë të afta të shkaktojnë ndikim serioz në një shërbim kritik. Ky sistem nuk dobëson fuqinë mbikëqyrëse të AKSK-së. Përkundrazi, e përqendron reagimin e fortë			

	ndëshkues te sjelljet që paraqesin risk real dhe shmang përdorimin e të njëjtit instrument për mangësi thelbësisht të ndryshme. **6.2. Propozime për shkallëzimin e masave** Për këto arsye, propozohet të merret në konsideratë: • Masa prej **5 000 000 lekësh** të përcaktohet si kufi maksimal, për shembull në intervalin **500 000–5 000 000 lekë**. • Masa prej **3 000 000 lekësh** të përcaktohet si kufi maksimal, për shembull në intervalin **300 000–3 000 000 lekë**. • Për mangësitë formale, të korrigjueshme dhe pa ndikim material në nivelin e sigurisë, operatorit t'i			

	lihet fillimisht një afat jo më i shkurtër se **10 ditë pune** për korrigjim. • Gjoba e menjëhershmet'i rezervohet për rastet e deklarimit të rremë me dashje, fshehjes së informacionit material, përsëritjes së shkeljes, moskorrigjimit brenda afatit të caktuar ose krijimit të një rreziku konkret për sigurinë. • Masa konkrete të përcaktohet duke vlerësuar rëndësinë dhe kohëzgjatjen e shkeljes, pasojat, shkallën e fajit, bashkëpunimin, masat korrigjuese, historikun e subjektit dhe kapacitetin e tij ekonomik. **6.3. Pasaktësia e referencës në nenin 44, shkronja "ç"**			

	Përpara rritjes së gjobës për shkeljet e nenit 44, shkronja “ç”, sugjerohet të korrigjohet referenca normative e kësaj dispozite. Neni 44, shkronja “ç”, e ligjit nr. 25/2024, i referohet “mospërmbushjes së detyrimeve të caktuara nga Autoriteti, në zbatim të pikës 1 të nenit 27”. Mirëpo, neni 27, pika 1, nuk vendos një detyrim për OIKI/OIRI-të. Ai detyron nëpunësit e AKSK-së që marrin pjesë në zgjidhjen e incidenteve të ruajnë konfidencialitetin e plotë të të dhënave të përpunuara. Edhe metodologjia aktuale e AKSK-së e ka interpretuar këtë dispozitë si kundërvajtje të			

	nëpunësve të Autoritetit. Një akt metodologjik, megjithatë, nuk mund të korrigjojë përmes interpretimit një referencë të pasaktë ligjore, të përcaktojë për herë të parë subjektin kundërvajtës ose të krijojë elemente të përgjegjësisë që nuk rezultojnë qartë nga ligji. Në vendimin nr. 30, datë 5.7.2021, Gjykata Kushtetuese ka theksuar se siguria juridike kërkon që norma të jetë e qartë, e përcaktuar dhe e kuptueshme. Ligji duhet të identifikojë subjektet të cilave u drejtohet, sjelljen e kërkuar, mënyrën e zbatimit dhe pasojat që rrjedhin nga mospërmbushja.			

	Një normë e pasaktë, e cila i lejon zbatuesit t'i japë kuptime të ndryshme dhe prodhon pasoja sanksionuese, nuk përmbush kërkesat e parimit të ligjshmërisë. Për rrjedhojë, sugjerohet që shkronja "ç" ose të hiqet nga neni 44 dhe nga kategoria e gjobave të parashikuara për operatorët ose, nëse synohet një detyrim tjetër i operatorit, të plotësohet me referencën e saktë dhe të përshkruhet në mënyrë të plotë sjellja e ndaluar. Rritja nga **200 000–400 000 lekë** në **2 000 000–4 000 000 lekë** e një gjobe të mbështetur në një referencë të pasaktë do ta thellonte pasigurinë juridike.			
Hyrja në fuqi	Abissnet, në cilësinë e	Abissnet	Refuzuar	AKSK vlerëson rëndësinë e sigurimit të një zbatimi

	operatorit të infrastrukturës kritike të informacionit, mbështet hyrjen në fuqi dhe zbatimin në kohë të ndryshimeve që synojnë forcimin e sigurisë kibernetike. Megjithatë, vlerësohet e përshtatshme që afati i hyrjes në fuqi të parashikohet në mënyrë të tillë që detyrimet e reja të jenë të përcaktuara, të aksesueshme dhe teknikisht të zbatueshme përpara se mosrespektimi i tyre të mund të sjellë përgjegjësi administrative. **7.1. Siguria juridike** Neni 19 i projektligjit parashikon hyrjen në fuqi 15 ditë pas botimit në Fletoren Zyrtare. Në të njëjtën kohë, neni 18 u lë organeve kompetente një			efektiv dhe të qartë të detyrimeve të përcaktuara në kuadrin ligjor për sigurinë kibernetike. Megjithatë, vlerësohet se parashikimi i një periudhe shtesë të përshtatjes për zbatimin e detyrimeve të reja nuk është i nevojshëm, pasi dispozitat e propozuara synojnë kryesisht qartësimin dhe forcimin e mekanizmave ekzistues të sigurisë kibernetike, të cilat burojnë nga detyrimet e përcaktuara tashmë në ligjin nr. 25/2024 "Për sigurinë kibernetike". Gjithashtu, aktet nënligjore që do të miratohen në zbatim të ligjit do të kenë si qëllim detajimin e kërkesave teknike dhe procedurale, duke siguruar qartësinë e nevojshme për subjektet e interesuara dhe duke lehtësuar zbatimin e tyre. Për këto arsye, nuk vlerësohet e nevojshme vendosja e një periudhe të posaçme shtesë përshtatjeje pas hyrjes në fuqi të akteve zbatuese, pasi subjektet e përfshira kanë tashmë detyrime të përcaktuara në kuadrin ekzistues ligjor për zbatimin e masave të sigurisë kibernetike.

	afat deri në 12 muaj për miratimin e akteve nënligjore që do të përcaktojnë elemente thelbësore të zbatimit të ligjit. Në veçanti, forma, përmbajtja, mënyra e paraqitjes, afatet dhe procedurat e vetëdeklarimit sipas nenit 20/1 përcaktohen më pas me urdhër të drejtorit të përgjithshëm të AKSK-së. Edhe mënyra, forma, përmbajtja dhe procedurat e deklarimit sipas nenit 20/2 i lihen një urdhri të mëvonshëm. Kjo strukturë krijon një mospërputhje kohore ndërmjet hyrjes formale në fuqi të ligjit dhe mundësisë reale të operatorit për ta zbatuar atë. Dispozitat që parashikojnë kundërvajtje të reja mund të konsiderohen në			

	fuqi pas 15 ditësh, ndërkohë që operatori ende nuk ka formularin, të dhënat e detyrueshme, nivelin e hollësisë së tyre, mënyrën e dorëzimit, procedurën e përditësimit ose afatin konkret. Afati 12-mujor i nenit 18 është afat për nxjerrjen e akteve nga organet publike. Ai nuk përbën periudhë përshtatjeje për operatorin. Nëse akti përcaktohet vetëm në fund të kësaj periudhe, operatorit praktikisht nuk i mbetet kohë për verifikimin e të dhënave, përshtatjen e proceseve të brendshme dhe miratimin e deklaratës nga strukturat përgjegjëse. Në rastin konkret, operatori nuk mund të parashikojë			

	plotësisht përmbajtjen e detyrimit dhe kufirin ndërmjet përmbushjes e kundërvajtjes përpara miratimit të akteve zbatuese. Për këtë arsye, hyrja në fuqi e ligjit mund të mbetet 15 ditë pas botimit, por propozohet të shtyhet shprehimisht fillimi i zbatimit të detyrimeve të reja dhe i dispozitave sanksionuese që lidhen me to. Një periudhë tremujore përshtatjeje nuk paraqitet si afat i imponuar drejtpërdrejt nga Kushtetuta ose nga NIS 2. Ajo propozohet si afat i arsyeshëm, duke pasur parasysh natyrën teknike të detyrimeve, numrin e sistemeve dhe ofruesve që duhet të verifikohen, ndërveprimin me			

	shërbimet cloud dhe nevojën për miratime të brendshme. Sugjerohet që afati të fillojë nga botimi i aktit të fundit nënligjor që është i nevojshëm për përmbushjen e detyrimit dhe jo nga hyrja në fuqi e ligjit. Kjo qasje mbështetet edhe nga jurisprudenca e Gjykatës së Drejtësisë së Bashkimit Evropian. Në çështjen **C-201/08, Plantanol GmbH & Co. KG kundër Hauptzollamt Darmstadt**, vendim i datës 10.9.2009, paragrafët 46, 49 dhe 52, GJED-ja ka arsyetuar se siguria juridike kërkon rregulla të qarta, të sakta dhe të parashikueshme dhe se kjo kërkesë është veçanërisht e fortë kur			

	rregullimi prodhon pasoja financiare. Gjykata ka sqaruar gjithashtu se ligjvënësi mund ta ndryshojë kuadrin rregullator, por duhet të marrë parasysh situatën e operatorëve dhe, kur është e nevojshme, të përshtatë zbatimin e rregullave të reja. Ndryshimi i papritur, veçanërisht kur kërkon investime të kushtueshme, mund të cenojë ndjeshëm operatorin nëse nuk i lihet kohë e mjaftueshme për t'iu përshtatur situatës së re juridike. Ky vendim nuk vendos një afat të pandryshueshëm gjashtëmujor, por konfirmon nevojën që koha e përshtatjes të vlerësohet në raport me barrën reale të ndërhyrjes.			

	7.2. Propozimi për dispozitën kalimtare Për të garantuar sigurinë juridike dhe zbatimin efektiv, propozohet shtimi i një dispozite kalimtare. Ky rregullim nuk pengon hyrjen në fuqi të dispozitave organizative dhe institucionale 15 ditë pas botimit. Ai siguron vetëm që detyrimet materiale dhe pasojat sanksionuese të fillojnë pasi përmbajtja e tyre të jetë e plotë, aktet normative të jenë botuar dhe operatorëve t'u jetë dhënë një periudhë reale për përshtatje. Një zgjidhje e tillë forcon zbatueshmërinë e ligjit, redukton mosmarrëveshjet administrative dhe siguron që mbikëqyrja e AKSK-së të fillojë mbi bazën e deklarimeve të			

	sakta, të verifikuara dhe teknikisht të qëndrueshme, në përputhje me parimet e sigurisë juridike, ligjshmërisë dhe proporcionalitetit.			
Komente mbi Nenin 4 për disa shtesa në nenin 13 të ligjit Nr. 25/2024 "Për Sigurinë Kibernetike"	Neni 13 i Ligjit nr. 25/2024 përcakton detyrat dhe përgjegjësitë e CSIRT-it Kombëtar, i cili, në kuptim të nenit 9 të këtij ligji, ushtrohet nga Autoriteti Kombëtar për Sigurinë Kibernetike. Projektligji synon të zgjerojë kompetencat e CSIRT-it Kombëtar duke i njohur Autoritetit kompetencën për të kryer simulime të sigurisë kibernetike në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit,	Vodafone Albania	Pranuar pjesërisht	Dispozita e propozuar nuk krijon një kompetencë të re për Autoritetin Kombëtar për Sigurinë Kibernetike, por vetëm qartëson dhe rregullon mënyrën e ushtrimit të një kompetence të parashikuar tashmë në Ligjin nr. 25/2024 "Për sigurinë kibernetike". Në funksion të rolit të tij si autoritet kombëtar kompetent dhe CSIRT Kombëtar, AKSK ka përgjegjësi për identifikimin, vlerësimin dhe adresimin e cenueshmërive që cenojnë sigurinë e infrastrukturave kritike dhe të rëndësishme të informacionit. Kryerja e simulimeve të sigurisë kibernetike është një instrument teknik në zbatim të këtyre përgjegjësive. Dispozita e propozuar parashikon kufizime dhe garanci procedurale, pasi simulimet kryhen vetëm mbi bazën e vulnerabiliteteve të evidentuara përmes

	duke shfrytëzuar vulnerabilitetet e identifikuara gjatë skanimeve proaktive. Në parim, zgjerimi i kompetencave të autoriteteve kombëtare nuk bie në kundërshtim me nenin 5 të Direktivës (BE) 2022/2555 (NIS2), i cili u lejon shteteve anëtare të miratojnë masa që sigurojnë një nivel më të lartë të sigurisë kibernetike. Megjithatë, këto masa duhet të respektojnë parimet themelore të së drejtës, veçanërisht parimet e proporcionalitetit, domosdoshmërisë, sigurisë juridike dhe mbrojtjes së të drejtave të subjekteve private. Dispozita e propozuar shkon përtej modelit			skanimeve proaktive, me njoftim paraprak të operatorit dhe sipas një procedure të miratuar nga Drejtori i Përgjithshëm i Autoritetit. Duke marrë në konsideratë shqetësimet e ngritura nga operatorët lidhur me ndikimin e mundshëm operacional të këtyre veprimeve dhe nevojën për garantimin e vazhdimësisë së shërbimeve, dispozita është riformuluar me qëllim forcimin e elementit të koordinimit paraprak me operatorët. Në këtë kuadër, është shtuar parashikimi që realizimi i simulimeve do të kryhet pas **dakordësimit paraprak me operatorët për fashat orare të zhvillimit të tyre**, duke synuar që procesi të realizohet në mënyrë të kontrolluar dhe me ndikim minimal në funksionimin e rrjeteve dhe sistemeve të informacionit. Ky ndryshim nuk cenon kompetencën e Autoritetit për kryerjen e simulimeve si pjesë e funksioneve të tij mbikëqyrëse dhe parandaluese në fushën e sigurisë kibernetike, por synon të garantojë një qasje të koordinuar me operatorët dhe të marrë në konsideratë specifikat teknike dhe

	rregullator të Bashkimit Evropian për dy arsye kryesore: a) njeh Autoritetit kompetencën për të kryer drejtpërdrejt simulime aktive (penetration testing) në sistemet e operatorëve privatë; b) lejon kryerjen e simulimeve duke shfrytëzuar vulnerabilitetet e identifikuara gjatë skanimeve proaktive, pa përcaktuar kufijtë materialë dhe proceduralë në ushtrimin e kësaj kompetence. • **Kuadri rregullator Europian** Në legjislacionin e BE-së, veçanërisht në Direktivën (BE) 2022/2555 (NIS2) dhe Rregulloren (BE) 2022/2554 (DORA), bëhet një ndarje e qartë ndërmjet:			operacionale të infrastrukturave përkatëse. Për rrjedhojë, ndryshimi synon vetëm të rrisë qartësinë dhe zbatueshmërinë e normës ekzistuese dhe nuk bie në kundërshtim me Direktivën (BE) 2022/2555 (NIS2), e cila u lejon shteteve të miratojnë masa shtesë për garantimin e një niveli më të lartë të sigurisë kibernetike.

	• kompetencës së autoritetit publik për të kërkuar, mbikëqyrur dhe verifikuar testimet e sigurisë; dhe • realizimit teknik të vetë testimeve. Në këtë model, autoritetet kombëtare nuk kryejnë vetë teste aktive depërtimi në sistemet e operatorëve privatë. Ato ushtrojnë funksione mbikëqyrëse dhe rregullatore, ndërsa testimet realizohen nga subjekte të pavarura dhe të kualifikuara. Ky model synon të garantojë: • paanshmërinë e procesit; • shmangien e konfliktit të interesit;			

	• proporcionalitetin e ndërhyrjes; • mbrojtjen e vazhdimësisë së shërbimeve kritike. **• Si zbatohet ky model në praktikë në shtetet e Bashkimit Evropian** Për të garantuar kryerjen e testeve të depërtimit pa i realizuar vetë, shtetet anëtare kanë krijuar tregje të strukturuara të certifikimit dhe auditimit. • **Franca - Agjencia Franceze për Sigurinë Kibernetike (ANSSI)** Sipas Ligjit francez, Operatorët e Rëndësisë Jetike (Operators of Vital Importance – OIV) janë të detyruar t'i			

	nënshtrohen testeve të depërtimit (Penetration test). Megjithatë, Agjencia Franceze për Sigurinë Kibernetike (ANSSI) nuk i kryen vetë këto testime. Për këtë qëllim, ANSSI ka krijuar skemën "PASSI", nëpërmjet së cilës certifikohen kompani private që kanë të drejtë të kryejnë auditime dhe teste depërtimi. Operatorët mund të angazhojnë vetëm kompani të certifikuara sipas kësaj skeme. • **Gjermania (BSI)** Edhe në Gjermani, Zyra Federale për Sigurinë e Informacionit (BSI) nuk kryen vetë penetration testing në sistemet e operatorëve privatë. BSI			

	kërkon që operatorët kritikë dhe ofruesit e caktuar të shërbimeve cloud të realizojnë teste të rregullta sipas standardeve kombëtare (p.sh. BSI C5), ndërsa vetë testimet realizohen nga ekspertë ose kompani të pavarura të certifikuara. Raportet përfundimtare dorëzohen pranë autoritetit për qëllime mbikëqyrjeje. • **Sektori financiar në Bashkimin Europian (DORA dhe TIBER-EU)** Për bankat dhe institucionet financiare me rëndësi sistemike, kuadri evropian parashikon Threat-Led Penetration Testing (TLPT).			

	Legjislacioni kërkon që subjektet financiare të angazhojnë testues të jashtëm të depërtimit dhe sigurisë kibernetike. Autoriteti mbikëqyrës miraton paraprakisht objektin dhe shtrirjen e testimit dhe më pas shqyrton raportin përfundimtar për të verifikuar respektimin e kërkesave ligjore, por nuk realizon vetë testimin teknik. • **Përjashtimi** Autoritetet kombëtare të sigurisë kibernetike mund të kryejnë drejtpërdrejt penetration testing vetëm mbi sistemet që janë në pronësi të shtetit, si ministritë, rrjetet qeveritare, sistemet e inteligjencës apo			

	infrastruktura ushtarake. Megjithatë, në momentin që infrastruktura është në pronësi të një subjekti privat, roli i autoritetit publik ndryshon nga ekzekutimi i testimeve, në mbikëqyrjen, autorizimin dhe verifikimin e tyre, ndërsa kryerja e testimeve mbetet përgjegjësi e subjekteve të pavarura dhe të certifikuara. Sa më sipër, nga praktika e shteteve anëtare të BE rezulton se autoritetet kombëtare të sigurisë kibernetike nuk ushtrojnë drejtpërdrejt kompetencën për të kryer penetration testing në sistemet e operatorëve privatë. Roli i tyre konsiston në: • përcaktim in e			

	standardeve dhe metodologjive; • certifikimin ose kualifikimin e ofruesve të shërbimeve; • kërkimin e kryerjes së testimeve kur është e nevojshme; • mbikëqyrjen dhe verifikimin e rezultateve të testimeve. Vetë penetration testing realizohen nga subjekte të pavarura dhe të certifikuara, duke garantuar paanshmërinë e procesit, shmangien e konfliktit të interesit, dhe respektimin e parimit të proporcionalitetit në ushtrimin e kompetencave mbikëqyrëse.			

	• **Kufijtë që vendos NIS2 për skanimet proaktive** Direktiva NIS2 nuk i njeh CSIRT-it kompetencën për të realizuar penetration testing në sistemet e operatorëve privatë. Kjo direktivë parashikon vetëm dy kompetenca: **a) Proactive scanning me kërkesë të subjektit** Sipas nenit 11(3)(c), CSIRT mund të kryejë skanime proaktive me kërkesë të subjektit për të identifikuar vulnerabilitete që mund të kenë ndikim të rëndësishëm. Pra, iniciativa i përket vetë operatorit. **b) Proactive non-intrusive scanning** Paragrafi vijues i të njëjtit nen			

	autorizon CSIRT-të të kryejnë skanime proaktive jo-ndërhyrëse të sistemeve të aksesueshme publikisht të entiteteve thelbësore dhe të rëndësishme. Direktiva vendos dy kufizime të qarta: • skanimi duhet të jetë **non-intrusive**; • nuk duhet të ketë ndikim negativ mbi funksionimin e shërbimeve. Asnjë dispozitë e NIS2 nuk autorizon CSIRT-in të shfrytëzojë vulnerabilitetet e identifikuara për të kryer simulime aktive apo penetration testing në sistemet e operatorëve privatë. Edhe Rregullorja BE 2022/2554 -			

	DORA (Digital Operational Resilience Act) për sektorin financiar ndjek të njëjtën qasje, duke rezervuar për autoritetet vetëm funksionet mbikëqyrëse dhe jo ekzekutimin e testimeve. • **Mungesa e garancive procedurale** Nga ana tjetër, në kryerjen e simulimeve në sistemet e operatorëve privatë, Projektligji parashikon vetëm detyrimin për njoftimin paraprak të operatorit dhe jo miratimin paraprak të tij sipas qasjes së Direktivës së BE. Njoftimi paraprak nuk është i barasvlershëm me pëlqimin e operatorit dhe nuk përbën garanci të mjaftueshme procedurale kur			

	bëhet fjalë për ndërhyrje aktive në sisteme kritike. Një njoftim i thjeshtë nuk garanton që testimi do të zhvillohet në një moment apo në një mënyrë që nuk cenon funksionimin normal të sistemeve të operatorit. Operatorët e infrastrukturave kritike dhe të rëndësishme ofrojnë shërbime thelbësore, të cilat duhet të jenë të disponueshme në mënyrë të pandërprerë. Kryerja e simulimeve aktive gjatë periudhave me ngarkesë të lartë operative, gjatë proceseve kritike të biznesit ose gjatë aktiviteteve të mirëmbajtjes së planifikuar mund të krijojë rrezik për ndërprerje të shërbimit, degradim të			

	performancës ose aktivizim të mekanizmave mbrojtës të sistemeve. Për këtë arsye, praktika evropiane bazohet në **koordinimin paraprak** ndërmjet autoritetit dhe operatorit për përcaktimin e kohës, shtrirjes, metodologjisë dhe masave teknike që garantojnë zhvillimin e testimit pa cenuar vazhdimësinë e shërbimeve. Ky koordinim nuk kufizon kompetencat e autoritetit, por përbën një garanci procedurale që siguron respektimin e parimit të proporcionalitetit dhe minimizon ndikimin operacional mbi subjektin privat. Nga ana tjetër, projektligji nuk			

	përcakton qartësisht: • kriteret objektive kur mund të kryhet simulimi; • nivelin e riskut që e justifikon atë; • metodologjinë teknike të testimit; • masat për mbrojtjen e vazhdimë sisë së shërbimit; • përgjegjësinë në rast dëmtimi të sistemit; • të drejtën e operatorit për të kundërshtuar ose kërkuar shtyrjen e testimit në raste të justifikuara. Mungesa e këtyre garancive cenon parimet e proporcionalitetit, sigurisë juridike dhe			

	parashikueshmëri së ndërhyrjes administrative. • **Propozimi i Vodafone** Për të siguruar harmonizimin me modelin e Bashkimit Evropian, propozohet që dispozita të riformulohet në mënyrë që: a) Autoriteti Kombëtar për Sigurinë Kibernetike të ketë kompetencën të kërkojë, autorizojë, koordinojë dhe mbikëqyrë kryerjen e simulimeve të sigurisë, ndërsa realizimi teknik i tyre të kryhet nga subjekte të pavarura dhe të certifikuara, sipas kritereve të përcaktuara me aktet nënligjore; b) Autoriteti të mund të kryejë vetë vetëm skanime proaktive jo-ndërhyrëse (**non-intrusive proactive**			

	scanning), në përputhje me nenin 11 të Direktivës (BE) 2022/2555; c) Çdo testim aktiv ose simulim në sistemet e operatorëve privatë të kryhet mbi bazën e një procedure të qartë ligjore dhe koordinimi paraprak me operatorin privat në lidhje me planifikimin dhe zhvillimin e çdo simulimi ose testimi të sigurisë, që të garantojë proporcionalitetin e ndërhyrjes, mbrojtjen e vazhdimësisë së shërbimeve, përgjegjësinë për dëmet e mundshme dhe respektimin e të drejtave procedurale të operatorit.			
Mbi marrjen e atributeve te Policisë	Projektligji parashikon në shkronjën "nj" të nenit 13 një kompetencë të	Vodafone Albania	Pranuar	Pas konsultimeve të zhvilluara dhe vlerësimit të çështjes, është dakordësuar që parashikimi për ushtrimin e atributeve të

Gjyqësore,	shtuar të AKSK si më poshtë: "Koordinon me Policinë e Shtetit dhe çdo institucion përgjegjës për të mundësuar mbledhjen dhe ruajtjen e provave si dhe hetimin teknik të incidentit kibernetik, kur dyshon për elementë të krimit kibernetik, apo veprave të tjera penale të lidhura me to e në infrastrukturat e informacionit, në rastet e kërkuara nga institucionet ligjzbatuese, duke gëzuar dhe atributet e Policisë Gjyqësore, në përputhje me Kodin e Procedurës Penale dhe ligjin për organizimin dhe funksionimin e Policisë Gjyqësore." Dispozita e propozuar kërkon rishikim për të garantuar			Policisë Gjyqësore të hiqet nga projektligji. Ky ndryshim synon të shmangë çdo paqartësi në lidhje me kompetencat institucionale dhe ndarjen e përgjegjësive ndërmjet institucioneve përkatëse.

	siguri juridike dhe përputhshmëri me Ligjin nr. 25/2019 "Për organizimin dhe funksionimin e Policisë Gjyqësore". Në formulimin aktual nuk përcaktohet: • së pari, cili departament, strukturë ose cilët nëpunës të Autoritetit do të ushtrojnë atributet e Policisë Gjyqësore, pasi këto atribute nuk mund t'i njihen institucionit në tërësi, por vetëm strukturave ose personave të caktuar sipas ligjit; • së dyti, nuk përcaktohet se cilat			

	janë konkretisht atributet e Policisë Gjyqësore që do të ushtrohen nga këto struktura apo nëpunës, duke lënë të paqartë shtrirjen e kompetencave të tyre. • **Propozimi i Vodafone Albania:** Rekomandohet që dispozita të specifikojë shprehimisht strukturën ose kategorinë e nëpunësve që do të ushtrojnë funksionet e Policisë Gjyqësore, si dhe të përcaktojë qartë kompetencat që u njihen, në përputhje me Kodin e Procedurës Penale dhe ligjin nr. 25/2019 "Për organizimin dhe funksionimin e			

	Policisë Gjyqësore”.			
Mbi zbatimin e masave për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabil iteteve	**Ndryshime në nenin 17 të ligjit nr. 25/2024 – Detyrimet e operatorëve të infrastrukturav e kritike dhe të rëndësishme të informacionit)** **• Përmbajtja e ndryshimit:** Neni 7 i projektligjit sjell dy ndryshime kryesore: a) riformulon shkronjën “ë”, duke detyruar operatorët të raportojnë çdo incident pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial dhe të bashkëpunojnë me këto struktura për koordinimin e veprimeve dhe rikuperimin nga incidentet; b) shton shkronjën “g”, sipas së cilës operatorët detyrohen të zbatojnë masat për bllokimin,	Vodafo ne Albania	Pranuar pjesërish t	Komenti pranohet pjesërisht lidhur me nevojën për të reflektuar në dispozitë parimin e realizueshmërisë teknike të masave të sigurisë të komunikuara nga Autoriteti. Në këtë kuadër, riformulimi synon të qartësojë se detyrimi i operatorëve për zbatimin e masave për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve të komunikuara nga Autoriteti, ushtrohet duke marrë parasysh mundësitë teknike të zbatimit të tyre në rrjetet dhe sistemet konkrete të informacionit. Megjithatë, nuk pranohet propozimi për të kushtëzuar në mënyrë të përgjithshme zbatimin e masave me vlerësimin subjektiv të operatorit mbi proporcionalitetin apo përshtatshmërinë e tyre, pasi këto masa komunikohen nga Autoriteti në bazë të vlerësimit të kërcënimeve, vulnerabiliteteve dhe riskut kibernetik të identifikuar.

	filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve , të komunikuara nga Autoriteti. Vodafone Albania mbështet bashkëpunimin operacional me Autoritetin Kombëtar për Sigurinë Kibernetike dhe shkëmbimin e informacionit për kërcënimet kibernetike, si elemente thelbësore për forcimin e sigurisë kibernetike. Megjithatë, dispozita e re e shkronjës "g" kërkon rishikim, pasi krijon një detyrim të përgjithshëm për zbatimin e masave teknike të komunikuara nga Autoriteti, pa përcaktuar kufijtë, kriteret			Gjithashtu, nuk vlerësohet e nevojshme parashikimi i një mekanizmi të posaçëm për miratim paraprak ose propozim masash alternative, pasi bashkëpunimi ndërmjet Autoritetit dhe operatorëve, përfshirë shkëmbimin e informacionit dhe koordinimin e veprimeve për adresimin e rreziqeve kibernetike, është i parashikuar në kuadrin ekzistues ligjor.

	dhe garancitë procedurale të ushtrimit të kësaj kompetence. Dispozitat përkatëse të Direktivës (BE) 2022/2555 (veçanërisht nenet 21, 23 dhe 32 të saj) parashikojnë se subjektet duhet të marrin masa teknike, operacionale dhe organizative të përshtatshme dhe proporcionale për të menaxhuar rreziqet që cenojnë sigurinë e rrjeteve dhe sistemeve të informacionit. Nga këto dispozita rezultojnë tre parime themelore të modelit të NIS2: • përgjegjësia për menaxhimin e riskut mbetet tek operatori; • masat e sigurisë duhet të jenë të përshtatsh			

	me dhe proporcionale; • përzgjedhja e masave duhet të bazohet në një vlerësim të riskut të kryer nga vetë operatori. Ndryshe nga projektligji, Direktiva nuk parashikon një kompetencë të përgjithshme të autoritetit kompetent për të imponuar masa teknike specifike që operatorët janë të detyruar t'i zbatojnë automatikisht. Dispozita e projektligjit krijon një detyrim automatik për zbatimin e masave të komunikuara nga Autoriteti, duke e kufizuar autonominë teknike të operatorit në përzgjedhjen e masave më të			

	përshtatshme për infrastrukturën që administron. Ky parashikim cenon parimin e proporcionalitetit të parashikuar në nenin 21 të Direktivës, i cili kërkon shprehimisht që masat e sigurisë të jenë "të përshtatshme dhe proporcionale". Ndërkohë dispozita e Projektligjit në shkronjën "g" të saj nuk parashikon që masat e komunikuara nga Autoriteti duhet të jenë: • proporcionale; • teknikisht të realizueshme; • të përshtatshme me nivelin konkret të riskut. **• Mungesa e një mekanizmi bashkëpunimi** Projektligji nuk parashikon asnjë			

	procedurë që i mundëson operatorit: • të argumentojë se një masë nuk është teknikisht e zbatueshme; • të propozojë masa alternative që arrijnë të njëjtin nivel mbrojtjeje; • të konsultohet me Autoritetin përpara vendosjes së masës; • formën në të cilën komunikohen IOC/IOA dhe vulnerabilitetet; • nëse komunikimi përbën rekomandim apo urdhër detyrues;			

	• afatet e zbatimit; • procedurën e verifikimit të zbatimit. Në sektorë kritikë, si komunikimet elektronike, energjia apo bankat, kjo mund të sjellë pasoja operative dhe të cenojë vazhdimësinë e shërbimeve. Si përfundim, edhe pse neni 5 i Direktivës u lejon shteteve anëtare të miratojnë masa që sigurojnë një nivel më të lartë të sigurisë kibernetike, këto masa duhet të respektojnë parimet e proporcionalitetit, domosdoshmërisë dhe sigurisë juridike. Për këtë arsye, rekomandohet riformulimi i dispozitës duke përfshirë kriteret e proporcionaliteti			

	t, realizueshmërisë teknike dhe menaxhimit të riskut, si dhe një mekanizëm konsultimi ndërmjet Autoritetit dhe operatorit. • **Propozimi i Vodafone Albania:** Propozohet që shkronja “g” të riformulohet si vijon: **g)** Veprojnë dhe, kur janë teknikisht të realizueshme, proporcionale dhe të përshtatshme me nivelin e riskut të identifikuar, zbatojnë masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve të komunikuara nga Autoriteti. Kur operatori vlerëson se masat e			

	komunikuara nuk janë teknikisht të realizueshme ose mund të cenojnë vazhdimësinë e shërbimeve, ai njofton pa vonesë Autoritetin dhe propozon masa alternative që sigurojnë një nivel të barasvlershëm mbrojtjeje.			
Regjistrimi i organeve të vlerësimit të konformitetit	**(Shtesa në nenin 20 të ligjit nr. 25/2024 – Regjistrimi i organeve të vlerësimit të konformitetit)** **• Përmbajtja e ndryshimit** Projektligji shton pikën 7 në nenin 20, me përmbajtjen: "Procedurat dhe kriteret për regjistrimin e organeve të vlerësimit të konformitetit për vlerësimin e masave të sigurisë kibernetike përcaktohen me udhëzimin e drejtorit të	Vodafone Albania	Refuzuar	Dispozita e propozuar nuk synon delegimin e përcaktimit të elementeve thelbësore të një veprimtarie të rregulluar, por krijimin e kuadrit procedural dhe teknik të nevojshëm për zbatimin e detyrimit të regjistrimit të organeve të vlerësimit të konformitetit pranë Autoritetit Kombëtar për Sigurinë Kibernetike. Përcaktimi i këtyre procedurave dhe kritereve nëpërmjet një udhëzimi të Drejtorit të Përgjithshëm të Autoritetit është i nevojshëm për të garantuar fleksibilitetin dhe përshtatjen e kërkesave teknike me zhvillimet në fushën e sigurisë kibernetike, standardet ndërkombëtare dhe

	përgjithshëm të Autoritetit.” Qëllimi i dispozitës është të autorizojë Drejtorin e Përgjithshëm të AKSK-së të miratojë procedurat dhe kriteret për regjistrimin e organeve të vlerësimit të konformitetit. • **Delegimi i kritereve me akt administrativ** Kjo dispozitë kërkon rishikim nga këndvështrimi i sigurisë juridike dhe hierarkisë së akteve normative. Projektligji i delegon Drejtorit të Përgjithshëm jo vetëm rregullimin e procedurave, por edhe përcaktimin e kritereve për regjistrimin e organeve të vlerësimit të konformitetit. Këto kritere nuk përbëjnë elemente thjesht			praktikat e vlerësimit të konformitetit. Kriteret për regjistrimin e këtyre organeve do të përcaktohen në përputhje me parashikimet e ligjit nr. 25/2024 “Për sigurinë kibernetike”, si dhe me kuadrin përkatës të standardizimit dhe akreditimit, duke garantuar që subjektet që kryejnë vlerësime të konformitetit të plotësojnë kërkesat e nevojshme për kompetencë teknike, pavarësi dhe paanshmëri. Gjithashtu, përcaktimi i procedurave të regjistrimit me akt të Drejtorit të Përgjithshëm nuk cenon parimin e sigurisë juridike, pasi ky akt do të miratohet në zbatim të autorizimit të shprehur ligjor dhe brenda kufijve të përcaktuar nga ligji. Për këto arsye, propozimi për përcaktimin e këtyre çështjeve me vendim të Këshillit të Ministrave nuk pranohet dhe dispozita mbetet e pandryshuar.

	procedurale apo teknike. Përkundrazi, ato përcaktojnë kushtet materiale për ushtrimin e një aktiviteti të rregulluar, duke ndikuar drejtpërdrejt në të drejtat dhe interesat e subjekteve private. Në praktikën e legjislacionit shqiptar dhe të BE-së, elementë të tillë zakonisht miratohen me vendim të Këshillit të Ministrave ose përcaktohen në vetë ligjin material, ndërsa aktet e drejtuesve të institucioneve përdoren për procedura zbatuese dhe implementimin e këtyre parashikimeve ligjore. Dispozita i njeh Drejtorit të Përgjithshëm kompetencën për të përcaktuar kriteret e regjistrimit, çka			

	nënkupton elemente thelbësore, si: • nëse organi duhet të jetë i akredituar; • standardet teknike që duhet të plotësojë; • kërkesat për personelin dhe kompetencën profesionale; • kushtet e pavarësisë dhe paanshmërisë; • rastet e refuzimit të regjistrimit. Për rrjedhojë, ato nuk mund të konsiderohen elemente thjesht teknike që mund të rregullohen me një udhëzim administrativ, dhe për rrjedhojë nuk ofron të njëjtin nivel garancish dhe kontrolli si një akt i Këshillit të Ministrave. • **Mungesa e garancive procedurale** Dispozita nuk parashikon			

	elemente minimale procedurale, si: • afatin për shqyrtimin e kërkesës për regjistrim; • të drejtën e ankimit në rast refuzimi; • rastet dhe procedurën e pezullimit ose çregjistrimit të organit të regjistruar. Mungesa e këtyre garancive cenon parimin e sigurisë juridike dhe krijon pasiguri për subjektet që ushtrojnë këtë veprimtari. • **Propozimi i Vodafone Albania:** Dispozita rekomandohet të rishikohet për të respektuar më mirë parimin e sigurisë juridike dhe të hierarkisë së akteve normative. Përcaktimi i kritereve thelbësore për regjistrimin dhe autorizimin e këtyre organeve			

	duhet të bëhet me vendim të Këshillit të Ministrave, ndërsa udhëzimi i Drejtorit të Përgjithshëm duhet të kufizohet në rregullimin e procedurave teknike të zbatimit. Për këtë arsye, rekomandojmë që me vendim të Këshillit të Ministrave të përcaktohet nëse organi duhet: • të jetë i akredituar; • të plotësojë standarde teknike; • të ketë personel të certifikuar; • të jetë i pavarur. Të parashikohen: • afatet për shqyrtimin e kërkesës; • të drejtën e ankimit në rast refuzimi; • kriteret e pezullimit ose çregjistrimit.			

	Këto janë garanci procedurale që duhet të parashikohen të paktën në nivelin e aktit të Këshillit të Ministrave, në mënyrë që të shmanget rreziku që kriteret thelbësore të ndryshojnë vetëm me një akt administrativ të brendshëm të Autoritetit, pa kontrollin dhe garancitë që ofron një akt i Këshillit të Ministrave.			
Komente mbi Nenin 9 të Projektligjit Vetëdeklarimi i masave të sigurisë kibernetike dhe vetëdeklarimi i hostimit dhe administri	**(Shtesa në nenin 20 të ligjit nr. 25/2024 – Shtimi i neneve 20/1 dhe 20/2 – Vetëdeklarimi i masave të sigurisë kibernetike dhe vetëdeklarimi i hostimit dhe administrimit të sistemeve)** **• Përmbajtja e ndryshimit** Neni 9 i projektligjit	Vodafone Albania	Pranuar pjesërisht	Dispozitat e propozuara nuk krijojnë një detyrim të pajustifikuar për operatorët, por vendosin një mekanizëm të nevojshëm për identifikimin, vlerësimin dhe monitorimin e nivelit të sigurisë kibernetike në nivel kombëtar. Vetëdeklarimi i masave të sigurisë kibernetike dhe i hostimit/administrimit të sistemeve synon t'i mundësojë Autoritetit një panoramë të përgjithshme mbi ekspozimin kibernetik

mit të sistemeve	parashikon detyrimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për të kryer vetëdeklarimin e masave të sigurisë kibernetike, si dhe vetëdeklarimin e hostimit dhe administrimit të sistemeve. Me këto parashikime, i ngarkohet Autoritetit kompetenca për administrimin dhe verifikimin e këtij procesi. Qëllimi i dispozitës është krijimi i një mekanizmi shtesë monitorimi për vlerësimin e nivelit të zbatimit të kërkesave të sigurisë kibernetike nga operatorët. Direktiva (BE) 2022/2555 nuk parashikon një detyrim të përgjithshëm për			të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, duke mbështetur një qasje të bazuar në risk dhe prioritizimin e masave mbrojtëse. Fakti që Direktiva (BE) 2022/2555 (NIS2) nuk parashikon një mekanizëm të tillë specifik nuk pengon miratimin e tij në nivel kombëtar, pasi neni 5 i saj u lejon shteteve anëtare të miratojnë masa shtesë që sigurojnë një nivel më të lartë të sigurisë kibernetike, për sa kohë që respektohen parimet e proporcionalitetit dhe sigurisë juridike. Informacioni që do të kërkohet në kuadër të vetëdeklarimit do të përcaktohet në mënyrë të detajuar me aktet nënligjore dhe do të kufizohet në të dhënat e nevojshme për ushtrimin e funksioneve ligjore të Autoritetit. Gjithashtu, trajtimi i informacionit do të bëhet në përputhje me legjislacionin në fuqi për mbrojtjen e informacionit dhe konfidencialitetin. Vetëdeklarimi nuk përbën një proces auditimi të dyfishtë dhe nuk zëvendëson apo përsërit detyrimet ekzistuese të operatorëve, por shërben si një instrument

	vetëdeklarimin e masave të sigurisë kibernetike. Përkundrazi, modeli i mbikëqyrjes i NIS2 mbështetet në: • detyrimin e subjekteve për të zbatuar masa të përshtatshme dhe proporcionale të menaxhimit të riskut (neni 21); • raportimin e incidenteve (neni 23); • kompetencat mbikëqyrëse të autoriteteve kompetente, përfshirë auditimet, inspektimet dhe kërkesën për informacion (neni 32). Megjithatë, neni 5 i Direktivës u njeh shteteve anëtare të drejtën të miratojnë masa që sigurojnë një nivel më të lartë të sigurisë kibernetike, për			administrativ për mbledhjen dhe analizimin e informacionit të nevojshëm për qëllime të mbikëqyrjes së sigurisë kibernetike. Duke marrë në konsideratë rëndësinë e garantimit të mbrojtjes së informacionit të administruar nga Autoriteti gjatë ushtrimit të funksioneve të tij ligjore, në projektligj është shtuar njëparashikim në dispozitat e ligjit 25/2024 që parashikon detyrimin për ruajtjen e konfidencialitetit të informacionit të marrë gjatë proceseve të kontrollit, mbikëqyrjes dhe vlerësimit të sigurisë kibernetike. Ky parashikim synon të garantojë që informacioni i siguruar nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, përfshirë të dhënat mbi organizimin, arkitekturën teknologjike dhe masat e sigurisë të zbatuara, të trajtohet në përputhje me kërkesat ligjore për mbrojtjen e informacionit sensitiv dhe të përdoret vetëm për qëllimet e ushtrimit të kompetencave të Autoritetit në fushën e sigurisë kibernetike. Në këtë kuadër, vlerësohet se shqetësimi i ngritur lidhur me garantimin e konfidencialitetit është

	sa kohë që ato janë proporcionale, të domosdoshme dhe në respektim të sigurisë juridike, garanci këto thelbësore të së drejtës së Bashkimit Evropian. **• Problematikat e identifikuara në dispozitën e projektligjit** **a. Mungesa e një vlerësimi të bazuar në risk** Dispozita nuk përcakton nëse vetëdeklarimi dhe deklarimi i hostimit, cloud-it dhe virtualizimit do të kërkohet nga të gjithë operatorët apo vetëm kur kjo është e nevojshme, bazuar në nivelin e riskut. Kjo përbën informacion teknik dhe operacional dhe kërkesa për një informacion të tillë duhet të jetë proporcionale dhe të bazohet në profilin e riskut të operatorit.			adresuar nëpërmjet plotësimit të kuadrit ligjor, pa cenuar nevojën e Autoritetit për të administruar informacionin e nevojshëm për përmbushjen e funksioneve të tij mbikëqyrëse.

	b. Shtrirja e informacionit që kërkohet të deklarohet Projektligji nuk përcakton qartë se çfarë informacioni duhet të deklarohet. Rekomandohet që operatorët të detyrohen të japin vetëm informacionin që është i nevojshëm për vlerësimin e riskut të sigurisë kibernetike. Në praktikë, kjo mund të çojë në kërkimin e informacionit shumë të detajuar mbi arkitekturën e sistemeve, konfigurimet teknike ose mjediset cloud, të cilat përbëjnë informacion të ndjeshëm nga pikëpamja e sigurisë. **c. Mbrojtja e informacionit konfidencial** Dispozita nuk parashikon se si do të mbrohet informacioni			

	teknik, operacional dhe tregtar që i dorëzohet Autoritetit. Rekomandohet të përcaktohet qartë se ky informacion do të përdoret vetëm për qëllime të mbikëqyrjes së sigurisë kibernetike dhe do të trajtohet si konfidencial. Kjo në përputhje me parashikimet e nenit 2(13) të NIS2 kërkon që shkëmbimi i informacionit të kufizohet në atë që është i nevojshëm dhe proporcional, duke ruajtur konfidencialiteti n dhe interesat tregtare të subjekteve. **d. Shmangia e dublikimit të detyrimeve** Operatorët janë tashmë subjekt i auditimeve, certifikimeve (si ISO/IEC 27001), raportimit të incidenteve dhe kërkesave të			

	tjera ligjore. Për këtë arsye, vetëdeklarimi nuk duhet të kthehet në një proces shtesë auditimi. Rekomandohet që Autoriteti të marrë në konsideratë dokumentacionin dhe certifikimet ekzistuese, për të shmangur përsëritjen e të njëjtave kërkesa dhe ngarkesën me një barrë administrative të panevojshme të operatorëve. • **Propozimi i Vodafone Albania:** Propozojmë rishikim të këtyre dispozitave pasi shkojnë përtej kërkesave të Direktivës dhe, në formën aktuale, nuk përmbajnë garanci të mjaftueshme për proporcionalitetin, mbikëqyrjen e bazuar në risk, kufizimin e informacionit të			

	kërkuar dhe mbrojtjen e konfidencialitetit.			
Komente mbi Nenin 10 të Projektligjit	**(Ndryshime në nenin 21 të ligjit nr. 25/2024 – Skema Kombëtare e Certifikimit të Sigurisë Kibernetike)** **• Përmbajtja e ndryshimit** Neni 10 ndryshon nenin 21 të ligjit nr. 25/2024 duke rregulluar elemente që lidhen me funksionimin e Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike, organet përgjegjëse dhe procedurat përkatëse. Gjithashtu, dispozita lidhet me autorizimin dhe regjistrimin e organeve të vlerësimit të konformitetit, të trajtuara edhe në nenet	Vodafone Albania	Refuzuar	Komenti nuk pranohet, pasi dispozita e propozuar është hartuar në përputhje me kuadrin evropian të certifikimit të sigurisë kibernetike dhe nuk synon krijimin e kërkesave të dyfishta apo të papajtueshme me skemat evropiane të certifikimit. Skema Kombëtare e Certifikimit të Sigurisë Kibernetike do të zbatohet duke marrë në konsideratë kuadrin evropian të certifikimit të sigurisë kibernetike dhe zhvillimet përkatëse në nivel të Bashkimit Evropian, në përputhje me parimet e Rregullores (BE) 2019/881 (Cybersecurity Act). Gjithashtu, krijimi i një skeme kombëtare certifikimi nuk përjashton njohjen apo marrjen në konsideratë të skemave evropiane të certifikimit, por synon të plotësojë nevojat kombëtare për kategori produktesh, shërbimesh ose procesesh TIK për të cilat nuk ekziston një skemë evropiane e harmonizuar. Për rrjedhojë, parashikimi i propozuar nga Vodafone

	paraprindëse të projektligjit. Në parim, dispozita është në përputhje me acquis, pasi Shqipëria mund të krijojë një skemë kombëtare certifikimi. Megjithatë, skema kombëtare duhet të jetë: • në përputhje me Kornizën Evropiane të Certifikimit; • e koordinuar me skemat evropiane të miratuara nga Komisioni Evropian; • të njohë certifikatat e lëshuara në shtete të tjera. **Propozimi i Vodafone Albania:** Propozojmë rishikimin e dispozitës në mënyrë që të mund të parashikohet se Skema Kombëtare e Certifikimit të Sigurisë Kibernetike merr			Albania konsiderohet i mbuluar nga kuadri ligjor ekzistues dhe nuk është e nevojshme të shtohet në dispozitë.

	në konsideratë edhe skemat evropiane të certifikimit të miratuara në nivel të Bashkimit Evropian. Në rast se për një kategori produktesh, shërbimesh ose proceseve TIK ekziston një skemë evropiane e certifikimit, zbatimi i skemës kombëtare nuk duhet të krijojë kërkesa të dyfishta ose të papajtueshme.			
Kundërvajtjet administrative	**(Ndryshime në nenin 44 të ligjit nr. 25/2024 – Kundërvajtjet administrative)** **• Përmbajtja e ndryshimit** Në nenin 44 “Kundërvajtjet administrative”, neni 15 i projektligjit zgjeron listën e kundërvajtjeve administrative dhe rrit ndjeshëm vlerën e sanksioneve në rast të	Vodafone Albania	Pranuar	Janë rishikuar dhe reflektuar në projektligj ndryshimet përkatëse lidhur me parashikimet për kundërvajtjet administrative dhe masat e gjobave.

	mosrespektimit nga ana e operatorëve të kërkesave të këtij ligji. Përkatësisht janë shtuar kundërvajtjet administrative si më poshtë: a) mosdorëzimi në afat i vetëdeklarimit të masave të sigurisë kibernetike; b) paraqitja e të dhënave të pasakta, të paplota ose të papërditësuara në vetëdeklarim; c) mosdeklarimi i mënyrës së hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit; c) moszbatimi i masave për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e IOC, IOA dhe vulnerabiliteteve të komunikuara nga Autoriteti. Dhe vlera e sanksioneve			

	administrative ndryshohet si më poshtë: Kur Autoriteti konstaton shkeljen e dispozitave, të cilat përbëjnë kundërvajtje administrative, sipas nenit 44 të këtij ligji vendos dënimin me gjobë si më poshtë: a) nga **1 000 000** deri në **10 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjat "a" dhe "d" të nenit 44 të këtij ligji; b) nga **2 000 000** deri në **4 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjat "b", "c", "ç", "e" të nenit 44 të këtij ligji; c) nga **4 000 000** deri në **10 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjat "dh", "h" të nenit 44 të këtij ligji;			

	ç) nga **2 000 000** deri në **5 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjën "ë" të nenit 44 të këtij ligji; d) **5 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjën "f" të nenit 44 të këtij ligji; dh) **3 000 000 lekë** në rast të shkeljeve administrative të përcaktuara në shkronjën "g" të nenit 44 të këtij ligji. Regjimi i sanksioneve administrative i parashikuar në nenet 44 dhe 45 nuk reflekton në mënyrë të plotë parimin e proporcionalitetit të kërkuar nga neni 36 i Direktivës (BE) 2022/2555. Në veçanti, disa shkelje me karakter thjesht administrativ, si mosdorëzimi në			

	afat i vetëdeklarimit ose deklarimi i pasaktë i informacionit, dënohen me gjoba të krahasueshme ose më të larta se shkelje që lidhen drejtpërdrejt me menaxhimin e riskut kibernetik dhe mbrojtjen e infrastrukturave kritike. Kjo krijon një disproporcion ndërmjet natyrës së shkeljes dhe masës së sanksionit. Në legjislacionin e BE-së (dhe në praktikën e Gjykatës së Drejtësisë së BE-së), një sistem sanksionesh duhet të respektojë parimin e proporcionalitetit, që do të thotë se masa e sanksionit duhet të jetë në raport me rëndësinë e shkeljes. Rrjedhojë edhe nga neni 36 i NIS2, sipas të cilit sanksionet			

	duhet të jenë efektive, proporcionale dhe parandaluese, ndërsa autoriteti duhet të marrë në konsideratë rrethanat e çdo rasti individual, përfshirë natyrën e shkeljes, kohëzgjatjen, dëmin e shkaktuar, bashkëpunimin e subjektit dhe masat korrigjuese të marra. **a) Sanksione jo proporcionale me shkeljen** Nëse analizojmë nenin 45 të projektligjit, rezulton një mospërputhje në proporcionalitetin e gjobave. **Projektligji parashikon:** **Shkelja** — **Gjoba** Mosdorëzimi i vetëdeklarimit (shkronja “f”) — 5 000 000 lekë Deklarimi i pasaktë — 3 000			

	ose i paplotë (shkronjat “g” dhe “gj”) 000 lekë Mosraportimi i incidenteve (shkronja “e”) 2 000 000 – 5 000 000 lekë Moszbatimi i IOC/IOA (shkronja “h”) 4 000 000 – 10 000 000 lekë Në pamje të parë duket logjike që moszbatimi i IOC/IOA dënohet më rëndë. Megjithatë, problemi qëndron tek vetëdeklarimi. Mosdorëzimi i vetëdeklarimit dënohet me **5 milionë lekë**, ndërkohë që: • vetëdeklarimi është një detyrim formal administrativ, i krijuar nga projektligji			

	dhe jo nga NIS2; • nuk nënkupton domosdoshmërisht se operatori nuk ka zbatuar masat e sigurisë; • nuk provon ekzistencën e një risku real për sigurinë kibernetike. Siç u analizua te neni 9, vetëdeklarimi është një mekanizëm kombëtar shtesë. Për rrjedhojë, sanksionimi i mosdorëzimit të tij duhet të jetë proporcional dhe të marrë parasysh: • nëse operatori është njoftuar; • nëse shkelja është formale apo materiale; • nëse ka shkaktuar cenim të sigurisë kibernetike. Në formën aktuale, dispozita nuk bën asnjë dallim.			

	• **Ndarja mes shkeljeve formale (administrative) dhe shkeljeve materiale** Projektligji nuk bën një dallim të qartë ndërmjet shkeljeve që kanë karakter formal ose procedural dhe atyre që kanë karakter material, pra që ndikojnë drejtpërdrejt në nivelin e sigurisë kibernetike të operatorëve ose në aftësinë e autoriteteve për të parandaluar dhe menaxhuar incidentet e sigurisë. Shkeljet formale janë ato që lidhen me përmbushjen e detyrimeve administrative ose deklarative, si p.sh.: • mosdorëzimi në afat i vetëdeklarimit të masave të sigurisë kibernetike; • deklarimi i të dhënave të			

	paplota ose të pasakta; • mosdeklarimi i të dhënave mbi hostimin ose administrimin e sistemeve. Këto shkelje, megjithëse mund të pengojnë ushtrimin efektiv të funksioneve mbikëqyrëse të Autoritetit, nuk krijojnë në vetvete një cenim të drejtpërdrejtë të sigurisë së rrjeteve dhe sistemeve të informacionit dhe as nuk provojnë automatikisht se operatori nuk ka zbatuar masat e nevojshme të sigurisë. Në të kundërt, shkeljet materiale lidhen me detyrime që përbëjnë thelbin e regjimit të sigurisë kibernetike të parashikuar nga Direktiva (BE) 2022/2555, si: • moszbatimi i masave të			

	menaxhimit të riskut; • mosraportimi i incidenteve të rëndësishme; • moszbatimi i masave të nevojshme për mbrojtjen e rrjeteve dhe sistemeve të informacionit; • mosbashkëpunimi në mënyrë efektive me autoritetet kompetente gjatë menaxhimit të incidenteve. Këto shkelje potencialisht krijojnë pasoja të drejtpërdrejta mbi disponueshmërinë, integritetin dhe konfidencialitetin e rrjeteve dhe sistemeve të informacionit, si dhe mbi vazhdimësinë e ofrimit të shërbimeve thelbësore ose të rëndësishme. Megjithatë, projektligji nuk vendos një diferencim të qartë në trajtimin			

	e këtyre dy kategorive të shkeljeve. Në disa raste, shkelje me karakter thjesht administrativ sanksionohen me gjoba të krahasueshme ose edhe më të larta se shkelje që mund të kenë ndikim real në sigurinë kibernetike. Për këtë arsye rekomandohet rishikimi i shkallëzimit të gjobave dhe krijimi i një sistemi të diferencuar që vendos sanksione më të rënda për shkeljet që prekin drejtpërdrejt sigurinë kibernetike dhe jo për mosrespektimin e detyrimeve formale administrative. **Propozimi i Vodafone Albania:** • Të shqyrtohet aplikimi i masave të			

	gjobave më të ulëta në proporcion me shkeljen dhe ndarjen e shkeljeve administrative nga ato materiale me impakt në sigurinë kibernetike. • Të vendosen mekanizma korrigjues për shkeljet formale. • Për shkeljet me karakter formal ose administrativ rekomandohet që projektligji të parashikojë një mekanizëm paraprak korrigjues përpara vendosjes së sanksionit administrativ. Për shkelje të tilla, si: a) mosdorëzimi në afat i vetëdeklarimit; b) paraqitja e të dhënave të paplota; c) mosdeklarimi i informacionit të kërkuar,			

	rekomandohet që ligji të parashikojë fillimisht nxjerrjen e një urdhri për korrigjimin e shkeljes, duke i lënë operatorit një afat të arsyeshëm për përmbushjen e detyrimit. Vendosja e gjobës duhet të aplikohet vetëm në rastet kur operatori nuk respekton urdhrin korrigjues brenda afatit të caktuar ose kur shkelja, për shkak të natyrës ose pasojave të saj, krijon një rrezik të menjëhershëm dhe serioz për sigurinë kibernetike.			
Grupi i Inteligjencës Kibernetike	AmCham Albania mbështet objektivat e projektligjit për forcimin e sigurisë kibernetike dhe harmonizimin e mëtejshëm të kuadrit ligjor	Dhoma Amerikane e Tregtisë	Refuzuar	Dispozita parashikon se rregullat e organizimit dhe funksionimit të Grupit të Bashkëpunimit për Inteligjencën Kibernetike, përfshirë procedurat e shkëmbimit të informacionit dhe mënyrën e koordinimit ndërinstitucional, do të

	shqiptar me acquis të Bashkimit Evropian, veçanërisht me Direktivën (BE) 2022/2555 (NIS2). Megjithatë, vlerësojmë se disa nga ndryshimet e propozuara kërkojnë rishikim të mëtejshëm për të garantuar proporcionalitetin, sigurinë juridike, neutralitetin teknologjik dhe një ndarje të qartë të funksioneve institucionale. Gjithashtu, konsiderojmë se projektligji duhet të shoqërohet me një analizë më të plotë të ndikimit mbi sektorin privat dhe me një dialog më të strukturuar me industrinë përpara miratimit të tij. Në këtë kuadër, bazuar në analizën e			përcaktohen me urdhër të Kryeministrit. Ky parashikim synon të garantojë një organizim të unifikuar dhe një mekanizëm të qartë bashkëpunimi ndërmjet institucioneve përkatëse, duke siguruar që shkëmbimi i informacionit të realizohet në përputhje me kuadrin ligjor në fuqi për mbrojtjen e informacionit, sigurinë dhe konfidencialitetin e të dhënave. Për rrjedhojë, nuk vlerësohet e nevojshme përfshirja në dispozitën ligjore e mekanizmave të detajuar, pasi këto elemente do të rregullohen në aktin nënligjor përkatës, sipas parashikimit të vetë dispozitës.

	projektaktit dhe në krahasimin e tij me dy aktet kryesore të Bashkimit Evropian në këtë fushë, Direktivën (BE) 2022/2555 (NIS2) dhe Rregulloren (BE) 2019/881 mbi ENISA-n dhe Certifikimin e Sigurisë Kibernetike ("Cybersecurity Act"), përcjellim vërejtjet kryesore si më poshtë: **1.** Krijimi i Grupit Ndërinstitucional të Inteligjencës Kibernetike (neni 11, që shton nenin 33/1) bashkon përfaqësues të institucioneve si: a) Autoriteti Kombëtar për Sigurinë Kibernetike; b) Ministria përgjegjëse për punët e jashtme; c) Ministria përgjegjëse për punët e brendshme;			

	ç) Shërbimi Informativ i Shtetit; d) Shtabi i Përgjithshëm i Forcave të Armatosura; dh) Agjencia e Inteligjencës dhe Sigurisë së Mbrojtjes, nën kryesimin e vetë Autoritetit. Funksionimi dhe organizimi lihet tërësisht tek një urdhër i Kryeministrit, pa asnjë referencë ndaj mekanizmash kontrolli apo garancive për mbrojtjen e të dhënave personale.			
Përqendrimi i funksioneve rregullatore, autorizuese, operacionale dhe sanksionuese te Autoriteti	Përqendrimi i funksioneve rregullatore, autorizuese, operacionale dhe sanksionuese te Autoriteti, pa asnjë ndarje të brendshme, bie ndesh me logjikën e nenit 58, paragrafi 4, i Rregullores (BE)	Dhoma Amerikane e Tregtisë	Refuzuar	Autoriteti Kombëtar për Sigurinë Kibernetike, në funksionin e tij si Autoritet Kombëtar i Certifikimit të Sigurisë Kibernetike, nuk lëshon certifikata të sigurisë kibernetike, siç është referuar në koment. Në kuadër të skemës kombëtare të certifikimit të sigurisë kibernetike, certifikatat lëshohen nga organet e vlerësimit të konformitetit, të cilat janë

	2019/881, i cili parashikon se: "Shtetet anëtare sigurojnë që veprimtaritë e autoriteteve kombëtare të certifikimit të sigurisë kibernetike, lidhur me lëshimin e certifikatave evropiane të sigurisë kibernetike, të jenë rreptësisht të ndara nga veprimtaritë e tyre mbikëqyrëse, dhe që këto veprimtari të kryhen në mënyrë të pavarur nga njëra-tjetra." Ky standard synon pikërisht shmangien e konfliktit të interesit që lind kur i njëjti institucion certifikon dhe njëkohësisht mbikëqyr e sanksionon të njëjtët subjekte. Projektligji shqiptar, përkundrazi, nuk parashikon asnjë			organizma të pavarur dhe ushtrojnë veprimtarinë e tyre në mënyrë të pavarur nga Autoriteti Kombëtar i Certifikimit të Sigurisë Kibernetike. Autoriteti ushtron funksionin e tij në lidhje me autorizimin dhe mbikëqyrjen e organeve të vlerësimit të konformitetit të sigurisë kibernetike, duke garantuar përmbushjen e kërkesave të përcaktuara në skemën kombëtare të certifikimit, por ruan pavarësi të plotë institucionale dhe funksionale nga këto organizma. Për rrjedhojë, nuk ekziston mbivendosje e kompetencave ndërmjet Autoritetit dhe organeve të vlerësimit të konformitetit, pasi roli i Autoritetit është rregullator, autorizues dhe mbikëqyrës, ndërsa veprimtaria e certifikimit kryhet nga organizma të pavarur të vlerësimit të konformitetit.

	kërkesë të ngjashme ndarjeje: Autoriteti mbetet njëkohësisht prokurues, autorizues i organeve të vlerësimit të konformitetit, administrues i skemës kombëtare të certifikimit, koordinator i Grupit të Inteligjencës Kibernetike, dhe autoritet sanksionues			
Mospërputhja mes akreditimit dhe autorizimit	Mospërputhja mes akreditimit dhe autorizimit, e krijuar nga neni 2 (shkronja "l") dhe neni 12 i projektaktit, lë të paqartë nëse akreditimi i pavarur i organeve të vlerësimit të konformitetit mbetet kusht paraprak, apo zëvendësohet tërësisht nga autorizimi i dhënë vetë nga Autoriteti.	Dhoma Amerikane e Tregtisë	Refuzuar	Projektligji synon të rregullojë dhe qartësojë dispozitën përkatëse që propozohet të ndryshohet, pa cenuar kërkesën për akreditimin e organeve të vlerësimit të konformitetit. Përkufizimi i organeve të vlerësimit të konformitetit për sigurinë kibernetike është i përcaktuar qartë që në ligjin nr. 25/2024 “Për sigurinë kibernetike”, ku parashikohet se këto organe janë persona juridikë kombëtarë ose ndërkombëtarë, të akredituar nga institucioni përgjegjës për akreditimin për kryerjen e vlerësimeve të konformitetit në fushën e sigurisë kibernetike.

				Gjithashtu, kërkesat lidhur me akreditimin dhe rolin e organeve të vlerësimit të konformitetit janë të përcaktuara edhe në kuadër të skemës kombëtare të certifikimit të sigurisë kibernetike. Në këtë kuadër, Autoriteti Kombëtar për Sigurinë Kibernetike, në zbatim të funksioneve të tij si Autoritet Kombëtar i Certifikimit të Sigurisë Kibernetike, autorizon organet e vlerësimit të konformitetit që plotësojnë kërkesat e përcaktuara në skemën kombëtare të certifikimit dhe ushtron mbikëqyrjen përkatëse mbi veprimtarinë e tyre. Ky autorizim nuk zëvendëson kërkesën për akreditim, por përbën një mekanizëm të veçantë kontrolli dhe mbikëqyrjeje në kuadër të administrimit të skemës kombëtare të certifikimit të sigurisë kibernetike.
Njohja e atributeve të Policisë Gjyqësore e CSIRT-it Kombëtar	Njohja e atributeve të Policisë Gjyqësore CSIRT-it Kombëtar (neni 4, shkronja "nj"), pa kufij të përcaktuar qartë, pa garanci procedurale	Dhoma Amerikane e Tregtisë	Panuar	Pas konsultimeve të zhvilluara dhe vlerësimit të çështjes, është dakordësuar që parashikimi për ushtrimin e atributeve të Policisë Gjyqësore të hiqet nga projektligji. Ky ndryshim synon të shmangë çdo paqartësi në lidhje me kompetencat institucionale dhe ndarjen

	shoqëruese dhe pa mekanizma të posaçëm mbikëqyrjeje, krijon paqartësi mes rolit teknik-rregullator dhe atij hetimor-penal të Autoritetit.			e përgjegjësive ndërmjet institucioneve përkatëse
Regjimi i ri i sanksioneve	Regjimi i ri i sanksioneve (neni 16) parashikon shuma gjobash fikse, të pavarura nga lloji i operatorit apo pesha e shkeljes, ndryshe nga praktika evropiane ku sanksionet shkallëzohen sipas kategorisë së subjektit (kritik/i rëndësishëm) dhe qarkullimit vjetor.	Dhoma Amerikane e Tregtisë	Panuar pjesërisht	Dispozita e propozuar lidhur me masat administrative është rishikuar dhe ripunuar në projektligj. Masat e gjobave nuk janë më të përcaktuara në vlera fikse, por parashikohen në intervale, duke mundësuar një vlerësim më të përshtatshëm të masës administrative në varësi të natyrës dhe rrethanave të shkeljes.
Vlerësimi i Ndikimit Rregullator	Relacioni nuk shoqërohet me një Vlerësim të Ndikimit Rregullator, as me ndonjë proces konsultimi të dokumentuar me sektorin privat,	Dhoma Amerikane e Tregtisë	Refuzuar	Vlerësimi i Ndikimit Rregullator (RIA) është hartuar nga Autoriteti Kombëtar për Sigurinë Kibernetike dhe është përcjellë për vlerësim pranë institucionit kompetent, në përputhje me kërkesat e kuadrit ligjor në fuqi për

	boshllëk që prek në veçanti vlerësimin e kostove për operatorët ekonomikë dhe barrën e re mbi njësitë e vetëqeverisjes vendore. Një çështje që meriton vëmendje është edhe raporti mes varësisë institucionale të Autoritetit dhe shkallës së përqendrimit të kompetencave të tij; kur një autoritet i mbajtur nën varësi ekzekutive merr njëkohësisht funksione rregullatore, certifikuese, operacionale dhe sanksionuese, siguria juridike dhe balanca institucionale kërkojnë garanci që sot mungojnë në projektligj, përfshirë kontroll mbi veprimtarinë e Grupit të Inteligjencës Kibernetike,			hartimin dhe vlerësimin e akteve rregullatore. Gjithashtu, projektligji është zhvilluar në përputhje me procedurat e konsultimit publik të parashikuara nga legjislacioni në fuqi, duke u mundësuar palëve të interesuara paraqitja e komenteve dhe propozimeve gjatë procesit të konsultimit. Për sa i përket organizimit institucional dhe ushtrimit të kompetencave nga Autoriteti, këto janë të përcaktuara në përputhje me kuadrin ligjor në fuqi dhe synojnë garantimin e një mekanizmi efektiv për mbikëqyrjen, koordinimin dhe forcimin e sigurisë kibernetike kombëtare.

	ndarje të qartë të brendshme mes funksionit të certifikimit dhe atij të mbikëqyrjes, si dhe një mekanizëm efektiv ankimi kundër vendimeve të Autoritetit.			
Kompetencat e AKSK	Projektligji i atribuon AKSK-së një numër të konsiderueshëm funksionesh, përfshirë: prokurues i përqendruar; autoritet autorizues për organet e konformitetit; administrues i skemës kombëtare të certifikimit; koordinator i Grupit të Inteligjencës Kibernetike; komunikues i masave detyruese; autoritet sanksionues. Ky përqendrim kompetencash mund të krijojë konflikt interesi	Dhoma Amerikane e Tregtisë	Refuzuar	Kompetencat e parashikuara për Autoritetin Kombëtar për Sigurinë Kibernetike janë funksione të përcaktuara në kuadrin ligjor në fuqi dhe janë të orientuara drejt garantimit të një qasjeje të koordinuar dhe efektive në menaxhimin e sigurisë kibernetike kombëtare. Ushtrimi i këtyre funksioneve realizohet në përputhje me parimet e ligjshmërisë, proporcionalitetit dhe paanshmërisë administrative, si dhe nëpërmjet strukturave dhe procedurave të brendshme organizative të Autoritetit, të cilat garantojnë ndarjen funksionale të përgjegjësive. Për sa i përket autorizimit dhe mbikëqyrjes së organeve të vlerësimit të konformitetit, si dhe administrimit të skemës

	dhe të ndikojë në pavarësinë e funksionit mbikëqyrës. Rekomandim Të rishikohet ndarja funksionale e kompetencave ose të parashikohet një mekanizëm i pavarur mbikëqyrjeje dhe ankimi.			kombëtare të certifikimit të sigurisë kibernetike, këto funksione ushtrohen në përputhje me rolin e Autoritetit si autoritet kompetent në këtë fushë, pa krijuar mbivendosje me veprimtarinë e organeve të pavarura të vlerësimit të konformitetit. Për këto arsye, propozimi për rishikimin e ndarjes së kompetencave ose krijimin e një mekanizmi të posaçëm mbikëqyrjeje nuk pranohet.
Siguria e Zinxhirit të Furnizimit	Siguria e Zinxhirit të Furnizimit Vërejtje Projektligji nuk adreson detyrimet mbi vlerësimin e riskut të furnizuesve dhe zinxhirit të furnizimit, ndonëse këto përbëjnë kërkesa të qarta të Direktivës NIS2. Dispozitat aktuale fokusohen kryesisht në: certifikimin; vetëdeklarimin; hostimin.	Dhoma Amerikane e Tregtisë	Refuzuar	Projektligji adreson kërkesat lidhur me menaxhimin e riskut dhe sigurinë e zinxhirit të furnizimit në përputhje me parashikimet e Direktivës (BE) 2022/2555 (NIS2), përmes detyrimeve të përcaktuara për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit lidhur me zbatimin e masave të sigurisë kibernetike. Vlerësimi i riskut të furnizuesve dhe i varësive nga palët e treta është pjesë e procesit të menaxhimit të riskut kibernetik dhe përfshihet në kërkesat për masat teknike dhe organizative që duhet të zbatohen nga subjektet përkatëse.

	Megjithatë mungon analiza mbi: pronësinë e furnizuesve; Ky është teksti që shihet në këtë faqe. Pika e fundit ("pronësinë e furnizuesve;") vazhdon në faqen pasuese, ndaj nuk është e plotë në këtë imazh. kontrollin; juridiksionin; praktikat e sigurisë së tyre. Rekomandim Të shtohet detyrimi për vlerësimin e riskut të furnizuesve dhe të zinxhirit të furnizimit, bazuar në kritere objektive sigurie.			Përcaktimi i kritereve të detajuara për vlerësimin e furnizuesve, përfshirë elemente të tilla si siguria e shërbimeve të ofruara, praktikat e sigurisë dhe menaxhimi i marrëdhënieve me palët e treta, do të trajtohet në aktet nënligjore dhe udhëzimet teknike përkatëse. Për këto arsye, propozimi për shtimin e një dispozite të veçantë në projektligj nuk pranohet.
Vetëdeklarimi	Procesi i vetëdeklarimit duhet të mbetet proporcional dhe i bazuar në analizën e riskut. Gjithashtu, të dhënat e deklaruara mbi	Dhoma Amerikane e Tregtisë	Pranuar pjesërisht	Sugjerimi është marrë në konsideratë vetëm lidhur me garantimin e konfidencialitetit të informacionit të administruar nga Autoriteti në kuadër të procesit të vetëdeklarimit.

	hostimin dhe infrastrukturën teknologjike përbëjnë informacion sensitiv. Rekomandim formularë standardë; konsultim me industrinë; garanci për konfidencialitetin; rregulla të qarta mbi ruajtjen dhe aksesin në të dhëna.			Në këtë kuadër, në projektligj është shtuar një parashikim që përcakton detyrimin për ruajtjen e konfidencialitetit të informacionit të marrë gjatë ushtrimit të funksioneve të kontrollit, mbikëqyrjes dhe vlerësimit të sigurisë kibernetike. Pjesët e tjera të propozimit lidhur me formularët standardë, konsultimin me industrinë dhe rregullat e detajuara për ruajtjen dhe aksesin në të dhëna nuk janë reflektuar në dispozitat e projektligjit, pasi këto çështje do të trajtohen në aktet nënligjore dhe procedurat përkatëse të zbatimit.
Hostimi dhe Cloud	Dispozitat nuk duhet të krijojnë kufizime të pajustifikuara për përdorimin e cloud-it ndërkombëtar. Vendndodhja gjeografike nuk duhet të jetë kriteri i vetëm. Rekomandim Qasja të mbetet technology-neutral dhe të bazohet në analizën e riskut të ofruesit të shërbimit.	Dhoma Amerikane e Tregtisë	Refuzuar	Dispozitat lidhur me hostimin dhe administrimin e sistemeve të informacionit nuk synojnë të kufizojnë përdorimin e shërbimeve cloud apo të përcaktojnë ndalime të bazuara vetëm në vendndodhjen gjeografike të ofruesit të shërbimit. Kërkesat e parashikuara synojnë garantimin e një niveli të përshtatshëm sigurie dhe rezilience për infrastrukturat kritike dhe të rëndësishme të informacionit, duke siguruar që Autoriteti të ketë informacionin e

				nevojshëm mbi mënyrën e hostimit, administrimit dhe varësitë teknologjike të sistemeve.
Masat detyruese të komunikimit, filtrimit dhe neutralizimit të IOC/IOA	Masat detyruese të komunikimit, filtrimit dhe neutralizimit të IOC/IOA nuk shoqërohen me: Teksti ndërpritet këtu dhe vazhdon në faqen pasuese. Nëse ma dërgon edhe faqen tjetër, do ta transkriptoj duke vazhduar nga fjalia "Masat detyruese të komunikimit, filtrimit dhe neutralizimit të IOC/IOA nuk shoqërohen me: • kritere proporcionaliteti; • afate; • procedura; • mekanizma ankimi. **Rekomandim** Të përcaktohen procedura të qarta dhe garanci procedurale.	Dhoma Amerikane e Tregtisë	Refuzuar	Masat lidhur me komunikimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve të identifikuara synojnë garantimin e një reagimi të shpejtë dhe efektiv ndaj kërcënimeve kibernetike që mund të cenojnë infrastrukturat kritike dhe të rëndësishme të informacionit. Zbatimi i këtyre masave do të kryhet në përputhje me parimet e proporcionalitetit dhe nevojës për mbrojtjen e sistemeve dhe shërbimeve kritike, ndërsa procedurat teknike dhe mënyra e komunikimit të këtyre masave do të përcaktohen në aktet dhe udhëzimet përkatëse të zbatimit.

Organet e Konformitetit	Projektligji kalon nga sistemi i akreditimit drejt autorizimit nga autoriteti përgjegjës. Ky ndryshim krijon paqartësi mbi marrëdhënien ndërmjet akreditimit të pavarur dhe autorizimit. Konkretisht, neni 2 i projektligjit (shkronja "l", që ndryshon nenin 9 të ligjit) parashikon se organet e vlerësimit të konformitetit autorizohen pasi janë akredituar nga institucioni përgjegjës për akreditimin, ndërsa neni 12 i projektligjit zëvendëson në nenin 39 të ligjit referencën ndaj organeve "të akredituara" me ato "të autorizuara nga autoriteti përgjegjës", duke krijuar paqartësi nëse	Dhoma Amerikane e Tregtisë	Refuzuar	Projektligji synon të rregullojë dhe qartësojë dispozitën përkatëse që propozohet të ndryshohet, pa cenuar kërkesën për akreditimin e organeve të vlerësimit të konformitetit. Përkufizimi i organeve të vlerësimit të konformitetit për sigurinë kibernetike është i përcaktuar qartë që në ligjin nr. 25/2024 “Për sigurinë kibernetike”, ku parashikohet se këto organe janë persona juridikë kombëtarë ose ndërkombëtarë, të akredituar nga institucioni përgjegjës për akreditimin për kryerjen e vlerësimeve të konformitetit në fushën e sigurisë kibernetike. Gjithashtu, kërkesat lidhur me akreditimin dhe rolin e organeve të vlerësimit të konformitetit janë të përcaktuara edhe në kuadër të skemës kombëtare të certifikimit të sigurisë kibernetike. Në këtë kuadër, Autoriteti Kombëtar për Sigurinë Kibernetike, në zbatim të funksioneve të tij si Autoritet Kombëtar i Certifikimit të Sigurisë Kibernetike, autorizon organet e vlerësimit të konformitetit që plotësojnë kërkesat e përcaktuara në skemën kombëtare të certifikimit dhe ushtron mbikëqyrjen përkatëse mbi

	autorizimi zëvendëson apo plotëson akreditimin. **Rekomandim** Të ruhet akreditimi si kusht bazë, ndërsa autorizimi të ketë rol plotësues.			veprimtarinë e tyre. Ky autorizim nuk zëvendëson kërkesën për akreditim, por përbën një mekanizëm të veçantë kontrolli dhe mbikëqyrjeje në kuadër të administrimit të skemës kombëtare të certifikimit të sigurisë kibernetike.
Delegimi në Aktet Nënligjore	Një numër i konsiderueshëm elementesh delegohen në VKM ose urdhra të Drejtorit të Përgjithshëm. **Rekomandim** Detyrimet kryesore që prekin operatorët ekonomikë të përcaktohen në ligj.	Dhoma Amerikane e Tregtisë	Refuzuar	Delegimi i disa elementeve në akte nënligjore është parashikuar me qëllim garantimin e zbatimit efektiv të dispozitave ligjore dhe përshtatjen e kërkesave teknike e procedurale me zhvillimet e vazhdueshme në fushën e sigurisë kibernetike. Projektligji përcakton në mënyrë të qartë detyrimet dhe parimet kryesore që duhet të zbatohen nga operatorët e infrastrukturave te informacionit ndërsa aktet nënligjore synojnë të përcaktojnë elementet teknike, procedurat dhe mënyrën e zbatimit të këtyre detyrimeve, brenda kufijve të autorizimit të parashikuar nga ligji.
Sanksionet	Regjimi i sanksioneve duhet të jetë proporcional dhe	Dhoma Amerikane e Tregtisë	Pranuar pjesërisht	Dispozita e propozuar lidhur me masat administrative është rishikuar dhe ripunuar në

	i bazuar në analizën e riskut. **Rekomandim** • periudhë korrigjimi për shkeljet formale; • periudhë tranzitore për subjektet e reja; • proporcionalitet.			projektligj. Masat e gjobave nuk janë më të përcaktuara në vlera fikse, por parashikohen në intervale, duke mundësuar një vlerësim më të përshtatshëm të masës administrative në varësi të natyrës dhe rrethanave të shkeljes.
Ndikimi mbi Vetëqeverisjen Vendore	Përfshirja e njësive të vetëqeverisjes vendore në sektorët me kritikalitet të lartë mund të krijojë barrë të konsiderueshme financiare dhe administrative. Ekziston gjithashtu rreziku që nevoja për përmbushje të menjëhershme të nxisë procedura të përshpejtuara prokurimi pa garantuar cilësinë e zgjidhjeve. **Rekomandim** Të parashikohet:	Dhoma Amerikane e Tregtisë	Refuzuar	Identifikimi i subjekteve si operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit nuk bëhet në mënyrë automatike, por do të realizohet në përputhje me metodologjinë për identifikimin e infrastrukturave të informacionit, të miratuar sipas kuadrit ligjor në fuqi. Në këtë proces do të vlerësohen kriteret përkatëse të kritikalitetit, nivelit të riskut dhe ndikimit të shërbimeve të ofruara, duke garantuar që detyrimet e përcaktuara në legjislacion t'u zbatohen vetëm subjekteve që plotësojnë kushtet e parashikuara. Për rrjedhojë, nuk vlerësohet e nevojshme parashikimi i një periudhe

	• periudhë tranzitore; • mbështetje teknike; • plan gradual implementimi.			të veçantë tranzitore, mbështetjes teknike apo një plani gradual implementimi në dispozitat e projektligjit.
Cilësia Legjislative	Projektligji përmban disa pasaktësi redaksionale dhe referenca të paplota. Rekomandim Të kryhet një rishikim teknik dhe gjuhësor përpara miratimit. Për lehtësi referimi, një listë e pasaktësive të identifikuara paraqitet në Shtojcën 1 të këtij dokumenti.	Dhoma Amerikane e Tregtisë	Pranuar	Projektligji, përpara miratimit, i nënshtrohet procesit të shqyrtimit dhe vlerësimit sipas procedurave të përcaktuara për hartimin dhe miratimin e akteve normative, duke kaluar nëpër disa nivele verifikimi dhe kontrolli institucional. Gjithashtu, institucionet përgjegjëse për shqyrtimin dhe miratimin e projektakteve kanë struktura dhe sektorë të dedikuar për kontrollin juridik, teknik dhe gjuhësor të tyre.
Lidhur me riformulimn e përkufizimit "CSIRT sektorial”, AKEP vlerëson se, krijimi i CSIRT për	Sektori i komunikimeve elektronike përbën një infrastrukturë kritike me karakteristika teknike specifike dhe me detyrime të veçanta. AKEP, si autoriteti rregullator i	AKEP	Refuzuar	CSIRT sektorial është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike për sektorin përkatës sipas anekseve të ligjit nr. 25/2024 “Për sigurinë kibernetike”. Ngritja e CSIRT-eve sektoriale do të realizohet nga Autoriteti Kombëtar për Sigurinë Kibernetike, institucioni përgjegjës për licencimin dhe

sektorin e komunikimeve elektronike duhet të mbetet tagër i AKEP.	sektorit, disponon kompetencat mbikëqyrëse, ekspertizën teknike dhe marrëdhëniet institucionale me operatorët e rrjeteve dhe shërbimeve të komunikimeve elektronike. Kufizimi i kompetencës për krijimin e CSIRT-ve sektoriale vetëm tek subjektet e listuara në dispozitë, kërkon përcaktim të qartë lidhur me koordinimin dhe shkëmbimin e informacionit, në mënyrë që operatorët subjekt i ligjit nr. 54/2024 të mos përballen me detyrime të dyfishta raportimi. Nëse riformulimi i përkufizimit të CSIRT sektorial do të ruhet në formën e propozuar në këtë projektligj, ky formulim			mbikëqyrjen e bankave dhe operatori qeveritar që menaxhon infrastruktura qeveritare dhe do të funksionojnë pranë ministrive përgjegjëse, institucionit rregullator për bankat, Autoritetit apo operatorit qeveritar që menaxhon infrastrukturat qeveritare. Lidhur me argumentin se CSIRT-i sektorial për sektorin e komunikimeve elektronike duhet të ngrihet pranë AKEP si autoriteti rregullator i sektorit që disponon kompetencat mbikëqyrëse, ekspertizën teknike dhe marrëdhëniet institucionale me operatorët e rrjeteve dhe shërbimeve të komunikimeve elektronike, sqarojmë se këto nuk përbëjnë kritere ligjore për përcaktimin e institucionit përgjegjës për ngritjen CSIRT-it sektorial. Autoriteti Kombëtar për Sigurinë Kiberneikte është institucioni që zotëron të gjithë ekspertizën e nevojshme në fushën e sigurisë kibernetike për të mundësuar funksionimin efektiv të CSIRT-eve sektoriale që ngrihen si pjesë e strukturës së tij. Formulimi sipas të cilit CSIRT-et sektoriale

	kërkon rishikim, pasi krijon përshtypjen se CSIRT-të sektoriale duhet të funksionojnë pranë autoriteteve ose institucioneve të sektorit përkatës. Duke qenë se ngrihen nga Autoriteti Kombëtar për Sigurinë Kibernetike, ushtrojnë funksionet e tyre në mënyrë të pavarur dhe aktiviteti i tyre koordinohet dhe raportohet pranë AKSK, vendosja e tyre organizative apo fizike pranë institucioneve sektoriale nuk përbën element thelbësor për përmbushjen efektive të detyrave funksionale. Në këto kushte, referimi në përkufizim ndaj funksionimit pranë institucioneve të sektorit përkatës, nuk sjell vlerë			funksionojnë pranë ministrive përgjegjëse, institucionit përgjegjës për mbikëqyrjen e bankave, Autoritetit apo operatorit qeveritar që administron infrastrukturat qeveritare, nuk përcakton varësi organizative apo institucionale, por tregon mënyrën e funksionimit dhe bashkëpunimit të këtyre strukturave me sektorin përkatës, me qëllim garantimin e koordinimit, shkëmbimin e informacionit dhe ofrimin e mbështetjes në nivel sektorial si dhe reagimin efektiv ndaj incidenteve të sigurisë kibernetike në bashkëpunim edhe me CSIRT-et pranë operatorëve dhe CSIRT-in Kombëtar sipas përcaktimeve të legjislacionit në fuqi për sigurinë kibernetike. Ky përkufizim nuk krijon detyrime të dyfishta për operatorët. Duhet theksuar se ligji nr. 25/2024 “Për sigurinë kibernetike”, i përafruar me Direktivën NIS 2, përcakton detyrimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për zbatimin e masave teknike, organizative dhe operacionale për menaxhimin e riskut të

	normative shtesë dhe mund të krijojë paqartësi lidhur me statusin organizativ dhe varësinë funksionale të CSIRT-ve sektoriale.			sigurisë kibernetike, me qëllim rritjen e nivelit të mbrojtjes dhe qëndrueshmërisë së sistemeve, rrjeteve dhe shërbimeve që ata administrojnë. Gjithashtu, sqarojmë se Direktiva (BE) 2022/2555 (Direktiva NIS2), me të cilën është përfaruar ligji nr. 25/2024 "Për sigurinë kibernetike" ka parashikuar se ofruesit e rrjeteve publike të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike i nënshtrohen mbikëqyrjes së autoritetit përgjegjës për sigurinë kibernetike sa i përket zbatimit të kërkesave të sigurisë kibernetike. Theksojmë se Direktiva NIS2 ka parashikuar ndryshime të rëndësishme në raport me kuadrin rregullator të komunikimeve elektronike, duke shfuqizuar nenet 40 dhe 41 të Direktivës (BE) 2018/1972 të Parlamentit Evropian dhe Këshillit, datë 11 dhjetor 2018, "Për krijimin e Kodit Evropian të Komunikimeve Elektronike". Për të shmangur çdo mbivendosje të mundshme apo detyrim të dyfishtë që mund të krijohet, vlerësohet se harmonizimi i mëtejshëm i

				kuadrit ligjor për komunikimet elektronike me ndryshimet e sjella nga kuadri evropian i NIS2 është një proces i nevojshëm, i cili duhet të realizohet në bashkëpunim ndërmjet autoriteteve përgjegjëse dhe subjekteve të sektorit. Ky harmonizim do të mundësojë një ndarje më të qartë të kompetencave ndërmjet autoriteteve, duke shmangur vendosjen e detyrimeve të dyfishta për ofruesit e komunikimeve elektronike lidhur me zbatimin dhe raportimin e masave të sigurisë për rrjetet dhe sistemet e tyre.
Lidhur me shtimin e pikës "ll", në nenin 13, që përcakton detyrat dhe përgjegjësitë e CSIRT-it Kombëtar	"Kryen simulime në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit, duke shfrytëzuar vulnerabilitetet e evidentuara nëpërmjet skanimeve proaktive sipas shkronjës "g" të këtij neni, duke njoftuar paraprakisht operatorët. Procedura e simulimit	AKEP	Refuzuar	Kryerja e simulimeve në rrjetet dhe sistemet e infrastrukturave kritike dhe të rëndësishme të informacionit është një kompetencë që Autoriteti Kombëtar për Sigurinë Kibernetike e ka aktualisht të parashikuar në nenin 13, shkronja ll, të ligjit nr. 25/2024 "Për sigurinë kibernetike" dhe synon vlerësimin e ekspozimit ndaj risqeve kibernetike duke u bazuar në vulnerabilitetet e evidentuara përmes skanimeve proaktive dhe marrjen e masave për forcimin e sigurisë kibernetike të operatorëve

	miratohet me urdhër të drejtorit të përgjithshëm të Autoritetit;".AKEP vlerëson se ky proces kërkon dakordësi paraprake me operatorin përkatës dhe duke njoftuar paraprakisht AKEP, si organ rregullator në fushën e komunikimeve elektronike dhe i ngarkuar me ligj për monitorimin e sigurimit të rrjeteve të komunikimeve elektronike.			të infrastrukturave kritike dhe të rëndësishme të informacionit. Siç parashikohet edhe në ligjin nr. 25/2024 “Për sigurinë kibernetike”, Autoriteti në këtë rast e njofton paraprakisht operatorin përkatës për kryerjen e simulimeve. Ndërsa lidhur me kërkesën për marrjen e dakordësisë paraprake nga operatori, vijon të mbetet siç ka qenë dhe në ligjin nr. 25/2024 “Për sigurinë kibernetike”, i përafruar me Direktivën NIS2, i cili nuk e parashikon një detyrim të tillë. Shtimi i një detyrimi të tillë do të krijonte një hap shtesë procedural të panevojshëm që do të cenonte si rrjedhojë efektivitetin operacional të CSIRT-it Kombëtar në ushtrimin e funksioneve të tij. Për më tepër, simulimi realizohet mbi bazën e një procedure të miratuar nga drejtori i përgjithshëm i Autoritetit, duke garantuar transparencën dhe besueshmërinë e procesit.
Lidhur me shtimin e nenit 20/1 "Vetëdeklarimi i masave të	AKEP vlerëson se dispozita e propozuar për vetëdeklarimin e masave të sigurisë kibernetike, krijon rrezik për mbivendosje të	AKEP	Refuzuar	Argumenti i paraqitur nga AKEP mbështetet në nenet 54 “Siguria e rrjeteve dhe shërbimeve” dhe 56 "Implementimi dhe detyrimi” të ligjit nr. 54/2024 “Për komunikimet elektronike në Republikën e Shqipërisë", për të cilat

sigurisë kibernetike"	detyrimeve ligjore dhe kompetencave mbikëqyrëse ndaj ofruesve të rrjeteve publike të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike të disponueshme për publikun. Konkretisht, ligji nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë", në nenet 54 dhe 56 të tij, parashikon tashmë detyrimin e këtyre subjekteve për të marrë masa të përshtatshme teknike, organizative dhe proporcionale për garantimin e sigurisë së rrjeteve dhe shërbimeve, si dhe ngarkon AKEP me kompetenca për monitorimin dhe mbikëqyrjen e zbatimit të këtyre detyrimeve. Në ushtrim të këtyre kompetencave, AKEP ka të			duhet theksuar se janë transpozime të nenit 40 “Security of netëorks and services” dhe nenit 41 “Implementation and enforcement” respektivisht, të Direktivës (BE) 2018/1972 për krijimin e Kodit Evropian të Komunikimeve Elektronike (EECC). Në lidhje me këtë, sqarojmë se dispozitat e sipërcituara të Direktivës (BE) 2018/1972 janë shfuqizuar nga Direktiva (BE) 2022/2555 (Direktiva NIS2), ndryshim i cili është reflektuar duke i hequr këto nene nga versioni i konsoliduar i Direktivës (BE) 2018/1972 i datës 18.10.2024.Për reference, linku i versionit të konsoliduar të Direktivës (BE) 2018/1972: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02018L1972-20241018Bashkimi Evropian e ka përcaktuar rregullimin e kërkesave për sigurinë kibernetike të ofruesve të rrjeteve publike të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike në kuadrin rregullator të Direktivës NIS2, ku këto subjekte përfshihen në fushën e zbatimit të kësaj Direktive, pavarësisht madhësisë së

	drejtë të kërkojë informacion, dokumentacion dhe evidenca për verifikimin e masave të zbatuara nga operatorët. Në këto kushte, vendosja e një detyrimi të përgjithshëm për vetëdeklarim pranë Autoritetit të Sigurisë Kibernetike, pa përcaktuar marrëdhënien me kompetencat sektoriale të AKEP, mund të çojë në raportim të dyfishtë të të njëjtit informacion dhe paqartësi lidhur me autoritetin përgjegjës për kontrollin dhe verifikimin e përmbushjes së detyrimeve në sektorin e komunikimeve elektronike. Duke qenë se ligji nr. 54/2024 përbën kuadrin sektorial që ka transpozuar dispozitat e Kodit Evropian të			tyre, dhe rrjedhimisht i nënshtrohen mbikëqyrjes së autoritetit përgjegjës për sigurinë kibernetike sa i përket zbatimit të këtyre kërkesave.Ligji nr. 25/2024 "Për sigurinë kibernetike", i cili transpozon Direktivën NIS2, ka përcaktuar Autoritetin Kombëtar për Sigurinë Kibernetike si autoritetin përgjegjës për zbatimin dhe mbikëqyrjen e këtij ligji. Për rrjedhojë, AKSK ushtron kompetenca që burojnë drejtpërdrejt nga legjislacioni në fuqi për sigurinë kibernetike me dhe nuk mund të kufizojë apo të heqë dorë nga këto kompetenca nëpërmjet ndryshimeve të reja ligjore në projektligjin e propozuar. Në këtë kontekst, për Autoritetin, detyrimi për vetëdeklarimin e masave të sigurisë kibernetike është një instrument për ushtrimin e kompetencave mbikëqyrëse të sigurisë kibernetike që i janë ngarkuar me ligj.Mbivendosja e kompetencave e pretenduar nga AKEP nuk buron nga shtimi i nenit 20/1 "Vetëdeklarimi i masave të sigurisë kibernetike", por nga fakti që ligji nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë" nuk ka

	Komunikimeve Elektronike (Direktiva (BE) 2018/1972) në fushën e sigurisë së rrjeteve dhe shërbimeve të komunikimeve elektronike, konsiderohet e nevojshme që kjo dispozitë, të saktësojë se detyrimi i vetëdeklarimit nuk cenon kompetencat e autoriteteve sektoriale dhe nuk krijon detyrime të dyfishta për subjektet që i nënshtrohen një regjimi të posaçëm mbikëqyrjeje. Mbajtur parasysh sa më sipër, propozojmë shtimin e një paragrafi në fund të pikës 1 të këtij neni, me përmbajtje: "Për operatorët e rrjeteve dhe ofruesit e shërbimeve të komunikimeve elektronike të disponueshme për publikun,			reflektuar ende ndryshimet që kanë ndodhur në Direktivën (BE) 2018/1972, ku janë shfuqizuar nenet 40 dhe 41 si rezultat i amendimit të kësaj Direktive nga Direktiva NIS2. Për rrjedhojë, nevoja për shmangien e mbivendosjeve duhet të adresohet përmes harmonizimit të legjislacionit sektorial në fushën e komunikimeve elektronike me acquis-in e përditësuar përkatëse të Bashkimit Evropian. Për sa më sipër, nuk vlerësohet i nevojshëm shtimi i paragrafit të propozuar nga AKEP.

	administrimi i vetëdeklarimit realizohet në koordinim me AKEP, duke shmangur kërkimin dhe raportimin e dyfishtë të të njëjtit informacion".			
Lidhur me shtimin e nenit 20/2 "Vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit",	**Lidhur me shtimin e nenit 20/2 "Vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit"**, AKEP vlerëson se dispozita nuk përmban garanci lidhur me trajtimin dhe mbrojtjen e informacionit që deklarohet nga operatorët, mbajtur parasysh që të dhënat e kërkuara përmbajnë informacion me karakter konfidencial, publikimi ose aksesimi i paautorizuar i të	AKEP	Refuzuar	Dispozita e shtuar në projektligj 20/2 "Vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit" ka për objekt përcaktimin e detyrimit të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për vetëdeklarimin e informacionit mbi hostimin dhe administrimin e sistemeve, rrjeteve dhe infrastrukturës së informacionit, në funksion të ushtrimit të kompetencave mbikëqyrëse të Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK) me qëllim forcimin e nivelit të sigurisë kibernetike në përputhje me kërkesat e legjislacionit në fuqi. Detyrimi i AKSK për të garantuar konfidencialitetin,

	cilit mund të cenojë sigurinë e sistemeve dhe infrastrukturave kritike të informacionit. Mungesa e këtyre garancive krijon pasiguri juridike për subjektet e detyruara dhe mund të rrisë ekspozimin ndaj rreziqeve të sigurisë kibernetike. Në këto kushte, propozojmë shtimin e një paragrafi me përmbajtje: "Autoriteti merr masat e nevojshme teknike, organizative dhe ligjore për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së këtij informacioni, si dhe kufizon aksesin në të vetëm për personat e autorizuar, në përputhje me legjislacionin në fuqi".			integritetin dhe disponueshmërinë e informacionit që administron, si dhe për të kufizuar aksesin vetëm për personat e autorizuar, buron drejtpërdrejt nga legjislacioni në fuqi për sigurinë kibernetike, mbrojtjen e të dhënave personale, si dhe nga detyrimet ligjore që lidhen me trajtimin e informacionit të klasifikuar, sipas rastit. Konkretisht, në zbatim të ligjit nr. 25/2024 "Për sigurinë kibernetike", për të kryer funksionin e tij mbikëqyrës, AKSK mund të mbledhë të dhëna, dokumente dhe informacionin e nevojshëm nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe ka detyrim ligjor garantimin e mbrojtjes së këtij informacioni. Për rrjedhojë, garancitë për trajtimin dhe mbrojtjen e informacionit që deklarohet nga operatorët ekzistojnë tashmë në kuadrin ligjor në fuqi dhe rrjedhimisht nuk vlerësohet i nevojshëm shtimi i një paragrafi të ri të propozuar nga AKEP në nenin 20/2 "Vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit".

Lidhur me ndryshimet në nenin 45, dhe vlerat e sanksioneve me gjobë të propozuara.	AKEP vlerëson se rritja e vlerave të gjobave të propozuara në nenin 45 është e konsiderueshme në raport me regjimin aktual sanksionues dhe nuk shoqërohet me një argumentim apo analizë të mjaftueshme që të justifikojë këtë rritje, pasi ekziston rreziku që nivelet e sanksioneve me gjobë, të rezultojnë joproporcionale me natyrën dhe rëndësinë e shkeljeve administrative. Gjithashtu, relacioni shoqërues i projektligjit nuk përmban një analizë krahasimore ndërmjet regjimit aktual dhe atij të propozuar të gjobave, si dhe arsyet konkrete që justifikojnë rritjen e ndjeshme të tyre, në mënyrë që të	AKEP	Refuzuar	Rishikimi i niveleve të gjobave të parashikuara në nenin 45, të projektligjit është i lidhur me nevojën për të garantuar efektivitetin e kuadrit sanksionues në fushën e sigurisë kibernetike dhe për të siguruar që masat administrative të jenë proporcionale me rëndësinë e interesit të mbrojtur. Shkeljet e detyrimeve të sigurisë kibernetike mund të sjellin pasoja të konsiderueshme për funksionimin e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe për vazhdimësinë e shërbimeve me rëndësi publike. Dëmi potencial që mund të shkaktohet nga moszbatimi i masave teknike, organizative dhe operacionale mund të jetë shumë herë më i lartë se vlera e sanksioneve të parashikuara, duke justifikuar nevojën për një regjim sanksionues efektiv dhe parandalues.Rritja e niveleve të gjobave nuk përbën një masë automatike ndëshkuese, por synon të sigurojë proporcionalitet ndërmjet natyrës së shkeljes, nivelit të rrezikut të krijuar dhe nevojës për respektimin e detyrimeve ligjore.

	vlerësohet nëse kjo ndërhyrje është e nevojshme dhe proporcionale për arritjen e objektivave të ligjit.			
Propozim për ndryshimin e nenit 33, pika 3, shkronja b)	Në kuadër të bashkëpunimit ndërinstitucional ndërmjet Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK) dhe Autoritetit Kombëtar për Sigurinë e Informacionit të Klasifikuar, si dhe me qëllim forcimin dhe qartësimin e mekanizmave të bashkëpunimit në rastet e kërcënimeve dhe incidenteve kibernetike që mund të prekin rrjetet dhe sistemet e klasifikuara AKSIK propozon shqyrtimin e mundësisë për ndryshimin dhe plotësimin e	AKSIK	Refuzuar	Ligji nr. 25/2024 "Për sigurinë kibernetike" në nenin 33, pika 3, shkronja b) parashikon detyrimin e Autoritetit Kombëtar për Sigurinë Kibernetike për të bashkëpunuar me institucionin përgjegjës për sigurinë e informacionit të klasifikuar në rastet kur merr dijeni për kërcënime të mundshme në rrjetet e klasifikuara, të infrastrukturave të informacionit, objekt i këtij ligji. Kjo dispozitë garanton bashkëpunimin institucional që realizohet në përputhje me kompetencat ligjore të institucioneve përkatëse dhe legjislacionin në fuqi. Për rrjedhojë, nuk vlerësohet e nevojshme ndërhyrja apo ndryshimi i saj, pasi qëllimi i propozuar është tashmë i reflektuar në kuadrin ligjor ekzistues.

	dispozitës përkatëse të ligjit nr. 25/2024 "Për sigurinë kibernetike". Dispozita aktuale konkretisht pika 3, shkronja b), neni 33, parashikon detyrimin e AKSK-së që të bashkëpunojë me institucionin përgjegjës për sigurinë e informacionit të klasifikuar, ne rastet kur merr dijeni për kërcënime të mundshme në rrjetet e klasifikuara të infrastrukturave të informacionit, objekt i këtij ligji Vlerësojmë se, për shkak të natyrës së veçantë të rrjeteve dhe sistemeve që trajtojnë informacion të klasifikuar, si dhe të nevojës për një ndarje të qartë të përgjegjësive dhe kompetencave			

	ndërmjet institucioneve përgjegjëse për sigurinë kibernetike dhe sigurinë e informacionit të klasifikuar, kjo dispozitë mund të plotësohet me elemente që përcaktojnë me qartë mënyrën e bashkëpunimit dhe mbështetjes institucionale në rastet e kërcënimeve ose incidenteve kibernetike. Në këtë kuadër, propozojmë që dispozita të riformulohet si më poshtë: "Me kërkesë të institucionit përgjegjës për sigurinë e informacionit te klasifikuar, bashkëpunon dhe ofron mbështetje teknike dhe ekspertizë në fushën e sigurisë kibernetike, ne rastet e kërcënimeve ose incidenteve kibernetike që prekin ose mund			

	te prekin rrjetet dhe sistemet e klasifikuara, brenda fushës së kompetencave të saj dhe në përputhje me legjislacionin në fuqi Propozimi synon të qartësojë ofrimin e mbështetjes teknike dhe ekspertizës në fushën sigurisë kibernetike, me kërkesë të AKSIK për sigurinë e informacionit të klasifikuar në rastet e kërcënimeve ose incidenteve kibernetike. Në këtë drejtim, vlerësojmë se një përcaktim më i qartë i këtij mekanizmi në kuadrin ligjor do të kontribuonte në forcimin e koordinimit institucional, në përmirësimin e reagimit ndaj kërcënimeve dhe incidenteve kibernetike dhe në garantimin e një qasjeje të			

	koordinuar mbrojtjen e rrjeteve dhe sistemeve që trajtojnë informacion të klasifikuar. Për sa më sipër, lutemi që propozimi i mësipërm të merret në konsideratë nga ana e Autoriteti Kombëtar për Sigurinë Kibernetike dhe të vlerësohet mundësia e përfshirjes së tij në kuadër te ndryshimeve dhe plotësimeve te ardhshme të ligjit nr. 25/2024 "Për sigurinë kibernetike".			