ZAKON BR. 03/L- 166

O SPREČAVANJU I SUZBIJANJU KIBERNETIČNOG ZLOČINA

Skupština Republike Kosovo;

Na osnovu člana 65 (1) Ustava Republike Kosova,

Usvaja

ZAKONA O SPREČAVANJU I SUZBIJANJU KIBERNETIČNOG ZLOČINA

Član 1
Cilj

Ovaj zakona ima za cilj sprečavanje i suzbijanje kibernetičnog zločina konkretnim merama, sprečavanje, otkrivanje i sankcionisanje kršenja preko kompjuterskih sistema, obezneđujući poštovanje prava čoveka i zaštitu ličnih podataka.

Član 2
Delokrug

Ovej zakon se primenjuje na teritoriji Republike Kosovo u delatnostima kompjuterskih sistema. Primenjuje se u celosti u čuvanju kompjuterskih sistema, te sankcioniše metode i procedure kako i ko može ove podatke koristiti.

Član 3
Definicije

1. Izrazi upotrebljeni u ovom zakonu imaju sledeće značenje:

1.1. **Kibernetikčki kriminal -** kriminalna aktivnost počinjena preko ili u kompjuterskoj mreži, koja ima za cilj izvršenje kriminala, zloupotrebu kompjuterskih sistema i kompjuterskih podataka.

1.2**. Kompjuterski sistem -** bilo koje sredstvo ili montiranje sredstava veze ili koje su u operativnoj vezi, od kojih jedno ili više njih pružaju automatske podatke koje se procesuiraju preko kompjuterskih programa.

1.3. A**utomatsko procesuiranje podataka -** proces preko kojeg se podaci u kompjuterskom sistemu procesuiraju pomoću kompjuterskih programa.

1.4. **Kompjuterski program -** niz uputstava koje se mogu primeniti preko kompjuterskog sistema u cilju dobijanja određenih rezultata.

1.5. **Kompjuterski podaci** - svako predstavljanje činjenica, informacija ili koncepcija u formi koja može da ae procesuira kompjuterskim sistemima. Ova kategorija obuhvata sve kompjuterske programe koji mogu pokretati kompjuterske sisteme da vrše određene funkcije.

1.6. **Ponuđivač usluga** - svako fizičko ili pravno lice korisnicima pruža mogućnost komuniciranja pomoću kompjuterskog sistema, kao i lice, koje procesuira ili prikuplja podatke za ove ponuđače usluga i za korisnike usluga pruženih od njih.

1.7. **Podaci o saobraćaju podataka-** kompjuterski podaci koji se odnose na komuniciranje koje se vrši preko kompjuterskog sistema i njegovih proizvoda, predstavljajući deo lanca komuniciranja, prikazujući poreklo komuniciranja, namenu, liniju, vreme, datum, veličinu, obim i trajanje, kao i vrstu korišćene usluge za komuniciranje.

1.8. **Podaci o korisnicima -** svaka informacija koja može dovesti do identifikacije korisnika, uključujući vrstu komuniciranja i korišćenu uslugu, poštansku adresu, geografsku adresu, adresu IP-a, telefonske brojeve ili bilo koji drugi broj pristupa i sredstva plaćanja za odgovarajuću uslugu, kao i bilo koji drugi podatak koji može dovesti do identifikacije korisnika.

1.9. **Mere sigurnosti -** korišćenje određenih procedura, sredstava ili specijalizovanih kompjuterskih programa pomoću kojih je pristup u kompjuterskom sistemu ograničen ili zabranjen za određene kategorije korisnika.

1.10**. Pornografski materijal sa maloletnicima -** svaki materijal koji predstavlja maloletnika ili odraslu osobu preobraženu u maloletnika sa izrazito seksualnim ponašanjem ili izgledom, koji iako ne predstavlja realan lik, originalno simulira maloletnika, sa izrazito seksualnim ponašanjem.

1.11. **Intercepcija –** nezakonito presretanje ili hvatanje podataka od strane neovlašenih lica.

Clan 4
Neovlašćene radnje

1. Prema ovom zakonu postupci lica ocenjuju se neovlašćenim postupcima, ako lice:

1.1. nije ovlašćeno prema zakonu ili ugovoru;

1.2. prekoračuje ovlašćenja;

1.3. nema odobrenje nadležnog i kvalifikovanog lica za zakonsko korišćeje, upravljanje ili kontrolu kompjuterskog sistema ili obavljanje naučnog istraživanja u kompjuterskom sistemu.

Član 5
Prevencija, zaštita i informativne kampanje

1. Radi zaštite i sigurnosti kompjuterskih sistema i ličnih podataka, vlasti i javne institucije, nadležne za ovu oblast, ponuđivači usluga, nevladine organizacije i predstavnici civilnog društva izvode aktivnosti i programe za sprečavanje kompjuterskog kriminala.

2. Vlasti i javne institucije, nadležne za ovu oblast, u saradnji sa ponuđačima usluga i nevladinim organizacijama, te ostalim predstavnicima civilnog društva unapređuju politike, prakse, mere, procedure i minimalne standarde za zaštitu kompjuterskih sistema.

3. Vlasti i javne institucije, nadležne za ovu oblast, u saradnji sa ponuđivačima usluga, nevladinim organizacijama i predstavnicima civilnog društva organizuju informativne kampanje o kompjuterskom kriminalu i ugrožavanju korisnika kompjuterskih sistema.

Član 6
Vođenje, ažuriranje i korišćenje baze podataka

1.Ministarstvo pravde, u saradnji sa Ministarstvom unutrašnjih poslova, održavaju i stalo ažuriraju bazu podataka o kopmjuterskom kriminalu.

2. Ministarstvo za transport i post-telekomunikacije, Obaveštajna služba Kosova i druge relevantne institucije mogu koristiti bazu podataka u skladu sa pravilima i procedurama posednika baze podataka.

3. Nacionalni institut za kriminalistiku obavlja periodična izučavaja radi identifikacije uzročnika i uslova koji determiniraju i podstiču kompjuteski kriminal.

Član 7
Specijalni programi i obuke

Ministarstvo pravde, Ministarstvo unutrašnjih poslova, Ministarstvo za transport i telekomunikacije, Ministarstvo javnih službi i Obaveštaja služa Kosova, u skladu sa njihovim nadležnosti, izvode specijalne programe za obuku personala u cilju sprečavanja i suzbijanja kompjuterskog kriminala .

Član 8
Obaveze vlasnika i administratora

1. Za jednu kategoriju kompjuterskih sistema, u kojem pristup je ograničen ili potpuno zabranjen, vlasnici, administratori ovog sistema su obavezni da ga regulišu tako da se jasno i automatski upozori korisnik: informacijom, kao i o uslovima pod kojima ga može koristiti, ili da je zabranjeno korišćenje ovog kompjuterskog sistema o i zakonskim posledicama za neovlašćeni pristup.

2.Nepoštovanje utvrđenih obaveza u stavu 1 ovog člana je prekršaj i prekršioc se kažnjava sa petsto (500) do pethiljada (5.000) evra.

Član 9
Krivična dela protiv poverljivosti, integriteta i raspoloživosti podataka kompjuterskih sistema

1.Nezakonit pristup kompjuterskim sistemima je krivično za koje se izvršilac kažnjava zatvorom od šest (6) meseci do tri (3) godine.

2. Kad se krivično delo iz stava 1 ovog člana vrši u cilju uzimanja kompjuterskih podataka, izvršilac ovog dela kažnajva se zatvorom od šest (6) meseci do četri (4) godina.

3. Kad se krivično delo iz stavova 1 i 2 ovog člana vrši, povređujući mere sigurnosti, izriće se kazna zatvorom od tri (3) godine do pet (5) godina.

Član 10
Nezakonito presretanje

1. Nezakonito presretanje nejavnih prenosa kompjuterskih podataka, od, za, u, ili unutar kompjuterskog sistema je krivično delo i njen izvršilac kažnjava se zatvorom od 6 (šest) meseci

do 3 (tri) godina. Ako se to obavi od pripadnika kriminalne organizacije, njen izvršilac kažnjava se zatvorom od 1 (jedan) do 5 (pet) godina.

2. Nezakonito presretanje elektromagnetskih emitovanja od kompijuterskih sistema, koji održavaju javne kompijuterske podatke, je krivično delo i njen izvršilac se kažnjava zatvorom od 1(jedne) do 5 (pet) godina.

Član 11
Neovlašćeni prenos

1. Promena, brisanje, uništavanje kompijuterskih podataka ili bespravno ograničenje je krivično delo i izvršilac se kažnjava zatvorom od jedne (1) do tri (3) godine.

2. Neovlašćen transfer podataka iz kompijuterskih sistema je krivično delo i njen izvršilac se kažnjava zatvorom od tri (3) do pet (5) godina.

3. Neovlašćeni prenos podataka iz njihove baze sa kompjuterskim sistemima je krivično delo i njen izvršilac se kažnjava zatvorom od tri (3) do pet (5) godina.

Član 12

Ozbiljno sprečavanje rada kompijuterskih sistema, ubacivanjem informacija, prenošenjem, promenom, brisanjem ili uništavanjem kompjuterskih podataka ili bespravno ograničavanje pristupa takvim podacima, krivično je delo i kažnjava se zatvorom od tri (3) meseci do tri (3) godine. Ako je to počinio član kriminalne organizacije, izvršilac se kažnjava zatvorom od jedne (1) do pet (5) godina.

Član 13
Neovlašćena proizvodnja, posedovanje i pokušaj

1. Bespravna proizvodnja, prodaja, uvoz, distribucija ili stavljanje na raspolaganje, na bilo koji način, kompjuterske opreme ili programa, dizajniran i prilagođen za izvršenje nekog krivičnog dela, kazniće se zatvorom od jedne (1) do četri (4) godine.

2. Bespravna proizvodnja, prodaja, uvoz, distribucija ili stavljanje na raspolaganju na bilo koji način pasword-a, koda za pristup ili drugih kompjuterskih podataka koji omogućavaju potpun ili delimićan pristup u kompjuterskom sistemu u nameri izvršenja krivičnog dela, kažnjava se zatvorom od jedne (1) do pet (5) godina.

3. Bespravno posedovanje opreme, kompjuterskog programa, pasword-a, pristupnog koda ili kompjuterskih podataka u nameri izvršenja krivičnog dela, kažnjava se zatvorom od jedne (1) do šest (6) godina.

4. Izvršilac, za pokušaj izvršenja krivičnog dela, prema stavu 2 i 3 ovog člana, kažnjava se zatvorom od tri (3) meseca do jedne (1) godine.

Član 14
Krivična dela u vezi sa kompjuterom

1. Uvođenje informacija, bespravna promena ili brisanje kompjuterskih podataka ili ograničavanje pristupa podacima, pretvarajući ih u neautentične podatke, radi njihovog korišćenja za pridobijanje nekog prava, krivično je delo i kažnjava se zatvorom od šest (6) meseci do tri (3) godine. Ako se počini od pripadnika kriminalne organizacije kažnjava se zatvorom od jedne (1) do pet (5) godina.

2. Za pokušaj izvršenja krivičnog dela, prema ovom članu, izvršilac kažnjava se zatvorom od tri (3) meseca do jedne (1) godine.

Član 15
Uzrokovanje nestanka imovine

1.Prouzrokovanje gubitka imovine drugog lica, uvođenjem informacija, promenom ili brisanjem kompjuterskih podataka, ograničavanjem pristupa tim podacima ili upadima u kompjuterski sistem radi obezbeđivanja ekonomske koristi za sebe ili za nekog drugog, kažnjava se zatvorom od tri (3) do deset (10) godina.

2. Za pokušaj izvršavanja krivičnog dela iz stava 1 ovog člana, izvršilac se kažnjava zatvorom od tri (3) meseca do jedne (1) godine.

Član 16
Pornografija s decom preko kompjuterskih sistema

1. Lice koje izvrši krivično delo prema podstavovima 1.1. do 1.5. ovog stava, kažnjava se zatvorom od šest (6) meseci do tri (3) godine. Ako se oceni da je izvršeno pod otežavajućim okolnostima, počinioc se kažnjava od jedne (1) do deset (10) godina.

1.1. proizvodnju pornografije s decom, u u nameri širenja iste preko kompjuterskog sistema;

1.2.ustupanje ili stavljanje na raspolaganju pornografije s decom preko kompjuterskog sistema;

1.3. širenje ili emitovanje dečje pornografije preko kompjuterskog sistema;

1.4. nabavku dečje pornografije preko kompjuterskog sistema za sebe ili za druge;

1.5. držanje dečje pornografije preko kompjuterskog sistema ili u opremi memorizacije kompjuterskih podataka.

2. Izvršilac pokušaja krivičnog dela iz stava 1 ovog člana, kažnjava se zatvorom od šest (6) meseci do tri (3) godine zatvora**.**

Član 17
Procedura gonjenja

1.U hitnim i potpuno opravdanim slučajevima, ili osnovanim sumnjama u vezi sa pripremom ili vršenjem krivičnog dela pomoću kompjuterskih sistema, u cilju prikupljanja dokaza ili identifikacije počinilaca, hitne zaštite kompjuterskih podataka ili podataka koji se odnose na promet podataka, zbog opasnosti od uništavanja ili promene, sprovode se proceduralne odredbe u nastavku:

1.1. za vreme istrage kriminala, na zahtev istražnog organa, zaštitu podataka naređuje tužilac, a u sudskom postupku nalaže sud;

1.2. mera iz stava 1 ovog člana važi devedeset (90) dana, uz mogućnost produženja za još trideset (30) dana;

1.3. nalog tužioca ili suda dostavlja se odmah bilo kom ponuđivaću usluga, ili drugom licu koji poseduje podatke iz podstava 1.1. ovog stava, a dotičo lice je dužo da ih hitno štiti, u skladu sa predviđenim uslovima o zaštiti tajnosti;

1.4. u slučaju kada se podaci odnose na promet podataka pod posedom nekoliko ponuđača usluga, ponuđač usluga, na koji se odnosi podstav 1.3 ovog člana, dužan je da organu za istragu kriminala odmah pruža potrebne informacije radi idetinifikacije drugih snabdevača usluga i spoznaje svih elemenata o iskorišćenom lancu komuniciranja;

1.5. tužilac je obavezan da do kraja istrage pismeno upozna lica koji su pod istragom za zločine i da pruži čuvane podatke o njima.

Član 18
Zaplena, kopiranje i održavanje podataka

1. U smislu člana 17 podstav 1.2. tužilac predlaže zaplenu objekata i opreme koja ima kompjuterske podatke, podatke o prometu podataka, podatke o korisniku, od osobe ili ponuđača usluga koji ih poseduje, u cilju njihovog kopiraja radi korišćenja kao dokazni materijal.

2. Ako objekti ili oprema koja sadrži podatke, odnosi se na podatke organa pravde radi njihovog kopiranja, prema stavu 1 ovog člana, sudski nalog o obaveznoj konfiskaciji se saopštava tužiocu, koji preduzima mere za jegovo sprovođeje.

3. Primerci iz stava 1 ovog člana, realizuju se putem tehničkih sredstava, kompjuterskih programa i procedura koje garantoju zaštitu integriteta informacije.

4. Tužilac može, u svako doba, narediti istragu u cilju otkrivanja ili prikupljanja dokaza, potrebnih za istraživanje kompjuterskog sistema ili kompjuterske opreme održavanja podataka.

5. Ako organ za istragu zločina ili sud smatra da će konfiskacija objekata, koji sadrže podatke koje iz stava 1, bitno uticati na aktivnosti, izvršenim od strane lica koja imaju u posed te objekte, može da naredi izradu primeraka koji će služiti kao dokaz, a formirane su prema stavu 3 ovog člana.

6. Ako se tokom istrage kompjuterskog sistema ili opreme kompjutera za održavanje podataka, saznaje da su traženi kompjuterski podaci uključeni u drugi kompjuterski sistem ili u nekoj drugoj kompjuterskoj opremi za održavanje podataka i da se sa početnog sistema ili opreme može pristupiti, može se narediti pretraga i izvršenje kako bi se istraživali svi kompjuterski sistemi ili kompjuterska oprema za održavanje traženih podataka.

Član 19
Pristup, presretanje ili snimanje komunikacija

1. Pristup u kompjuterskom sistemu, kao i presretanje ili snimanje obavljenih komunikacija opremom kompjuterskih sistema, preduzima se kada je u korist otkrivanja stine, činjenica ili identifikacije počinilaca, koje se ne može postići na osnovu drugih dokaza.

2.Mere iz stava 1 ovog člana, na predlog tužioca, preduzimaju organi za istragu kriminala pomoću specijalizovanih osoba, koji su dužni da čuvaju tajnost operacije.

3. Ovlašćenje iz stava 2 ovog člana, izdaje se za trideset (30) dana, a zbog osnovanih razloga, može se produžiti za još trideset (30) dana, međutim maksimalno trajanje ne može trajati više od četiri (4) meseci.

4.Tužilac je dužan da, do kraja istrage, pismeno informiše lica protiv kojih su preduzete mere iz stava 1 ovog člana.

Član 20
Međunarodna saradnja

1. Kosovske vlasti, u skladu sa odredbama zakona, sarađuju neposredno sa srodnim institucijama drugih država i međunarodnim organizacijama, specijalizovanim iz ovu oblast, poštujući obaveze koje proizilaze iz međunarodnih pravnih instrumenata.

2. Saradnja iz stava 1 ovog člana, može konsistirati na međunarodnu pravnu pomoć po krivičnim pitanjima, ekstradiciji, identifikaciji, blokiranju, konfiskaciji, sekvestraciji proizvoda i sredstava kojima je počinjeno krivično delo, obavljanje istrage, razmenu informacija, tehničku pomoć ili prikupljanje informacija, specijalizovanu obuku osoblja, te druge aktivnosti.

Neni 21
Istraga

1. Države i druge organizacije, na njihov zahtev, mogu da u saradnji sa kosvskim vlastima sprovode istragu radi sprečavanja i suzbijanje kompjuterskog kriminala na čitavoj teritoriji Kosova.

2.Opšte istražne aktivnosti iz stava 1 ovog člana, sprovode se na osnovu bilateralnih i multilateralnih sporazuma.

3.Predstavnici kosovskih nadležnih organa mogu učestvovati u istražnim aktivnostima, izvođenim na teritoriji drugih zemalja, u skladu sa odredbama međunarodnih sporazuma.

Član 22
Kontaktna tačka

1. Da bi se obezbedila stalna međunarodna saradnja iz oblasti kompjuterskog kriminala, vlada stavlja na raspolaganje stalnu tačku kontakta.

2. Ta stalna tačka kontakta ima sledeće nadležnosti:

2.1.oruža specijalizovanu pomoć i informacije o zakonodavstvu iz oblasti kompjuterskog kriminala i informiše kontaktne tačke drugih država;

2.2. naređuje hitno čuvanje podataka i konfiskaciju opreme koja sadrži kompjuterske podatke ili podatke koje se odnose na podatke o prometu podataka, tražene od stranog nadležnog organa;

2.3. izvršava ili pomaže izvršenje, prema zakonskim odredbama, u slučajevima suzbijanja kompjuterskog kriminala, sarađujući sa svim kosovskim nadležnim organima.

3. Šest (6) meseci nakon stupanja na smagu ovog zakona, vlada će podzakonskim aktom utvrditi kontaktnu tačku, predviđenu stavom 1 ovog člana.

Član 23
Zahtev za hitnu zaštitu podataka

1. U okviru međunarodne saradnje, strani nadležni organi, preko kontakte tačke, mogu tražiti od službe za suzbijanje kompjuterskog kriminala hitno zaštitu kompjuterskih podataka ili podataka

koji se odnose na prometu podataka unutar kompjuterskog sistema na teritoriji Kosova u vezi s kojima je strani organ podnela zahtev pravne međunarodne pomoći po krivičnim pitanjima.

2. Zahtev za hitno čuvanje, iz stava 1 obuhvata sledeće podatke:

2.1. organa koji traži zaštitu podataka;

2.2. kratko prezentiranje činjenica koja podležu kriminalističkoj istrazi i zakonska osnovi;

2.3. kompjuterski podaci o kojima se zahteva zaštita;

2.4. sve raspoložive infomacije, potrebne za identifikaciju vlasnika kompjuterskih podataka i lokacija kompjuterskog sistema;

2.5. usluga kompjuterskih podataka i potreba za njihovu zaštitu;

2.6. cilj strane vlasti za sastavljanje zahteva o pravnoj međunarodnoj pomoći po krivičnim pitanjima.

3. Zahtev o zaštiti podataka izvršava se, prema članu 17, za period od šesdeset (60) dana. Ta zaštita u vezi sa zahtevom o međunarodnoj pravnoj pomoći po krivičnim pitanjima važi do donošenja odluke kosovskih nadležnih organa.

Član 24
Zaštita podataka

Ako se u izvršenju sastavljenog zahteva iz člana 23 stav 1 ovog zakona, ponuđač usluga u drugoj zemlji je shvaćen da bude u posedu podataka u vezi sa prometom podataka. Služba za suzbijanje kompjuterskog kriminala upoznaće odmah strani organ o tome, saopštavajući takođe sve identifikacione podatke odgovarajućeg ponuđača usluga.

Član 25
Pristup javnim otvorenim izvorima

1.Strani nadležni organ može pristupiti i primiti, pomoću sistema, postavljenog na njgovoj teritoriji, kompjuterske podatke čuvane na Kosovu, ako ima odobrenje ovlašćenog lica, prema zakonskim odredbama, za stavljanje na raspolaganje pomoću kompjuterskog sistema, bez podnošenja zahteva od strane kosovskih organa.

2. Strani nadležni organ može pristupiti kosovskim javnim izvorima kompjuterskih podataka bez podnošenja zahteva kosovskim organima.

Član 26
Zakonske odredbe o ustupanje informacija i potrebnih podataka za strane autoritete

Kosovski nadležni organi mogu dostaviti po službenoj dužnosti, kod stranih nadležnih organa, poštujući zakonske odredbe o zaštiti ličnih podataka, informacije i podatke potrebne za strane nadležne organe za otkrivanje dela izvršenih pomoću kompjuterskog sistema ili za rešavanje pitanja koje se odnose na taj kriminal.

Član 27
Završne odredbe

U slučaju kolizije odredaba ovog zakona sa odredbama Zakona o krivičnom postupku preovladaće odredbe Zakona o krivičnom postupku.

Član 28
Prihodi

Prihodi naplaćeni po osnovu ovog zakona uplaćuju se u budžet Republike Kosovo.

Član 29
Stupanje na snagu

Ovaj zakon stupa na snagu petnaest (15) dana od dana objavljivanja u Službenom listu Republike Kosovo

Zakon br. 03/L-166
10. juna 2010.godine

Proglašeno Dekretom Br. DL-028-2010, dana 02.07.2010, od Predsednika Republike Kosovo, Dr. Fatmir Sejdiu