Komentari i sugestije za unapređenje Nacrta zakona o informacionoj bezbednosti Ambasade SAD, Američke privredne komore u Srbiji i DIPLO fondacije

23. jul 2015. godine

Načelne primedbe i sugestije:

1. Zakon vrlo šturo i uopšteno uređuje celu oblast i Vladi ostavlja preširoka diskreciona ovlašćenja da kroz podzakonske propise bliže reguliše i definiše odredbe Zakona, čime se Vladi daje uloga zakonodavca, a što njena uloga ne može biti. Navedeno se posebno ogleda u odredbama članova 6., 8., 9., 10., 17., 19., 26. i 27. Nacrta Zakona. S toga, smatramo da je potrebno ova pitanja bliže urediti samim Zakonom, a posebno imajući u vidu da bi u ovoj sadržini bio gotovo neprimenljiv u praksi i kao takav izazvao mnogo nedoumica.

2. Obzirom da bi Vlada trebalo da donese podzakonske akte za sprovođenje Zakona u roku od 12 meseci od dana stupanja na snagu zakona, isti se faktički neće primenjivati dok Vlada ne donese potrebna akta, a što iz iskustva znamo da ne mora biti 12 meseci, već je najčešće i duže od zakonom propisanog roka.

3. Mišljenja smo da bi trebalo da se Zakonom osnuje jedno posebno nezavisno državno telo koje bi okupilo stručnjake iz predmetne oblasti, kao i predstavnike nadležnih ministarstva, a koje bi bilo nadležno za sprovođenje Zakona, kao i za pružanje pomoći državnim organima i privrednim subjektima u sprovođenju Zakona.

Pojedinačne primedbe i sugestije:

1. **Predmet uređivanja (član 1) –** Dodati "i u upotrebi sistema" tako da glasi:

   "Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima i *upotrebi sistema* (…) ".

2. **Značenje pojedinih termina (član 2) –** U tački 1, stav 1, potrebno je preciznije definisati i klasifikovati informaciono-komunikacione (IKT) sisteme, a pogotovo sisteme od posebnog značaja. Iz sadašnje definicije nije jasno koji IKT sistem je predmet mera bezbednosti, a posebno imajući u vidu da u Nacrtu nije definisano šta je to kritična infrastruktura – ona mora da biti bliže definisana ovde da bi se jasno znalo šta je predmet ovog zakona. Ovo se naročito vidi u tački tri, stav 1 ovog člana, gde definicija informacione bezbednosti obuhvata i bilo koju kućnu mrežu. U tom smislu moguć predlog dopune tačke 1, stava 1 bi glasio:

   1) informaciono-komunikacioni sistem (IKT sistem) *je svaka kombinacija računarske, programske i komunikacione opreme, fizičke i programske infrastrukture, procesa i ljudi, povezana i organizovana sa ciljem obrade elektronskih podataka.*

   Takođe, potrebno je predvideti da IKT sistem može biti i "virtuelna infrastruktura, logička platforma ili aplikativni ili servis za skladištenje podataka", koji se nalazi na fizičkoj infrastrukturi obezbeđenoj od strane *Cloud provajdera.*

   Tačku 2, stav 1 dopuniti tako da glasi:

   2) Rukovalac IKT sistema je organ javne vlasti ili organizaciona jedinica organa javne vlasti, odnosno pravno lice *koje određuje svrhu uspostavljanja, organizaciju i način rada IKT sistema;*

2a) davalac IKT usluge je svako pravno ili fizičko lice koje korisnicima svoje usluge pruža mogućnost obrade i/ili prenosa računarskih ili računarski obrađenih informacija. Davalac IKT usluge je svako ko učestvuje u planiranju, opremanju, integraciji, upravljanju i održavanju IKT sistema, za račun rukovaoca IKT sistemom ili korisnika IKT usluge.

2b) korisnik IKT usluge je pravno ili fizičko lice koje svoje legitimne aktivnosti realizuje koristeći usluge nekog IKT sistema.

2v) učesnici IKT sistema su rukovaoci IKT sistema, davaoci IKT usluga i korisnici IKT usluga.

U tački 3, stav 1, potrebno je preciziranje –neporecivosti podataka zameniti sa *informacija koje nose podaci.*

3. **Načela (član 3) –** Načelo celovite zaštite preimenovati u načelo *sveobuhvatne* zaštite. Takođe, ako se već navode načela zaštite IKT, poželjno je držati se nekog od opšteprihvaćenih međunarodnih okvira, na primer OECD, ali bi u svakom slučaju trebalo dodati sledeća načela:
   5) načelo odgovornosti – svi učesnici su odgovorni za bezbednost IKT sistema, i usluga, srazmerno svojoj ulozi.
   6) načelo minimizacije upotrebe podataka – mere zaštite IKT sistema treba da se baziraju na minimalnoj obradi podataka, isključivo u meri koja je neophodna i proporcionalna svrsi razrešavanja konkretnog bezbednosnog izazova.

4. **Nadležni organ (član 4)** – Umesto organ državne uprave nadležan za bezbednost IKT sistema, predvideti da je nadležan organ državne uprave za *informacionu bezbednost*. Naime, bezbednost IKT sistema nije definisana, dok je informaciona bezbednost definisana, i predmet je ovog zakona.

   Takođe, ovim članom je predviđeno da će ministarstvo nadležno za poslove informacione bezbednosti biti nadležno za ova pitanja, što može izazvati problem u budućnosti ako ne bude postojalo jedinstveno ministarstvo koje pokriva i informaciono društvo i telekomunikacije, kao što je slučaj danas. Ovako je implicitno navedeno da neko buduće ministarstvo, koje ne bi pokrivalo kao danas i telekomunikacije i informaciono društvo, već samo informaciono društvo bude nadležno za Nacionalni CERT, a da drugo ministarstvo za telekomunikacije bude nadležno za RATEL pa samim tim i za CERT. Ovo može predstavljati opasnost koja može dovesti do lošeg funkcionisanja Nacionalnog CERT-a.

5. **Telo za koordinaciju poslova informacione bezbednosti (član 5)** – Dodati "više-partnersko Telo". Naime, neophodno je zakonski osigurati učešće drugih sektora u koordinaciji i planiranju savetima; u suprotnom bi se to ostavilo na volju trenutnoj Vladi ili ministru. Više-partnerski model je osnova za efikasnu sajber-bezbednost: većina komunikacione i IKT infrastrukture je u privatnom vlasništvu, a detaljno znanje, pa i kontakti, su u tehničkoj i akademskoj zajednici kao i u nevladinom sektoru. Ovo bi ujedno predstavljalo i priliku da se koordinacija i strateško planiranje o digitalnim politikama formalno radi uz pomoć svih partnera na sistemskom nivou, a ne samo kroz moguće radne grupe i konsultacije koje zavise od toga ko vodi koje ministarstvo i političkog raspoloženja.

   U tom smislu, imajući u vidu da se digitalne politike, pa i mere za informacionu bezbednost, odražavaju na sve segmente društva, potrebno je predvideti da u sastav ovog tela ulaze i predstavnici ministarstva nadležnih za privredu, saobraćaj, obrazovanje i nauku, kulturu i informisanje", a po mogućstvu i drugi (zdravstvo, turizam, ...), predstavnici regulatornog tela za elektronske komunikacije i organ nadležan za zaštitu podataka o ličnosti, kao i predstavnici operatora kritične i komunikacione infrastrukture, IKT i internet industrije, tehničke, stručne i akademske zajednice i nevladinog sektora.

   Konačno, neophodno je definisati odnos ovog tela sa nadležnim organom, Vladom i organima za nacionalnu bezbednost i nacionalnog CERT-a, kao i definisati njegove nadležnosti i urediti njegov status – da li je ono savetodavno i da li je razmatranje saveta od strane organa obavezujuće (što je preporučljivo). Ovo je izuzetno važno regulisati da bi telo imalo smisla.

6. **Odgovornost za bezbednost IKT sistema (član 6)** – Ubaciti novi stav 2 koji bi glasio:

Korisnici su odgovorni za bezbedno rukovanje informacijama, uključujući unos, pristup i brisanje i korišćenje resursa IKT sistema u skladu sa bezbednosnim zahtevima.

7. **Obaveza dostavljanja podataka (član 7)** – Ova odredba je formulisana veoma široko, tako da su mogući problemi prilikom njene primene, a postoji mogućnost i dvojakog tumačenja:
   - » u skladu sa zakonom» se odnosi na to da službe obavljaju delatnost u skladu sa zakonom,
   - službe mogu zatražiti od rukovaoca podatke na način »u skladu sa zakonom» (to bi trebalo da podrazumeva nalog suda).

   U tom smislu, potrebno je – ako ostane izričito navođenje obaveze da se određeni podaci stavljaju na raspolaganje – da se izričito navede i uslov pod kojim ova obaveza obuhvata sve podatke, pa i one kojima se zadire u privatnost/tajnost sredstava komunikacije, tj. uslov da se podaci stavljaju na raspolaganje na osnovu odluke suda.

   Ovo je jedna od ključnih odredbi Zakona, na osnovu koje se ograničavaju Ustavna prava građana (tajnost pisma i drugih sredstava opštenja, član 41 Ustava RS). Navedena ustavna odredba određuje da se to može učiniti samo na zahtev suda i da takva mera ima određeno trajanje.

   Najzad, obzirom da Ustav RS u članu 42 garantuje zaštitu podataka o ličnosti, trebalo bi konsultovati poverenika za informacije od javnog značaja, ukoliko već nije konsultovan, prilikom definisanja predmetne odredbe, kako ovaj Zakon ne bi došao u koliziju sa Zakonom o zaštiti podataka o ličnosti. Naročito što nije definisano koje podatke i na šta se ti podaci odnose koje su rukovaoci dužni po zahtevu da dostave.

   Takođe, "podaci od značaja za informacionu bezbednost" nisu definisani. Ako se već ne definišu ti podaci, treba dati predlog da se ograniči opseg situacija kada organi mogu tražiti podatke (npr. samo za potrebe zaštite nacionalne bezbednosti, sprečavanja težih posledica po privredu i zdravlje ljudi i sl.) i odrediti mere čuvanja tajnosti dostavljenih podataka.

8. **Bezbednost IKT sistema od posebnog značaja (glava II)** – Ovde je potrebno dodati i:
   - imenovanje osoba odgovornih za bezbednost podataka i IKT sistema u svim organima uprave,
   - izradu planova zaštite i kontinuiteta,
   - uspostavljanje mehanizma za razmenu iskustava.

9. **IKT sistemi od posebnog značaja (član 8)** – Nije jasno šta se podrazumeva pod delatnostima od opšteg interesa (tačka 2, stav 1), te bi to trebalo precizirati, tj. tačno navesti šta se smatra delatnošću od opšteg interesa u smislu ovog zakona.

   Dodatno, trebalo bi brisati tačku 5, jer nije jasno šta predviđene delatnosti podrazumevaju.

   Takođe, primena stava 2 u praksi bi značila da Vlada, kao organ izvršne vlasti može po svom nahođenju da proširi navedenu listu delatnosti i derogira zakon.

10. **Mere zaštite IKT sistema od posebnog značaja (član 9)** – Osim stava 1, prepisana je odredba člana 6 Zakona. Ovim članom bi trebalo predvideti dodatne mere zaštite kada su u pitanju sistemi od posebnog značaja.

    Takođe, u stavu 3 je potrebno dodati da se uvažavaju i
    - stavovi više-partnerskog Tela – ovo je primer gde je potrebno jasnije označiti ulogu Tela. U njemu bi zapravo trebalo da sede lica dovoljno stručna da ovakve predloge pripremaju i prate međunarodne standarde, čak i ako potom takvi predlozi do Vlade stižu preko nadležnog organa.
    - međunarodne smernice i sporazumi – mnoge norme i smernice nalaze se u međunarodnim sporazumima, poput Konvencije 185 Saveta Evrope o sajber-kriminalu, odluke 1106 Stalnog

Saveta OEBS o merama izgradnje poverenja, dokumenata UN Grupe državnih eksperata (UN GGE), OECD zemalja i slično.

11. **Akt o bezbednosti IKT sistema od posebnog značaja (član 10)** – Potrebno je predvideti rok u kome su rukovaoci dužni da donesu predmetni akt.

12. **Poveravanje aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima (član 11) – U stavu 3, k**orisno je dodatno definisati, na primer da li treće lice može obuhvatiti i privredne subjekte sa teritorije drugih zemalja; potrebno je razjasniti slučaj da je IKT sistem u Srbiji i da je rukovalac IKT sistema u Srbiji (zbog specifičnosti *Cloud* servisa). Sa druge strane, ovaj stav može biti neodrživ, jer na ovaj način institucije od posebnog značaja ne mogu da angažuju privatne privredne subjekte.

13. **Obaveštavanje Nadležnog organa o incidentima (član 13) –** U stavu 1 izmeniti: "da obaveste nacionalni CERT". Naime, vrlo je loša praksa da se o incidentima obaveštava Ministarstvo koje ima svoje procedure i prateću birokratiju, te retko može da ima kapaciteta za operativno delovanje. Informacije o incidentima i reagovanje na njih zahteva efikasno operativno delovanje, a ovim bi se zakon bi se Zakon obesmislio i postao nesprovodiv. Nacionalni CERT je treba da bude obaveštavano rizicima kako bi se sagledala šira sliku, procenili rizici i dalje reagovalo ka sprečavanju ili zaustavljanju incidenta. U slučaju većih incidenata, nacionalni CERT treba da alarmira koordinaciono telo, nadležno ministarstvo i Savet za nacionalnu bezbednost. Ovo je posebno važno za zaštitu kritične infrastrukture gde je neophodno brzo reagovanje: ako ti incidenti budu prijavljivani nadležnom ministarstvu, operativno delovanje će biti značajno usporeno, a neophodna je reakcija reda nekoliko sati, ako ne i minuta. Ni predlog NIS direktive Evropske unije ne prepoznaje operativno delovanje nadležnog ministarstva.

    Takođe, u stavu 4, potrebno je dodati da listu incidenata i način obaveštavanje bliže uređuje Nadležni organ "u saradnji sa nacionalnim CERT-om i koordinacionim Telom". Naime, iako Nadležni organ može formalno da bude telo koje uspostavlja način obaveštavanja i listu incidenata, ni jedno ministarstvo neće imati stručnosti ni kapaciteta da radi ovako nešto. Ovo je svrha CERT-a i/ili Tela, a nadležni organ može samo da formalno donosi odluke o listi, ukoliko je to zaista potrebno.

14. **Ovlašćenja Nadležnog organa (član 14) –** Ovlašćenja nadležnog organa su preširoka i izmešana: ministarstvo u ovih se spominje u Nacrtu na političkom nivou, na strategijskom-koordinacionom nivou (što je Telo za koordinaciju), a potom i na operativnom nivou (što je funkcije Nacionalnog CERT-a).

15. **Međunarodna saradnja i rana upozorenja o rizicima i incidentima (član 15)** – Stav 1 je potrebno prebaciti pod oblast delovanja CERT-a, nakon člana 16. Naime, nadležni organ već ima ovlašćenja međunarodne saradnje iz svoje oblasti pa to nije neophodno ponavljati. Međutim, međunarodnu saradnju na operativnom nivou treba jasno omogućiti nacionalnom CERT-u i obezbediti resurse za to, jer bez toga CERT neće moći uspešno da radi. Takođe, izdavanje ranih upozorenja i upozorenja uopšte je polje delovanja stručnog Nacionalnog CERT koji ima kapacitet da prikuplja i obrađuje podatke i priprema stanje nacije u sajber-prostoru. Takav presek potom, na političkom nivou, ka nadležnom Ministarstvu i eventualno treba da ide ka Savetu za nacionalnu bezbednost i Vladi. Nadležno ministarstvo neće imati kapaciteta ni vremena da redovno i stručno objavljuje rana upozorenja niti vrši presek stanja; to je vrlo loša praksa.

    U stavu 2 je pomešano ono što Telo za koordinaciju treba da dostavi Vladi i ono što CERT radi u osnovi. Nejasan član, a Nadležni organ dobija nove funkcije obaveštavanja. Problem je u tome što CERT i MUP sarađuju direktno, a MUP podnosi Europolu. Problem nastaje što se neki predmeti javljaju u Africi, neki u Rusiji i Kini, a neki u SAD, pa CERT i MUP sarađuju sa svim inostranim policijama, te stoga ovo navođenje samo Europola nije jasno.

16. **Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (članovi 16 , 17 i 18)** – U članu 16, potrebno je precizirati rok za formiranje – predlog je da to bude 6 meseci i razmotriti da li je RATEL najbolje rešenje. Naime, ovde je sasvim jasno, kada se pravo ime RATEL-a ne piše u skraćenici, da neko ko se bavi fizičkim nivoom Interneta, Telefonijom i Poštanskim uslugama, po prirodi nije najpogodniji da

bude Nacionalni CERT. Oni će morati da formiraju posebno odeljenje koje će samo na papiru pripadati RATEL-u, što je jednako formiranju novog entiteta. S druge strane, RATEL po prirodi nema kontakte sa hosting provajderima, koji su vrlo često na udaru incidenata. Ovo možda treba ostaviti Telu za koordinaciju i Vladi da odredi instituciju, a ovde da se precizira da se imenuje na pet godina.

Dalje, neki od predviđenih poslova nacionalnog CERT-a, iz člana 17, se podudaraju sa određenim nadležnostima Tela za koordinaciju, iz člana 5 Nacrta Zakona, te bi to trebalo uskladiti. Takođe, potrebno je dodati u stav 1 da CERT:

- ima ulogu međunarodne operativne kontakt tačke za deljenje informacija o rizicima
- prikuplja informacije o rizicima i incidentima od međunarodnih i domaćih partnera
- pruža rana upozorenja o rizicima i incidentima
- priprema redovan presek stanja informacione bezbednosti u Srbiji, u saradnji sa koordinacionim Telom
- formira repozitorijum najboljih praksi
- unapređuje kapacitete na osnovu razmene stručnih znanja i iskustava.

Naime, nacionalna operativna kontakt tačka je osnova i OEBS Mera za poverenje (odluka Stalnog saveta broj 1106) i predloga NIS direktive EU, kao i drugih smernica poput ENISA, UN GGE i drugo. Pominjanje međunarodne saradnje za izgradnju kapaciteta je važno da bi bilo jasno da CERT mora da ima resurse za međunarodnu saradnju i putovanja, bez čega nema efikasnog delovanja. Pripremu preseka stanja informacione bezbednosti najbolje može da radi CERT (pod uslovom da ima resurse, naravno) jer je na izvoru informacija i inače priprema redovne preseke i izveštaje. Izdavanje ranih upozorenja je jedan od osnovnih zadataka CERT-a. Formiranje repozitorijuma najboljih praksi, kada je u pitanju informaciona bezbednost (ček-liste, modeli akata, studije slučaja itd.), može da bude korisno malim preduzećima (npr. praktični koraci kako da se zaštiti sajt: angažuje administrator ili ugovori održavanje, redovno ažurira CMS, koriste netrivijalne lozinke, prave rezervne kopije podataka itd.). Ovo su u praksi najčešće delatnosti CERT-a.

U članu 18 je potrebno dodati da Nadležni organ "i obezbeđuje resurse". Ovo iz razloga jer nije dovoljna samo provera, važno je da nadležni organ ima i obavezu da obezbedi neophodne resurse ili nađe modalitet za to.

17. **Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima (član 19) -** Bliže uslove za upis u evidenciju bi trebalo urediti zakonom, a ne aktom nadležnog organa. Nije jasno na osnovu kog kriterijuma će se formirati posebni CERT-ovi i da li oni imaju prenete nadležnosti Nacionalnog CERT-a.

    Takođe, organizacione jedinice nekih privrednih subjekata (*information security operations center - SOC*) mogu da vrše opisane delatnosti bez da budu upisane u evidenciju posebnih CERT-ova. Nije realno da će svaki SOC biti evidentiran, niti je to potrebno.

18. **Centar za bezbednost IKT sistema u republičkim organima (članovi 20 i 21) –** Naziv bi trebalo uskladiti sa prevodom iz člana 16.

    U članu 20, stav 3, tačka 2, dodati "i nacionalnim CERT-om", koji će mu biti izvor informacija.

    U članu 21, stav 1 precizirati rok.

19. **Kriptobezbednost i zaštita od kompromitujućeg elektromagnetnog zračenja**

    - Nadležnost (član 22) – Oblast kriptozaštite i KEMZ nije neophodna na ovom nivou u ovakvom krovnom zakonu; nesrazmerno detaljno je definisana u odnosu na celu prethodnu oblast, ali opet sa druge strane, nije jasno kako i po kom kriterijumu ministarstvo daje odobrenje.

    Dodatno, potrebno je nedvosmisleno precizirati da se ovi poslovi odnose na organe javne vlasti i IKT sisteme od posebnog značaja, a ne na ostale subjekte (kompanije, građane) koji moraju imati slobodu izbora da li i kako kriptuju svoje podatke. Alternativno, moguće je povezati i sa sistemima koji vrše obradu

tajnih podataka i podataka o ličnosti; no i dalje mora biti jasno da se odnosi samo na precizno definisane grupe sistema, ne na sve.

- Poslovi i zadaci (član 23) – U tački 8, stav 1, potrebno je definisati akreditaciju i proceduru akreditacije, ili se pozvati na definiciju u drugom zakonu ako postoji.

20. **Izdavanje odobrenja za kriptografski proizvod (član 27) –** Ova procedura bi trebalo da bude predviđena podzakonskim aktom.

21. **Poslovi inspekcije za informacionu bezbednost (član 31) –** Formiranje odeljenja informacione bezbednosti inspektorata je definisano samo u jednom članu, a da nije precizirano kako se imenuju i ko vrši obuku inspektora, koje su kaznene mere koje inspektor može da izrekne i sl. – ovo je potrebno bliže urediti.

22. **Ovlašćenja inspektora za informacionu bezbednost (član 33) –** U tački 1, stav 1, nije jasno da li se ostavlja mogućnost da se pregled obavi sa udaljene lokacije ili posrednim putem (posebno ukoliko je u konkretnom slučaju to racionalno rešenje). Takođe, potrebno je na kraju tačke dodati "kao i organizacione polise, procedure i nivo obučenosti osoblja", a imajući u vidu da većina incidenata nastaje kroz propuste u delanju, a ne u IKT sistemu.

    Tačka 3, stav 1, daje potencijalno vrlo široko ovlašćenje za pristup svim vrstama podataka i dokumentacije, te je ovo potrebno detaljnije precizirati i uskladiti sa drugim relevantnim zakonima iz ove oblasti.

23. **Kaznene odredbe (Član 34)** - Kaznene odredbe bi trebalo detaljnije regulisati, a posebno imajući u vidu da je predviđen jako širok raspon između minimalne i maksimalne novčane kazne, praktično za bilo koje kršenje odredaba ovog zakona. Dodatno, kažnjavanje za prekršaj bi trebalo da se odnosi na sva lica, a ne samo na pravna lica. Ovako proizilazi da su organi vlasti isključeni od kažnjavanja zbog nepoštovanja odredaba ovog Zakona.