

Poštovana gospodo,

Šaljem vam ovu poruku elektronskom poštom kao moj prilog javnoj raspravi o nacrtu Zakona o informacionoj bezbednosti održanoj 03.02.2012. godine.

Kako je raspoloživo vreme za diskusiju bilo ograničeno a moji stavovi uglavnom različiti od stavova diskutantata koji su dobili reč, odlučio sam da ne diskutujem jer vremena za argumentovanu raspravu nije bilo ali sam ipak osetio potrebu da vam svoje stavove prezentujem na ovaj način.

U pogledu definicija pojmova koji se javljaju u zakonu, navedenih u uvodnom delu Zakona, bilo je više primedbi, ja ću se osvrnuti na dve:

Bilo je primedbi da je tajnost svojstvo podatka. Onako kako ja vidim stvari podatak je zapis koji interpretacijom u odgovarajućem kontekstu dobija značenje i postaje informacija. Da bi informacija bila dostupna samo ovlašćenom krugu korisnika i tako se sačuvala njena tajnost, sa njom se postupa na unapred definisan način u toku njenog životnog ciklusa. Shodno tome tajnost se postiže definisanim načinom postupanja sa podacima i nije imanentna podatku samom po sebi.

Pojam kompromitujućeg elektromagnetnog zračenja predstavlja ona elektromagnetna zračenja koja doprinose kompromitaciji informacije koja se nekim uređajem štiti. Pojam nije nepoznat, kako su neki učesnici konstatovali, u stručnoj javnosti i u nekim stručnim tekstovima može se naći u formi skraćenice COMPREME.

I za većinu preostalih primedbi koje se odnose na terminologiju mogu se lako naći razlozi koji opravdavaju formulacije navedene u Zakonu.

Što se tiče primedbi da kroz akreditaciju IKT sistema država u suštini akredituje samu sebe, lično mislim da ne stoje. Naime Zakon se bavi IKT sistemima u organima javne vlasti i prirodno je da zakonodavac kaže da će se propisati kriterijumi i način njihove provere a da će se proces sprovesti preko odgovarajućeg organa, Kancelarija saveta za nacionalnu bezbednost. Po meni ovo ima smisla jer "država" uređuje stvari u svom dvorištu i prirodno je da ih uređuje na način za koji smatra da je najbolji. Ako se ispostavi da su zahtevi dobri i ispunjavaju svoju svrhu, onda će je slediti i "šira zajednica, (privreda, banke). A ako se pak ispostavi da zahtevi ne doprinose "željenom nivou bezbednosti" ce će platiti onaj ko je takve zahteve i postavio kroz kompromitaciju sopstvenih informacionih sistema i oticanje informacija. Dakle, odgovornost je onoga ko odluku i donosi. Ovakvo rešenje je primenjeno i u nekim značajnim evropskim zemljama .

Što se tiče primedbi na AMRES nisam kompetentan za primedbe u vezi pravnog statusa, ali kako mi se čini njihova jedina funkcionalnost u okviru ovog zakona je uloga nacionalnog CERT-a.

I na kraju, smatram da je donošenje zakona u ovoj oblasti, s obzirom na vreme i situaciju u kojoj živimo i radimo, predstavlja esencijalnu potrebu našeg društva. Naravno da ću se složiti da je možda trebalo strateška dokumenta i zakone iz ove oblasti donositi drugim redom, da ovaj zakon nije savršen i sa još "sijaset" primedbi opšteg tipa. Ali je isto tako činjenica da ovaj nacrt predstavlja razuman okvir za uređenje odnosa u ovoj oblasti i da nema realne potrebe da se stvari odlažu. Ono čega zakonodavac takođe treba i mora da bude svestan jeste činjenica da na kraju ako se ovaj zakon i usvoji tek tada predstoji značajan posao

donošenja propisa koji iz ovog zakona proističu. Tim propisima će biti definisani tehnički uslovi, procedure, organizacija i odgovornosti, i u suštini, tek njima će biti zaokružen sistem kojim će biti određena primenjljivost i kvalitet ovog zakona.

Sa poštovanjem,
T. Unkašević