

Poštovani gospodine Vojvodiću,

Moje shvatanje da je oblast koju bi zakon o informacionoj bezbednosti trebalo da uređuje daleko šira od oblasti koja obuhvata samo IKT sisteme državnih organa i sa njima povezanih pravnih i fizičkih lica koja se bave tajnim podacima, ne poklapa se sa shvatanjima autora Nacrta Zakona o informacionoj bezbednosti. Ne sporim potrebu za postojanje propisa koji reguliše obavezu obezbeđenja informacija i u posebnim slučajevima, ali se najodlučnije protivim da se takav propis nazove Zakon o bezbednosti informacija.

Ovaj Nacrt se odnosi samo na odabranu podgrupu vlasnika IKT sistema ("rukovaoci i samostalni rukovaoci IKT sistema"). Šta je sa svim ostalim vlasnicima IKT sistema u Republici Srbiji? Kako njima obezbediti pravnu sigurnost u pogledu bezbednosti njihovih IKT sistema? Nadam se da nije bila namera (ili zadatak) autora Nacrta da oni koji žele da ostvare pravnu sigurnost treba da akredituju svoje IKT sisteme svake tri godine, uz naknadu. Oprostite mi na hiperboli, ali ovo mi liči na situaciju kao kada bi država rekla da će od nasilja štiti samo građane koji mogu da kupe pancirni prsluk i plate telohranitelje naoružane "do zuba".

Ukoliko želimo da razvijamo privrednu aktivnost moramo stvoriti što bolje uslove za razvoj poslovanja. Verujem da ćete se saglasiti da je IKT sistem bilo koje veličine postao neizbežni i neodvojivi deo bilo koje poslovne aktivnosti. Stoga sam ubeđen da se država mora potruditi da ovu oblast reguliše opštim a ne parcijalnim propisima o bezbednosti informacija. Mišljenja sam da bi fizički IKT sistem (opremu i podatke ili informacije) trebalo tretirati kao svojinu i svaki neodobren pokušaj pristupa istom trebalo bi sankcionisati i tretirati kao: smetanje poseda, neosnovano bogaćenje, prisvajanje, krađu, kako god, srazmerno posledicama po vlasnika predmetnog sistema. Takav zakon bi, pre svega, trebalo da odvraća potencijalne prekršioce suočavajući ih sa ozbiljnim posledicama ukoliko vrše neodobrene aktivnosti prema tuđim IKT sistemima. Samim tim bi, kod vlasnika IKT sistema, proizveo osećaj pravne sigurnosti i uverenje da ih država štiti, pod uslovom da se oni sami odgovorno i sa pažnjom odnose prema bezbednosti sopstvenih IKT sistema, odnosno primenjuju propisana načela u razumnoj meri.

Biću slobodan da predložim da autori Nacrta, ukoliko to već nisu imali priliku, pročitaju priloženi rad "The State of Information Security Law - A Focus on the Key Legal Trends", autora Thomas J. Smedinghoff-a, člana američke delegacije pri UNCITRAL-u (United Nations Commission on International Trade Law).

U navedenom radu dat je i popis zakona većeg broja država. Sledeće zakone smatram kao primere dobrog regulisanja ove oblasti, na osnovu kojih bi se mogao izraditi Zakon o bezbednosti informacija Republike Srbije:

1. Personal Data Protection Law - Argentina 2. Act on Promotion of Information and Communication Network Utilization and Information Protection - Južna Koreja 3. Personal Information Protection and Electronic Documents Act - Kanada 4. Data Protection Act 1998 - Velika Britanija

Što se predmetnog Nacrta tiče, izričito sam protiv naziva Zakon o bezbednosti informacija. Naziv istog bi trebalo uskladiti sa užim područjem koje uređuje (o obezbeđivanju posebnih državnih IKT sistema ili slično).

Sličan komentar sam postavio na Internet stranicu Digitalne agende koja se odnosi na javnu raspravu o ovom Nacrtu, ali se isti ni posle 24 sata nije pojavio u listi komentara (i dalje je prazna).

Nadam se da će ovaj pokušaj doprinosa u oblasti regulisanja bezbednosti informacija u Republici Srbiji biti dobronamerno shvaćen i prihvaćen.

S poštovanjem,

--

Ljubomir Ćirović  
Direktor Biroa za informatiku  
GP "Mostogradnja" AD, Beograd  
Vlajkovićeva 19a