Izvorni znanstveni rad
Original scientific paper

JEL Classification:: K2, K24

Veljko Trivun *

PRAVNO UREĐENJE KIBERNETIČKOG KRIMINALA U BOSNI I HERCEGOVINI

LEGAL REGULATION OF CYBERNETIC CRIME IN BOSNIA AND HERZEGOVINA

Sažetak

Uvođenjem krivično-pravne odgovornosti pravnih lica u pravni sistem Bosne i Hercegovine 2002. nastupile su radikalne promjene u sferi odgovornosti i za kibernetički kriminal. Sam kibernetički kriminal usko se veže za djelovanje pojedinaca, odnosno fizičkih lica, međutim nezobilazna je i odgovornost privrednih društava. Ova konstatacija se posebno ističe kada se dostupnim čine resursi (oprema i propadajući software) koji omogućavaju počinjenje kibernetskog kriminala. Revolucija u sferi informatike, brojne društvene mreže, e-eduakcije, pa sve do brojnih oblika internet komunciranja koji omogućavaju elektronsko ugovaranje, plaćanje i e-banking, dovelo je do obaveznog normiranja u ovoj oblasti. Kao i u svakoj drugoj oblasti postoji više nego zavidan nivo zloupotreba koje imaju zabranjen i to najšeće krivično-pravni karakter. Bosna i Hercegovina se može smatrati zemljom koja je ova pitanje pravno uredila na adekvatan način i uskladila sa zahtjevima međunarodne zajednice. Tako, imamo državno (BiH) zakonodavstvo u krivično-pravnoj oblasti, elektronsko zaključivanje ugovora, siguran i kvalifikovani elektronski potpis, pravo konkurencije i pravo zaštite potrošača. Pobrojano predstavlja osnovni set propisa u ovoj oblasti. Entiteti i BD BiH imaju pravno određenje u oblastima elektronske komunikacije i krivično-

* **Profesor dr Veljko Trivun, Ekonomski fakultet u Sarajevu**

pravnoj oblasti. U Krivičnom zakonu FBiH imamo posebno poglavlje pod nazivom Krivična djela protiv sistema elektronske obrade podataka, dok u RS-u imamo poglavlje pod nazivom Krrivična djela protiv bezbjednosti kompjuterskih podataka. U BD BiH, isto kao i u FBiH, imamo istu sistematizaciju i naziv poglavlja koje se bavi sankcionisanjem ove vrste krivičnih djela. Elektronsko plaćanje i prodaja na daljinu posebno su uređeni državnim Zakonom o zaštiti potrošača u BiH.

Ključne riječi: *kibernetski kriminal, konkurencija, krivično djelo, elektronski podaci, elektronsko poslovanje.*

Abstract

With the introduction of criminal liability of legal entities in the legal system of Bosnia and Herzegovina in 2002, radical changes took place in the sphere of responsibility for cybercrime as well. Cybercrime itself is closely linked to the actions of individuals, i.e. natural erson, but the responsibility of companies is also unavoidable. This statement is especially emphasized when resources (equipment and declining software) are made available that enable the commission of cybercrime. The revolution in the field of informatics, numerous social networks, e-education, and all the way to numerous forms of internet communication that enable electronic contracting, payment and e-banking, has led to mandatory standardization in this area. As in any other area, there is a more than enviable level of abuses that are prohibited, especially criminal law. Bosnia and Herzegovina can be considered a country that has legally regulated this issue in an adequate manner and harmonized it with the requirements of the international community.Thus, we have state (B&H) legislation in the field of criminal law, electronic conclusion of contracts, secure and qualified electronic signature, competition law and consumer protection law. Enumerated is the basic set of regulations in this area. The Entities and the BD BiH have a legal definition in the areas of electronic communication and criminal justice. In the Criminal Code of the FB&H we have a special chapter called Crimes against electronic data processing systems, while in the RS we have a chapter called Crimes against the security of computer data. In BD B&H, as well as in FBiH, we have the same systematization and the title of the chapter that deals with the sanctioning of this type of criminal offenses. Electronic payment and distance selling are specifically regulated by the Law on Consumer Protection in BiH.

Keywords: *cybercrime, competition, crime, electronic data, electronic business.*

1. POJAM KIBERNETSKOG KRIMINALA

Brojne su definicije kibernetskog kriminala.U osnovnom smislu riječi to je svako nezakonito ponašanje usmjereno na elektronske operacije protiv sigurnosti računarskih sisitema i podataka koji se u njima obrađuju, tesvako nezakonito ponašanje vezano za ili u odnosu na računarski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posjedovanje, nuđenje i distribucija informacija preko računarskih sistema i mreža. Iz ove osnovne definicije mogu se izdvojiti zajednička obilježja (konkretni oblici ovog oblika kriminala). Radi se o sljedećim obilježjima:

a) neovlašten pristup računarskom sistemu ili mreži kršenjem mjera bezbjednosti;
b) oštećenje (uništenje) računarskih podataka ili programa;
c) neovlašteno korištenje zaštićenih i tuđih podataka;
d) razne računarske sabotaže (brisanje ili promjena ulaznih podataka);
e) neovlašteno presretanje komunikacija (prema, od ili unutar računarskih sistema i mreža);
f) različiti oblici prevarnog postupanja korištenjem tuđih računarskih sistema, mreža i njima pripisanih podataka;
g) računarskašpijunaža (otkrivanje poslovnih tajni, neovlašteno prisvajanje tuđih zaštićenih podataka, odavanje tuđih poslovnih tajnu uz nadoknadu, i dr.);
h) prouzrokovanje velikih direktnih i indirektnih šteta (gubitaka);
i) unošenje različitih oblika virusa sa namjerom da se izazove zastoj, oštećenje računarskog sistema, i drugo.

Postoje i različite terminološke dileme u stručnoj literaturi. Tako, svakako smatramo potrebnim navesti kako je u Republici Hrvatskoj napravljena mala terminološka zbrka lošim prijevodom Konvencije-engleski naziv *Convention on Cybercrime* preveden je kao Konvencija o kibernetičkom kriminalu, mada riječ kibernetika (engl. *Cybernetics*) nije istoznačnica riječi cyber. Kibernetikubi najkraće mogli definirati kao "sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta, a za cyber još ne postoje precizne definicije, no Rječnikstranih riječi navodi daje cyber prvi element u riječima koji označava što vezano uzsvijet prividne stvarnosti koji nastaje pomoću kompjutera... pored toga svakako želimo naglasiti da pod pojam cyber-kaznena djela treba svrstavatisamo kaznena djela kod kojih je uporaba računala ili računalne mreže bitna zabiće

kaznenog djela, a ne sva kaznena djela u kojima se na neki način kaosredstvo izvršenja pojavljuje računalo s pripadnom perifernom opremom. Takoprimjerice kazneno djelo krivotvorenja novca nije računalno kazneno djelo bezobzira da li se počinitelj prilikom krivotvorenja novca služio računalom - bit togkaznenog djela je izrada lažnog novca ili preinačenje pravog novca s ciljem da gastavi u optjecaj, a računalo (uključujući skener i pisač) se tu pojavljuju samo kaotehničko sredstvo za lakše počinjenje kaznenog djela (Vojković i ostali: 123-124).

Bez obzira na ove jezičke dileme očigledno je da se radi o vrsti kriminala koji je upravljen protiv sistema računarske obrade podataka i sa njima povezanim djelima. Kada vidimo generalno određenje zabranjenih djela prema Konvenciji onda je više nego razvidno da se radi o sinonimima između pojmova kibernetskog kriminala i krivičnih djela protiv sistema elektronske obrade podataka, odnosno sistema bezbjednosti kompjuterskih podataka. Ovo je terminologija koja se koristi KZ FBiH, Glava XXXII-ga. Istu definiciju koristi i KZ BD BiH. KZ RS-a u Glavi XXXII koristi naziv Krivična djela protiv bezbjednosti kompjuterskih podataka, pri čemu se može konstatovati da se u oba slučaja radi o sinonimima.

Nadalje se možemo se koristiti osnovnom definicijom iz KZ FBiH prema kojoj (čl. 393 KZ FBiH, Oštećenje računarskih podataka i programa) ko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ilinepristupačnim tuđe računarske podatke ili računarske programe počinio je krivično djelo koje se može karakterisati kao jedan od pojavnih oblika računarskog kriminala. Računarski kriminal je i svaki neovlašteni upad (napad) na računarski sistem koji je u vlasništvu drugog pravnog ili fizičkog lica sa namjerom da se izazove šteta, počini krivotvorenje,prevara, ometanje rada, sabotaža, ili da se izvrši neki drugi oblik nedozvoljenog ponašanja. Pored toga, postoji i kvalifikovani oblik ove vrste krivičnh djela a to je kada je krivično djelo počinjeno protv sistema koji su značajni organima vlasti, javnim službama, javnim ustanovama, privrednim društvima ili drugom pravnim licima od posebnog javnog interesa. U ovom posljednjem slučaju radilo bi se o kvalifikovanom obliku krvičnog djela.

2. IZVORI PRAVA

Pozitivni izvori prava su svi oni zakonski i podzakonski akti kojima se uređuje neki od oblika kibernetskog kriminala. Uvažavajući složenost ustavnog uređenja ova problematika je normirana na sljedećim nivoima vlasti u BiH:

a) Državni nivo Bosne i Heregovine,
b) Entitetski nivoi (FBiH i RS) i

c) Nivo Brčko distrikta Bosne i Hercegovine.

Radi se o sljedećim krivično-pravnim, zakonodavnim aktima:

a) Krivični zakon BiH,
b) Krivični zakon FBiH,
c) Krivični zakon RS-a i
d) Krivični zakon BD BiH.

Opšta materija elektronskog polsovanja uređena je na državnom nivou BiH i entitetskim nivoima. U pregled su uvršteni i pravni akti čija je izrada u toku, odnosno nalaze se u nekoj od zakonodavnih procedura. Radi se o sljedećim zakonskim i podzakonskim aktima:

a) Zakon o elektronskom potpisu BiH,
b) Zakon o elektronskom dokumentu BiH,
c) Zakon o elektronskom pravnom i poslovnom prometu BiH,
d) Zakon o elektronskom dokumentu FBiH,
e) Zakon o elektronskom potpisu RS-a,
f) Zakon o elektronskom dokumentu RS-a,
g) Zakon o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka BiH,
h) Zakon o akreditaciji BiH,
i) Zakon o upravnom postupku BiH,
j) Nacrt Zakona o elektronskoj identifikaciji i elektronskim transakcijama BiH,
k) Nacrt Zakon o elektronskoj identifikaciji BiH,
l) Nacrt Zakona o elektronskom potpisu FBiH,
m) Zakon o elektronskom potpisu Brčko distrikta BiH (usvojen 2010 a stavljen van snage 2015),
n) Odluka o osnovama za upotrebu elektronskog potpisa i ovjeravanja u BiH,
o) Odluka o elektronskom poslovanju i elektronskoj vladi BiH,
p) Uputstvo o razvoju i održavanju web stranica institucija BiH,
q) Pravilnik o mjerama i postupcima upotrebe i zaštite elektronskog potpisa, sredstava za formiranje elektronskog potpisa i sistema certficiranja BiH,
r) Pravilnik o evidenciji ovjerilaca BiH,
s) Odluka o dopuni tarife administrativnih taksi BiH,
t) Pravilnik o bližim uslovima za izdavanje kvalificiranih potvrda BiH,
u) Odluka o stavljanju van snage odluke o osnovama upotrebe elektronskog potpisa i pružanja uskluga ovjeravanja BiH,
v) Pravilnik o evidenciji certifikacionih tijela u RS-u,

w) Pravilnik o posebnim uslovima koje moraju da ispunjavaju certifikaciona tijela RS-a,
x) Pravilnik o tehničko-tehnološkim procedurama u RS-u,
y) Pravilnik o mjerama informacione bezbjednosti RS-a,
z) Pravilnik o izdavanju vremenskog pečata u RS-u,
aa) Pravilnik o postupku izdavanja dozvole i upisu u registar certifikovanih tijela za izdavanje ES u RS.

Potrebno je još izdvojiti i ratifikovanu Konvenciju o kibernetskom kriminalu iz 2001. godine koja je činom ratifikacije postala sastavni dio pravnog poretka BiH. Uvažavajući pravnu snagu i važnost međunarodnih ratifikovanih konvencija poći ćemo od definicije kibernetskog kriminala koja postoji u ovoj Konvenciji.

3. KONVENCIJA O KIBERNETSKOM KRIMINALU - POJAM KIBERNETSKOG KRIMINALA

Konvencija nam ne daje jednu jedinstvenu definciju kibernetskog kriminala pošta se ista koristi tehnikom koja nam kroz opise pojedinih nedozvoljenih (zabranjenih) oblika ponašanja u ovoj oblasti daje i njihova osnovna obilježja. Terminologija koja se koristi u zvaničnom prevodu Konvencije nam govori i o:

a) vrstama kompjuterskih prekršaja,
b) kompjuterskim prekršajima u vezi sa sadržajem,
c) prekršajima u vezi napada na intelektualnu svojinu i odnosna prava i
d) drugi oblici odgovornosti.

Konvencija nastoji nastaviti zajedničku kriminalističku politiku usmjerenu na zaštitu društva od cyber kriminala, osobito usvajanjem odgovarajućeg zakonodavstva i poticanjem međunarodne suradnje. Odredbe Konvencije odnose se na kršenje autorskih prava, prijevaru na računalu, dječju pornografiju i kršenje sigurnosti mreže, nezakonitog pristupa, ometanju podataka, ometanju sustava, zlouporabi uređaja, krivotvorenju računala, itd. Sve države koje ratificiraju ili pristupaju Konvenciji suglasne su osigurati da njihovi nacionalni zakoni kriminaliziraju tamo utvrđene postupke (Rakonić, 20).

Prvi naziv i obilježje je Nedozvoljeni pristup (čl. 2 Konvencije) koji nam kaže da svaka strana usvaja takve zakonodavne i druge neophodne mjere koje se ukažu potrebnim dabi se neko ponašanje utemeljio kao krivično djelo, shodno njenom internom pravu, namjerni ili bespravnimpristupom dijelu kompjuterskog sistema. Jedna strana može postaviti za uslov da prekršaj bude počinjen kršenjem mjera

sigurnosti u namjeri da se pridobiju kompjuterski podaci ili u bilokojoj drugoj bespravnoj namjeri, ili da bude u vezi sa kompjuterskim sistemom povezanim naneki drugi kompjuterski sistem.

Drugi naziv i obilježje je Nezakonito presretanje (čl. 3 Konvencije) koji kaže da svaka strana usvaja zakonodavne i druge mjere koje se ukažu potrebnim da bi se utemeljilokao krivično djelo, shodno internom pravu, namjerno i bespravo presretanje(izvršenotehničkim sredstvima) kompjuterskih podataka, tokom nejavnih prenosa, u odredištu, napočetku ili unutar kompjuterskog sistema, ubrajajući tu i elektromagnetske emisije koje potičuiz kompjuterskog sistema koji prenosi te kompjuterske podatke. Jedna strana može postavitiza uslov da djelo bude počinjeno u nepoštenoj namjeri namjeri ili da bude u vezi sakompjuterskim sistemom povezanim na neki drugi kompjuterski sistem.

Treći naziv i obilježje je Povreda integriteta podataka (čl. 4 Konvencije) koji kaže da svaka strana usvaja zakonodavne i druge mjere koje se ukažu potrebnim da bi seutemeljilo kao krivično djelo, shodno internom pravu, djelo, učinjeno sa namjerom ibespravno, oštećivanja, brisanja, izmjenjivanja ili poništavanja kompjuterskih podataka.Strana može sebi ostaviti za pravo da zahtijeva da prethodno opisani postupak prouzrokujeozbiljne štete.

Četvrti naziv i obilježje je Povreda integriteta sistema (čl. 5 Konvencije) koji kaže da svaka strana usvaja zakonodavne i druge mjere koje se ukažu potrebnim da bi se utemeljilakao krivično djelo, shodno internom pravu, ozbiljna povreda, učinjena sa namjerom ibespravno, funkcionisanja kompjuterskog sistema, putem unošenja, prenosa, oštećenja,brisanja, izmjene ili ukidanja podataka.

Peti naziv i oblježje je Zloupotreba uređaja (čl. 6 Konvencije) kojikaže da svaka strana usvaja zakonodavne i druge mjere koje se ukažu potrebnim da bi seutemeljilo kao krivično djelo, shodno internom pravu, kada se počini s namjerom i bespravno:

a) proizvodnja, prodaja, dobijanje na korištenje, uvoz, distribucija ili drugi oblici stavljanja na raspolaganje:
   - uređaja, ubrajajući tu i kompjuterske programe prvenstveno napravljene ili prilagođene za omogućavanje činjenja jednog od utvrđenih prekršaja;
   - lozinke, koda za pristup ili sličnih kompjuterskih podataka koji omogućavaju pristup cjelini ili dijelu kompjuterskog sistema, u namjeri da se iskoriste za činjenje jednog ili drugog od pobrojanih prekršaja;

b) posjedovanje elementa gore navedenih u namjeri da bude iskorišten za činjenje jednog ili drugog od navedenih prekršaja. Strana može odlučiti da se u internom pravu izvjesnom broju tih elemenata pridoda krivična odgovornost.

Ovaj član se ne može interpretirati kao onaj koji nameće krivičnu odgovornost u slučajukada proizvodnja, prodaja, dobijanje na korištenje, uvoz, distribucija ili drugi oblici stavljanjana raspolaganje (citirani u ovom člana) nemaju za cilj činjenje prekršaja kako je toustanovljeno shodno Konvenciji, kao u slučaju ovlaštenih pokušajaili zaštite kompjuterskog sistema.Svaka strana može sebi ostaviti za pravo da ne primjenjuje ovaj dio Konvencije poduslovom da to ograničenje ne utiče na prodaju, distribuciju ili svako drugo stavljanje naraspolaganje elemenatautvrđenih Konvencijom.

Konvencija vrši klasifikacijuzabranjenih aktivnosti na:

a) kompjuterske prekršaje, koji mogu biti:
   - kompjutersko falsifikovanje i
   - kompjuterska prevara;
b) prekršaji u vezi sadržaja, a koji mogu bitiprekršaji koji se odnose na dječiju pronografiju;
c) prekršaji u vezi napada na intelektualnu svojinu i odnosna prava, a koji mogu biti prekršaji u vezi napada na intelektualnu svojinu i odnosna prava.

Ukoliko bi imali namjeru da definišemo određena zajednička obilježja pojedinih djela onda ćemo vidjeti da Konvencija sadrži i određeni nivo obilježja bića krivičnog djela. Tako se kod djela kompjuterskog falsifikata govori o unošenju, izmjeni, brisanju ili ukidanju, namjernoi bespravno, kompjuterskih podataka, proizvodeći neautentične podatke, u namjeri da onibudu uzeti u obzir ili korišteni u legalne svrhe kao da su autentični, pa bili oni ili ne čitki irazumljivi. Kada ovo usporedimo sa rješenjima u nacionalnom pravu vidjećemo da je većina termina preuzeta u odgovarajućem značenju i prenešena u pojedina krivčna djela koja se odnose na ovu oblast.

Konvencija daje osnova i za odgovornost pravnog lica. Ovo je posebno značajno sa stanovišta opšteg koncepta odgovornosti pravnih i odgovornih lica u pravnom licu koja je u naš krivično-pravni sistem uvedena spomenute 2002. godine. Pa tako, svaka strana usvaja zakonodavne i druge mjere koje se ukažu potrebnim da bi se pravna lica mogla smatrati odgovornim za prekršaje utvrđene u primjeni ove Konvencije, kada suoni počinjeni za njihov račun od strane bilo kojeg fizičkog lica

koje djeluje bilo individualno bilo kao član nekog organa pravnog lica, a koje vrši ovlasti upravljanja u svom sjedištu, naosnovu:

a) zastupanja pravnog lica;
b) ovlaštenja da donosi odluke u ime pravnog lica;
c) ovlaštenja da vrši kontrolu u okviru pravnog lica.

Osim pobrojanih slučajeva svaka strana usvaja mjere neophodne da bise osiguralo da se pravna lica mogu smatrati odgovornim za slučaj kada izostanaknadgledanja ili kontrole od strane pravnog lica omogući činjenjeprekršaja za račun tog pravnog lica a od strane fizičkog lica kojedjeluje pod njegovom ingerencijom.Prema sudskim principima odgovornost pravnog lica može biti krivična,građanska ili upravna.Ta odgovornost se utvrđuje bez obzira na krivičnu odgovornost fizičkih lica koja supočinila prekršaj.

Ova materija je uređena putem KZ BiH Glavom XIV, Odgovornost pravnih lica za krivična djela. Ova glava propisuje odgovornost pravnog lica, izuzimajući BiH, FBiH, RS, BD BiH, kanton, grad, opštinu i mjesnu zajednicu, za krivično djelo koje je počinilac učinio u ime, za račun ili u korist pravnog lica.Ova glava propisuje kazne i druge krivično-pravne sankcije koje se mogu izreći pravnom licu, kao i pravne posljedice osude pravnog lica za krivično djelo.Pod uslovima propisanim zakonom, za određena pravna lica može biti isključena ili ograničena primjena pojedinih kazni ili drugih krivično-pravnih sankcija koje se mogu izreći pravnim licima. Krivični postupak protiv pravnih lica vodi se po odredbama Zakona o krivičnom postupku Bosne i Hercegovine (čl. 122 KZ BiH). Na isti način ova materija je uređena putem KZ FBiH (Glava XIV, Odgovornost pravnih lica za krivična djela), kao i u KZ BDiH. U RS-u ovo pitanje je uređeno na isti način samo u okviru već spomenute Glave X, Odgovornost pravnih lica za krivična djela.

Konvencija posebno uređuje pitanja koja se odnose na tzv. brzo čuvanje sačuvanih kompjuterskih podataka i isto se odnosi na:

a) brzuzaštitu pohranjenih kompjuterskih podataka i
b) zaštitu i brzu distribuciju podataka u vezi prometa.

U pogledu pretresanje i pljenidbeveć pohranjenih kompjuterskih podataka Konvencija podrazumijeva pretraživanje i pljenidbu pohranjenih kompjuterskih podataka. U pogledu prikupljanje u realnom vremenu kompjuterskih podataka Konvencija podrazumijeva sljedeće:

a) prikupljanje u realnom vremenu podataka u vezi prometa i

b) presretanje podataka u vezi sadržaja.

Pored iznešenog Knvencija reguliše i niz proceduralnih pitanja koja se odnose na problematiku: jurisdikcije, privremenih mjera, međunarodne pomoći, međusobne saradnjei drugo.

4. PRAVNO UREĐENJE KINERNETIČKOG KRIMINALA U BOSNI I HERCEGOVINI

Već smo izložili pravne izvore koji se odnose na pravno uređenje kibernetičkog kriminala. Materijalno uređenje ovog pravnog isntituta se vrši putem krivičnog zakonodavstva, entitetskog i BD BiH. Uređenje osnovnh pojmova koji su u direktnoj i tijesnoj vezi sa pravnim određenjem kibernetičkog kriminala uređeni su na državnom nivou (BiH), entitetskom i nivou BD BiH. Radi se o propisima kojima se uređuju pravna pitanja:

a) elektronskog potpisa,
b) sigurnog (kvalifikovanog) elektronskog potpisa,
c) elektronskog dokumenta i
d) pravnih aspekata elektronskog poslovanja.

Ova materija je predmetom obrade samo sa stanovišta pravnog definsanja pojedinih instituta pošto isti mogu biti medij putem koga se odvijaju određene nezakonite aktivnosti. Kao primjer možemo uzeti zloupotrebu elektronskog potpisa, presretanje elektronskih poruka, preinačavanje sadržine i uslova kod ugovora zaključenih elektronskim putem, etc. Bez namjere da se ulazi u elaboriranje pojedinih od pobrojanih pravnih instituta skrenućemo pažnju samo na činjenicu da je od 2006. godine data pravna validnost (dokazna snaga) ugovorima koji su zaključeni elektronskim putem, odnosno razmjenom eelektronskih poruka. Tako je Zakonom o elektronskom pravnom i poslovnom prometu BiH regulisano da pravno djelovanje podataka u elektronskoj formi i njihova upotreba kao dokaznog sredstva ne može se isključiti zbog činjenice da su u elektronskoj formi (čl. 12. Pravno djelovanje podataka u elektronskoj formi).

Suština materije kibernetičkih (računarskih-kompjuterskih) krivičnih djela uređena je entitetskim i BD BiH krivičnim zakonodavstvom. Ova materija je jedinstveno uređena u FBiH i BD BiH, dok u entitetu RS imamo nešto drugačije definicije, kao i drugačija krivična djela, iako se može reći da je suština uređena na istim principima. Nadalje će se izložiti rješenja koja postoje u oba entiteta i BD BiH. U

entitetu RS u okviru Glave XXXII, Krivična djela protiv bezbjednosti kompjuterskih podatala poznajemo sljedeća krivična djela:

a) Oštećenje kompjuterskih podataka i programa;
b) Kompjuterska sabotaža;
c) Izrada i unošenje kompjuterskih virusa;
d) Kompjuterska prevara;
e) Neovlašteni pristup zaštićenom kompjuteru, kompjuterskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka;
f) Sprječavanje i ograničavanje pristupa javnoj kompjuterskoj mreži;
g) Neovlašteno korištenje kompjutera ili kompjuterske mreže.

U entitetu FBiH i BD BiH u okviru Glave XXXII, Krivična djela protiv sistema elektronske obrade podataka poznajemo sljedeća krivična djela:

a) Oštećenje računarskih podataka i programa;
b) Računarsko krivotvorenje;
c) Računarska prevara;
d) Ometanje rada sistema i mreže elektronske obrade podataka;
e) Naovlašten pristup zaštićenom sistemu i mreži elektronske obrade podataka i
f) Računarska sabotaža.

Nadalje će se zajednički komentarisati zajednička i posebna obilježja bića pojedinog krivičnog djela. Prvo krivično djelo se odnosi na oštećenje računarskih podataka i programa. Biće krivičnog djela je sadržano u činjenici da je nezakonita aktivnost upravljena ka tome da se: oštete, izmijene, izbrišu, unište ili na drugi način učine neupotrebljivim ili nepristupačnim tuđi računarski podaci ili računarski programi a što je zapriječeno novčanom kaznom ili kaznom zatvora do 1 (jedne) godine. Sve naprave, sredstva, računarski programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja krvičnog djela biće oduzeti. U entitetu RS razlikuje se sistem sankcija u ovisnosti od visine prouzrokovane štete (preko 10.000,00 i preko 50.000,00 KM), razlikuju se i zatvorske sankcije a koje mogu da idu do 5 (pet) godina.

KZ FBiH poznaje i opis koji nam govori o neovlaštenom presretanju prenosa računarskih podataka a što za posljedicu ima onemugućavanje ili otežavanje rada ili korištenja računarskog sistema, računarskih podataka ili programa ili same računarske komunikacije. Dodatno, KZ FBiH poznaje i kvalifikovani oblik ovog krivičnog djela kada je isto upravljeno ili počinjeno u odnosu na računarski sistem, podatak ili program organa vlasti, javne službe, javne ustanove ili privrednog

društva od posebnog javnog interesa, ili je prozrokovana znatna šteta tada je zapriječena kazna zatvora do 5 (pet) godina. Definicija i razrada ovog krivičnog djela u FBiH je šira u odnosu na KZ RS-a jer je sankcionisana i neovlaštena izrada, nabava, prodaja, posjedovanje ili činjenje drugome dostupnim posebne naprave, sredstva, računarskih programa ili računarskih podataka stvornih ili prilagođenih radi počinjenja ovog krivičnog djela. Vidimo da su osnovna obilježja ovog krivičnog djela neovlašteni pritup računarskoj opremi, podacima i programima sadržanim u istoj sa ciljem njihovog oštećenja putem izmjene, brisanja ili prikrivanja kako bi se drugoj strani prouzrokovala šteta. Štetna posljedica može biti različita i uvijek će predstavljati faktičko pitanje koje se treba cijeniti od slučaja do slučaja. U obzir se može uzeti:

a) obim napada,
b) vrste i značaj podataka koji su npr. izmijenjeni,
c) materijalna šteta koja je nastupila, npr. gubitak poslova,
d) nematerijalna šteta, npr. gubitak poslovnog ugleda na tržištu,
e) vrijeme potrebno za otklanjanje štetnih posljedica, te
f) ponovno dovođenje sistema u funkcionalno stanje, etc.

U vezi sa krivičnim djelom krivotvorenja računarskih podataka u opisu djela je navedeno da ko neovlašeno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računarske podatke ili programe koji imaju vrijednost za pravne odnose, sa ciljem da se upotrijebe kao pravi ili ukoliko sam upotrijebi takve podatke ili programe, kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine. Ukoliko je krivično djelo u odnosu na računarske podatke ili programe organa javne službe, javne ustanove ili privrednog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kazniće se kaznom zatvora od 3 (tri) mjeseca do 5 (pet) godina, a pošto ova djelopredstavlja kvalifikovani oblik krivičnog djela. Pored toga ko neovlašćeno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom pristupačnim posebne naprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi učinjenja opisanog krivičnog djela kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine. Kao i u prethodnom slučaju posebne naprave, sredstva, računarski programi ili podaci stvoreni, korišćeni ili prilagođeni radi učinjenja krivičnih djela kojima je učinjeno već opisano krivično djelo oduzeće se.

KZ RS-a ne poznaje ovaj oblik krivičnog djela računarskog kriminala što ne znači da se iz opisa nekih drugih krivičnoh djela ove glave KZ RS-a ne može izvući zaključak da je ovakav vid zabranjenih aktivnosti inkriminisan. Takav opis

možemo naći u čl. 408 KZ RS-a (Kompjuterska sabotaža) gdje zakonodavac određuje da ko unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili programili uništi ili ošteti kompjuter ili drugi uređaj za elektronsku obradu i prenos podataka sa namjerom da onemogući ili znatno ometa postupak elektronske obrade i prenosa podataka koji su od značaja za republičke organe, javne službe, ustanove, privredna društva ili druge subjekte, kazniće se kaznom zatvora od 6(šest) mjeseci do 5 (pet) godina. Ovaj nam se opis čini najprihližnijim za krivično djelo krivotovrenje iako KZ FBiH (time i BD BiH) poznaje posebno djelo Računarska sabotaža (KZ FBiH, čl. 398) sa istovjetnim opisom bića krivičnog djela samo što je zapriječena druga sankcija. Tako, ukoliko je šteta veća od 500.000,00 KM počinilac će se kazniti kaznom zatvora u trajanju od 1 (jedne) do 8 (osam) godina zatvora. Ovo krivično djelo je u KZ FBiH opisano na slijedeći način: ko unese, izmijeni, izbriše ili prikrije računarski podatak ili program ili se na drugi način umiješa u računarski sistem, ili uništi ili ošteti naprave za elektronsku obradu podataka s ciljem da onemogući ili znatno omete postupak elektronske obrade podataka značajnim organima vlasti, javnim službama, javnim ustanovama, privrednim društvima ili drugim pravnim licima od posebnog javnog interesa kazniće sena opisani način.

Oba entitetska zakona poznaju krivično djela računarske ili kompjuterske prevare. U FBiH ovo je uređeno na slijedeći način: ko neovlašteno unese, ošteti, izmijeni ili prikrije računarski podatak ili program ili na drugi način utiče na ishod elektronske obrade podataka sa ciljem da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se kaznom zatvora od 6 (šest) mjeseci do 5 (pet) godina. Ukoliko je krivičnim djelom pribavljena imovinska korist koja prelazi 10.000 KM, počinitelj će se kazniti kaznom zatvora od 2 (dvije) do 10 (deset) godina. Ukoliko je krivičnim djelom pribavljena imovinska korist koja prelazi 50.000 KM, počinitelj će se kazniti kaznom zatvora od 2 (dvije) do 12 (dvanaest) godina. Ukoliko se predmetno krivično djelo počini samo sa ciljem da se drugog ošteti, kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine. Sličan opis bića krivičnog djela nailazimo i u entiteu RS samo što se zapriječene sankcije nešto blaže pošto je najteža zapriječena sankcija kazna zatvora u trajanju od 10 (deset) godina.

KZ FBiH poznaje dva krivična djela koja nemamo u sistematici KZ RS-a. Radi se o krivičnim djelima Ometanje rada sistema i mreže elektronske obrade podataka (čl. 396 KZ FBiH) i krivično djelo Neovlaštenog pristupa zaštićenom sistemu i mreži elektronske obrade podataka (čl. 397 KZ FBiH). Ovo pitanje je normirano na slijedeći način. Ometanje rada sistema i mreže elektronske obrade podataka postoji

kada imamo neovlašteni pristup u sistem ili mrežu elektronske obrade podataka koji izaziva zastoj ili poremećaj rada tog sistema ili mreže, kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine. Kod neovlaštenog pristupa zaštićenom sistemu i mreži elektronske obrade podataka imamo djelo neovlaštenog uključivanja u sistem ili mrežu elektronske obrade podataka kršenjem mjera zaštite, a počinilac će se kazniti novčanom kaznom ili kaznom zatvora do 1 (jedne) godine. Pored toga, ko upotrijebi podatak dobiven na prednje opisan način kazniće se kaznom zatvora do 3 (tri) godine.Ako su ovim krivičnim djelom prouzrokovane drugom teške posljedice, počinitelj će se kazniti kaznom zatvora u trajanju od 6 (šest) mjeseci do 5 (pet) godina. Ovaj neovlašteni pristup u KZ RS-a (čl. 411, Neovlašteni pristup zaštićenom kompjuteru, kompjuterskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka) uređen je na slijedeći način. Ko se, kršeći mjere zaštite, neovlašteno uključi u kompjuter ili kompjutersku mrežu ili neovlašteno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili kaznom zatvora do 6 (šest) mjeseci. Ko snimi ili upotrijebi podatak dobiven na prethodno utvrđen utvrđen način kazniće se novčanom kaznom ili kaznom zatvora do 2 (dvije) godine.Ako je usljed ovog djela došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posljedice, učinilac će se kazniti kaznom zatvora do 3 (tri) godine. Istom kaznom kazniće se i ko izradi, pribavi, proda ili da na korištenje uputstvo ili sredstvo koje je namijenjeno za ulaženje u kompjuterski sistem. U ovom kontekstu treba posmatrati i krivično djelo Neovlašteno korištenje kompjutera ili kompjuterske mreže (KZ RS-a, čl. 413). Ko neovlašteno koristi kompjuterske usluge ili kompjutersku mrežu u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili kaznom zatvora do 6 (šest) mjeseci.

Pored pobrojanog, u pravni sistem RS-a (KZ RS-a) poznaje sljedeća dva djela koja nisu sistematizovana u KZ FBiH. Radi se o djelima Izrade i unošenje kompjuterskog virusa (čl. 409 KZ RS-a) i krivično djelo Sprečavanja i ograničavanja pristupa javnoj kompjuterskoj mreži (čl, 412 KZ RS-a). Kod krivičnog djela izrada i unošenje kompjuterskih virusa sankcioniše se da ko napravi računarski virus u namjeri njegovog unošenja u tuđi kompjuter ili kompjutersku ili telekomunikacionu mrežu, kazniće se novčanom kaznom ili kaznom zatvora do 6 (šest) mjeseci. Ko unese računarski virus u tuđi kompjuter ili kompjutersku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili kaznom zatvora do 2 (dvije) godine.Uređaj i sredstva kojima je izvršeno ovo krivično djelo oduzeće se.Kod krivičnog djela sprečavanje i ograničavanje pristupa javnoj kompjuterskoj mreži radi se o situaciji kada neko neovlašteno sprječava ili ometa pristup javnoj

kompjuterskoj mreži, kazniće se novčanom kaznom ili kaznom zatvora do 1 (jedne) godine.Ako ovo djelo učini službeno lice u vršenju službe, kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine.

Iako izlazi iz konteksta ovog priloga potrebno je spomenuti i djela kod kojih korištenje računara predstavlja sredstvo za počinjenje krivičnih djela. Ona se spominju u kontekstu Dodatnog protokola Konvenciji. U odnosu na izložena entitetska rješenja izvan ove dvije posebne glave krivično zakonodavstva poznaje i djela kod kojih se računari, odnosno kompjuteri koriste kao sredstvo za vršenje drugih vrsta krivičnih djela. Tako, ko sa djetetom starijim od 15 (petnaest) godina, koristeći kompjutersku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sastanak radi vršenja obljube ili sa njom izjednačene polne radnje, ili radi proizvodnje pornografskog materijala, ili radi drugih oblika seksualnog iskorištavanja i pojavi se na dogovorenom mjestu radi sastanka, kazniće se kaznom zatvora od 1 (jedne) do 5 (pet) godina.

Ukoliko je ovo djelo izvršeno prema djetetu mlađem od 15 (petnaest) godina, učinilac će se kazniti kaznom zatvora od 2 (dvije) do 8 (osam) godina (čl. 178 KZ RS-a, Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta). U ovu kategoriju spada i djelo kada se putem štampe, radija, televizije, kompjuterskog sistema ili društvene mreže, na javnom skupu ili javnom mjestu ili na drugi način javno poziva, izaziva ili podstiče ili učini dostupnim javnosti letke, slike ili neke druge materijale kojima se poziva na nasilje ili mržnju usmjerenu prema određenom licu ili grupama zbog njihove nacionalne, rasne, vjerske ili etničke pripadnosti, boje kože, pola, seksualno opredjeljenja, invaliditeta, rodnog identiteta, porijekla ili kakvih drugih osobina, kazniće se novčanom kaznom ili kaznom zatvora do 3 (tri) godine (čl. 359 KZ RS-a, Javno izazivanje i podsticanje nasilja i mržnje). Ovdje se radi o prihvatanju Dodatnog protokola uz Konvenciju o kibernetičkom kriminalu i o kriminalizacijiakata rasizma i ksenofobije počinjenih putem računarskih sistemakoju je donijelo Vijeće Europe 28. januara 2003. godine. Dodatni protokol zahtijeva, od zemalja sudionica, kriminalizaciju širenja rasističkih i ksenofobnih sadržaja putem računarskih sisitema, kao i rasističko iksenofobno obojene prijetnje i uvrede, te negiranje holokausta i ostalih genocida.

5. POSLJEDICE KOJE MOŽE IMATI KIBERNETIČKI KRIMINAL PO PRIVREDNE, A POSEBNO FINANSIJSKE AKTIVNOSTI

U suvremenom poslovanju kako gospodarstva, tako i javne uprave te drugih osoba sve se češće koriste elektroničke baze podataka, tako se danas brojne evidencije i očevidnici vode primarno, pa i isključivo, u elektroničkom obliku. Mnoge od tih elektroničkih baza podataka imaju iznimnu vrijednost za pravne odnose. Izmjena, uništavanje, brisanje, činjenje neuporabljivim takvih podataka-pa i takve i slične akcije napravljene od osobe ovlaštene za uporabu takvih podataka, a kako bi se takvi lažni podaci uporabili-danas mogu prouzročiti velike štete i predstavljaju iznimnu društvenu opasnost (Vojković i ostali: 131). Ovaj citat posebno možemo staviti u kontekst pandemije i sve češćeg i obimnijeg (vrlo često i jedinog) komuniciranja on-line putem. Već duže vremena brojne se aktivnosti odvijaju u on-line formi a što rapidno povećava mogućnost različitih inkriminisanih aktivnosti. Kao veliki izvor potencijalne opasnosti javlja se podnošenje različitih oblika finansijskih dokumenata i izvještaja, kao što su:

a) bilans stanja, bilans uspjeha i bilješke uz finansijske izvještaje,
b) podnošenje PDV prijava,
c) podnošenje poreznih prijava na dohodak,
d) podnošenje prijava za porez na imovinu,
e) e-plaćanje,
f) e-banking,
g) transferi noca (WU, WM, etc.)
h) elektronske doznake,
i) kartično poslovanje,
j) zaključivanje ugovora u elektronskoj formi, etc.

Ovo su samo neki od oblika poslovanja u elektronskoj formi koji daju jednu široku lepezu mogućnosti različittih zloupotreba. Kao počinitelji se mogu navesti: programeri sa detaljnim poznavanjem programa; zaposlenici ili bivši zaposlenici; programeri financijskih sustava; računalni korisnici i računalni operateri. U kontekstu utvrđivanja napadača ne može se tvrditi da su ovo jedini napadači (Potrka, str. 90).

Kako bi se spriječio kriminal pravnih lica, u pravnim sistemimaevropskih i sjevernoameričkih država pojavila se potreba za uvođenjemkrivične odgovornosti pravnih lica. Kriminalitet pravnihlica poznat je u stručnoj i široj javnosti kao kriminal bijelog okovratnikaili kriminal društava (korporacija). Ime je dobio po engleskomizrazu white-collar (bijeli okovratnik) koji, pogotovo u SAD-u,označava

zaposlenike koji se uglavnom bave intelektualnimradom. Oni stoga zauzimaju više položaje u preduzećima, imajubolje plate kao i veći ugled i položaj u društvu u odnosu na klasičnuradničku klasu (blue-collar) koja se uglavnom bavi fizičkimradom (www.wikipedia, 2012). Uglavnom se radi o različitim oblicima kriminalnih aktivnosti koje imaju prevaran karakter sa glavnim ciljem, sticanje protivpravne imovinske koristi. Osnovne karakteristike kriminalabijelog okovratnika su oblasti u kojoj se vrši, a to su: oblast realnog poslovanja, osiguranja, bankarstva, berze, finansije, računovodstvo i revizija... Poredtoga obilježje ove vrste kriminala je i društveni status počiniocate zaštićenost počinilaca od progona i kažnjavanja s obzirom nauticaj koji učinioci imaju zahvaljujući svom društvenom i političkompoložaju. Za krivična djela koja se ubrajaju u kriminal bijelogokovratnika karakteristično je i to da se vrše tiho, prikriveno,sofisticiranim metodama i na prevaran način. Posljednjih godinase i za kriminalitet korporacija koristi naziv kriminalitet bijelogokovratnika. Jedina razlika između ta dva vida kriminaliteta ješto je kod kriminaliteta bijelog okovratnika jače istaknut lični koristoljubivimotiv. Šteta koja nastaje izvršenjem tih krivičnih djelaje izuzetno velika, ne samo za pojedince već i za čitavo društvo (Trivun, 2019: 315).

Kada napravimo pregled pojedinih oblika krivičnih djela vezanih za kibernetički kriminal vidjećemo da se najčešće koriste sljedeći opisi: oštećenje računarskih podataka i programa, neovlašten pristup, računarsko krivitvorenje, neovlaštenja izmjena i brisanje, računarska prevara, računarska sabotaža, ometanje rada sistema obrade podataka, neovlašten pritup zaštićenom računarskom sistemu, unošenje virusa, etc. Posebno se kvalifikuju djela koja se odnose na neovlašten pristup i (zlo)upotrebu sistema elektronske obrade podataka koji imaju javni značaj. Već se spomenuto da se radi o tzv. kvalifikovanim oblicima krivičnih djela. Ono što se neizostavno nameće kao zaključak da je za svako od pobrajanih djela karakteristično da računari sa pripadajućim programima i podacima (baze podataka) predstavljaju sredstvo za izvršenje pobrojanih krivičnih djela. Posve je sigurno da će se brojna krivična djela preliti u ovu sferu i to sa stanovišta sve masovnijeg korištenja informaciono-komunikacionih tehnologija. Pored toga, posve je sigurno da sektori finansija, računovodstva i revizije,naročito zbog obima izvještavanja u elektronskoj formi, predstavljaju vrlo osjetljivu oblast za različite oblike kibernetičkog kriminala.

Vezano za perspektive u prevenciji i suzbijanju kibernetičkog i drugih oblika kriminala možemo se referisati na UNODC. U svom radnom dokumentu, Tajništvo Ureda UN-a za droge i kriminal (UNODC) primjećuje da zbog transnacionalne prirode kibernetičkog kriminala pitanja nacionalnog suvereniteta mogu ometati

kaznene istrage u nedostatku aktivne suradnje između tijela za provedbu zakona nadležnih sudbenih tijela. Brzina kojom kibernetički kriminalci mogu nanijeti štetu i krenuti na izbjegavanje otkrivanja također dovode do agresivnih agencija pod velikim vremenskim pritiscima, što sve više zahtijeva potrebu međunarodne suradnje. UNODC identificira zakonodavnu konvergenciju kao ključnu za učinkovitu suradnju. Divergencija u zakonodavstvu može potkopati učinkovitu provedbu. Države gdje određena jurisdikcija nedostaje ili se sveobuhvatno zakonodavstvo o kibernetičkom kriminalu slabo provodi, najčešća su sigurna utočišta za računalne kriminalce. Ovakvu vrstu razilaženja može se riješiti samo usuglašenim naporima za usklađivanje pravnih standarda i unaprjeđivanjem suradnje između jurisdikcija (Mikulin, 2019: 22).

KORIŠTENI PROPISI

1. Službeni glasnik BiH, Krivični zakon, (Sl. glasnik BiH, br. 3/03)
2. Službene novine FBiH, Krivični zakon (Sl. novine FBiH, br. 36/03).
3. Službeni glasnik RS-a, Krivični zakon (Sl. glasnik RS-a, br. 49/03)
4. Službeni glasnik BD BiH, Krivični zakon (Sl. glasnik BD BiH, br. 10/03)
5. Službeni glasnik BiH, Zakon o elektronskom, pravnom i poslovnom prometu (Sl. glasnik BiH, br. 126/07)
6. Službeni glasnik BiH, Zakon o elektronskom potpisu BiH (Sl. glasnik BiH, br. 91/06)
7. Službeni glasnik BiH, Zakon o elektronskom dokumentu BiH (Sl. glasnik BiH, br. 91/06)
8. Službene novine FBiH, Zakon o elektronskom dokumentu FBiH (Sl. novine FBiH, br. 55/13)
9. Službeni glasnik RS-a, Zakon o elektronskom potpisu RS-a (Sl. glasnik RS-a, br. 106/15)
10. Službeni glasnik RS-a, Zakon o elektronskom dokumentu RS-a (Sl. glasnik RS-a, br. 106/15)
11. Službeni glasnik BiH, Zakon o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka BiH (Sl. glasnik BiH, br. 56/08)
12. Službeni glasnik BiH, Zakon o akreditaciji BiH (Sl. glasnik BiH, br. 19/01)
13. Službeni glasnik BiH, Zakon o upravnom postupku BiH (Sl. glasnik BiH, br. 29/02, 12/04, 88/07, 93/09, 41/13, 53/16)
14. Konvencija o kibernetičkom kriminalu iz 2001. godine

LITERATURA

1. Vojković, G. Štambuk-Šunjić, M. Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske
2. Trivun, V. Odgovornost privrednih društava, Ekonomski fakultet Sarajevo, Sarajevo, 2019.
3. Mikulin, R. Kaznenopravna zaštita od kibernetičkog kriminala i uloga davatelja telekom usluga, Master's thesis / Diplomski rad, fakultete prometnih znanosti, Zagreb, 2019.
4. Rakonić, I. Kaznenopravni aspekti kibernetičkog ratovanja,Master's thesis/ Diplomski rad, Pravni fakultet zagreb, 2019.
5. Protrka, N. Međunarodna suradnja i sigurnost u suzbijanjukriminaliteta u kibernetičkom prostoru, Doctoral thesis / Disertacija, Univerzitet u Zadru, Zadar, 2018.