DIREKTIVA 2013/40/EU EUROPSKOG PARLAMENTA I VIJEĆA

od 12. kolovoza 2013.

o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 83. stavak 1.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ([1]),

u skladu s redovnim zakonodavnim postupkom ([2]),

budući da:

(1) Ciljevi su ove Direktive približiti kazneno pravo država članica u području napada na informacijske sustave, utvrđivanjem minimalnih pravila o definiranju kaznenih djela i odgovarajućih sankcija te poboljšati suradnju između nadležnih tijela, uključujući policiju i druge specijalizirane službe zadužene za izvršavanje zakona država članica, kao i nadležnih specijaliziranih agencija i tijela Unije kao što su Eurojust, Europol i njegov Europski centar za kibernetički kriminal te Europska agencija za sigurnost mreža i podataka (ENISA).

(2) Informacijski su sustavi ključni element političke, društvene i gospodarske interakcije u Uniji. Društvo sve više ovisi o takvim sustavima. Nesmetano djelovanje i sigurnost tih sustava u Uniji ključni su za razvoj unutarnjeg tržišta i konkurentnog i inovativnog gospodarstva. Osiguranje odgovarajuće razine zaštite informacijskih sustava trebalo bi biti sastavni dio učinkovitog sveobuhvatnog okvira preventivnih mjera koje prate odgovore kaznenog prava na kibernetički kriminal.

(3) Napadi na informacijske sustave, a posebno napadi povezani s organiziranim kriminalom sve su veća prijetnja kako u Uniji tako i u svijetu te postoji sve veća zabrinutost zbog potencijalnih terorističkih ili politički motiviranih napada na informacijske sustave koji su dio ključne infrastrukture država članica i Unije. To predstavlja prijetnju ostvarenju sigurnijeg informacijskog društva i područja slobode, sigurnosti i pravde te stoga zahtijeva odgovor na razini Unije te poboljšanu suradnju i koordinaciju na međunarodnoj razini.

(4) U Uniji postoji određen broj ključnih infrastruktura čiji bi poremećaj u radu ili uništenje imalo značajan prekogranični učinak. Iz potrebe da se poveća sposobnost zaštite ključne infrastrukture u Uniji postalo je jasno da bi mjere protiv kibernetičkih napada trebale biti dopunjene strogim kaznenopravnim sankcijama koje bi odražavale ozbiljnost takvih napada. Ključna infrastruktura mogla bi se protumačiti kao element, sustav ili njihov dio smješten u državi članici te je izvanredno važna za održavanje ključnih društvenih funkcija, zdravlja, zaštite, sigurnosti, gospodarske ili socijalne dobrobiti naroda, kao što su elektrane, prometne mreže ili državne mreže, te bi njihov poremećaj ili uništenje imalo značajan učinak u državi članici kao rezultat nemogućnosti održavanja tih funkcija.

(5) Postoje dokazi o tendenciji prema sve opasnijim i češćim napadima velikih razmjera na informacijske sustave, što često može imati ključnu važnost za države članice ili određene funkcije u javnom ili privatnom sektoru. Tu tendenciju prati razvoj sve sofisticiranijih metoda, kao što je stvaranje i uporaba takozvanih „botneta", što uključuje nekoliko faza kaznenog djela, pri čemu bi svaka faza mogla samostalno predstavljati ozbiljnu opasnost javnim interesima. Cilj je ove Direktive, među ostalim, uvesti kaznenopravne sankcije za stvaranje „botneta", to jest za uspostavu kontrole na daljinu nad značajnim brojem računala tako što se zaraze zlonamjernim softverom putem ciljnih kibernetičkih napada. Nakon što je stvorena, zaražena mreža računala koja čine „botnet" može biti aktivirana bez znanja korisnika računala kako bi se pokrenuo kibernetički napad velikih razmjera, što u pravilu može uzrokovati ozbiljnu štetu, kako je navedeno u ovoj Direktivi. Države članice mogu u skladu sa svojim nacionalnim pravom i praksom odrediti što predstavlja ozbiljnu štetu, kao što je prekid mrežnih usluga od velikog javnog značenja ili uzrokovanje velikih financijskih troškova ili gubitak osobnih podataka ili osjetljivih informacija.

(6) Kibernetički napadi velikih razmjera mogu uzrokovati znatnu gospodarsku štetu zbog prekida rada informacijskih sustava i komunikacija te zbog gubitka ili mijenjanja komercijalno važnih povjerljivih informacija ili drugih podataka. Trebalo bi se posebno potruditi da inovativna mala i srednja poduzeća budu bolje informirana o prijetnjama povezanima s takvim napadima i svojoj osjetljivosti na takve napade, s obzirom na to da sve više ovise o ispravnom funkcioniranju i dostupnosti informacijskih sustava, a resursi za informacijsku sigurnost često su ograničeni.

([1]) SL C 218, 23.7.2011., str. 130.

([2]) Stajalište Europskog parlamenta od 4. srpnja 2013. (još nije objavljeno u Službenom listu) i odluka Vijeća od 22. srpnja 2013.

(7) U ovom su području zajedničke definicije važne kako bi se u državama članicama osigurao dosljedan pristup primjeni ove Direktive.

(8) Potrebno je postići zajednički pristup sastavnim elementima kaznenih djela uvođenjem zajedničkih kaznenih djela nezakonitog pristupa informacijskom sustavu, nezakonitog ometanja sustava, nezakonitog ometanja podataka i nezakonitog presretanja.

(9) Presretanje uključuje, ali se nužno ne ograničava na slušanje, praćenje ili nadzor sadržaja komunikacija te pribavljanje sadržaja podataka bilo izravno kroz pristup i uporabu informacijskih sustava, ili neizravno tehničkim sredstvima uporabom elektroničkih naprava za prisluškivanje.

(10) Države članice trebale bi predvidjeti sankcije za napade na informacijske sustave. Te bi sankcije trebale biti učinkovite, proporcionalne i odvraćajuće te bi trebale uključivati kazne oduzimanja slobode i/ili novčane kazne.

(11) Ovom se Direktivom predviđaju kaznenopravne sankcije barem kada nije riječ o lakšim slučajevima. Države članice mogu u skladu sa svojim nacionalnim pravom i praksom odrediti što čini lakši slučaj. Slučaj se može smatrati lakšim kada su, primjerice, šteta uzrokovana kaznenim djelom i/ili rizik za javne ili privatne interese, kao što je integritet računalnog sustava ili računalni podaci, ili integritet, prava i drugi interesi osobe, nevažni ili su takve prirode da nije potrebno nametanje kaznenopravne sankcije u zakonskom okviru ni uvođenje kaznene odgovornosti.

(12) Utvrđivanje i izvješćivanje o prijetnjama i rizicima koje predstavljaju kibernetički napadi i povezana osjetljivost informacijskih sustava bitan su element učinkovitog sprječavanja i odgovora na kibernetičke napade te poboljšane sigurnosti informacijskih sustava. U tom bi kontekstu pomoglo osiguranje poticajnih mjera za izvješćivanje o sigurnosnim propustima. Države članice trebale bi nastojati predvidjeti mogućnosti otkrivanja i izvješćivanja o sigurnosnim propustima u pravnom smislu.

(13) Prikladno je predvidjeti strože sankcije kada napad na informacijski sustav počini zločinačka organizacija, kako je definirano u Okvirnoj odluci Vijeća 2008/841/PUP od 24. listopada 2008. o borbi protiv organiziranog kriminala ([1]), kada je počinjen kibernetički napad velikih razmjera, čime je zahvaćen znatan broj informacijskih sustava, uključujući i kada je cilj napada stvaranje „botneta", ili kada kibernetički napad prouzroči ozbiljnu štetu, uključujući i kada je napad izveden putem „botneta". Također je prikladno predvidjeti strože sankcije kada je napad počinjen na ključnu infrastrukturu država članica ili Unije.

([1]) SL L 300, 11.11.2008., str. 42.

(14) Uspostava učinkovitih mjera protiv krađe identiteta i drugih kaznenih djela povezanih s identitetom predstavlja još jedan važan element integriranog pristupa borbi protiv kibernetičkog kriminala. Svaka potreba za djelovanjem na razini Unije u borbi protiv ovakve vrste kriminalnog ponašanja također bi se mogla razmatrati u kontekstu evaluacije potrebe za sveobuhvatnim horizontalnim instrumentom Unije.

(15) Zaključci Vijeća od 27. do 28. studenog 2008. naznačili su kako bi s državama članicama i Komisijom trebalo izraditi novu strategiju, uzimajući u obzir sadržaj Konvencije Vijeća Europe o kibernetičkom kriminalu iz 2001. Ta je Konvencija pravni referentni okvir za borbu protiv kibernetičkog kriminala, uključujući napade na informacijske sustave. Ova se Direktiva nadovezuje na tu konvenciju. Dovršetak procesa ratifikacije te konvencije od svih država članica u najkraćem mogućem roku trebalo bi smatrati prioritetom.

(16) S obzirom na različite načine na koje se napadi mogu izvesti i s obzirom na brzinu kojom se hardver i softver razvijaju, ova Direktiva upućuje na alate putem kojih je moguće počiniti kaznena djela utvrđena u ovoj Direktivi. Takvi bi alati mogli uključivati zlonamjeran softver, uključujući one koji mogu stvoriti „botnete", koji se koriste za izvođenje kibernetičkih napada. Čak i kada je takav alat prikladan ili osobito prikladan za izvođenje nekog od kaznenih djela utvrđenih u ovoj Direktivi, moguće je da je proizveden u zakonitu svrhu. S ciljem da se izbjegne kriminalizacija u slučajevima kada se takvi alati proizvode i plasiraju na tržište u zakonite svrhe, kao što je testiranje pouzdanosti proizvoda informacijskih tehnologija ili sigurnosti informacijskih sustava, ti alati, uz uvjete opće namjere, također moraju ispunjavati uvjet izravne namjere uporabe tih alata za počinjenje jednog ili više kaznenih djela utvrđenih u ovoj Direktivi.

(17) Ovom se Direktivom ne nameće kaznena odgovornost kada su ispunjeni objektivni kriteriji za kaznena djela utvrđena u ovoj Direktivi, ali su djela počinjena bez namjere da se počini djelo, primjerice kada osoba ne zna da pristup nije dopušten ili u slučaju obveznog testiranja ili zaštite informacijskih sustava, primjerice, kada poduzeće ili prodavatelj zaduži neku osobu da testira snagu njegovog sigurnosnog sustava. U kontekstu ove Direktive, ugovorne obveze ili dogovori da se ograniči pristup informacijskim sustavima putem korisničkih uvjeta ili općih uvjeta, kao i radni sporovi koji se odnose na pristup informacijskim sustavima poslodavca i njihovo korištenje za privatne svrhe ne bi trebali uzrokovati kaznenu odgovornost kada bi se pristup pod takvim okolnostima smatrao neovlaštenim te bi na taj način predstavljao jedinu osnovu za kazneni postupak. Ovom se Direktivom ne dovodi u pitanje pravo na pristup informacijama kako je utvrđeno u nacionalnom pravu i u pravu EU-a, ali istodobno ne može služiti kao opravdanje za nezakonit ili proizvoljan pristup informacijama.

(18) Razne okolnosti mogu olakšati kibernetičke napade, kao što je situacija kada počinitelj u okviru svojeg zaposlenja ima pristup sigurnosnim sustavima koji su neodvojivi od zahvaćenih informacijskih sustava. U kontekstu nacionalnog prava, takve bi okolnosti trebalo na odgovarajući način uzeti u obzir tijekom kaznenog postupka.

(19) Države članice trebale bi u svojem nacionalnom pravu predvidjeti otegotne okolnosti u skladu s mjerodavnim pravilima koje su njihovi pravni sustavi uspostavili za otegotne okolnosti. Trebale bi osigurati da suci te otegotne okolnosti mogu uzeti u obzir prilikom izricanja kazne za počinitelje. Sudac zadržava slobodu ocjenjivanja tih okolnosti zajedno s drugim činjenicama određenog slučaja.

(20) Ovom se Direktivom ne uređuju uvjeti za izvršavanje nadležnosti nad bilo kojim kaznenim djelom koje je u njoj navedeno, kao što je izjava žrtve na mjestu gdje je kazneno djelo počinjeno, odricanje od strane države mjesta gdje je kazneno djelo počinjeno, ili činjenica da protiv počinitelja nije bio poduzet kazneni progon u mjestu gdje je kazneno djelo počinjeno.

(21) U kontekstu ove Direktive, države i tijela javnog prava ostaju u potpunosti obvezna jamčiti poštovanje ljudskih prava i temeljnih sloboda, u skladu s postojećim međunarodnim obvezama.

(22) Ova Direktiva jača važnost mreža kao što je mreža kontaktnih točaka G8 ili Vijeća Europe koje su dostupne dvadeset četiri sata dnevno i sedam dana u tjednu. Te bi kontaktne točke trebale biti u mogućnosti pružiti učinkovitu pomoć kako bi se, primjerice, olakšala razmjena dostupnih relevantnih informacija ili pružanje tehničkih savjeta ili pravnih informacija u svrhu istrage ili postupka koji se tiču kaznenih djela u vezi s informacijskim sustavima i povezanim podacima koji uključuju državu članicu koja podnosi zahtjev. Kako bi se osigurao nesmetan rad mreža, svaka kontaktna točka trebala bi imati kapacitet za komunikaciju s kontaktnom točkom druge države članice po žurnom postupku, uz potporu, među ostalim, osposobljenog osoblja koje posjeduje odgovarajuću opremu. S obzirom na brzinu kojom se kibernetički napadi velikih razmjera mogu izvršavati, države članice trebale bi biti u stanju brzo odgovoriti na hitne zahtjeve koji dolaze iz ove mreže kontaktnih točaka. U takvim slučajevima bilo bi korisno da zahtjev za informacijama bude popraćen telefonskim kontaktom kako bi se osigurala brza obrada zahtjeva od strane države članice kojoj je zahtjev upućen te da se povratna informacija pruži u roku od osam sati.

(23) Suradnja između tijela javne vlasti, s jedne strane, i privatnog sektora te civilnog društva, s druge strane, od velike je važnosti u sprječavanju i borbi protiv napada na informacijske sustave. Potrebno je poticati i poboljšavati suradnju između pružatelja usluga, proizvođača, tijela zaduženih za izvršavanje zakona i pravosudnih tijela, istodobno u potpunosti poštujući vladavinu prava. Takva suradnja može uključivati potporu od pružatelja usluga u smislu pomoći da se očuvaju potencijalni dokazi, iznošenja elemenata koji mogu pomoći u utvrđivanju počinitelja te, kao posljednja opcija, a u skladu s nacionalnim pravom i praksom, cjelokupnog ili djelomičnoga gašenja informacijskih sustava ili funkcija koji su zahvaćeni ili korišteni u nezakonite svrhe. Države članice također bi trebale razmotriti formiranje mreža suradnje i partnerstva s pružateljima usluga i proizvođačima s ciljem razmjene informacija o kaznenim djelima u okviru područja primjene ove Direktive.

(24) Postoji potreba za prikupljanjem usporedivih podataka o kaznenim djelima utvrđenima u ovoj Direktivi. Relevantni bi se podaci trebali staviti na raspolaganje nadležnim specijaliziranim agencijama i tijelima Unije kao što su Europol i ENISA u skladu s njihovim zadaćama i potrebama za informacijama, kako bi se dobila kompletnija slika problema kibernetičkog kriminala i sigurnosti mreža i informacija na razini Unije, čime bi se doprinijelo oblikovanju učinkovitijeg odgovora. Države članice trebale bi Europolu i njegovom Europskom centru za kibernetički kriminal dostaviti informacije o načinu djelovanja počinitelja s ciljem procjena opasnosti i provođenja strateških analiza kibernetičkog kriminala u skladu s Odlukom Vijeća 2009/371/PUP od 6. travnja 2009. o osnivanju Europskog policijskog ureda (Europol) ([1]). Pružanje informacija može olakšati bolje razumijevanje sadašnjih i budućih prijetnji te na taj način doprinijeti prikladnijem i ciljnom donošenju odluka o borbi i sprječavanju napada na informacijske sustave.

(25) Komisija bi trebala dostaviti izvješće o primjeni ove Direktive te izraditi potrebne zakonodavne prijedloge koji bi mogli dovesti do širenja njezinog područja primjene, uzimajući u obzir razvoj u području kibernetičkog kriminala. Takav bi razvoj mogao obuhvaćati tehnološka poboljšanja, primjerice, ona koja omogućuju učinkovitije izvršavanje zakona u području napada na informacijske sustave ili koja olakšavaju sprječavanje odnosno svode na najmanju moguću mjeru učinak takvih napada. U tu bi svrhu Komisija trebala uzeti u obzir dostupne analize i izvješća koja su izradili relevantni sudionici, a posebno Europol i ENISA.

(26) Kako bi borba protiv kibernetičkog kriminala bila učinkovita, potrebno je povećati otpornost informacijskih sustava poduzimanjem odgovarajućih mjera kako bi se što učinkovitije zaštitili od kibernetičkih napada. Države članice trebale bi poduzeti potrebne mjere za zaštitu svojih ključnih infrastruktura protiv kibernetičkih napada, a u okviru toga trebale bi razmotriti zaštitu svojih informacijskih sustava i povezanih podataka. Osiguranje odgovarajuće razine zaštite i sigurnosti informacijskih sustava od pravnih osoba, primjerice u vezi s

([1]) SL L 121, 15.5.2009., str. 37.

pružanjem javno dostupnih elektroničkih komunikacijskih usluga u skladu s postojećim zakonodavstvom Unije o privatnosti i elektroničkim komunikacijama te zaštiti podataka, ključan je dio sveobuhvatnog pristupa učinkovitom suzbijanju kibernetičkog kriminala. Protiv prijetnji i osjetljivosti koje se na razuman način mogu utvrditi trebalo bi osigurati odgovarajuće razine zaštite u skladu s najsuvremenijom tehnologijom za pojedine sektore i konkretnim okolnostima obrade podataka. Trošak i opterećenje takve zaštite trebali bi biti razmjerni mogućoj šteti koju bi kibernetički napad prouzročio onima koji su njime zahvaćeni. Države članice potiču se da osiguraju, u okviru svojeg nacionalnog prava, relevantne mjere koje bi uključivale odgovornost pravnih osoba u slučajevima kada one nisu jasno osigurale odgovarajuću razinu zaštite protiv kibernetičkih napada.

(27) Značajni nedostaci i razlike u zakonodavstvima i kaznenim postupcima država članica u području napada na informacijske sustave mogu usporiti borbu protiv organiziranog kriminala i terorizma te otežati učinkovitu policijsku i pravosudnu suradnju u ovom području. Kako su suvremeni informacijski sustavi nadnacionalni i bezgranični, napadi na takve sustave imaju prekograničnu dimenziju, zbog čega su potrebne daljnje žurne mjere kako bi se uskladilo kazneno pravo u tom području. Osim toga, koordiniranje progona slučajeva napada na informacijske sustave trebalo bi biti olakšano odgovarajućom provedbom i primjenom Okvirne odluke Vijeća 2009/948/PUP od 30. studenoga 2009. o sprečavanju i rješavanju sporova o izvršavanju nadležnosti u kaznenim postupcima ([1]). Države članice u suradnji s Unijom također bi trebale težiti poboljšanju međunarodne suradnje koja se odnosi na sigurnost informacijskih sustava, računalnih mreža i računalnih podataka. U svakom međunarodnom sporazumu koji uključuje razmjenu podataka trebalo bi posebnu pozornost pridati sigurnosti prijenosa i skladištenja podataka.

(28) Poboljšana suradnja između nadležnih tijela za izvršavanje zakona i pravosudnih tijela u Uniji ključna je za učinkovitu borbu protiv kibernetičkog kriminala. U tom bi kontekstu trebalo poticati jačanje napora za osiguravanje odgovarajućeg osposobljavanja relevantnih tijela kako bi se poboljšalo razumijevanje kibernetičkog kriminala i njegovog utjecaja te potaknula suradnja i razmjena najboljih praksi, primjerice, putem nadležnih specijaliziranih agencija i tijela Unije. Cilj takvog osposobljavanja, među ostalim, trebalo bi biti podizanje svijesti o različitim nacionalnim pravnim sustavima, mogućim pravnim i tehničkim izazovima kaznenih istraga i podjeli nadležnosti između relevantnih nacionalnih tijela.

(29) Ova Direktiva poštuje ljudska prava i temeljne slobode i drži se načela koja su posebno priznata u Povelji Europske unije o temeljnim pravima i u Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda, uključujući zaštitu osobnih podataka, pravo na privatnost, slobodu izražavanja i informiranja, pravo na pošteno suđenje, pretpostavku nedužnosti i pravo na obranu, kao i načela zakonitosti i proporcionalnosti kaznenih djela i kazni. Ovom se Direktivom posebno nastoji osigurati potpuno poštovanje tih prava i načela i mora se na odgovarajući način provesti.

(30) Zaštita osobnih podataka temeljno je pravo u skladu s člankom 16. stavkom 1. UFEU-a i člankom 8. Povelje o temeljnim pravima. Stoga bi svaka obrada osobnih podataka u kontekstu provedbe ove Direktive trebala biti potpuno u skladu s relevantnim pravom Unije o zaštiti podataka.

(31) U skladu s člankom 3. Protokola o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, koji je priložen Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, te države članice obavijestile su da žele sudjelovati u usvajanju i primjeni ove Direktive..

(32) U skladu s člancima 1. i 2. Protokola o stajalištu Danske, koji je priložen Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Danska ne sudjeluje u usvajanju ove Direktive te ona za nju nije obvezujuća niti podliježe njezinoj primjeni.

(33) Budući da ciljeve ove Direktive, to jest podvrgavanje napada na informacijske sustave u svim državama članicama učinkovitim, proporcionalnim i odvraćajućim kaznenopravnim sankcijama te poboljšanje i poticanje suradnje između pravosudnih i drugih nadležnih tijela, ne mogu dostatno ostvariti države članice, nego se, zbog svojeg opsega i učinka, mogu na bolji način ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti određenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti određenim u tom članku, ova Direktiva ne prelazi ono što je potrebno za ostvarivanje tih ciljeva.

(34) Cilj je ove Direktive izmijeniti i proširiti odredbe Okvirne odluke Vijeća 2005/222/PUP od 24. veljače 2005. o napadima na informacijske sustave ([2]). Budući da su izmjene koje treba izvršiti brojne i važne, Okvirnu odluku 2005/222/PUP radi jasnoće bi trebalo u cijelosti zamijeniti u odnosu na države članice koje sudjeluju u usvajanju ove Direktive,

([1]) SL L 328, 15.12.2009., str. 42.

([2]) SL L 69, 16.3.2005., str. 67.

DONIJELI SU OVU DIREKTIVU:

Članak 1.

Predmet

Ovom se Direktivom utvrđuju minimalna pravila o definiranju kaznenih djela i sankcija u području napada na informacijske sustave. Njezin je cilj također olakšavanje sprečavanja takvih djela i poboljšavanje suradnje između pravosudnih i drugih nadležnih tijela.

Članak 2.

Definicije

Za potrebe ove Direktive primjenjuju se sljedeće definicije:

(a) „informacijski sustav" znači uređaj ili skupina međupovezanih ili srodnih uređaja, od kojih jedan ili više njih, sukladno programu, provodi automatsku obradu računalnih podataka, te računalni podaci koji su pohranjeni, obrađeni, pronađeni ili preneseni pomoću tog uređaja ili skupine uređaja za potrebe njegovog ili njihovog funkcioniranja, uporabe, zaštite i održavanja;

(b) „računalni podaci" znači predstavljanje činjenica, informacija ili koncepata u obliku koji je prikladan za obradu u informacijskom sustavu, uključujući odgovarajući program kojim informacijski sustav provodi neku funkciju;

(c) „pravna osoba" znači pravni subjekt koji ima status pravne osobe prema primjenjivom pravu, ali ne uključuje države ni tijela javnog prava u obnašanju državne vlasti ni javne međunarodne organizacije;

(d) „bespravan" znači postupanje iz ove Direktive, uključujući pristup, ometanje ili presretanje, bez dopuštenja vlasnika ili drugog nositelja prava sustava ili njegova dijela, ili koje nacionalno pravo ne dopušta.

Članak 3.

Nezakonit pristup informacijskim sustavima

Države članice poduzimaju potrebne mjere kojima osiguravaju da je bespravni pristup cjelokupnom informacijskom sustavu ili nekom njegovom dijelu, kada se počini s namjerom, kažnjiv kao kazneno djelo ako je počinjen kršenjem sigurnosne mjere, barem kada nije riječ o lakšim slučajevima.

Članak 4.

Nezakonito ometanje sustava

Države članice poduzimaju potrebne mjere kojima osiguravaju da je ozbiljno ometanje ili prekidanje funkcioniranja informacijskog sustava unosom, prijenosom, oštećivanjem, brisanjem, uništavanjem, mijenjanjem ili prikrivanjem računalnih podataka, ili onemogućavanjem pristupa takvim podacima, kada se počini s namjerom i bespravno, kažnjivo kao kazneno djelo, barem kada nije riječ o lakšim slučajevima.

Članak 5.

Nezakonito ometanje podataka

Države članice poduzimaju potrebne mjere kojima osiguravaju da je brisanje, oštećivanje, uništavanje, mijenjanje ili prikrivanje računalnih podataka informacijskog sustava, ili onemogućavanje pristupa takvim podacima, kada se počini s namjerom i bespravno, kažnjivo kao kazneno djelo, barem kada nije riječ o lakšim slučajevima.

Članak 6.

Nezakonito presretanje

Države članice poduzimaju potrebne mjere kojima osiguravaju da je presretanje, pomoću tehničkih sredstava, prijenosa računalnih podataka koji nije javan prema informacijskom sustavu, iz informacijskog sustava ili unutar njega, uključujući elektromagnetne emisije iz informacijskog sustava koji prenosi takve računalne podatke, kada se počini s namjerom i bespravno, kažnjivo kao kazneno djelo, barem kada nije riječ o lakšim slučajevima.

Članak 7.

Alati koji se koriste za počinjenje kaznenih djela

Države članice poduzimaju potrebne mjere kojima osiguravaju da su namjerna proizvodnja, prodaja, nabava radi korištenja, uvoz, distribucija ili drugo stavljanje na raspolaganje jednog od sljedećih alata, kada se počine bespravno i s namjerom da se koriste u svrhu počinjenja bilo kojeg od kaznenih djela iz članaka od 3. do 6., kažnjivi kao kazneno djelo, barem kada nije riječ o lakšim slučajevima:

(a) računalnog programa, namijenjenog ili prilagođenog ponajprije u svrhu počinjenja bilo kojeg od kaznenih djela iz članaka od 3. do 6.;

(b) računalne lozinke, pristupnog koda ili sličnih podataka pomoću kojih se može pristupiti cijelom informacijskom sustavu ili nekom njegovom dijelu.

Članak 8.

Poticanje i pomaganje te pokušaj

1. Države članice osiguravaju da je poticanje na počinjenje ili pomaganje u počinjenju djela iz članaka od 3. do 7. kažnjivo kao kazneno djelo.

2. Države članice osiguravaju da je pokušaj počinjenja djela iz članaka 4. i 5. kažnjiv kao kazneno djelo.

Članak 9.

Sankcije

1. Države članice poduzimaju potrebne mjere kojima osiguravaju da su kaznena djela iz članaka od 3. do 8. kažnjiva učinkovitim, proporcionalnim i odvraćajućim kaznenopravnim sankcijama.

2. Države članice poduzimaju potrebne mjere kojima osiguravaju da su kaznena djela iz članaka od 3. do 7. kažnjiva maksimalnom kaznom oduzimanja slobode u trajanju od najmanje dvije godine, barem kada nije riječ o lakšim slučajevima.

3. Države članice poduzimaju potrebne mjere kojima osiguravaju da su kaznena djela iz članaka 4. i 5., kada se počine s namjerom, kažnjiva maksimalnom kaznom oduzimanja slobode

u trajanju od najmanje tri godine kada je značajan broj informacijskih sustava pogođen korištenjem nekog od alata iz članka 7., namijenjenog ili prilagođenog za tu svrhu.

4. Države članice poduzimaju potrebne mjere kojima osiguravaju da su kaznena djela iz članaka 4. i 5. kažnjiva maksimalnom kaznom oduzimanja slobode u trajanju od najmanje pet godina kada:

(a) su počinjena u okviru zločinačke organizacije, kako je definirana u Okvirnoj odluci 2008/841/PUP, neovisno o sankciji predviđenoj u toj okvirnoj odluci;

(b) prouzroče ozbiljnu štetu; ili

(c) su počinjena protiv informacijskog sustava ključne infrastrukture.

5. Države članice poduzimaju potrebne mjere kojima osiguravaju da se, kada su kaznena djela iz članaka 4. i 5. počinjena zloporabom osobnih podataka druge osobe, s ciljem zadobivanja povjerenja treće strane, i time nanoseći štetu legitimnom vlasniku identiteta, ti elementi mogu u skladu s nacionalnim pravom smatrati otegotnim okolnostima, osim ako su te okolnosti već obuhvaćene drugim djelom kažnjivim prema nacionalnom pravu.

Članak 10.

Odgovornost pravnih osoba

1. Države članice poduzimaju potrebne mjere kojima osiguravaju da pravne osobe mogu biti odgovorne za kaznena djela iz članaka od 3. do 8. koja u njihovu korist počini bilo koja osoba samostalno ili kao član tijela pravne osobe, čiji se rukovodeći položaj pri toj pravnoj osobi temelji na:

(a) ovlasti za zastupanje pravne osobe;

(b) ovlasti za donošenje odluka u ime pravne osobe;

(c) ovlasti za provedbu kontrole unutar pravne osobe.

2. Države članice poduzimaju potrebne mjere kojima osiguravaju da pravne osobe mogu biti odgovorne ako je nedostatak nadzora ili kontrole osobe iz stavka 1. omogućio da osoba koja je podređena toj pravnoj osobi počini kaznena djela iz članaka od 3. do 8. u korist te pravne osobe.

3. Odgovornost pravne osobe u skladu sa stavcima 1. i 2. ne isključuje kaznene postupke protiv fizičkih osoba koje kao počinitelji, poticatelji ili pomagači sudjeluju u kaznenim djelima iz članaka od 3. do 8.

Članak 11.

Sankcije za pravne osobe

1. Države članice poduzimaju potrebne mjere kojima osiguravaju da su za pravnu osobu odgovornu na temelju članka 10. stavka 1. predviđene učinkovite, proporcionalne i odvraćajuće sankcije, koje uključuju novčane kazne prema kaznenom i drugom pravu, a mogu uključivati i druge sankcije kao što su:

(a) isključenje iz prava na javne naknade ili pomoć;

(b) privremena ili stalna zabrana obavljanja poslovne djelatnosti;

(c) stavljanje pod sudski nadzor;

(d) sudski nalog za likvidaciju;

(e) privremeno ili trajno zatvaranje ustanova koje su korištene za počinjenje kaznenog djela.

2. Države članice poduzimaju potrebne mjere kojima osiguravaju da su za pravnu osobu odgovornu na temelju članka 10. stavka 2. predviđene učinkovite, proporcionalne i odvraćajuće sankcije ili druge mjere.

Članak 12.

Nadležnost

1. Države članice utvrđuju svoju nadležnost za kaznena djela iz članaka od 3. do 8. kada je kazneno djelo počinjeno:

(a) u potpunosti ili djelomično na njihovom državnom području; ili

(b) od strane njezinog državljanina, barem u slučajevima kada djelo predstavlja kazneno djelo ondje gdje je počinjeno.

2. Pri utvrđivanju nadležnosti u skladu sa stavkom 1. točkom (a), država članica osigurava da ima nadležnost u slučajevima u kojima:

(a) počinitelj počini kazneno djelo kada je fizički prisutan na njezinom državnom području, neovisno o tome radi li se o kaznenom djelu protiv informacijskog sustava na njezinom državnom području; ili

(b) se radi o kaznenom djelu protiv informacijskog sustava na njezinom državnom području, neovisno o tome je li počinitelj bio fizički prisutan na njezinom državnom području kada je počinio kazneno djelo.

3. Država članica obavješćuje Komisiju ako odluči utvrditi nadležnost nad kaznenim djelom iz članaka od 3. do 8. počinjenim izvan njezinog državnog područja, uključujući ako:

(a) počinitelj ima uobičajeno boravište na njezinom državnom području; ili

(b) je kazneno djelo počinjeno u korist pravne osobe s poslovnim nastanom na njezinom državnom području.

Članak 13.

Razmjena informacija

1. Za potrebe razmjene informacija koje se odnose na kaznena djela iz članaka od 3. do 8., države članice osiguravaju raspolaganje operativnom nacionalnom kontaktnom točkom i uporabu postojeće mreže operativnih kontaktnih točaka koje su dostupne 24 sata dnevno i sedam dana u tjednu. Države članice također osiguravaju uspostavu postupaka kako bi, u slučaju hitnih zahtjeva za pomoć, nadležno tijelo u roku od osam sati od primitka moglo barem naznačiti hoće li odgovoriti na zahtjev, kao i oblik i procijenjeno vrijeme za takav odgovor.

2. Države članice obavješćuju Komisiju o svojim utvrđenim kontaktnim točkama iz stavka 1. Komisija dostavlja te informacije drugim državama članicama i nadležnim specijaliziranim agencijama i tijelima Unije.

3. Države članice poduzimaju potrebne mjere kojima osiguravaju dostupnost prikladnih kanala izvješćivanja kako bi se olakšalo izvješćivanje nadležnih nacionalnih tijela o kaznenim djelima iz članaka od 3. do 6. bez nepotrebne odgode.

Članak 14.

Praćenje i statistički podaci

1. Države članice osiguravaju uspostavu sustava za snimanje, proizvodnju i pružanje statističkih podataka o kaznenim djelima iz članaka od 3. do 7.

2. Statistički podaci iz stavka 1. obuhvaćaju barem postojeće podatke o broju kaznenih djela iz članaka od 3. do 7. zabilježenih u državama članicama i broj osoba protiv kojih je poduzet kazneni progon i koje su osuđene za kaznena djela iz članaka od 3. do 7.

3. Države članice Komisiji dostavljaju podatke prikupljene na temelju ovog članka. Komisija osigurava da se konsolidirani pregled tih statističkih izvješća objavi i preda nadležnim specijaliziranim agencijama i tijelima Unije.

Članak 15.

Zamjena Okvirne odluke 2005/222/PUP

Okvirna odluka 2005/222/PUP ovime se zamjenjuje u odnosu na države članice koje sudjeluju u donošenju ove Direktive, ne dovodeći u pitanje obveze država članica u vezi s rokom za prenošenje Okvirne odluke u nacionalno pravo.

U odnosu na države članice koje sudjeluju u donošenju ove Direktive, upućivanja na Okvirnu odluku 2005/222/JHA smatraju se upućivanjima na ovu Direktivu.

Članak 16.

Prenošenje

1. Države članice donose zakone i druge propise potrebne za usklađivanje s ovom Direktivom do 4. rujna 2015.

2. Države članice dostavljaju Komisiji tekst mjera kojima se u njihovo nacionalno pravo prenose obveze koje im nameće ova Direktiva.

3. Kada države članice donose ove mjere, te mjere prilikom njihove službene objave sadržavaju uputu na ovu Direktivu ili se uz njih navodi takva uputa. Načine tog upućivanja određuju države članice.

Članak 17.

Izvješćivanje

Komisija do 4. rujna 2017. Europskom parlamentu i Vijeću podnosi izvješće u kojem ocjenjuje u kojoj su mjeri države članice poduzele mjere potrebne za usklađivanje s ovom Direktivom, prema potrebi zajedno sa zakonodavnim prijedlozima. Komisija također uzima u obzir tehnički i pravni razvoj u području kibernetičkog kriminala, posebno u odnosu na područje primjene ove Direktive.

Članak 18.

Stupanje na snagu

Ova Direktiva stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 19.

Adresati

Ova je Direktiva upućena državama članicama u skladu s Ugovorima.

Sastavljeno u Bruxellesu 12. kolovoza 2013.

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*
M. SCHULZ	L. LINKEVIČIUS