32005F0222

OKVIRNA ODLUKA VIJEĆA 2005/222/PUP

od 24. veljače 2005.

o napadima na informacijske sustave

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegov članak 29., članak 30. stavak 1. točku (a), članak 31. stavak 1., točku (e) i članak 34. stavak 2. točku (b),

uzimajući u obzir prijedlog Komisije,

uzimajući u obzir mišljenje Europskog parlamenta ([1]),

budući da:

(1) Cilj je ove Okvirne odluke unaprijediti suradnju između pravosudnih i drugih nadležnih tijela, uključujući policiju i druge specijalizirane službe za provedbu zakona država članica, putem usklađivanja pravila kaznenoga prava u državama članicama u području napada na informacijske sustave.

(2) Postoje dokazi o napadima na informacijske sustave, posebno kao posljedica prijetnje od organiziranoga kriminala, te sve veća zabrinutost zbog potencijalnih terorističkih napada na informacijske sustave koji su dio ključne infrastrukture država članica. To je prijetnja ostvarenju sigurnijeg informacijskog društva i područja slobode, sigurnosti i pravde te stoga zahtijeva odgovor na razini Europske unije.

(3) Učinkovit odgovor na te prijetnje zahtijeva sveobuhvatan pristup mrežnoj i informacijskoj sigurnosti, kako je istaknuto u akcijskom planu eEuropa u priopćenju Komisije „Mrežna i informacijska sigurnost: Prijedlog europske politike pristupa" te u Rezoluciji Vijeća od 28. siječnja 2002. o zajedničkom pristupu i posebnim mjerama u području mrežne i informacijske sigurnosti ([2]).

(4) Potreba da se i dalje jača svijest o problemima povezanima sa informacijskom sigurnošću te pruži praktična pomoć naglašena je i u Rezoluciji Europskog parlamenta od 5. rujna 2001.

(5) Značajne praznine i razlike u pravima država članica u tom području mogu priječiti borbu protiv organiziranog kriminala i terorizma te otežati učinkovitu policijsku i pravosudnu suradnju u području napada na informacijske sustave. Kako su suvremeni informacijski sustavi nadnacionalni i bezgranični, napadi na takve sustave često su prekogranične naravi i potrebne su daljnje žurne mjere kako bi se uskladile odredbe kaznenog prava u tom području.

(6) Akcijski plan Vijeća i Komisije o najboljoj primjeni odredaba Ugovora iz Amsterdama o području slobode, sigurnosti i pravde ([3]), Europsko vijeće iz Tamperea od 15. i 16. listopada 1999., Europsko vijeće iz Santa Maria da Feira od 19. i 20. lipnja 2000., Komisija u „tablici o postignućima" i Europski parlament u svojoj Rezoluciji od 19. svibnja 2000. navode ili traže zakonodavne mjere protiv kriminala u području visoke tehnologije, uključujući zajedničke definicije, inkriminacije i sankcije.

(7) Treba dopuniti rad međunarodnih organizacija, posebno rad Vijeća Europe na usklađivanju kaznenog prava i rad skupine G8 na transnacionalnoj suradnji u području kriminala u području visoke tehnologije, osiguravajući zajednički pristup u Europskoj uniji u tom području. Taj je poziv detaljnije određen u priopćenju Komisije Vijeću, Europskom parlamentu, Gospodarskom i socijalnom odboru i Odboru regija o „stvaranju sigurnijega informacijskog društva poboljšanjem sigurnosti informacijskih infrastruktura i borbom protiv računalnog kriminala".

(8) Kazneno pravo u području napada na informacijske sustave treba uskladiti kako bi se osigurala najveća moguća policijska i pravosudna suradnja u području kaznenih djela koja se odnose na napade na informacijske sustave i doprinijelo borbi protiv organiziranoga kriminala i terorizma.

([1]) SL C 300 E, 11.12.2003., str. 26.
([2]) SL C 43, 16.2.2002., str. 2.
([3]) SL C 19, 23.1.1999., str. 1.

(9) Sve države članice ratificirale su Konvenciju Vijeća Europe od 28. siječnja 1981. o zaštiti pojedinaca pri automatskoj obradi osobnih podataka. Osobni podaci obrađeni u kontekstu primjene ove Okvirne odluke moraju biti zaštićeni u skladu s načelima te Konvencije.

(10) Zajedničke definicije u tom području, posebno informacijskih sustava i računalnih podataka, važne su za osiguranje dosljednog pristupa pri primjeni ove Okvirne odluke u državama članicama.

(11) Za osiguranje zajedničke definicije kaznenih djela nezakonitog pristupa informacijskim sustavima, nezakonitog zahvaćanja u sustav i nezakonitog zahvaćanja u podatke treba ostvariti zajednički pristup sastavnim elementima kaznenih djela.

(12) U interesu sprečavanja računalnog kriminala svaka država članica treba osigurati učinkovitu pravosudnu suradnju u pogledu kaznenih djela koja se temelje na vrstama postupanja iz članaka 2., 3., 4. i 5.

(13) Potrebno je izbjegavati prekomjernu kriminalizaciju, posebno u slučaju lakših kaznenih djela te kriminalizaciju nositelja prava i ovlaštenih osoba.

(14) Države članice trebaju predvidjeti kazne za napade na informacijske sustave. Takve kazne moraju biti učinkovite, razmjerne i odvraćajuće.

(15) Primjereno je predvidjeti strože kazne kada je napad na informacijski sustav počinjen u okviru zločinačke organizacije, kako je određena u Zajedničkoj akciji 98/733/PUP od 21. prosinca 1998. o proglašenju kaznenim djelom sudjelovanja u zločinačkoj organizaciji u državi članici Europske unije [1]. Prikladno je predvidjeti strože kazne ako je takav napad prouzročio veliku štetu ili utjecao na ključne interese.

(16) Treba također predvidjeti mjere za potrebe suradnje među državama članicama radi osiguravanja učinkovitog djelovanja protiv napada na informacijske sustave. Države članice trebaju stoga za razmjenu informacija iskoristiti postojeću mrežu operativnih kontaktnih točki iz Preporuke Vijeća od 25. lipnja 2001. o kontaktnim točkama koje održavaju 24-satnu službu za borbu protiv kriminala u području visoke tehnologije [2].

(17) Budući da ciljeve ove Okvirne odluke, osiguranje da napadi na informacijske sustave budu sankcionirani u svim državama članicama učinkovitim, razmjernim i odvraćajućim kaznama te poboljšanje i poticanje pravosudne suradnje uklanjanjem potencijalnih prepreka, države članice ne mogu u dovoljnoj mjeri same postignut jer pravila moraju biti zajednička i usklađena, i stoga se mogu bolje ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti kako je određeno u članku 5. Ugovora o EZ-u. U skladu s načelom razmjernosti i kako je određeno u tom članku, ova Okvirna odluka ne prelazi ono što je potrebno za postizanje tih ciljeva.

(18) Ova Okvirna odluka poštuje temeljna prava i uzima u obzir načela priznata u članku 6. Ugovora o Europskoj uniji i sadržana u Povelji o temeljnim pravima Europske unije, posebno u njezinim poglavljima II. i VI.,

DONIJELO JE OVU OKVIRNU ODLUKU:

Članak 1.

Definicije

Za potrebe ove Okvirne odluke primjenjuju se sljedeće definicije:

(a) „informacijski sustav" znači svaki 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 za potrebe njihovog funkcioniranja, korištenja, zaštite i održavanja;

(b) „računalni podaci" znači svako 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 svaki pravni subjekt koji ima takav status prema primjenjivom pravu, osim država ili drugih tijela javnoga prava u obnašanju državne vlasti te javnih međunarodnih organizacija;

[1] SL L 351, 29.12.1998., str. 1.

[2] SL C 187, 3.7.2001., str. 5.

(d) „bespravan" znači pristup ili ometanje bez dopuštenja vlasnika, drugoga nositelja prava sustava ili njegova dijela, ili koje nacionalno zakonodavstvo ne dopušta.

Članak 2.

Nezakonit pristup informacijskim sustavima

1. Svaka država članica poduzima potrebne mjere kojima osigurava da se namjerni bespravni pristup cjelokupnom ili jednom dijelu informacijskog sustava kazni kao kazneno djelo, barem kada se ne radi o lakšim slučajevima.

2. Svaka država članica može odlučiti da je ponašanje iz stavka 1. kažnjivo samo ako je kazneno djelo počinjeno kršenjem sigurnosnih mjera.

Članak 3.

Nezakonito ometanje sustava

Svaka država članica poduzima potrebne mjere kojima osigurava da se namjerno ozbiljno ometanje ili prekidanje funkcioniranja informacijskoga sustava unosom, prijenosom, oštećivanjem, brisanjem, uništavanjem, mijenjanjem, suzbijanjem ili onemogućivanjem pristupa računalnim podacima kazni kao kazneno djelo, kad se počini bespravno, barem kada nije riječ o lakšim slučajevima.

Članak 4.

Nezakonito ometanje podataka

Svaka država članica poduzima potrebne mjere kojima osigurava da se namjerno brisanje, oštećivanje, uništavanje, mijenjanje, prikrivanje ili onemogućavanje pristupa računalnim podacima kazni kao kazneno djelo kada se bespravno počini, barem kada nije riječ o lakšim slučajevima.

Članak 5.

Poticanje, pomaganje i sudioništvo te pokušaj

1. Svaka država članica osigurava da se poticanje, pomaganje i sudioništvo ili pokušaj počinjenja djela iz članaka 2., 3. i 4. kazni kao kazneno djelo.

2. Svaka država članica osigurava da se pokušaj počinjenja djela iz članaka 2., 3. i 4. kazni kao kazneno djelo.

3. Svaka država članica može odlučiti ne primijeniti stavak 2. za kaznena djela iz članka 2.

Članak 6.

Kazne

1. Svaka država članica poduzima potrebne mjere kojima osigurava da se kaznena djela iz članaka 2., 3., 4. i 5. kazne učinkovitim, razmjernim i odvraćajućim kaznama.

2. Svaka država članica poduzima potrebne mjere kojima osigurava da se kaznena djela iz članaka 3. i 4. kazne kaznama zatvora u trajanju od najmanje jedne do tri godine.

Članak 7.

Otegotne okolnosti

1. Svaka država članica poduzima potrebne mjere kojima osigurava da se kazneno djelo iz članka 2. stavka 2. i kaznena djela iz članaka 3. i 4. kazne kaznom zatvora u trajanju od najmanje dvije do pet godina kada su djela počinjena u okviru zločinačke organizacije kako je određena u Zajedničkoj akciji 98/733/PUP, neovisno o visini kazne iz te Zajedničke akcije.

2. Država članica može također poduzeti mjere iz stavka 1. i kada je djelovanje prouzročilo veliku štetu ili je ugrozilo bitne interese.

Članak 8.

Odgovornost pravnih osoba

1. Svaka država članica poduzima potrebne mjere kojima osigurava odgovornost pravnih osoba za kaznena djela iz članaka 2., 3., 4. i 5., počinjena u njihovu korist od strane bilo koje osobe koja je djelovala samostalno ili kao dio tijela pravne osobe i koja ima rukovodeći položaj unutar pravne osobe, a temelji se na:

(a) ovlaštenju za zastupanje pravne osobe; ili

(b) ovlaštenju za donošenje odluka u ime pravne osobe; ili

(c) ovlaštenju za nadzor unutar pravne osobe.

2. Osim slučajeva predviđenih u stavku 1., države članice osiguravaju odgovornost pravne osobe i ako je nedostatak nadzora ili kontrole osobe iz stavka 1. omogućio da osoba koja je podređena toj pravnoj osobi počini kaznena djela iz članaka 2., 3., 4. i 5. u korist te pravne osobe.

3. Odgovornost pravnih osoba sukladno stavcima 1. i 2. ne isključuje kaznene postupke protiv fizičkih osoba koje su uključeni kao počinitelji, poticatelji ili pomagači u kaznenim djelima iz članaka 2., 3., 4. i 5.

Članak 9.

Kazne za pravne osobe

1. Svaka država članica poduzima potrebne mjere kojima osigurava da se pravna osoba odgovorna na temelju članka 8. stavka 1. kazni učinkovitim, razmjernim i odvraćajućim kaznama, koje uključuju kaznene sankcije i novčane kazne te druge kazne kao što su:

(a) isključenje iz prava na državne naknade ili pomoći;

(b) privremenu ili trajnu zabranu obavljanja poslovne djelatnosti;

(c) sudski nadzor; ili

(d) sudski nalog za likvidaciju.

2. Svaka država članica poduzima potrebne mjere kojima osigurava da se pravna osoba, koja je odgovorna na temelju članka 8. stavka 2. kazni učinkovitim, razmjernim i odvraćajućim kaznama ili mjerama.

Članak 10.

Nadležnost

1. Svaka država članica poduzima potrebne mjere kako bi utvrdila svoju nadležnost u kaznenim djelima iz članaka 2., 3., 4. i 5. kad je kazneno djelo počinjeno:

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

(b) od strane njezinog državljanina; ili

(c) u korist pravne osobe čije je sjedište na državnom području te države članice.

2. Pri utvrđivanju svoje nadležnosti u skladu sa stavkom 1. točkom (a), svaka država članica osigurava da nadležnost uključuje slučajeve 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) je kazneno djelo počinjeno protiv informacijskog sustava na njezinom državnom području, neovisno o tome je li počinitelj počinio kazneno djelo kada je bio fizički prisutan na njezinom državnom području.

3. Država članica koja, sukladno svojem pravu ne izručuje i ne predaje svoje državljane, poduzima potrebne mjere kako bi utvrdila svoju nadležnost i progon, prema potrebi, za kaznena djela iz članaka 2., 3., 4. i 5. kada ih počine njezini državljani izvan njezinog državnog područja.

4. Ako je kazneno djelo u nadležnosti više država članica i ako svaka od tih država može valjano kazneno goniti na temelju istih činjenica, te države članice surađuju kako bi odlučile koja će goniti prijestupnike s ciljem, ako je to moguće, centraliziranja postupaka u jednoj državi članici. Stoga se države članice mogu obratiti bilo kojem tijelu ili mehanizmu ustanovljenom u okviru Europske unije zbog lakše suradnje između njihovih pravosudnih tijela i koordinacije njihovog djelovanja. Pritom se redom može uzeti u obzir sljedeće:

— država članica je ona na čijem su državnom području počinjena kaznena djela prema stavku 1. točki (a) i stavku 2.,

— država članica je ona čiji je državljanin počinitelj,

— država članica je ona u kojoj je počinitelj pronađen.

5. Država članica može odlučiti ne primijeniti pravila o nadležnosti iz stavka 1. točaka (b) i (c) ili ih primijeniti samo u određenim slučajevima ili okolnostima.

6. Države članice obavješćuju Glavno tajništvo Vijeća i Komisiju ako odluče primijeniti stavak 5. te, prema potrebi, u kojim posebnim slučajevima i pod kojim posebnim uvjetima se ta odluka primjenjuje.

Članak 11.

Razmjena informacija

1. Za potrebe razmjene informacija koje se odnose na kaznena djela iz članaka 2., 3., 4. i 5. te u skladu s pravilima o zaštiti podataka države članice osiguravaju uporabu postojeće mreže operativnih kontaktnih točaka koje su dostupne 24 sata dnevno, sedam dana u tjednu.

2. Svaka država članica obavješćuje Glavno tajništvo Vijeća i Komisiju o svojim utvrđenim kontaktnim točkama za potrebe razmjene informacija o kaznenim djelima koja se odnose na napade na informacijske sustave. Glavno tajništvo prosljeđuje te informacije ostalim državama članicama.

Članak 12.

Provedba

1. Države članice poduzimaju potrebne mjere za ispunjavanje odredaba ove Okvirne odluke do 16. ožujka 2007.

2. Do 16. ožujka 2007. države članice dostavljaju Glavnom tajništvu Vijeća i Komisiji tekst svih odredaba kojima se u njihovo nacionalno pravo prenose obveze iz ove Okvirne odluke. Vijeće do 16. rujna 2007. na temelju izvješća utvrđenog na temelju informacija i pisanoga izvješća Komisije ocjenjuje do koje su mjere države članice ispunile odredbe ove Okvirne odluke.

Članak 13.

Stupanje na snagu

Ova Okvirna odluka stupa na snagu na dan objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 24. veljače 2005.

Za Vijeće
Predsjednik
N. SCHMIT