EUROPOS BENDRIJŲ KOMISIJA

Briuselis, 22.5.2007
KOM(2007) 267 galutinis

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI IR EUROPOS REGIONŲ KOMITETUI

Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme

{SEK(2007) 641}
{SEK(2007) 642}

KOMISIJOS KOMUNIKATAS
EUROPOS PARLAMENTUI, TARYBAI
IR EUROPOS REGIONŲ KOMITETUI

Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme

1. ĮVADAS

1.1. Elektroniniai nusikaltimai – kas tai?

Vis svarbesnių informacinių sistemų saugumas mūsų visuomenėse apima daugelį aspektų, o pagrindinis jų elementas – kova su elektroniniais nusikaltimais. Terminai „elektroniniai nusikaltimai“, „kompiuteriniai nusikaltimai“, „su kompiuteriais susiję nusikaltimai“ arba „modernių technologijų nusikaltimai“ dažnai vartojami kaip sinonimai, nes nėra sutartos elektroninių nusikaltimų apibrėžties. Šiame komunikate elektroniniai nusikaltimai suprantami kaip nusikalstamos veikos, padarytos naudojant elektroninių ryšių tinklus ir informacines sistemas, arba nusikalstamos veikos prieš tokius tinklus ir sistemas.

Praktikoje terminas „elektroniniai nusikaltimai“ apima tris nusikalstamų veikų rūšis. Pirmoji apima **įprastas nusikaltimų rūšis**, pavyzdžiui, sukčiavimas arba klastojimas, tačiau elektroninių nusikaltimų atveju konkrečiai susijusias su nusikaltimais, padarytais per elektroninių ryšių tinklus ir informacines sistemas (toliau – elektroniniai tinklai). Antroji susijusi su **neteisėto turinio** skelbimu elektroninėje žiniasklaidoje (pavyzdžiui, seksualinio vaikų išnaudojimo medžiaga arba rasinės neapykantos kurstymas). Trečioji apima **specifinius elektroninių tinklų nusikaltimus**, t. y. atakos prieš informacines sistemas, sistemos išėjimas iš rikiuotės (angl. *denial of service*) ir kompiuterinis įsilaužimas. Šios atakų rūšys taip pat gali būti nukreiptos prieš pagrindinius ypatingos svarbos infrastruktūros objektus Europoje ir padaryti poveikį daugelio sričių esamoms skubaus įspėjimo sistemoms, o tai gali turėti pražūtingų pasekmių visai visuomenei. Visoms nusikaltimų rūšims bendra tai, kad jos gali būti padarytos dideliu mastu ir esant dideliam geografiniam atstumui tarp nusikalstamos veikos ir jos padarinių. Todėl techniniai taikomų tyrimo metodų aspektai dažnai yra tokie patys. Šiame komunikate dėmesys sutelkiamas į šiuos bendrumus.

1.2. Naujausi pokyčiai elektroninių nusikaltimų srityje

1.2.1. Bendra apžvalga

Dėl nuolat kintančių nusikalstamų veikų ir patikimos informacijos trūkumo derinio sunku susidaryti tikslų dabartinės situacijos vaizdą. Tačiau galima išskirti kelis bendrus bruožus:

- elektroninių nusikaltimų daugėja, o nusikalstamos veikos darosi vis sudėtingesnės ir vis labiau tarptautinio pobūdžio[1];

[1] Dauguma šio komunikato teiginių apie dabartinius bruožus yra paimti iš tyrimo, skirto komunikato dėl elektroninių nusikaltimų poveikiui įvertinti, užsakyto Komisijos 2006 m. (Sutarties Nr. JLS/2006/A1/003).

- aiškūs požymiai rodo, kad elektroninius nusikaltimus vis dažniau daro organizuotos nusikalstamos grupės;

- tačiau nedaugėja Europos lygmens traukimo baudžiamojon atsakomybėn, remiantis tarpvalstybiniu teisėsaugos bendradarbiavimu, atvejų.

1.2.2. Įprasti elektroninių tinklų nusikaltimai

Daugelis nusikaltimų gali būti padaryti naudojant elektroninius tinklus, o įvairios sukčiavimo ir pasikėsinimo sukčiauti rūšys yra ypač dažnos elektroninių tinklų nusikaltimų rūšys ir jų nuolat daugėja. Tapatybės vagystė, duomenų vagystė[2] (angl. *phishing*), nepageidaujamas e. paštas ir žalingi kodai – tai priemonės, kurios gali būti naudojamos sukčiauti dideliu mastu. Taip pat iškilo didėjanti problema – neteisėta nacionalinė ir tarptautinė prekyba internetu. Tai apima prekybą narkotikais, nykstančiomis rūšimis ir ginklais.

1.2.3. Neteisėtas turinys

Daugėja Europoje prieinamų neteisėto turinio tinklaviečių, susijusių su seksualinio vaikų išnaudojimo medžiaga, teroristinių išpuolių kurstymu, neteisėtu smurto, terorizmo, rasizmo ir ksenofobijos garbinimu. Teisėsaugai labai sunku imtis veiksmų prieš tokias tinklavietės, nes jų savininkai ir administratoriai dažnai įsisteigę ne tikslinėje šalyje, o kitose šalyse ir dažnai už ES ribų. Tinklavietes galima labai greitai perkelti, taip pat už ES teritorijos ribų, o neteisėtumo apibrėžtis įvairiose valstybėse labai skiriasi.

1.2.4. Specifiniai elektroninių tinklų nusikaltimai

Vis labiau paplitusios didelio masto atakos prieš informacines sistemas arba organizacijas ir asmenis (dažnai per vadinamąjį „zombių“ tinklą[3] (angl. *botnet*)). Taip pat neseniai buvo pastebėti sistemingų, gerai koordinuotų ir didelio masto tiesioginių atakų prieš valstybės ypatingos svarbos informacijos infrastruktūros objektus atvejai. Šį reiškinį sudarė sujungtos technologijos ir pagreitintos informacinių sistemų sąsajos, o tai lėmė didesnį šių sistemų pažeidžiamumą. Atakos dažnai yra gerai organizuotos ir naudojamos turtui prievartauti. Galima manyti, kad pranešimo apie atakų skaičių mastas yra sumažintas iki minimumo iš dalies dėl žalos įmonėms, kuri gali atsirasti, jeigu būtų paviešintos saugumo problemos.

1.3. Tikslai

Atsižvelgiant į šią kintančią aplinką, nacionaliniu ir Europos lygmeniu reikia nedelsiant imtis veiksmų prieš visas elektroninių nusikaltimų rūšis, kurios yra vis reikšmingesnės grėsmės ypatingos svarbos infrastruktūros objektams, visuomenei, įmonėms ir piliečiams. Asmenų apsaugą nuo elektroninių nusikaltimų dažnai pablogina problemos, susijusios su kompetentingos jurisdikcijos, taikomos teisės, tarpvalstybinio vykdymo nustatymu arba su elektroninių įrodymų atpažinimu ir naudojimu. Iš esmės tarpvalstybinis elektroninių nusikaltimų pobūdis pabrėžia šiuos sunkumus. Komisija, atsižvelgdama į šias grėsmes, pradeda bendrosios politikos iniciatyvą, skirtą pagerinti Europos ir tarptautinio lygmens kovos su elektroniniais nusikaltimais derinimą.

---

[2] Duomenų vagystė apibūdina pastangas apsimetant patikimu asmeniu elektroniniame ryšyje apgaule įgyti slaptą informaciją, pavyzdžiui, slaptažodžius, kreditinių kortelių duomenis.

[3] „Zombių“ tinklas – tai sukompromituotų kompiuterių, vykdančių programas pagal bendrą komandą, grupė.

Tikslas – sustiprinti kovą su elektroniniais nusikaltimais nacionaliniu, Europos ir tarptautiniu lygmeniu. Visų pirma valstybės narės ir Komisija seniai suteikė pirmenybę tolesnei konkrečiai ES politikos raidai. Iniciatyva bus nukreipta į šios kovos teisėsaugos ir baudžiamosios teisės sritis, o politika papildys kitus ES veiksmus, skirtus bendrai pagerinti elektroninės erdvės saugumą. Politiką ilgainiui sudarys: pagerintas operatyvinis teisėsaugos bendradarbiavimas; geresnis politinis valstybių narių bendradarbiavimas ir jų tarpusavio veiksmų derinimas; politinis ir teisinis bendradarbiavimas su trečiosiomis šalimis; informuotumo gerinimas; mokymas; moksliniai tyrimai; intensyvesnis dialogas su pramonės subjektais ir galimas teisės aktų priėmimas.

Politika, skirta kovai su elektroniniais nusikaltimais, ir patraukimo baudžiamojon atsakomybėn dėl elektroninių nusikaltimų politika bus apibrėžta ir įgyvendinta gerbiant pagrindines teises, visų pirma saviraiškos laisvę, pagarbą privačiam ir šeimos gyvenimui, ir asmens duomenų apsaugą. Jei imamasi bet kokių su šia politika susijusių teisinių veiksmų, pirmiausiai bus tikrinama, ar jie suderinami su šiomis teisėmis, visų pirma su ES pagrindinių teisių chartija. Taip pat reikėtų pažymėti, kad visos tokios politikos iniciatyvos bus vykdomos atsižvelgiant į vadinamosios Elektroninės komercijos direktyvos[4] 12–15 straipsnius, kai taikomas šis teisės aktas.

Šio komunikato tikslą galima suskirstyti į tris pagrindines operatyvines dalis, kurias galima apibendrinti taip:

- pagerinti ir palengvinti elektroninių nusikaltimų skyrių, kitų atitinkamų institucijų ir kitų ekspertų tarpusavio veiksmų derinimą ir bendradarbiavimą Europos Sąjungoje;

- derinant su valstybėmis narėmis, atitinkamomis ES bei tarptautinėmis organizacijomis ir kitomis suinteresuotosiomis šalimis plėtoti nuoseklią ES politikos sistemą, skirtą kovai su elektroniniais nusikaltimais;

- gerinti informuotumą apie išlaidas ir pavojus, kuriuos sukelia elektroniniai nusikaltimai.

2. GALIOJANTYS TEISĖS AKTAI, SKIRTI KOVAI SU ELEKTRONINIAIS NUSIKALTIMAIS

2.1. Galiojantys ES lygmens aktai ir veiksmai

Šis komunikatas dėl politikos, skirtos kovai su elektroniniais nusikaltimais, konsoliduoja ir išplečia 2001 m. Komunikatą dėl saugesnės informacinės visuomenės sukūrimo pagerinant informacijos infrastruktūrų saugumą ir kovojant su kompiuteriniais nusikaltimais[5] (toliau – 2001 m. komunikatas). 2001 m. komunikate pateiktos atitinkamos materialinės ir procesinės teisės nuostatos, skirtos kovoti su nacionalinėmis ir tarptautinėmis nusikalstamomis veikomis. Šis komunikatas – kelių svarbių pasiūlymų pagrindas. Visų pirma tai pasiūlymas, lėmęs Pamatinį sprendimą 2005/222/TVR dėl atakų prieš informacines sistemas[6]. Šiuo atveju taip pat reikėtų pažymėti, kad buvo priimti kiti bendresnio pobūdžio teisės aktai, taip pat apimantys kovos su elektroniniais nusikaltimais aspektus, pavyzdžiui, Pamatinis sprendimas

---

4 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (OL L 178, 2000 7 17, p. 1).

5 KOM(2000) 890, 2001 1 26.

6 OL L 69, 2005 3 16, p. 67.

2001/413/TVR, skirtas kovai su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu[7].

Komisija skiria ypatingą dėmesį **vaikų apsaugai**, ypač kovai su visų rūšių seksualinio vaikų išnaudojimo medžiaga, neteisėtai paskelbta naudojant informacines sistemas, – horizontaliajam prioritetui, kurio bus laikomasi ateityje, o Pamatinis sprendimas 2004/68/TVR dėl kovos su seksualiniu vaikų išnaudojimu ir vaikų pornografija[8] yra geras to pavyzdys.

Europos bendrija, siekdama įveikti su informacinės visuomenės saugumu susijusius sunkumus, parengė trijų dalių modelį tinklų ir informacijos saugumui: konkrečios tinklų ir informacijos saugumo priemonės, elektroninių ryšių reguliavimo sistema ir kova su elektroniniais nusikaltimais. Nors šiuos tris aspektus tam tikru mastu galima plėtoti atskirai, tačiau jie yra labai tarpusavyje susiję, todėl reikia glaudaus derinimo. Susijusioje tinklų ir informacijos saugumo srityje greta 2001 m. Komunikato dėl elektroninių nusikaltimų 2001 m. buvo priimtas Komisijos komunikatas dėl tinklų ir informacijos saugumo: pasiūlymas dėl ES politikos požiūrio[9]. Direktyvoje 2002/58/EB dėl privatumo ir elektroninių ryšių nustatyta viešai prieinamų elektroninių ryšių paslaugų teikėjų pareiga užtikrinti savo paslaugų saugumą. Toje direktyvoje taip pat pateiktos nuostatos, skirtos kovai su nepageidaujamu e. paštu ir šnipinėjimo programomis. Vėliau tinklų ir informacijos saugumo politika buvo plėtojama tam tikrais veiksmais, paskutiniai iš jų – Komunikatas dėl saugios informacinės visuomenės strategijos[10], kuriame nustatyta atnaujinta strategija ir pateikiami pagrindiniai principai, kaip plėtoti ir patobulinti vieningą požiūrį į tinklų ir informacijos saugumą, Komunikatas dėl kovos su nepageidaujamu e. paštu, šnipinėjimo programomis ir žalinga programine įranga[11] ir 2004 m. Europos tinklų ir informacijos apsaugos agentūros (ENISA) įsteigimas[12]. Pagrindinis ENISA tikslas – plėtoti specialiąsias žinias, siekiant skatinti viešojo ir privačiojo sektorių bendradarbiavimą ir teikti pagalbą Komisijai ir valstybėms narėms. **Mokslinių tyrimų rezultatai** technologijų, skirtų informacijos sistemų saugumui, srityje taip pat bus svarbūs kovojant su elektroniniais nusikaltimais. Todėl informacijos bei ryšių technologijos ir saugumas yra pateikti kaip 2007–2013 m. laikotarpio ES Septintosios bendrosios mokslinių tyrimų programos (BP 7) tikslai[13]. Elektroninių ryšių reguliavimo sistemos peržiūra gali lemti pakeitimus, išplečiančius Direktyvos dėl privatumo ir elektroninių ryšių bei Universaliųjų paslaugų direktyvos 2002/22/EB[14] nuostatų, susijusių su saugumu, veiksmingumą.

---

7 OL L 149, 2001 6 2, p. 1.

8 OL L 13, 2004 1 20, p. 44.

9 KOM(2001) 298.

10 KOM(2006) 251.

11 KOM(2006) 688.

12 Reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, (OL L 77, 2004 3 13, p. 1).

13 Europos Sąjunga jau pagal 6-ąją pamatinę mokslinių tyrimų ir technologijų plėtros programą rėmė kai kuriuos atitinkamus ir sėkmingus mokslinių tyrimų projektus.

14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.

2.2. Galiojantys tarptautiniai aktai

Jokia politika, skirta kovai su elektroniniais nusikaltimais, negali būti veiksminga, jei pastangos apsiriboja ES, nes informacijos tinklai yra pasaulinio pobūdžio. Nusikaltėliai ne tik gali rengti atakas prieš informacines sistemas arba daryti nusikaltimus įvairiose valstybėse narėse, bet jie lengvai tą gali daryti iš už ES jurisdikcijos ribų. Todėl Komisija buvo aktyvi tarptautinių diskusijų ir bendradarbiavimo struktūrų, pavyzdžiui, G8 Liono–Romos modernių technologijų nusikaltimų grupės ir Interpolo vykdomų projektų dalyvė. Visų pirma Komisija įdėmiai stebi 24 valandų ryšių dėl tarptautinių modernių technologijų nusikaltimų tinklo (24/7 tinklas)[15], kurio narėmis yra nemažai valstybių visame pasaulyje, įskaitant daugelį ES valstybių narių, darbą. G8 tinklą sudaro mechanizmas, per 24 valandų ryšio punktus pagreitinantis dalyvaujančių valstybių ryšius su elektroniniais įrodymais susijusiais atvejais ir tais atvejais, kai reikia greitos užsienio teisėsaugos institucijų pagalbos.

Be abejo, svarbiausias Europos ir tarptautinis aktas šioje srityje yra 2001 m. Europos Tarybos konvencija dėl elektroninių nusikaltimų[16]. 2004 m. priimtoje ir įsigaliojusioje konvencijoje pateiktos bendros įvairių elektroninių nusikaltimų rūšių apibrėžtys ir nustatyti susitariančiųjų šalių teisinio bendradarbiavimo veikimo pagrindai. Ją pasirašė daug valstybių, įskaitant Jungtines Amerikos Valstijas ir kitas ne Europos valstybes, ir visos valstybės narės. Tačiau kai kurios valstybės narės dar neratifikavo konvencijos arba konvencijos Papildomo protokolo dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo. Atsižvelgiant į sutartą konvencijos svarbą, Komisija ragins valstybes nares ir atitinkamas trečiąsias šalis ratifikuoti konvenciją ir svarstys galimybę Europos bendrijai tapti konvencijos šalimi.

3. TOLESNĖ KONKREČIŲ AKTŲ, SKIRTŲ KOVAI SU ELEKTRONINIAIS NUSIKALTIMAIS, RAIDA

3.1. Operatyvinio teisėsaugos bendradarbiavimo stiprinimas ir ES lygmens mokymo pastangos

Tiesioginių **tarpvalstybinio operatyvinio bendradarbiavimo** struktūrų stoka arba nepakankamas naudojimasis šiomis struktūromis išlieka pagrindiniu teisingumo, laisvės ir saugumo srities trūkumu. Įprasta savitarpio pagalba skubiais elektroninių nusikaltimų atvejais yra lėta ir neveiksminga, o naujos bendradarbiavimo struktūros dar nėra pakankamai išvystytos. Nors nacionalinės teisminės ir teisėsaugos institucijos Europoje glaudžiai bendradarbiauja per Europolą, Eurojustą ir kitas struktūras, tačiau išlieka akivaizdus poreikis sustiprinti ir išaiškinti pareigas. Komisijos rengtos konsultacijos rodo, kad nėra optimaliai naudojamasi šiais svarbiais kanalais. Labiau suderintas Europos požiūris turi būti operatyvaus bei strateginio pobūdžio ir taip pat turi apimti keitimąsi informacija ir geriąja patirtimi.

Artimiausiu metu Komisija skirs ypatingą dėmesį **mokymo** poreikiams. Įrodyta, kad technologijų raida lemia nuolatinio teisėsaugos ir teisminių institucijų pareigūnų mokymo apie elektroninių nusikaltimų problemas poreikį. Todėl numatyta sustiprinta ir geriau suderinta ES finansinė pagalba tarptautinėms mokymo programoms. Komisija, glaudžiai bendradarbiaudama su valstybėmis narėmis ir kitomis kompetentingomis institucijomis,

---

15 Žr. Europos Tarybos konvencijos dėl elektroninių nusikaltimų 35 straipsnį.

16 http://conventions.coe.int/treaty/en/treaties/html/185.htm.

pavyzdžiui, Europolu, Eurojustu, Europos policijos koledžu (CEPOL) ir Europos teisėjų mokymo tinklu (EJTN), taip pat dirbs, siekdama visų atitinkamų mokymo programų suderinimo ir sujungimo ES lygmeniu.

2007 m. Komisija surengs valstybių narių, Europolo, CEPOL ir EJTN teisėsaugos ekspertų **susitikimą**, skirtą aptarti, kaip pagerinti strateginį bei operatyvinį bendradarbiavimą ir mokymą, susijusį su elektroniniais nusikaltimais, Europoje. Be to, bus aptartas nuolatinio ES ryšio punkto, skirto keistis informacija, įsteigimas ir ES mokymo, susijusio su elektroniniais nusikaltimais, programos sukūrimas. 2007 m. susitikimas bus pirmasis iš artimiausiu metu ketinamų surengti susitikimų.

3.2. Sustiprinti dialogą su pramonės subjektais

Privatusis ir viešasis sektoriai yra suinteresuoti kartu plėtoti nusikalstamomis veikomis padarytos žalos nustatymo metodus ir metodus, skirtus užkirsti kelią tokiai žalai atsirasti. Bendras viešojo ir privačiojo sektorių dalyvavimas, kuris remiasi savitarpio pasitikėjimu ir bendru žalos sumažinimo tikslu, gali būti veiksmingas būdas sustiprinti saugumą, taip pat kovojant su elektroniniais nusikaltimais. Viešieji ir privatieji Komisijos politikos, skirtos kovai su elektroniniais nusikaltimais, aspektai tinkamu laiku taps planuojamos pasaulinės ES politikos dėl viešojo ir privačiojo sektorių dialogo, apimančios visą Europos saugumo sritį, dalimi. Šią politiką visų pirma plėtos Europos saugumo mokslinių tyrimų ir naujovių forumas, kurį Komisija ketina netrukus įsteigti, ir kuris pergrupuos atitinkamas suinteresuotąsias viešojo ir privačiojo sektorių šalis.

Modernių informacinių technologijų ir elektroninių ryšių sistemų raidą iš esmės kontroliuoja privatūs subjektai. Privačios bendrovės atlieka grėsmių vertinimus, nustato kovos su nusikaltimais programas ir plėtoja techninius sprendimus, skirtus nusikaltimų prevencijai. Pramonės subjektai parodė, kad jie yra labai linkę teikti pagalbą valstybės institucijoms kovojant su elektroniniais nusikaltimais, ypač stengiantis kovoti su vaikų pornografija[17] ir kitomis neteisėto turinio internete rūšimis.

Kita problema yra susijusi su akivaizdžiu viešojo ir privačiojo sektorių keitimosi informacija, specialiosiomis žiniomis ir gerąja patirtimi trūkumu. Privačiojo sektoriaus subjektai, siekdami apsaugoti verslo modelius ir paslaptis, dažnai nenori, arba jiems nėra nustatyta jokia aiški teisinė pareiga pateikti teisėsaugos institucijoms atitinkamą informaciją, susijusią su nusikaltimų paplitimu. Tačiau tokia informacija gali būti reikalinga, siekiant kad valstybės institucijos nustatytų veiksmingą ir tinkamą politiką, skirtą kovai su nusikaltimais. Galimybės pagerinti skirtingų sektorių keitimąsi informacija bus aptartos taip pat atsižvelgiant į galiojančias taisykles dėl asmens duomenų apsaugos.

Komisija jau atlieka svarbų vaidmenį įvairiose viešosiose ir privačiosiose struktūrose, susijusiose su elektroniniais nusikaltimais, pavyzdžiui, Sukčiavimo prevencijos ekspertų grupėje[18]. Komisija įsitikinusi, kad veiksminga bendroji politika, skirta kovai su elektroniniais nusikaltimais, taip pat turi apimti viešojo ir privačiojo sektorių subjektų, įskaitant pilietinės visuomenės organizacijas, bendradarbiavimo strategiją.

---

[17] Vienas nesenas bendradarbiavimo šioje srityje pavyzdys – teisėsaugos ir kredito kortelių bendrovių bendradarbiavimas, kai pastarosios padėjo policijai nustatyti vaikų pornografijos internete pirkėjus.

[18] Žr. http://ec.europa.eu/internal_market/payments/fraud/index_en.htm.

2007 m. Komisija, siekdama platesnio viešojo ir privačiojo sektorių bendradarbiavimo šioje srityje, surengs konferenciją teisėsaugos ekspertams ir privačiojo sektoriaus atstovams, ypač interneto paslaugų teikėjams, skirtą aptarti, kaip pagerinti viešojo ir privačiojo sektorių operatyvinį bendradarbiavimą Europoje[19]. Konferencijoje bus aptartos visos temos, kurios, manoma, gali suteikti pridėtinės vertės abiems sektoriams, tačiau ypač:

- operatyvinio bendradarbiavimo kovojant su neteisėtomis veikomis ir neteisėtu turiniu internete, ypač terorizmo, seksualinio vaikų išnaudojimo medžiagos ir kitų neteisėtų veikų, ypač žalingų vaikų apsaugos atžvilgiu, srityse, pagerinimas;

- viešojo ir privačiojo sektorių susitarimų, skirtų neteisėto turinio tinklavietėms, ypač vaikų seksualinio išnaudojimo medžiagai, blokuoti ES mastu inicijavimas;

- Europos modelio, skirto viešajam ir privačiajam sektoriams keistis būtina ir atitinkama informacija, kad *inter alia* būtų paskatinta savitarpio pasitikėjimo aplinka ir būtų atsižvelgta į visų šalių interesus, sukūrimas;

- teisėsaugos ryšio punktų tinklo viešajame ir privačiajame sektoriuose įsteigimas.

3.3. Teisės aktai

Bendras elektroninių nusikaltimų srities nusikaltimų apibrėžčių ir nacionalinių baudžiamųjų įstatymų derinimas dar nėra tinkamas, nes ši sąvoka apima įvairias nusikalstamų veikų rūšis. Veiksmingas teisėsaugos institucijų bendradarbiavimas dažnai priklauso nuo bent iš dalies suderintų nusikaltimų apibrėžčių, todėl išlieka ilgalaikis tikslas tęsti valstybių narių teisės aktų derinimą[20]. Kai kurių esminių nusikaltimų apibrėžčių atžvilgiu jau žengtas svarbus žingsnis, priimant Pamatinį sprendimą dėl atakų prieš informacines sistemas. Kaip pirmiau apibūdinta, vėliau kilo naujos grėsmės, o Komisija atidžiai stebi šią raidą, atsižvelgdama į papildomų teisės aktų poreikio nuolatinio vertinimo svarbą. Kintančių grėsmių stebėsena glaudžiai derinama su Europos programa dėl ypatingos svarbos infrastruktūros objektų apsaugos.

Tačiau dabar taip pat reikėtų aptarti tikslinius teisės aktus, skirtus kovai su elektroniniais nusikaltimais. Ypatinga problema, kuriai gali reikėti teisės akto, susijusi su situacija, kai elektroniniai nusikaltimai padaromi pasinaudojant **tapatybės vagyste**. Paprastai tapatybės vagystė suprantama kaip asmens tapatybę atskleidžiančios informacijos panaudojimas, pavyzdžiui, kredito kortelės numeris, kaip priemonė padaryti kitus nusikaltimus. Daugelyje valstybių narių labiausiai tikėtina, kad nusikaltėlis būtų patrauktas baudžiamojon atsakomybėn ne už tapatybės vagystę, o už sukčiavimą arba kitą galimą nusikaltimą, kurie laikomi sunkesniais nusikaltimais. Tapatybės vagystė nėra kriminalizuota visose valstybėse narėse. Dažniausiai tapatybės vagystės nusikaltimą įrodyti lengviau negu sukčiavimo nusikaltimą, todėl tapatybės vagystės kriminalizavimas visose valstybėse narėse pagerintų ES teisėsaugos bendradarbiavimą. 2007 m. Komisija pradės konsultacijas, skirtas įvertinti, ar tinkama priimti teisės aktus.

---

[19] Konferenciją galima laikyti ES forumo, nurodyto Kompiuterinių nusikaltimų komunikato 6.4 skirsnyje, tęsiniu.

[20] Šis ilgalaikis tikslas jau buvo paminėtas 2001 m. komunikato 3 puslapyje.

3.4. Statistinių duomenų raida

Paprastai sutariama, kad dabartinė informacijos, susijusios su nusikaltimų paplitimu, būklė yra labai netinkama, ir, visų pirma, kad reikia žymiai pagerinti valstybių narių duomenų palyginimą. Siekiant įveikti šią problemą Komisijos komunikate dėl *ES nusikalstamumo ir baudžiamosios teisenos visapusiškos ir nuoseklios vertinimo strategijos kūrimo: 2006–2010 m. ES veiksmų planas*[21] nustatytas ambicingas penkerių metų planas. Pagal šį veiksmų planą įsteigtos ekspertų grupės darbas būtų tinkama priemonė plėtoti atitinkamus rodiklius, skirtus elektroninių nusikaltimų mastui apskaičiuoti.

4. KELIAS PIRMYN

Komisija dabar plėtos bendrąją politiką, skirtą kovai su elektroniniais nusikaltimais. Ši politika gali tik papildyti valstybių narių ir kitų institucijų veiksmus, nes Komisijos galios baudžiamosios teisės srityje yra ribotos. Svarbiausi veiksmai (kiekvienas iš šių veiksmų reikš vieno, kelių ar visų aktų, pateiktų 3 skyriuje, panaudojimą) taip pat bus remiami per finansinę programą „Nusikalstamumo prevencija ir kova su nusikalstamumu“:

4.1. Kova su elektroniniais nusikaltimais apskritai

- Nustatyti sustiprintą operatyvinį valstybių narių teisėsaugos ir teisminių institucijų bendradarbiavimą; šis veiksmas prasidės paskirtų ekspertų susitikimo surengimu 2007 m. ir gali apimti centrinio ES elektroninių nusikaltimų ryšio punkto įsteigimą.

- Skirti daugiau lėšų iniciatyvoms, skirtoms teisėsaugos ir teisminių institucijų pareigūnų mokymui, susijusiam su elektroninių nusikaltimų bylų nagrinėjimu, gerinti ir imtis veiksmų, skirtų visoms tarptautinėms šios srities mokymo pastangoms derinti, sukuriant ES mokymo programą.

- Skatinti stipresnį valstybių narių ir visų valstybės institucijų įsipareigojimą imtis veiksmingų priemonių, skirtų kovai su elektroniniais nusikaltimais, ir skirti pakankamai išteklių kovai su elektroniniais nusikaltimais.

- Remti mokslinius tyrimus, padedančius kovoti su elektroniniais nusikaltimais.

- (2007 m.) surengti bent vieną svarbią teisėsaugos institucijų ir privačių subjektų konferenciją, ypač inicijuoti bendradarbiavimą kovojant su neteisėtomis interneto veikomis elektroniniuose tinkluose bei prieš juos ir skatinti veiksmingesnį keitimąsi neasmeninio pobūdžio informacija, ir įgyvendinti šios 2007 m. konferencijos išvadas per konkrečius viešojo ir privačiojo sektorių bendradarbiavimo projektus.

- Inicijuoti viešojo ir privačiojo sektorių veiksmus, skirtus (ypač vartotojų) informuotumui apie elektroninių nusikaltimų sąnaudas ir apie jų pavojus gerinti, ir dalyvauti tokiuose veiksmuose, tačiau nepakenkti vartotojų ir naudotojų tikėjimui ir pasitikėjimui, sutelkiant dėmesį tik į neigiamus saugumo aspektus.

- Aktyviai bendradarbiauti pasauliniame tarptautiniame lygmenyje kovojant su elektroniniais nusikaltimais ir skatinti tokį bendradarbiavimą.

---

[21] KOM(2006) 437, 2006 8 7.

- Inicijuoti ir remti tarptautinius projektus, suderintus su šios srities Komisijos politika, pavyzdžiui, G 8 vykdomi projektai, suderinti su šalių ir regionų strateginiais dokumentais (atsižvelgiant į bendradarbiavimą su trečiosiomis šalimis), ir prisidėti prie tokių tarptautinių projektų.

- Imtis konkrečių veiksmų skatinant visas valstybes nares ir atitinkamas trečiąsias šalis ratifikuoti Europos Tarybos konvenciją dėl elektroninių nusikaltimų bei jos papildomą protokolą ir svarstyti galimybę Bendrijai tapti konvencijos šalimi.

- Kartu su valstybėmis narėmis ištirti suderintų ir didelio masto atakų prieš valstybių narių informacijos infrastruktūros objektus reiškinį, siekiant užkirsti joms kelią ir su jomis kovoti, įskaitant suderintus atsakus ir dalijimąsi informacija bei geraja patirtimi.

4.2. Kova su įprastiniais nusikaltimais elektroniniuose tinkluose

- Inicijuoti nuodugnų tyrimą, siekiant parengti pasiūlymą dėl konkretaus ES teisės akto, skirto kovai su tapatybės vagyste.

- Skatinti techninių metodų ir procedūrų, skirtų kovoti su sukčiavimu ir neteisėta prekyba internete, plėtrą, taip pat per viešojo ir privačiojo sektorių bendradarbiavimo projektus.

- Tęsti ir toliau plėtoti darbą konkrečiose tikslinėse srityse, pavyzdžiui, Sukčiavimo prevencijos ekspertų grupėje kovojant su sukčiavimu negrynosiomis mokėjimo priemonėmis elektroniniuose tinkluose.

4.3. Neteisėtas turinys

- Toliau plėtoti veiksmus, skirtus kovai su konkrečiu neteisėtu turiniu, ypač su seksualinio vaikų išnaudojimo medžiaga bei terorizmo kurstymu ir ypač tęsiant Pamatinio sprendimo dėl seksualinio vaikų išnaudojimo įgyvendinimą.

- Paraginti valstybes nares skirti papildomų lėšų teisėsaugos agentūrų darbui sustiprinti, ypatingą dėmesį skiriant seksualinio išnaudojimo per internete platinamą medžiagą aukų nustatymui.

- Inicijuoti ir paremti veiksmus, skirtus kovai su neteisėtu turiniu, kuris gali paskatinti nepilnamečių smurtą ir kitokį pavojingą neteisėtą elgesį, pavyzdžiui, kai kurios itin smurtinių vaizdo žaidimų internete rūšys.

- Inicijuoti ir skatinti valstybių narių ir jų bei trečiųjų šalių dialogą dėl techninių metodų, skirtų kovai su neteisėtu turiniu, ir dėl procedūrų, skirtų neteisėtoms tinklavietėms uždaryti, taip pat atsižvelgiant į galimą oficialių susitarimų su kaimyninėmis ir kitomis šalimis šiuo klausimu raidą.

- Sudaryti ES lygmens valstybės institucijų ir privačių subjektų, ypač interneto paslaugų teikėjų, savanoriškus susitarimus ir konvencijas dėl procedūrų, skirtų neteisėtoms interneto tinklavietėms blokuoti ir uždaryti.

4.4. Tęsinys

Šiame komunikate kai kurie veiksmai, skirti bendradarbiavimo struktūroms ES pagerinti, buvo išdėstyti kaip tolesnės pakopos. Komisija plėtos šiuos veiksmus, įvertins pažangą, pasiektą įgyvendinant veiksmus, ir atsiskaitys Tarybai bei Parlamentui.