Byla C-70/10

Scarlet Extended SA

prieš

Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)

(*cour d'appel de Bruxelles*
prašymas priimti prejudicinį sprendimą)

„Informacinė visuomenė — Autorių teisės — Internetas — Peer to peer programinė įranga — Interneto prieigos paslaugų teikėjai — Elektroninių pranešimų filtravimo sistemos įdiegimas siekiant užkirsti kelią keitimuisi elektroninėmis rinkmenomis pažeidžiant autorių teises — Bendros prievolės stebėti perduodamą informaciją nebuvimas“

Generalinio advokato P. Cruz Villalón išvada, pateikta 2011 m. balandžio 14 d. . . . . I - 11962

2011 m. lapkričio 24 d. Teisingumo Teismo (trečioji kolegija) sprendimas . . I - 12006

Sprendimo santrauka

Teisės aktų derinimas — Informacinė visuomenė — Autorių teisės ir gretutinės teisės — Asmens duomenų apsauga elektroninių ryšių sektoriuje — Interneto prieigos paslaugų teikėjui nustatytas įpareigojimas įdiegti visų elektroninių pranešimų filtravimo sistemą visų jo klientų atžvilgiu, prevenciškai, jo sąskaita ir neterminuotai, siekiant užkirsti kelią intelektinės nuosavybės teisės pažeidimams — Nepriimtinumas

(Europos Sąjungos pagrindinių teisių chartijos 8 ir 11 straipsniai; Europos Parlamento ir Tarybos direktyva 95/46, Direktyvos 2000/31 15 straipsnio 1 dalis, direktyvos 2001/29, 2002/58 ir Direktyvos 2004/48 3 straipsnio 1 dalis)

Kartu skaitomas ir atsižvelgiant į iš taikytinų pagrindinių teisių apsaugos kylančius reikalavimus aiškinamas direktyvas, būtent Direktyvą 2000/31 dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje, Direktyvą 2001/29 dėl autorių teisių ir gretutinių teisių informacinėje visuomenėje tam tikrų aspektų suderinimo, Direktyvą 2004/48 dėl intelektinės nuosavybės teisių gynimo, Direktyvą 95/46 dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir Direktyvą 2002/58 dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje reikia aiškinti taip, kad jomis draudžiama interneto prieigos paslaugų teikėjui nustatyti įpareigojimą įdiegti filtravimo sistemą:

— visiems naudojantis jo paslaugomis gaunamiems ir siunčiamiems elektroniniams pranešimams, pasinaudojant, be kita ko, „peer-to-peer“ programine įranga,

— visų jo klientų atžvilgiu,

— prevenciškai,

— tik jo sąskaita,

— neterminuotai,

kuri leistų nustatyti tokio tiekėjo tinklu siunčiamas muzikos, kinematografijos ar audiovizualinių kūrinių, kurių intelektinės nuosavybės teisės tariamai priklauso ieškovui, elektronines rinkmenas, kad būtų galima užblokuoti rinkmenų, kuriomis keičiantis pažeidžiamos autorių teisės, persiuntimą.

Iš tiesų dėl tokio įpareigojimo minėtas teikėjas privalėtų aktyviai stebėti visus ir su visais jo klientais susijusius duomenis, kad užkirstų kelią bet kokiam būsimam intelektinės nuosavybės teisių pažeidimui ir taip jam būtų nustatyta bendra stebėjimo prievolė, draudžiama pagal Direktyvos 2000/31 15 straipsnio 1 dalį. Be to, toks įpareigojimas akivaizdžiai pažeistų atitinkamo teikėjo įmonės laisvę užsiimti verslu, nes pagal šį įpareigojimą ji privalėtų įdiegti sudėtingą, brangiai kainuojančią, nuolat veikiančią ir tik savo lėšomis finansuojamą informacinę sistemą, o tai irgi prieštarautų Direktyvos 2004/48 3 straipsnio 1 dalyje, pagal kurią reikalaujama, kad priemonės, skirtos užtikrinti intelektinės nuosavybės teisių apsaugą, nebūtų nereikalingai sudėtingos ar brangios, numatytiems reikalavimams. Be to, toks įpareigojimas pažeidžia reikalavimą užtikrinti tinkamą pusiausvyrą tarp intelektinės nuosavybės teisės apsaugos, kuria naudojasi autorių teisių turėtojai, ir ūkio subjektams, kaip antai interneto prieigos paslaugų teikėjams, suteiktos laisvės užsiimti verslu apsaugos. Toks įpareigojimas paveiktų ne tik šiuos teikėjus, nes filtravimo sistema gali pažeisti ir jų klientų pagrindines teises, būtent jų teisę į asmens duomenų apsaugą ir laisvę gauti ar skleisti informaciją; šios teisės saugomos pagal Europos Sąjungos pagrindinių teisių

chartijos 8 ir 11 straipsnius. Viena vertus, įpareigojimas reikštų, kad reikia sistemingai analizuoti visų pranešimų turinį ir rinkti informaciją apie vartotojų, kurie siųstų neleistino turinio pranešimus tinklu, IP adresus ir juos nustatyti, nors šie adresai yra saugomų asmens duomenų dalis, nes leidžia tiksliai nustatyti tokius vartotojus. Kita vertus, kiltų pavojus, kad toks įpareigojimas pažeis informacijos laisvę, nes yra rizika, kad naudojantis šia sistema nebus galimybės tinkamai atskirti neleistino ir leistino turinio pranešimų, taigi ją naudojant galėtų būtų blokuojami leistino turinio pranešimai.

(žr. 40, 48–52 punktus ir rezoliucinę dalį)