32000D0520

ODLUKA KOMISIJE

od 26. srpnja 2000.

sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a

(priopćena pod brojem dokumenta C(2000) 2441)

(Tekst značajan za EGP)

(2000/520/EZ)

KOMISIJA EUROPSKIH ZAJEDNICA,

uzimajući u obzir Ugovor o osnivanju Europske zajednice,

uzimajući u obzir Direktivu 95/46/EZ Europskog Parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka ([1]), a posebno njezin članak 25. stavak 6.,

budući da:

(1) Sukladno s Direktivom 95/46/EZ države članice obvezne su osigurati da se prijenos osobnih podataka u treću zemlju može izvršiti samo ako dotična treća zemlja osigurava primjerenu razinu zaštite i da se zakoni države članice kojima se provode ostale odredbe Direktive poštuju prije prijenosa.

(2) Komisija može utvrditi da treća zemlja osigurava primjerenu razinu zaštite. U tom se slučaju osobni podaci mogu prenositi iz Države članice a da nisu potrebna dodatna jamstva.

(3) Sukladno s Direktivom 95/46/EZ, razinu zaštite podataka trebalo bi procjenjivati s obzirom na sve okolnosti koje okružuju postupak prijenosa podataka ili niz postupaka prijenosa podataka i uzimajući u obzir dane uvjete. Radna skupina za zaštitu pojedinaca pri obradi osobnih podataka osnovana prema toj Direktivi ([2]) izdala je uputu za izvršenje takvih procjena ([3]).

(4) S obzirom na različite pristupe zaštiti podataka u trećim zemljama, trebalo bi ocijeniti primjerenost zaštite i izvršiti svaku odluku koja se temelji na članku 25 stavka 6. Direktive 95/46/EZ tako da ne dođe do samovoljne ili neopravdane diskriminacije protiv trećih zemalja ili među trećim zemljama gdje prevladavaju slični uvjeti, ni da se stvore prikrivene prepreke za trgovanje, uvažavajući trenutačne međunarodne obveze Zajednice.

(5) Trebala bi se postići primjerenu razinu zaštite prijenosa podataka iz Zajednice u Sjedinjene Američke Države koju priznaje ova Odluka, ako organizacije poštuju načela zaštite privatnosti „sigurne luke" za zaštitu osobnih podataka koji se prenose iz države članice u Sjedinjene Američke Države (dalje u tekstu „načela") i često postavljana pitanja koja daju smjernice za provedbu načela koje je izdala Vlada Sjedinjenih Američkih Država 21. srpnja 2000. Nadalje, organizacije bi trebale javno objaviti svoje politike zaštite privatnosti i podlijegati nadležnošću Savezne trgovinske komisije (Federal Trade Commission, FTC), sukladno s odjeljkom 5. Federal Trade Commission Act-a, koji zabranjuje nepravedne ili prijevarne radnje ili postupke u trgovini ili koje utječu na trgovinu, ili podlijegati nadležnosti nekog drugog državnog tijela koje će učinkovito osigurati usklađenost s načelima koja se provode u skladu s često postavljanim pitanjima.

(6) Sektori i/ili obrada podataka koji ne podliježu nadležnosti nijednog vladinog tijela u Sjedinjenim Američkim Državama navedenog u Prilogu VII. ovoj Odluci trebali bi biti izvan područja primjene ove Odluke.

(7) Kako bi se osigurala pravilna primjena ove Odluke, potrebno je da zainteresirane stranke, kao što su osobe čiji se podaci obrađuju, iznositelji podataka i tijela za zaštitu podataka mogu prepoznati organizacije koje poštuju načela i često postavljana pitanja. U tu svrhu

([1]) SL L 281, 23.11.1995., str. 31.

([2]) Internetska adresa radne skupine je: http://www.europa.eu.int/comm/internal_tržištu/en/media/dataprot/wpdocs/index.htm

([3]) RS 12: Prijenosi osobnih podataka u treće zemlje: primjena članaka 25. i 26. Direktive EU-a o zaštiti podataka, koju je donijela radna skupina 24. srpnja 1998.

Ministarstvo trgovine SAD-a ili njegov ovlašteni predstavnik trebao bi održavati i javnosti učiniti dostupnim popis organizacija koje same potvrđuju svoje poštivanje načela provedenih u skladu s često postavljanim pitanjima koja podliježu nadležnosti barem jednog vladinog tijela navedenog u Prilogu VII. ove Odluke.

(8) U interesu transparentnosti i radi zaštite sposobnost nadležnih tijela u državama članicama da osiguraju zaštitu pojedinaca s obzirom na a obradu njihovih osobnih podataka, potrebno je u ovoj Odluci navesti iznimne okolnosti u kojima suspenzija određenih protoka podataka može biti opravdana, neovisno o pronalaženje primjerene zaštite.

(9) Moguće je da će se morati ponovno razmatrati zaštita privatnosti „sigurne luke" koju su stvorila načela i često postavljana pitanja, s obzirom na iskustvo, razvoj što se tiče zaštite privatnosti u okolnostima u kojima tehnologija stalno olakšava prijenos i obradu osobnih podataka te s obzirom na izvješća uključenih provedbenih tijela o samom provođenju.

(10) Radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka, koja je osnovana sukladno s člankom 29. Direktive 95/46/EZ dostavila je mišljenja o razini zaštite koju pružaju načela zaštite privatnosti „sigurne luke", a koja je uzeta u obzir pri pripremi ove Odluke ([4]).

(11) Mjere utvrđene u ovoj Odluci u skladu su s mišljenjem Odbora osnovanog sukladno s člankom 31. Direktive 95/46/EZ.

(12) Sukladno s Odlukom Vijeća 1999/468/EZ, a posebno njezinom članku 8., Europski je parlament 5. srpnja 2000. usvojio Rezoluciju A5-0177/2000 o nacrtu odluke Komisije o primjerenosti zaštite koju pružaju „načela zaštite privatnosti sigurne luke" i za njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a ([5]). Komisija je preispitala nacrt odluke uzimajući u obzir tu Rezoluciju i zaključila da, iako je Europski parlament izrazio mišljenje da treba napraviti određena poboljšanja u „načelima zaštite privatnosti sigurne luke" i za njih vezanim često postavljanim pitanjima prije nego što se može smatrati da pružaju „primjerenu zaštitu", nije utvrdio da bi Komisija prekoračila svoje ovlasti usvajanjem ove Odluke,

DONIJELA JE OVU ODLUKU:

Članak 1.

1. Za potrebe članka 25. stavka 2. Direktive 95/46/EZ, u svim aktivnostima koje su obuhvaćene područjem primjene te Direktive, smatra se da „načela privatnosti sigurne luke" (dalje u tekstu „načela") iz Priloga I. ove Odluke, provedena u skladu sa smjernicama iz često postavljanih pitanja koje je izdalo Ministarstvo trgovine SAD-a 21. srpnja 2000., navedena u Prilogu II. ove Odluke, osiguravaju primjerenu razinu zaštite osobnih podataka, koji se prenose iz Zajednice u organizacije osnovane u Sjedinjenim Američkim Državama, uzimajući u obzir sljedeće dokumente koje je izdalo Ministarstvo trgovine SAD-a:

(a) pregled provedbe „sigurne luke" iz Priloga III.;

(b) memorandum o odštetama za kršenja privatnosti i izričitih ovlasti prema zakonima SAD–a iz Priloga IV.;

(c) pismo od Savezne trgovinske komisije iz Priloga V.;

(d) pismo od Ministarstva prometa SAD-a iz Priloga VI.

2. Kod svakog prijenosa podataka moraju biti zadovoljeni sljedeći uvjeti:

(a) da je organizacija koja prima podatke nedvosmisleno i javno objavila svoju obvezu da poštuje načela provedena u skladu s često postavljanim pitanjima; i

(b) da organizacija podliježe zakonskim ovlastima nekog vladinog tijela u Sjedinjenim Američkim Državama navedenog u Prilogu VII. ovoj Odluci, ovlaštenog da istražuje pritužbe i da ostvari pravnu zaštitu od nepoštenih ili prijevarnih postupaka, kao i naknadu za pojedince, bez obzira na njihovu zemlju boravišta ili državljanstvo, u slučaju nepridržavanja načela provedenih u skladu s često postavljanim pitanjima.

3. Smatra se da je svaka organizacija ispunila uvjete iz stavka 2. ako sama potvrdi svoje pridržavanje načela provedenih u skladu s često postavljanim pitanjima od datuma kad organizacija obavijesti Ministarstvo trgovine SAD-a (ili njegova ovlaštenog predstavnika) o javnoj objavi obveze iz stavka 2. točke (a) i o identitetu vladinog tijela iz stavka 2. točke (b).

([4]) RS 15: Mišljenje 1/99 o razini zaštite podataka u Sjedinjenim Američkim Državama i tekućim pregovorima između Europske komisije i Sjedinjenih Američkih Država.
RS 19: Mišljenje 2/99 o primjerenosti „međunarodnih načela sigurne luke" koje je izdalo Ministarstvo trgovine SAD-a 19. travnja 1999.
RS 21: Mišljenje 4/99 o često postavljanim pitanjima koja treba izdati Ministarstvo trgovine SAD-a vezano za predložena „načela sigurne luke" o primjerenosti „međunarodnih načela sigurne luke".
RS 23: Radni dokument o sadašnjem statusu tekućih rasprava između Europske komisije i Vlade Sjedinjenih Američkih Država o „međunarodnim načelima, sigurna luka".
RS 27: Mišljenje 7/99 o razini zaštite podataka koju pružaju načela „sigurne luke", koja je objavilo Ministarstvo trgovine SAD-a zajedno s često postavljanim pitanja i ostalim povezanim dokumentima 15. i 16. studenog 1999.
RS 31: Mišljenje 3/200 o dijalogu EU-a/SAD-a s obzirom na sporazum „sigurne luke".
RS 32: Mišljenje 4/2000 o razini zaštite koju pružaju „načela sigurne luke".

([5]) Rezolucija još nije objavljena u Službenom listu.

Članak 2.

Ova se Odluka odnosi samo na primjerenost zaštite koju pružaju načela provedena u skladu s često postavljanim pitanjima u Sjedinjenim Američkim Državama s ciljem ispunjavanja zahtjeva članka 25. stavka 1. Direktive 95/46/EZ i ne utječe na primjenu ostalih odredaba Direktive koje se odnose na obradu osobnih podataka u državama članicama, a osobito na njezin članak 4.

Članak 3.

1. Ne dovodeći u pitanje svoje ovlasti da poduzimaju radnje koje bi osigurale usklađenost s nacionalnim odredbama usvojenima u skladu s odredbama koje nisu iz članka 25. Direktive 95/46/EZ, nadležna tijela država članica mogu iskoristiti svoje postojeće ovlasti da suspendiraju protok podataka prema organizaciji koja je sama potvrdila svoje pridržavanje načela provedenih u skladu s često postavljanim pitanjima, kako bi zaštitila pojedince s obzirom na obradu njihovih osobnih podataka u slučajevima da:

(a) je vladino tijelo u Sjedinjenim Američkim Državama, iz Priloga VII. ove Odluke, ili neovisni mehanizam pravne zaštite u smislu dopisa (a) provedbenih načela iz Priloga I. ove Odluke utvrdilo da organizacija krši načela provedena u skladu s često postavljanim pitanjima; ili

(b) da postoji stvarna vjerojatnost da se krše načela; ako postoje opravdani razlozi da se vjeruje da dotični mehanizam provedbe ne poduzima ili neće poduzeti primjerene i pravovremene korake da razriješi dotični slučaj; ako bi nastavak prijenosa stvorio trenutačnu opasnost da ozbiljno našteti osobama čiji se podaci obrađuju, te ako su nadležna tijela država članica poduzela odgovarajuće napore da u tim okolnostima obavijeste organizaciju i dala joj mogućnost da se očituje.

Suspenzija prestaje važiti čim se osigura primjena načela provedenih u skladu s često postavljanim pitanjima i čim dotično nadležno tijelo u Zajednici bude o tome obaviješteno.

2. Države članice obavješćuju Komisiju bez odlaganja kada se usvoje mjere na temelju stavka 1.

3. Države članice i Komisija obavješćuju jedne druge o slučajevima kada neka radnja tijela odgovornog za osiguranje usklađenosti s načelima provedenima u skladu s često postavljanim pitanjima ne osigura takvu usklađenost.

4. Ako podaci prikupljeni sukladno stavcima 1., 2. i 3. pruže dokaz da neko tijelo odgovorno za osiguranje usklađenosti s načelima provedenima u skladu s često postavljanim pitanjima u Sjedinjenim Američkim Državama stvarno ne izvršava svoju ulogu, Komisija obavješćuje Ministarstvo trgovine SAD-a i prema potrebi, iznosi prijedloge mjera u skladu s postupkom iz članka 31. Direktive 95/46/EZ radi ukidanja ili suspenzije ove Odluke ili ograničenja njezina područja primjene.

Članak 4.

1. Ova se Odluka može izmijeniti bilo kada uzimajući u obzir iskustva u njezinoj provedbi i/ili ako razinu zaštite koju pružaju načela i često postavljana pitanja usvoji zakonodavstvo SAD-a.

Komisija u svakom slučaju ocjenjuje provedbu ove Odluke na temelju dostupnih informacija tri godine nakon njezina priopćenja državama članicama, te o relevantnim rezultatima izvješćuje Odbor osnovan sukladno s člankom 31. Direktive 95/46/EZ, uključujući sve dokaze koji mogu utjecati na procjenu da odredbe članka 1. ove Odluke pružaju adekvatnu zaštitu u smislu članka 25. Direktive 95/46/EZ te sve dokaze da se ova Odluka provodi na diskriminirajući način.

2. Komisija prema potrebi iznosi nacrt mjera u skladu s postupkom utvrđenim u članku 31. Direktive 95/46/EZ.

Članak 5.

Države članice poduzimaju sve mjere potrebne za usklađivanje s ovom Odlukom najkasnije u 90 dana od dana njezine objave u državama članicama.

Članak 6.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 26. srpnja 2000.

Za Komisiju

Frederik BOLKESTEIN

Član Komisije

PRILOG I.

NAČELA PRIVATNOSTI SIGURNE LUKE

koje je izdalo Ministarstvo trgovine SAD-a 21. srpnja 2000.

Opsežno zakonodavstvo Europske unije o privatnosti, Direktiva o zaštiti podataka (Direktiva), stupila je na snagu 25. listopada 1998. Ona nalaže da se osobni podaci prenose samo u one države nečlanice EU-a koje pružaju „primjerenu" razinu zaštite privatnosti. Iako i Sjedinjene Američke Države i Europska unija imaju isti cilj povećanja zaštite privatnosti svojih građana, Sjedinjene Američke Države imaju drugačiji pristup privatnosti nego Europska unija. Sjedinjene Američke Države koriste sektorski pristup koji se oslanja na kombinaciju zakonodavstva, propisa i samoregulacije. S obzirom na te razlike, mnoge su organizacije iz SAD-a izrazile nesigurnost s obzirom na utjecaj „standarda primjerenosti" koji EU zahtijeva, na prijenose osobnih podataka iz Europske unije u Sjedinjene Američke Države.

Da smanji ovu nesigurnost i pruži predvidljiviji okvir za takve prijenose podataka, Ministarstvo trgovine izdaje ovaj dokument i često postavljana pitanja („načela") prema svojoj zakonskoj ovlasti da jača, promiče i razvija međunarodnu trgovinu. Načela su izrađena u dogovoru s gospodarstvenicima i javnošću kako bi se olakšali trgovanje i trgovina između Sjedinjenih Američkih Država i Europske unije. Načela su namijenjena isključivo organizacijama SAD-a koje primaju osobne podatke iz Europske unije radi kvalificiranja za „sigurnu luku" i iz nje proizašlog preduvjeta „primjerenosti" zaštite podataka. Budući da su načela bila namijenjena isključivo u ovu određenu svrhu, njihova primjena u ostale svrhe može biti neprikladna. Načela se ne mogu koristiti kao zamjena za nacionalne odredbe za provedbu Direktive, koje se odnose na obradu osobnih podataka u državama članicama.

Odluke organizacija za kvalificiranje za „sigurnu luku" potpuno su dobrovoljne, a organizacije se mogu kvalificirati za „sigurnu luku" na različite načine. Organizacije koje odluče da će se pridržavati načela moraju poštovati načela da bi dobile i zadržale pogodnosti„sigurne luke" i javno izjaviti da to čine. Na primjer, ako se organizacija uključi u samoregulativni program privatnosti koji se pridržava načela, kvalificirana je za „sigurnu luku". Organizacije također mogu ispuniti uvjete tako da stvore vlastite samoregulativne politike zaštite privatnosti ako su one u skladu s načelima. Ako se pri poštovanju načela organizacija u potpunosti ili djelomično oslanja na samoregulaciju, njezino nepridržavanje takve samoregulacije mora također biti utuživo prema odjeljku 5. Federal Trade Commission Act-a koji zabranjuje nepravedne ili prijevarne radnje, ili prema nekom drugom zakonu ili propisu koji zabranjuje takve radnje. (Vidjeti Prilog s popisom državnih tijela SAD-a koje priznaje EU.) Osim toga, organizacije koje podliježu zakonskim, regulatornim, upravnim ili drugim propisima (ili pravilima) i učinkovito štiti osobnu privatnost, mogu se također kvalificirati za prednosti koje pruža „sigurna luka". U svim ovim slučajevima prednosti „sigurne luke" su osigurane od dana kada svaka organizacija koja se želi kvalificirati za „sigurnu luku" sama potvrdi Ministarstvu trgovine (ili njegovom ovlaštenom predstavniku) da se pridržava načela u skladu sa smjernicom o vlastitom potvrđivanju iz često postavljanih pitanja.

Pridržavanje ovih načela može biti ograničeno: (a) u onoj mjeri koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa, ili uvjeti za provedbu zakona; (b) zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepoštivanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje; ili (c) ako direktiva ili nacionalno pravo države članice predviđa iznimke ili odstupanja, uz uvjet da se takve iznimke ili odstupanja primjenjuju u sličnim kontekstima. U skladu s ciljem povećanja zaštite privatnosti, organizacije trebaju nastojati u potpunosti i transparentno provoditi ova načela, uključujući i tako da u svojim postupcima zaštite privatnosti navode kada će se redovito primjenjivati iznimke od načela, dopuštene u gore opisanom slučaju (b). Iz istog razloga, ako je mogućnost odabira dopuštena prema načelima i/ili zakonodavstvu SAD-a, očekuje se da se organizacije odluče za veću zaštitu tamo gdje je moguće.

Organizacije mogu htjeti iz praktičnih ili drugih razloga primjenjivati načela u svim svojim postupcima obrade podataka, ali obvezne su ih primjenjivati samo na podatke koje prenose nakon što pristupe „sigurnoj luci". Da se kvalificiraju za „sigurnu luku", organizacije nisu obvezne primjenjivati ova načela na osobne podatke u sustavima odlaganja dokumentacije koji se ručno obrađuju. Organizacije koje žele imati koristi od „sigurne luke" za primanje ručno obrađenih podataka

iz EU-a moraju primjenjivati načela na sve takve podatke koji se prenose nakon pristupa navedenim načelima. Organizacija koja želi proširiti koristi „sigurne luke" na osobne podatke o ljudskim potencijalima koje se prenose iz EU-a za uporabu u kontekstu radnog odnosa, mora to navesti kada se bude obvezivala Ministarstvu trgovine (ili njegovom ovlaštenom predstavniku) s obzirom na načela, te mora ispuniti zahtjeve iz često postavljanog pitanja o vlastitom potvrđivanju. Organizacije će također moći pružati zaštitu koja se traži člankom 26. Direktive ako načela uvrste u pisane sporazume sa strankama koje prenose podatke iz EU-a, u temeljne odredbe o privatnosti, kada ostale odredbe za takve ogledne sporazume odobre Komisija i države članice.

Pravo SAD-a će se primjenjivati u pitanjima tumačenja i usklađenosti s načelima „sigurna luka" (uključujući često postavljana pitanja) i relevantne politike privatnosti organizacija „sigurna luka", osim ako se organizacije nisu obvezale na suradnju s europskim tijelima za zaštitu podataka. Osim ako nije drukčije navedeno, sve odredbe načela „sigurna luka" i često postavljana pitanja primjenjuju se tamo gdje su relevantni.

„Osobni podaci" i „osobne informacije" su podaci o identificiranom pojedincu ili pojedincu kojeg se može identificirati, koji su obuhvaćeni područjem primjene Direktive, a koje je iz Europske unije primila organizacija u SAD-u i pohranila ih u bilo kojem obliku.

OBAVIJEST

Organizacija mora obavijestiti pojedince o namjeni prikupljanja i uporabi njihovih osobnih podataka, kako mogu kontaktirati organizaciju radi upita ili pritužbi, o kategorijama trećih strana kojima otkriva te podatke te mogućnostima i sredstvima koje organizacija nudi pojedincima za ograničivanje njihove uporabe i otkrivanja. Ova obavijest mora biti sastavljena jasnim i razumljivim jezikom kada se od pojedinaca prvi put zatraži da daju osobne podatke organizaciji ili čim prije nakon toga, ali u svakom slučaju prije nego organizacija koristi takve informacije u neku drugu svrhu osim one za koju ih je prvotno prikupila ili obradila organizacija koja je izvršila prijenos ili prije nego što ih po prvi put otkrije trećoj osobi ([1]).

MOGUĆNOST IZBORA

Organizacija mora pojedincima ponuditi mogućnost da odaberu (odustanu) hoće li se njihovi osobni podaci moći (a) otkriti trećoj osobi ([1]) ili (b) koristiti u svrhu koja nije sukladna sa svrhom(svrhama) za koju su izvorno prikupljeni ili za koju je pojedinac naknadno dao odobrenje. Pojedincima moraju biti ponuđeni jasni i očigledni, već dostupni i prihvatljivi mehanizmi odabira.

Kod osjetljivih informacija (tj. osobnih podataka o medicinskom ili zdravstvenom stanju, rasi ili etničkom podrijetlu, političkim stavovima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili podataka o spolnom životu pojedinca), mora im biti ponuđena potvrdna ili izričita mogućnost odabira (pristanak) ako će se te informacije otkriti trećoj osobi ili koristiti u neku drugu svrhu osim one za koju su prvotno prikupljene ili za koju je pojedinac naknadno dao odobrenje koristeći mogućnost odabira. U svakom slučaju, organizacija treba smatrati osjetljivima one informacije koje je primila od treće osobe kada ih treća osoba smatra osjetljivima i odnosi se prema njima kao takvima.

DALJNJI PRIJENOS

Pri otkrivanju podataka trećoj osobi, organizacije moraju primjenjivati načela obavijesti i mogućnosti izbora. Ako organizacija želi prenijeti podatke trećoj osobi koja ima ulogu posrednika, kao što je opisano u bilješci, može to učiniti ako se prvo uvjeri da se treća osoba obvezala na načela ili podliježe direktivi ili nekoj drugoj potvrdi o primjerenosti, ili ako sklopi pisani sporazum s tom trećom osobom u kojem se zahtjeva da treća osoba pruži barem istu razinu zaštite privatnosti koju traže relevantna načela. Ako organizacija ispunjava ove zahtjeve, nije odgovorna (osim ako se organizacija suglasi drukčije) ako treća osoba kojoj otkrije takve podatke obrađuje iste na način suprotan ograničenjima ili izjavama, osim ako je organizacija znala ili trebala znati da će ih treća osoba obrađivati na takav način, a nije poduzela odgovarajuće korake da spriječi ili prekine takvu obradu.

([1]) Nije potrebno dati obavijest ili ponuditi mogućnost odabira kad se podaci otkrivaju trećoj osobi koja kao posrednik izvršava posao (poslove) u ime i prema uputama organizacije. Međutim, načelo daljnjeg prijenosa primjenjuje se na takvo otkrivanje podataka.

SIGURNOST

Organizacije koje stvaraju, održavaju, koriste ili prenose osobne podatke moraju poduzeti odgovarajuće mjere da bi ih zaštitile od gubitka, zlouporabe i neovlaštenog pristupa, otkrivanja, izmjene i uništenja.

NEPOVREDIVOST PODATAKA

U skladu s načelima, osobni podaci moraju biti važni za namjenu za koju će se koristiti. Organizacija ne može obrađivati osobne podatke na način koji nije sukladan namjenama za koje su prikupljeni ili za koje je pojedinac naknadno dao odobrenje. U onoj mjeri koja je potrebna za tu namjenu, organizacija treba poduzeti odgovarajuće korake da podaci budu pouzdani za namjeravano korištenje, točni, potpuni i ažurirani.

PRISTUP

Pojedinci moraju imati pristup osobnim podacima koje organizacija čuva, te ih moći ispraviti, promijeniti ili obrisati ako su netočni, osim ako teret ili trošak omogućavanja pristupa ne bi bio u skladu s ugroženošću privatnosti pojedinca u danom slučaju, ili ako bi se time kršila prava drugih osoba.

PROVEDBA

Učinkovita zaštita privatnosti mora uključivati mehanizme kojima se osigurava poštovanje načela, pravna zaštita pojedinaca na koje se odnose podaci na koje nepridržavanja načela utječe, te posljedice za organizaciju kad ne poštuje načela. Takvi mehanizmi moraju uključivati najmanje (a) lako dostupne i prihvatljive neovisne mehanizme pravne zaštite prema kojima se svaka pritužba pojedinca i spor istražuje i rješava pozivajući se na načela kao i naknade štete ako je tako predviđeno mjerodavnim zakonom ili inicijativama privatnog sektora; (b) postupke praćenja kojima se provjerava jesu li potvrde i navodi koje poduzeća daju o svojim praksama u pogledu privatnosti istinite i jesu li postupanja prema privatnosti provedena kao što je navedeno; i (c) obveze da se riješe problemi koji proizlaze iz nepoštovanja načela od strane organizacija koje objavljuju da ih se pridržavaju i posljedice za takve organizacije. Sankcije moraju biti dovoljno stroge da bi ih se organizacije pridržavale.

Prilog

Popis državnih tijela SAD-a koje priznaje Europska unija

Europska unija priznaje sljedeća vladina tijela SAD-a kao ovlaštena da istražuju pritužbe i ponude pravnu zaštitu od nepoštenih ili prijevarnih praksi, kao i naknadu za pojedince u slučaju nepoštovanja načela koja se provode u skladu s često postavljanim pitanjima:

— Federal Trade Commission, na temelju svog ovlaštenja sukladno s odjeljkom 5. Federal Trade Commission Act-a,

— Department of Transportation, na temelju svog ovlaštenja sukladno s glavom 49. odjeljka 41712 United States Code.

PRILOG II.

ČESTO POSTAVLJANA PITANJA

ČESTO POSTAVLJANO PITANJE 1 - Osjetljivi podaci

P: *Mora li organizacija uvijek ponuditi izričitu (pristanak) mogućnost izbora u pogledu osjetljivih podataka?*

O: Ne, takva mogućnost izbora nije potrebna ako je obrada: 1. od životnog interesa za osobu čiji se podaci obrađuju ili neku drugu osobu; 2. potrebna za ostvarivanje zakonskih prava ili obrane; 3. potrebna da bi se pružila medicinska skrb ili dijagnoza; 4. se vrši tijekom zakonitih aktivnosti zaklade, udruge ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem i uz uvjet da se obrada odnosi isključivo na članove tog tijela ili osobe koje imaju redovne kontakte s istom u te svrhe, te da podaci ne otkriju trećoj osobi bez privole osoba čiji se podaci obrađuju; 5. potrebna da organizacija izvrši svoje obveze u području radnog prava; ili 6. vezana za podatke koje je očigledno objavio pojedinac.

ČESTO POSTAVLJANO PITANJE 2 - Novinarske iznimke

P: *Obzirom na ustavne zaštite slobode tiska u SAD-u i izuzeće iz Direktive koje se odnosi na novinarske materijale, primjenjuju li se načela zaštite privatnosti na osobne podatke prikupljene, čuvane ili objavljene u novinarske svrhe?*

O: Ako se prava na slobodu tiska uvrštena u prvi amandman Ustava SAD-a kose s interesima zaštite privatnosti, prvi amandman mora uravnotežiti te interese s obzirom na aktivnosti državljana ili organizacija iz SAD-a. Osobni podaci koji se prikupljaju radi objavljivanja, emitiranja ili ostalih oblika javne objave novinarskih materijala, bez obzira koriste li se ili ne, kao i informacije pronađene u prethodno objavljenom materijalu iz medijskih arhiva, ne podliježu zahtjevima načela „sigurne luke".

ČESTO POSTAVLJANO PITANJE 3 - Sekundarna odgovornost

P: *Jesu li pružatelji internetskih usluga (ISP), telekomunikacijski operateri ili ostale organizacije odgovorni prema načelima „sigurne luke" kada u ime neke druge organizacije samo prenose, usmjeravaju, prespajaju ili privremeno pohranjuju informacije koje mogu kršiti njihove uvjete?*

O: Ne. Kao što je slučaj sa samom Direktivom, „sigurna luka" ne stvara sekundarnu odgovornost. U onoj mjeri u kojoj organizacija djeluje samo kao posrednik podataka koje prenose treće osobe i ne određuje svrhu i sredstva obrade tih osobnih podataka, ona nije odgovorna.

ČESTO POSTAVLJANO PITANJE 4 - Investicijske banke i revizori

P: *Djelatnosti revizora i investicijskih banaka mogu uključivati obradu osobnih podataka bez pristanka ili znanja pojedinca. Pod kojim okolnostima je ovo dopušteno prema načelima obavijesti, mogućnosti izbora i pristupa?*

O: Investicijski bankari ili revizori mogu obrađivati informacije bez znanja pojedinca samo u onoj mjeri i u onom razdoblju koje je potrebno da se zadovolje zahtjevi zakonskog ili javnog interesa i u ostalim okolnostima u kojima bi primjena ovih načela naškodila zakonitim interesima organizacije. Ti zakoniti interesi uključuju nadziranje ispunjava li trgovačko društvo svoje zakonske obveze i zakonite računovodstvene djelatnosti, te potrebu za tajnošću podatka vezanih za moguća preuzimanja, udruživanja, zajedničke pothvate ili ostale slične transakcije investicijskih bankara ili revizora.

ČESTO POSTAVLJANO PITANJE 5 - Uloga tijela nadležnih za zaštitu podataka [1]

P: *Kako će trgovačka društva koja su se obvezala na suradnju s tijelima Europske unije nadležnima za zaštitu podataka ispuniti te obveze i kako će one biti provedene?*

O: Prema „sigurnoj luci", organizacije iz SAD-a koje primaju osobne podatke iz EU-a moraju se obvezati na primjenu učinkovitih mehanizama za poštovanje načela „sigurne luke". Kao što je konkretnije navedeno u načelu provedbe, one moraju osigurati (a) pravnu zaštitu za pojedince na koje se podaci odnose, (b) postupke praćenja kojima se provjerava jesu li potvrde i navodi koje su dali o svojim postupanjima prema privatnosti istinite i (c) obveze da se riješe problemi koji proizlaze iz nepoštovanja načela i posljedice za takve organizacije. Organizacija može zadovoljiti točke (a) i (c) načela provedbe, ako zadovoljava zahtjeve ovog pitanja za suradnju s tijelima nadležnima za zaštitu podataka.

Organizacija se može obvezati na suradnju s tijelima za zaštitu podataka izjavljujući u svojoj potvrdi o „sigurnoj luci"za Ministarstvo trgovine SAD-a (vidjeti često postavljano pitanje 6. o vlastitom potvrđivanju) da:

1. svojevoljno pristaje udovoljiti zahtjevima iz točaka (a) i (c) načela provedbe „sigurne luke", obvezujući se na suradnju s tijelima za zaštitu podataka;

2. surađivat će s tijelima za zaštitu podataka pri istraživanju i rješavanju pritužbi podnesenih u skladu s načelima „sigurne luke"; i

3. postupit će u skladu s bilo kojim savjetom tijela za zaštitu podataka i ako ta tijela smatraju da organizacija treba izvršiti određenu radnju da bi poštovala načela „sigurne luke", uključujući mjere za zaštitu prava ili naknadu u korist pojedinaca pogođenih nepoštovanjem načela, te da će dati pisanu potvrdu tijelima za zaštitu podataka da je takva radnja poduzeta.

Suradnja tijela za zaštitu podataka očitovat će se u obliku informacija i savjeta na sljedeći način:

— savjet tijela za zaštitu podataka bit će dostavljen putem neslužbenog odbora tijela za zaštitu podataka organiziranog na razini Europske unije, koji će *inter alia* pomoći da se osigura usklađen i dosljedan pristup,

— odbor će ponuditi savjet dotičnim organizacijama iz SAD-a o neriješenim pritužbama pojedinaca na postupanje s osobnim podacima koji su prenijeti iz EU-a sukladno sa zaštitom privatnosti. Namjena ovog savjeta je osiguravanje ispravne primjene načela „sigurne luke" i uključivat će sva pravna sredstva za dotičnog pojedinca(e) koje tijela za zaštitu podataka smatraju prikladnima,

— odbor će ponuditi takav savjet kao odgovor na smjernice uključenih organizacija i/ili pritužbe primljene izravno od pojedinaca protiv organizacija koje su se obvezale surađivati s tijelima za zaštitu podataka u svrhe „sigurne luke", istodobno potičući i prema potrebi pomažući takvim pojedincima da prvo iskoriste interne načine rješavanja pritužbi koje organizacija može ponuditi,

— savjet će biti objavljen tek nakon što su obje stranke u sporu imale razumnu mogućnost dati primjedbe i dostaviti dokaze koje žele. Odbor će pokušati dati savjet onom brzinom koju omogućuje propisani postupak. U pravilu, odbor će nastojati dati savjet u roku od 60 dana od primitka pritužbe ili upute, a ako je moguće i brže,

— odbor će objaviti rezultate svog razmatranja podnijete mu pritužbe, ako to smatra prikladnim,

— davanje savjeta putem odbora ne uključuje bilo kakvu odgovornost za odbor ili pojedino tijelo za zaštitu podataka.

[1] Uvrštenje ovog često postavljenog pitanja u paket ovisi o sporazumu tijelâ za zaštitu podataka. Radna skupina iz članka 29. razgovarala je o sadašnjem tekstu i većina ga smatra prihvatljivim, ali spremni su zauzeti konačno stajalište u kontekstu općenitog mišljenja koje će radna skupina objaviti o konačnom paketu.

Kao što je gore navedeno, organizacije koje se odluče za ovu mogućnost rješavanja sukoba moraju se obvezati da će poslušati savjet tijela za zaštitu podataka. Ako ga organizacija ne provede u roku od 25 dana od primitka savjeta i ne ponudi prihvatljivo objašnjenje za kašnjenje, odbor će poslati obavijest o svojoj namjeri da preda predmet Federal Trade Commission-u ili drugom saveznom ili državnom tijelu SAD-a sa zakonskim ovlastima da poduzme provedbene radnje u slučajevima prijevare ili lažnog prikazivanja, ili da zaključi da je sporazum o suradnji ozbiljno prekršen te se stoga mora smatrati ništavim. U potonjem slučaju odbor će obavijestiti Department of Commerce (ili njegova ovlaštenog predstavnika) tako da se popis sudionika u „sigurnoj luci" može promijeniti u skladu s tim. Svako neispunjenje obveze o suradnji s tijelima za zaštitu podataka, kao i nepoštovanje načela „sigurne luke", bit će kažnjivo kao prijevarno postupanje sukladno s odjeljkom 5. Federal Trade Commission Act-a ili nekom drugom sličnom propisu.

Organizacije koje odaberu ovu mogućnost morat će platiti godišnju naknadu koja će biti namijenjena za pokrivanje operativnih troškova odbora, od njih se može dodatno zatražiti da podmire potrebne troškove prevođenja koji proizlaze iz razmatranja članova odbora uputa ili pritužbi protiv njih. Godišnja naknada neće premašivati 500 USD i iznosit će manje za manja trgovačka društva.

Mogućnost suradnje s tijelima za zaštitu podataka stajat će na raspolaganju organizacijama koje prihvate načela„sigurne luke" tijekom razdoblja od tri godine. Tijela za zaštitu podataka razmotrit će ovaj dogovor prije isteka navedenog roka ako broj organizacija iz SAD-a koje odaberu ovu opciju postane prevelik.

ČESTO POSTAVLJANO PITANJE 6 – Vlastito potvrđivanje

P: *Kako organizacija sama potvrđuje da se pridržava načela „sigurne luke"?*

O: Prednosti „sigurne luke" osigurane su od datuma kada organizacija sama potvrdi Department of Commerc-u (ili njegovu ovlaštenom predstavniku) svoje pridržavanje načela u skladu s dolje navedenom smjernicom.

Da bi same potvrdile pridržavanje načela„sigurne luke", organizacije mogu poslati u Department of Commerce (ili njegovu ovlaštenom predstavniku) pismo koje je potpisao rukovoditelj u ime organizacije koja prihvaća načela „sigurne luke", a koje mora sadržavati najmanje sljedeće informacije:

1. naziv organizacije, adresu, internetsku adresu, broj telefona i telefaksa;

2. opis aktivnosti organizacije s obzirom na osobne podatke primljene iz EU-a; i

3. opis politike organizacije u pogledu zaštite privatnosti takvih osobnih podataka, uključujući: (a) gdje javnost može pregledati tu politiku zaštite privatnosti; (b) datum od kojega se provodi; (c) kontaktni ured za rješavanje pritužbi, zahtjeva za pristup i sva ostala pitanja koja proizlaze iz načela „sigurne luke"; (d) određeno državno tijelo koje je nadležno rješavati pritužbe protiv organizacije u pogledu mogućih nepoštenih ili prijevarnih praksi i kršenja zakona ili propisa koji uređuju privatnost (navedeno u prilogu načelima); (e) naziv programa za zaštitu privatnosti u kojima organizacija sudjeluje kao član; (f) metodu provjere (npr. unutar organizacije, treća osoba) [2]; i (g) neovisni mehanizam pravne zaštite koji je dostupan za istraživanje neriješenih pritužbi.

Ako organizacija želi da njezine pogodnosti„sigurne luke" obuhvaćaju informacije o ljudskim potencijalima prenijete iz EU-a za korištenje u kontekstu radnog odnosa, može to učiniti ako postoji državno tijelo s nadležnošću da rješava pritužbe protiv organizacije koje proizlaze iz informacija o ljudskim potencijalima, a koje je navedeno u Prilogu načelima. Osim toga, organizacija to mora navesti u svom dopisu i izjasniti se o svojoj obvezi suradnje s dotičnim tijelom ili tijelima EU-a u skladu s često postavljanim pitanjima 9 i 5 ako se primjenjuju, te da će uvažiti savjet koje mu daju takva tijela.

Department (ili njegov ovlašteni predstavnik) će voditi popis svih organizacija koje pošalju takva pisma, osiguravajući time pogodnosti „sigurne luke" i ažurirat će takav popis na temelju pisama i obavijesti koje godišnje primi sukladno s često postavljanim pitanjem 11. Takva pisma s vlastitom potvrdom treba dostaviti najmanje jednom godišnje. U suprotnom će organizacija biti uklonjena s popisa i neće više imati pogodnosti „sigurne luke". I popis i pisma s

[2] Vidjeti često postavljano pitanje 7 o provjeri.

vlastitom potvrdom koje dostave organizacije bit će javno dostupne. Sve organizacije koje daju vlastitu potvrdu za u vezi sa„sigurnom lukom" moraju također navesti u svojim relevantnim objavljenim izjavama o politici privatnosti da poštuju načela „sigurne luke".

Preuzeta obveza poštovanja načela „sigurne luke" nije vremenski ograničena s obzirom na podatke koje primi tijekom razdoblja u kojem organizacija koristi pogodnosti „sigurne luke". Njezina obveza znači da će nastaviti primjenjivati načela na takve podatke sve dok ih organizacija pohranjuje, koristi ili otkriva, čak i ako kasnije od njih odustane iz bilo kojeg razloga.

Organizacija koja prestane postojati kao zasebna pravna osoba zbog spajanja ili preuzimanja, mora unaprijed obavijestiti Department of Commerce (ili njegova ovlaštenog predstavnika) o tome. U obavijesti treba također navesti hoće li društvo koje je steklo organizaciju ili ono koje je rezultat udruživanja: 1. nastaviti biti vezano načelima „sigurne luke" na temelju zakona koji regulira preuzimanje ili spajanje; ili 2. se odlučiti da samo potvrdi svoje pridržavanje načela „sigurne luke" ili primijeni drugu zaštitu, kao što je pisani sporazum koji će osigurati pridržavanje načela „sigurne luke". Ako se ne primjenjuju ni 1. ni 2., svi podaci koji su prikupljeni sukladno „sigurnoj luci" moraju se odmah obrisati.

Organizacija ne mora podvrgnuti sve osobne podatke načelima „sigurne luke", ali mora podvrgnuti načelima „sigurne luke" sve osobne podatke koje prima iz EU-a nakon što prihvati načela „sigurne luke.

Zbog bilo kojeg krivog prikazivanja neke organizacije s obzirom na pridržavanja načela „sigurne luke" u javnosti, Federal Trade Commission ili drugo nadležno vladino tijelo može pokrenuti postupak. Zbog krivog prikazivanja Department of Commerc-a SAD-a (ili njegovom ovlaštenom predstavniku) može se pokrenuti postupak prema False Statements Act-u (18 U.S.C. § 1001).

ČESTO POSTAVLJANO PITANJE 7 - Provjera

P: *Kako organizacije provode postupke praćenja za provjeru istinitosti potvrda i navoda koje su dale o svojim praksama u provođenju načela „sigurne luke" i jesu li te prakse vezane za privatnost provedene kao što je prikazano i u skladu s načelima „sigurne luke"?*

O: Da zadovolji zahtjeve provjere načela provedbe, organizacija može provjeriti takve potvrde i navode samoprocjenom ili vanjskim preispitivanjima njihova poštovanja.

Prema pristupu samoocjene, takva bi provjera trebala pokazati da je objavljena politika zaštite privatnosti neke organizacije u pogledu osobnih podataka primljenih iz EU-a točna, sveobuhvatna, jasno prikazana, u potpunosti provedena i dostupna. Također bi trebala pokazati da je njezina politika zaštite privatnosti usklađena s načelima „sigurne luke"; da su pojedinci obaviješteni o unutarnjim mehanizmima za rješavanje pritužbi i o neovisnim mehanizmima putem kojih mogu podnositi pritužbe; da ima uvedene postupke za obuku zaposlenika o njezinoj primjeni i kažnjavanje za njezino neprovođenje; te da ima uvedene unutarnje postupke za periodično provođenje objektivnih provjera poštuje li se gore navedeno. Izjavu koja potvrđuje samoocjenu treba potpisati rukovoditelj poduzeća ili neki drugi ovlašteni predstavnik organizacije barem jednom godišnje i staviti je na raspolaganje pojedincima na njihov zahtjev ili u kontekstu istrage ili pritužbe o nepoštovanju.

Organizacije trebaju čuvati svoje evidencije o provedbi svoje prakse „sigurne luke" i na zahtjev ih učiniti dostupnima u kontekstu istrage ili pritužbe o nepoštovanju neovisnom tijelu odgovornom za istraživanje pritužbi ili agenciji s nadležnošću za nepoštena i prijevarna postupanja.

Ako organizacija odabere vanjsku provjeru poštovanja, takva provjera treba pokazati da je njezina politika zaštite privatnosti s obzirom na osobne podatke primljene iz EU-a usklađena s načelima „sigurne luke", da se poštuje i da su pojedinci obaviješteni o mehanizmima putem kojih mogu podnositi pritužbe. Metode provjere mogu bez ograničenja uključivati reviziju, slučajno odabrane provjere, korištenje „mamaca" ili korištenje tehnoloških sredstava

kada je moguće. Izjavu kojom se potvrđuje da je vanjska provjera poštovanja uspješno završena treba potpisati voditelj provjere, ili rukovoditelj poduzeća ili neki drugi ovlašteni predstavnik organizacije najmanje jednom godišnje i staviti je na raspolaganje pojedincima na njihov zahtjev, ili u kontekstu istrage ili pritužbe na poštovanje.

ČESTO POSTAVLJANO PITANJE 8 - Pristup

Načelo pristupa:

Pojedinci moraju imati pristup osobnim podacima koje organizacija čuva, te ih moći ispraviti, izmijeniti ili obrisati te informacije ako su netočne, osim ako teret ili trošak omogućivanja pristupa ne bi bio razmjeran ugroženosti privatnosti pojedinca u danom slučaju, ili ako bi se time kršila prava drugih pojedinaca.

1. P: *Je li pravo pristupa apsolutno?*

1. O: Ne. Prema načelima „sigurne luke", pravo pristupa je neophodno za zaštitu privatnosti. Ono osobito omogućuje pojedincima da provjere točnost informacija koje se čuvaju o njima. Međutim, obveza organizacije da omogući pristup osobnim podacima koje čuva o pojedincu podliježe načelu razmjernosti ili razboritosti i mora se ublažiti u određenim slučajevima. Već se u obrazloženju uz Smjernice OECD-a o privatnosti iz 1980. jasno navodi da obveza organizacije da omogući pristup nije apsolutna. Ne zahtijeva izrazito temeljito pretraživanje koje nalaže, na primjer, sudski nalog, niti pristup svim različitim oblicima u kojima organizacija može čuvati informacije.

Naprotiv, iskustvo je pokazalo da se pri odgovoru na zahtjeve pojedinaca za pristup, organizacije trebaju prvenstveno voditi motivom (motivima) koji su uopće doveli do takvih zahtjeva. Na primjer, ako je zahtjev za pristup nejasan ili preširok, organizacija može razgovarati s pojedincem kako bi bolje shvatila motive za zahtjev i dala povratnu informaciju. Organizacija se može raspitati s kojim je dijelom (dijelovima) organizacije pojedinac kontaktirao i/ili o vrsti informacija (ili njihovom korištenju) za koje se zahtjeva pristup. Pojedinci, međutim, ne moraju obrazlagati zahtjeve za pristup vlastitim podacima.

Trošak i teret su bitni faktori i trebaju se uzeti u obzir, ali oni nisu presudni u odlučivanju je li omogućivanje pristupa opravdano. Na primjer, ako se informacije koriste za odluke koje će značajno utjecati na pojedinca (npr. uskraćenje ili odobrenje bitnih pogodnosti, kao što je osiguranje, hipoteka ili posao), tada bi u skladu s ostalim odredbama ovih često postavljanih pitanja, organizacija morala otkriti informacije čak i ako je to relativno teško ili skupo izvesti.

Ako tražena informacija nije osjetljiva ili se ne koristi za odluke koje će značajno utjecati na pojedinca (npr. tržišni podaci koji nisu osjetljivi a koji se koriste za odlučivanje hoće li ili neće pojedincu poslati katalog), ali je lako dostupna i nije je skupo dati, organizacija bi trebala omogućiti pristup činjeničnim podacima o pojedincu koje organizacija ima pohranjene. Takva informacija može uključivati činjenice dobivene od pojedinca, činjenice prikupljene tijekom transakcije ili činjenice dobivene od ostalih, a koje se odnose na pojedinca.

U skladu s osnovnom prirodom pristupa, organizacije uvijek trebaju poduzeti napore u dobroj vjeri da omoguće pristup. Na primjer, ako određenu informaciju treba zaštititi, a moguće ju je lako izdvojiti od ostalih informacija za koje se traži pristup, organizacija treba redigirati zaštićenu informaciju i učiniti dostupnima ostale informacije. Ako organizacija odluči da treba uskratiti pristup u nekom određenom slučaju, treba objasniti podnositelju zahtjeva za pristup zašto je donijela takvu odluku i uputiti ga na kontaktno mjesto za sve daljnje upite.

2. P: *Što je povjerljiva poslovna informacija i mogu li organizacije uskratiti pristup kako bi je zaštitile?*

2. O: Povjerljiva poslovna informacija (u onom smislu kako se pojam koristi u Federal Rules of Civil Procedure o otkrivanju) je informacija u vezi koje je organizacija poduzela korake zaštite od otkrivanja, ako bi otkrivanje pomoglo konkurentu na tržištu. Određeni računalni program koji organizacija koristi, kao što je program za modeliranje ili pojedinosti tog programa mogu predstavljati povjerljivu poslovnu informaciju. Ako se povjerljivu poslovnu informaciju može lako izdvojiti od ostalih informacija za koje se traži pristup, organizacija treba redigirati povjerljivu poslovnu informaciju i učiniti dostupnima nepovjerljive informacije. Organizacije mogu

uskratiti ili ograničiti pristup u onoj mjeri u kojoj bi njegovo omogućivanje razotkrilo vlastitu povjerljivu poslovnu informaciju koje je ranije definirana, kao što su zaključci vezani za tržište ili razvrstavanje koje je napravila organizacija ili povjerljiva poslovna informacija treće osobe ako takva informacija podliježe ugovornoj obvezi o povjerljivosti u okolnostima kada bi takva obveza povjerljivosti bila uobičajeno prihvaćena ili nametnuta.

3. P: *Može li organizacija pri omogućavanju pristupa otkriti pojedincima osobne podatke o njima iz vlastite baze podataka ili je potreban pristup samoj bazi podataka?*

3. O: Pristup se može omogućiti u obliku otkrivanja podataka organizacije pojedincu i ne zahtijeva pristup pojedinca bazi podataka organizacije.

4. P: *Mora li organizacija restrukturirati svoje baze podataka da može omogućiti pristup?*

4. O: Pristup treba omogućiti samo u onoj mjeri u kojoj organizacija ima pohranjene informacije. Načelo pristupa samo po sebi ne znači obvezu da se zadrže, održavaju, reorganiziraju ili restrukturiraju datoteke s osobnim podacima.

5. P: *Iz ovih je odgovora jasno da se pristup može uskratiti u određenim okolnostima. U kojim još okolnostima organizacija može uskratiti pojedincima pristup njihovim osobnim podacima?*

5. O: Takve okolnosti su ograničene i svaki razlog za uskraćivanje pristupa mora biti utemeljen. Organizacija može odbiti omogućavanje pristupa informaciji u onoj mjeri u kojoj bi se otkrivanje moglo kositi sa zaštitom bitnih prevladavajućih javnih interesa, kao što su nacionalna sigurnost, obrana ili javna sigurnost. Osim toga, ako se osobni podaci obrađuju isključivo u istraživačke ili statističke svrhe, pristup se može uskratiti. Ostali razlozi za uskraćivanje ili ograničivanje pristupa su:

(a) ometanje izvršenja ili provedbe zakona, uključujući sprečavanje, istraživanje ili otkrivanje kažnjivih djela ili prava na pravično suđenje;

(b) ometanje osnove za privatnu tužbu, uključujući sprečavanje, istraživanje ili otkrivanje pravnih osnova ili prava na pravično suđenje;

(c) otkrivanje osobnih podataka koji se odnose na drugog pojedinca (druge pojedince) ako se takvi navodi ne mogu redigirati;

(d) kršenje obveze čuvanja pravnih ili profesionalnih tajni ili obveza;

(e) kršenje nužne tajnosti budućih ili tekućih pregovora, kao što je ono koje uključuje preuzimanje trgovačkih društava uvrštenih na burzu;

(f) ugrožavanje istraga o sigurnosti zaposlenika ili žalbenih postupaka;

(g) narušavanje tajnosti koja može biti potrebna u određenom razdoblju vezano za planiranje zamjene zaposlenika i korporativnu reorganizaciju; ili

(h) narušavanje tajnosti koja može biti potrebna radi praćenja, nadzora ili regulatorne funkcije povezane sa dobrim ekonomskim ili financijskim upravljanjem, ili

(i) ostale okolnosti u kojima bi teret ili trošak omogućavanja pristupa bio nerazmjeran ili bi se prekršila zakonska prava ili interesi ostalih.

Organizacija koja zatraži iznimku snosi teret dokaza njezine opravdanosti (kao što je uobičajeno). Kako je već ranije spomenuto, pojedincima treba objasniti razloge uskraćivanja ili ograničivanja pristupa i uputiti ih na kontaktno mjesto za daljnje upite.

6. P: *Može li organizacija naplatiti naknadu da pokrije trošak omogućavanja pristupa?*

6. O: Da. Smjernice OECD-a dozvoljavaju organizacijama da naplate naknadu, uz uvjet da ne bude visoka. Tako organizacije mogu naplatiti razumnu naknadu za pristup. Naplata naknade može biti korisna za destimuliranje učestalih i neugodnih zahtjeva.

Organizacije koje se bave prodajom javno dostupnih informacija mogu tako naplatiti uobičajenu naknadu organizacije pri ispunjavanju zahtjeva za pristup. Pojedinci mogu, kao alternativu, tražiti pristup svojim informacijama od organizacije koja je prvotno prikupila podatke.

Pristup se ne može uskratiti radi troška ako pojedinac ponudi da će platiti troškove.

7. P: *Je li organizacija obvezna omogućiti pristup osobnim podacima koji su preuzeti iz državnih evidencija?*

7. O: Prvo da razjasnimo da su javne evidencije one koje čuvaju vladine agencije ili tijela na bilo kojoj razini, koje su općenito otvorene javnosti na uvid. Nije potrebno primjenjivati načelo pristupa na takve informacije ako nisu povezane s ostalim osobnim podacima, osim kada su male količine informacija iz nejavnih evidencija korištene za indeksaciju ili organizaciju informacija u javnim evidencijama. Međutim, moraju se poštovati svi uvjeti za uvid koje je utvrdilo nadležno tijelo. Ako je pak informacija iz javne evidencije povezana s ostalim informacijama iz nejavne evidencije (osim kao što je gore točno navedeno), organizacija mora omogućiti pristup svim takvim informacijama, ako za njih ne vrijede ostale dopuštene iznimke.

8. P: *Primjenjuje li se načelo pristupa na javno dostupne osobne podatke?*

8. O: Kao što je slučaj s informacijama iz javne evidencije (vidjeti P. 7), nije potrebno omogućiti pristup informacijama koje su već javno dostupne široj javnosti, osim ako nisu povezane s informacijama koje nisu javno dostupne.

9. P: *Kako se organizacija može zaštiti protiv učestalih ili neugodnih zahtjeva za pristup?*

9. O: Organizacija ne mora odgovoriti na takve zahtjeve za pristup. Iz tih razloga organizacije mogu naplatiti razumnu naknadu i mogu postaviti opravdana ograničenja s obzirom na to koliko će se puta u određenom razdoblju ispuniti zahtjev određenog pojedinca za pristup. Pri postavljanju takvih ograničenja organizacija treba uzeti u obzir faktore kao što su učestalost ažuriranja informacija, svrhu za koju su podaci korišteni i prirodu informacija.

10. P: *Kako se organizacija može zaštiti od lažnih zahtjeva za pristup?*

10. O: Organizacija ne mora omogućiti pristup ako joj se ne da dovoljno informacija koje joj omogućavaju da provjeri identitet osobe koja podnosi zahtjev.

11. P: *Postoji li rok u kojem se mora odgovoriti na zahtjeve za pristup?*

11. O: Da, organizacije trebaju odgovoriti bez pretjeranog kašnjenja i u razumnom roku. Ovaj je zahtjev moguće ispuniti na različite načine, kako se navodi u obrazloženju uz Smjernice OECD-a o privatnosti iz 1980. Na primjer, nadzornik koji redovito daje informacije osobama čiji se podaci objavljuju može biti izuzet od obveze da odmah odgovori na zahtjeve pojedinca.

ČESTO POSTAVLJANA PITANJA 9 - Ljudski resursi

1. P: *Primjenjuju li se načela „sigurne luke" na prijenos osobnih podataka prikupljanih u kontekstu radnog odnosa iz EU-a u Sjedinjene Američke Države?*

1. O: Da, ako neko trgovačko društvo iz EU-a prenosi osobne podatke o svojim zaposlenicima (bivšim ili sadašnjim) prikupljene u kontekstu radnog odnosa, matičnom, povezanom ili nepovezanom pružatelju usluga u Sjedinjenim Američkim Državama koji sudjeluje u „sigurnoj luci", prijenos uživa pogodnosti „sigurne luke". U takvim

slučajevima prikupljanje podataka i njihova obrada prije prijenosa podliježu nacionalnom pravu države EU-a u kojoj su prikupljeni i moraju se poštovati svi uvjeti ili ograničenja za njihov prijenos prema tom pravu.

Načela „sigurne luke" bitna su samo kada se prenose datoteke koje se mogu pojedinačno identificirati ili se istima pristupa. Statističko izvješćivanje koje se temelji na skupnim podacima o zaposlenima i/ili korištenje anonimnih podataka ili onih pod pseudonimom ne otvara pitanja privatnosti.

2. P: *Kako se načela obavijesti i mogućnosti izbora primjenjuju na takve informacije?*

2. O: Organizacija iz SAD-a koja je primila informacije o zaposlenicima iz EU-a sukladno sa „sigurnom lukom" može ih otkriti trećih stranama i/ili koristiti u različite svrhe samo u skladu s načelima obavijesti i mogućnosti izbora. Na primjer, ako organizacija namjerava koristiti osobne podatke prikupljene tijekom radnog odnosa u svrhe koje nisu vezane uz radni odnos, kao što su komercijalne obavijesti, organizacija iz SAD-a mora ponuditi izbor pojedincima kojih se to tiče prije nego što tako učini, osim ako su oni već odobrili da se informacije koriste u takve svrhe. Štoviše, takve se mogućnosti izbora ne smiju koristiti da se ograniče mogućnosti zapošljavanja ili poduzmu kaznene mjere protiv takvih zaposlenika.

Treba napomenuti da određeni opće važeći uvjeti za prijenos iz nekih država članica mogu isključivati ostalo korištenje takvih informacija čak i nakon prijenosa izvan EU-a, i takve uvjete se mora poštovati.

Osim toga, poslodavci trebaju uložiti razumne napore da bi udovoljili zaposlenikovom izboru s obzirom na privatnost. To može, na primjer, uključivati ograničivanje pristupa podacima, anonimnost određenih podataka ili korištenje šifri ili pseudonima kad stvarna imena nisu potrebna za postojeću svrhu upravljanja.

U onoj mjeri i onom razdoblju koje je potrebno da se izbjegne ugrožavanje zakonitih interesa organizacije pri unapređivanju, imenovanjima ili ostalim sličnim odlukama o zaposlenju, organizacija ne mora nuditi obavijest i mogućnost izbora.

3. P: *Kako se primjenjuje načelo pristupa?*

3. O: Često postavljena pitanja o pristupu pružaju smjernice o razlozima zbog kojih je opravdano uskratiti ili ograničiti zahtjev za pristup u kontekstu ljudskih resursa. Naravno, poslodavci u Europskoj uniji moraju poštovati lokalne propise i osigurati da zaposlenici Europske unije imaju pristup takvim informacija kako nalaže pravo u njihovoj domovini, bez obzira na mjesto obrade i čuvanja podataka. Zaštita privatnosti zahtijeva da organizacija koja obrađuje takve podatke u Sjedinjenim Američkim Državama surađuje u omogućivanju takvog pristupa bilo izravno ili putem poslodavca iz EU-a.

4. P: *Kako će se tretirati provedba podataka o zaposlenicima koji podliježu načelima „sigurne luke"?*

4. O: Ako se informacije koriste samo u kontekstu radnog odnosa, temeljna odgovornost za podatke *vis-à-vis* zaposlenika ostaje na trgovačkom društvu u EU-u. Iz toga proizlazi da ako se europski zaposlenici žale na kršenje njihovih prava na zaštitu podataka i nisu zadovoljni s rezultatima internih postupaka provjere, pritužbi i žalbi (ili nekog žalbenog postupka koji se primjenjuje sukladno ugovoru sa sindikatom), treba ih uputiti državnom ili nacionalnom tijelu za zaštitu podataka ili tijelu za rad nadležnom za područje u kojem zaposlenik radi. Ovo također uključuje slučajeve kada se navodna zlouporaba njihovih osobnih podataka dogodila u Sjedinjenim Američkim Državama i za nju je odgovorna organizacija iz SAD-a koja je primila informacije od poslodavca, a ne poslodavac, te stoga uključuje navodno kršenje načela zaštite privatnosti, a ne nacionalnog zakonodavstva za provedbu Direktive. To će biti najučinkovitiji način da se riješe često preklapajuća prava i obveze koje nameće lokalno radno pravo i kolektivni ugovori te pravo o zaštiti podataka.

Organizacija iz SAD-a, sudionica u „sigurnoj luci", koja koristi podatke o ljudskim resursima EU-a prenijete iz Europske unije u kontekstu radnog odnosa i koja želi da takvi prijenosi budu u okviru sigurnosti mora se iz tog razloga obvezati na suradnju u istragama i poštovanje savjeta nadležnih tijela EU-a u takvim slučajevima. Tijela za zaštitu podataka koja su pristala surađivati na ovakav način obavijestit će Europsku komisiju i Department of

Commerce. Ako organizacija iz SAD koja sudjeluje u „sigurnoj luci" želi prenijeti podatke o ljudskim resursima iz države članice s čim se tijelo za zaštitu podataka nije složilo, primjenjuju se odredbe često postavljanog pitanja 5.

ČESTO POSTAVLJANO PITANJE 10 – ugovori iz članka 17.

P: *Kada se podaci iz EU-a prenose u Sjedinjene Američke Države samo radi obrade, je li potreban ugovor, bez obzira što onaj koji obavlja obradu sudjeluje u „sigurnoj luci"?*

O: Da. Nadzornici podataka iz Europske unije uvijek su obvezni sklopiti ugovor kada se prijenos izvršava radi same obrade, bez obzira hoće li se radnje obrade izvršiti u EU-u ili izvan nje. Svrha je ugovora zaštiti interese nadzornika podataka, tj. osobe ili tijela koji određuju svrhe i sredstva obrade i koji snose punu odgovornost za podatke prema dotičnom pojedincu (pojedincima). Stoga se u govoru definira obrada koja se treba izvršiti i sve mjere potrebne za očuvanje sigurnosti podataka.

Organizacija iz SAD koja sudjeluje u „sigurnoj luci" i prima osobne podatke iz EU-a samo radi obrade ne mora primijeniti načela na ove informacije budući da je nadzornik iz EU-a i dalje odgovoran za njih prema pojedincu, u skladu s odgovarajućim odredbama EU-a (koje mogu biti strože od jednakovrijednih načela „sigurne luke").

Budući da sudionici „sigurne luke" pružaju primjerenu zaštitu, za ugovore sa sudionicima u „sigurnoj luci" radi same obrade nije potrebno prethodno odobrenje (ili će takvo ovlaštenje automatski davati države članice), kao što bi bilo potrebno za ugovore s primateljima koji ne sudjeluju u „sigurnoj luci" ili ne pružaju adekvatnu zaštitu na drugi način.

ČESTO POSTAVLJANO PITANJE br. 11 – Rješavanje sporova i provedba

P: *Kako treba provoditi zahtjeve načela provedbe o rješavanju sporova i kako će se postupati prema konstantnom neuspjehu organizacije da se pridržava načela?*

O: Načelo provedbe navodi zahtjeve za provedbu „sigurne luke". Kako ispuniti zahtjeve iz točke (b) načela navedeno je u često postavljanom pitanju o provjeri (često postavljeno pitanje 7). Ovo često postavljano pitanje 11 raspravlja o točkama (a) i (c), koje obje traže neovisne mehanizme pravne zaštite. Ti mehanizmi mogu imati različite oblike, ali moraju ispunjavati zahtjeve načela provedbe. Organizacije mogu udovoljiti zahtjevima na sljedeće načine: 1. poštovanjem programa privatnosti koje je razvio privatni sektor koji imaju inkorporirana načela „sigurne luke" u svoja pravila i koji uključuju učinkovite mehanizme provedbe opisane u načelu provedbe; 2. poštovanjem zakonskih ili regulatornih nadzornih tijela koja predviđaju rješavanje pritužbi pojedinaca i sporova; ili 3. preuzimanjem obveze suradnje s tijelima nadležnima za zaštitu podataka smještenima u Europskoj uniji ili s njihovim ovlaštenim predstavnicima. Ovaj popis trebao bi biti ilustrativan, a ne ograničavajući. Privatni sektor može osmisliti druge mehanizme provedbe sve dok oni ispunjavaju zahtjeve načela provedbe i često postavljanih pitanja. Uzmite u obzir da su zahtjevi iz načela provedbe dodatak zahtjevima utvrđenima u stavku 3. uvoda u načela koji nalažu da samoregulatorni napori moraju biti provedivi prema članku 5. Fedral Trade Commission Act-a ili sličnog propisa.

Mehanizmi pravne zaštite

Potrošače treba poticati da podnose pritužbe koje mogu imati na određenu organizaciju prije nego što prijeđu na neovisne mehanizme pravne zaštite. Neovisnost mehanizma pravne zaštite činjenično je pitanje na koje se može odgovoriti na brojne načine, na primjer, transparentnom strukturom i financiranjem ili dokazima o poslovanju.

Kao što zahtijeva načelo provedbe, pravna zaštita koja je na raspolaganju pojedincima mora biti lako dostupna i prihvatljiva. Tijela koja se bave rješavanjem sporova trebaju razmotriti svaku pritužbu koju prime od pojedinaca osim ako je očigledno neutemeljena ili neozbiljna. To ne sprečava organizaciju koja upravlja mehanizmom pravne zaštite da donese zahtjeve o prihvatljivosti, ali takvi zahtjevi trebaju biti transparentni i opravdani (na primjer, da isključuju pritužbe koje nisu obuhvaćene područjem primjene programa ili koje treba razmotriti na drugom forumu) i ne smiju potkopavati obvezu razmatranja opravdanih pritužbi. Osim toga, mehanizmi odštete trebaju ponuditi pojedincima potpune i lako dostupne informacije o funkcioniranju postupka rješavanja sporova kada ulažu žalbu. Takve informacije trebaju obuhvatiti obavijest o odnosu mehanizma prema praksama u vezi s privatnosti, u skladu s načelima„sigurne luke", ([3]). Također trebaju surađivati u izradi alata kao što su standardni obrasci žalbi kako bi olakšali postupak rješavanja žalbi.

Pravni lijekovi i sankcije

Rezultat bilo kojeg pravnog lijeka koji nudi tijelo za rješavanje sporova treba biti takav da organizacija poništi ili ispravi učinke nepoštivanja, koliko god je to izvedivo i da ubuduće obrada organizacije bude u skladu s načelima i ako je primjereno, da se prestanu obrađivati osobni podaci pojedinca koji je podnio žalbu. Sankcije trebaju biti dovoljno stroge da osiguraju da organizacija poštuje načela. Niz sankcija različitih stupnjeva oštrine omogućavaju tijelima za rješavanje sporova da na odgovarajući način reagiraju na različite stupnjeve nepoštivanja. Sankcije trebaju uključivati i javno objavljivanje otkrivenih slučajeva nepoštivanja i zahtjev da se podaci obrišu u određenim okolnostima ([4]). Ostale sankcije mogu uključivati privremeno ukidanje i oduzimanje pečata, nadoknadu gubitaka pojedincima koje su pretrpjeli kao posljedicu nepoštivanja i sudske zabrane. Tijela privatnog sektora za rješavanje sporova i samoregulatorna tijela moraju obavijestiti vladina tijela odgovarajuće nadležnosti ili sudove o slučajevima nepoštivanja njihovih odluka od strane organizacija potpisnica načela sigurnosti, već prema tome što je primjerenije, te obavijestiti Department of Commerce (ili njegova ovlaštenog predstavnika).

Djelovanje Federal Trade Commission-a

Federal Trade Commission obvezao se prioritetno razmatrati proslijeđene obavijesti primljene od organizacija koje same reguliraju privatnost, kao što su BBBOnline i TRUSTe i od država članica EU-a o navodnom nepoštovanju načela „sigurne luke" kako bi utvrdila je li prekršen odjeljak 5. Federal Trade Commission Act-a koji zabranjuje nepošteno ili prijevarno djelovanje u trgovini. Ako Federal Trade Commission zaključi da je opravdano vjerovati da je prekršen odjeljak 5., može riješiti stvar traženjem upravnog naloga koji zabranjuje osporene radnje, ili ulaganjem tužbe saveznom okružnom sudu, koja ako bude uspješna, može dovesti do naloga saveznog suda s istim učinkom. Federal Trade Commission može ishoditi građansku sankciju za kršenja sudskog naloga o zabrani te može pokrenuti građansku parnicu ili kazneni postupak zbog nepoštivanja sudskog postupka na temelju kršenja naloga saveznog suda. Federal Trade Commission obavijestit će Department of Commerce o svakom takvom djelovanju koje je poduzelo. Department of Commerce potiče ostala vladina tijela da ga obavješćuju o konačnoj presudi o takvim proslijeđenim obavijestima ili ostalim odlukama kojima se utvrđuje poštuju li se načela „sigurne luke".

Trajno nepridržavanje.

Ako se organizacija konstantno ne pridržava načela, više nema pravo na pogodnosti „sigurne luke". Trajno nepridržavanje nastaje kada se organizacija koja se sama potvrdila Department of Commerc-u (ili njegovu ovlaštenom predstavniku) odbije pridržavati konačne odluke samoregulatornog ili vladinog tijela ili ako takva tijela utvrde da organizacija tako učestalo ne poštuje načela da njezina tvrdnja o pridržavanju više nije vjerodostojna. U tim slučajevima organizacija mora hitno obavijestiti Department of Commerce SAD-a (ili njegova ovlaštenog predstavnika) o tim činjenicama. Ako to propusti učiniti može biti kažnjena prema False Statements Act-u (18 U.S.C. § 1001).

Department (ili njegov ovlašteni predstavnik) navest će u svom javnom popisu organizacija koje same potvrđuju da se pridržavaju načela „sigurne luke" svaku obavijest o trajnom nepridržavanju bez obzira primi li je od same organizacije, od samoregulatornog tijela ili od vladina tijela, ali tek nakon što je prvo obavijesti trideset (30) dana unaprijed i pruži organizaciji koja se ne pridržava načela mogućnost da se očituje. Sukladno s tim, iz javnog popisa koji vodi Department of Commerce (ili njegov ovlašteni predstavnik) bit će jasno kojim organizacijama jesu, a kojima više nisu zajamčene pogodnosti „sigurne luke".

([3]) Tijela za rješavanje sporova ne moraju se pridržavati načela provedbe. Ona također mogu odstupiti od načela ako im se pojave proturječne obveze ili izričita ovlaštenja u izvršenju njihovih specifičnih zadaća.

([4]) Tijela za rješavanje sporova imaju slobodu odlučivanja o okolnostima u kojima primjenjuju te sankcije. Osjetljivost dotičnih podataka je jedan od faktora koje treba uzeti u obzir pri odlučivanju hoće li biti potrebno brisati podatke, kao što je i činjenica je li organizacija prikupila, koristila ili otkrila informacije u očitoj suprotnosti s načelima.

Organizacija koja se prijavi za sudjelovanje u samoregulatornom tijelu kako bi ponovno stekla uvjete za sigurnost mora tom tijelu dostaviti sve informacije o svom prijašnjem sudjelovanju u zaštiti privatnosti.

ČESTO POSTAVLJANO PITANJE 12 – Mogućnost odabira - Trenutak odbijanja

P: *Dopušta li načelo mogućnosti izbora pojedincu da iskoristi mogućnost odabira samo na početku odnosa ili bilo kada?*

O: Općenito je svrha načela mogućnosti izbora osigurati korištenje i otkrivanje osobnih podataka na načine koji su u skladu s očekivanjima i željama pojedinca. Stoga, pojedincu treba biti omogućeno da „odustane" (ili ima izbor) korištenja njegovih osobnih podataka u svrhe izravnog marketinga bilo kada podložno razumnim ograničenjima koja je postavila organizacija, kao što je davanje organizaciji vremena da odustanak stupi na snagu. Organizacija može također tražiti dovoljno informacija da potvrdi identitet pojedinca koji zahtijeva „odustajanje". U Sjedinjenim Američkim Državama pojedinci mogu koristiti ovu opciju uporabom središnjeg programa za „odustajanje" kao što je usluga *mail preference* organizacije Direct Marketing Association. Organizacije koje koriste uslugu *mail preference* organizacije Direct Marketing Association trebaju promicati njezinu dostupnost potrošačima koji ne žele primati komercijalne informacije. U svakom slučaju, pojedincu treba biti ponuđen lako dostupan i prihvatljiv mehanizam za korištenje ove mogućnosti.

Slično tome, organizacija može koristiti informacije u određene svrhe izravnog marketinga kada nije praktično ponuditi pojedincu mogućnost „odustajanja" prije korištenja informacija, ako organizacija bez odgađanja ponudi pojedincu mogućnost istodobnog (i na zahtjev bilo kada) odbijanja (bez troška za pojedinca) primanja izravnih komercijalnih obavijesti i organizacija ispoštuje želju pojedinca.

ČESTO POSTAVLJANO PITANJE 13 – Putne informacije

P: *Kada se podaci o rezervaciji putnika avionom i ostale putne informacije, kao što su informacije o učestalim putnicima ili hotelskim rezervacijama i posebnim potrebama, kao što su obroci koji ispunjavaju vjerske zahtjeve ili fizička pomoć, mogu prenositi u organizacije izvan EU-a?*

O: Takve se informacije mogu prenositi u nekoliko različitih okolnosti. Prema članku 26. Direktive, osobni se podaci mogu prenositi „u treću zemlju koja ne osigura primjerenu razinu zaštite u smislu članka 25 stavka 2." ako je: 1. to potrebno da bi se pružile usluge koje traži potrošač ili da bi se ispunili uvjeti ugovora, kao što je ugovor o „čestim putnicima"; ili 2. je potrošač dao nedvosmislenu privolu za to. Organizacije iz SAD-a koje su sudionice„sigurne luke" pružaju primjerenu zaštitu osobnih podataka i stoga mogu primati podatke prenijete iz EU-a bez ispunjavanja ovih uvjeta ili ostalih uvjeta iz članka 26. Direktive. Budući da „sigurna luka" uključuje posebna pravila s obzirom na osjetljive informacije, takve informacije (koje možda moraju biti prikupljene, na primjer, vezano za potrebe korisnika za fizičkom pomoći) mogu biti obuhvaćene prijenosom sudionicima „sigurne luke". U svim slučajevima, međutim, organizacija koja prenosi informacije mora poštovati pravo države članice EU-a u kojoj djeluje, koje može među ostalim nametnuti posebne uvjete za postupanje prema osjetljivim podacima.

ČESTO POSTAVLJANO PITANJE 14. Farmaceutski i medicinski proizvodi

1. P: *Ako su osobni podaci prikupljeni u EU-u i prenijeti u Sjedinjene Američke Države radi farmaceutskog istraživanja i/ili ostalih svrha, primjenjuju li se zakoni države članice ili načela „sigurne luke"?*

1. O: Pravo države članice primjenjuje se na prikupljanje osobnih podataka i na obradu koja se obavlja prije prijenosa u Sjedinjene Američke Države. Načela „sigurne luke" primjenjuju se na podatke tek kad budu prenijeti u Sjedinjene Američke Države. Podatke koji se koriste za farmaceutsko istraživanje i ostale svrhe treba učiniti anonimnima kada je to prikladno.

2. P: *Osobni podaci koji se razrađuju u određenim studijama medicinskih ili farmaceutskih istraživanja često imaju vrijednu ulogu u budućem znanstvenom istraživanju. Ako se osobni podaci prikupljeni za jedno istraživanje prenose u organizaciju iz SAD-a koja je sudionica „sigurne luke", može li organizacija koristiti podatke za novu znanstveno-istraživačku aktivnost?*

2. O: Da, ako je inicijalno bila ponuđena odgovarajuća obavijest i mogućnost izbora. Takva obavijest treba dati informaciju o svim budućim specifičnim korištenjima podataka, kao što je periodično praćenje, povezano istraživanje ili marketing. Podrazumijeva se da ne mogu sva buduća korištenja podataka biti precizirana, budući da novo korištenje pri istraživanju može proizaći iz novih saznanja o izvornim podacima, novim medicinskim otkrićima i napretku, te razvojem u javnom zdravstvu i regulatornim događajima. Ako je to prikladno, obavijest stoga treba uključivati objašnjenje da je moguće da će se osobni podaci koristiti u budućim medicinskim i farmaceutskim istraživanjima koja su nepredviđena. Ako korištenje nije u skladu s općom istraživačkom svrhom (svrhama) za koju su podaci prvotno prikupljeni ili na koju je pojedinac pristao, naknadno se mora ishoditi novi pristanak.

3. P: *Što se događa s podacima pojedinca ako se sudionik dobrovoljno ili na zahtjev sponzora odluči povući iz kliničkog ispitivanja?*

3. O: Sudionici mogu odlučiti ili biti zamoljeni da se povuku iz kliničkog ispitivanja bilo kada. Svi podaci prikupljeni prije povlačenja ipak se mogu obraditi zajedno s ostalim podacima prikupljenima kao dio kliničkog ispitivanja, međutim ako je to bilo pojašnjeno sudioniku u obavijesti u trenutku kada je pristao sudjelovati.

4. P: *Poduzeća koja proizvode lijekove i medicinske proizvode smiju davati osobne podatke iz kliničkih ispitivanja provedenih u EU-u regulatornim tijelima u Sjedinjenim Američkim Državama za regulatorne i nadzorne svrhe. Jesu li slični prijenosi dozvoljeni i prema drugim stranama osim regulatornih tijela, kao što su podružnice trgovačkih društava i ostali istraživači?*

4. O: Da, u skladu s načelima obavijesti i mogućnosti izbora.

5. P: *Kako bi se zajamčila objektivnost kliničkih ispitivanja njihovi sudionici, a često i istraživači, ne mogu dobiti pristup informacijama koju terapiju dobiva koji sudionik. Ako bi se to otkrilo ugrozila bi se valjanost istraživanja i rezultata. Hoće li sudionici takvih kliničkih ispitivanja (nazvanih istraživanja „naslijepo") imati pristup podacima o svome liječenju tijekom ispitivanja?*

5. O: Ne, takav pristup ne mora biti omogućen sudioniku ako mu je ovo ograničenje bilo objašnjeno kad je pristupio ispitivanju i kada bi otkrivanje takve informacije ugrozilo integritet istraživačkog napora. Pristanak na sudjelovanje u ispitivanju pod tim uvjetima je opravdan razlog za odricanje od prava pristupa. Nakon zaključenja ispitivanja i analize rezultata sudionici trebaju imati pristup svojim podacima ako to zatraže. Trebaju ga prvenstveno tražiti od liječnika ili drugih zdravstvenih djelatnika koji su ih liječili u sklopu kliničkog ispitivanja, ili tek zatim od poduzeća koje je sponzor.

6. P: *Mora li poduzeće koje proizvodi farmaceutske i medicinske proizvode primjenjivati načela „sigurne luke" s obzirom na obavijest, mogućnost izbora, daljnji prijenos i pristup u svojim aktivnostima praćenja sigurnosti i učinkovitosti proizvoda, uključujući izvješćivanje o neželjenim učincima i praćenju pacijenata/osoba koje koriste određene lijekove ili medicinske proizvode (npr. pacemaker)?*

6. O: Ne, u onoj mjeri u kojoj se pridržavanje načela kosi s poštovanjem regulatornih zahtjeva. To se odnosi i na izvješća, na primjer, pružatelja zdravstvene skrbi poduzećima koja proizvode lijekove i medicinske proizvode i na izvješća poduzeća koja proizvode lijekove i medicinske proizvode vladinim agencijama, poput Food and Drug Administration.

7. P: *Podatke o istraživanju glavni istraživač redovito zaštićuje jedinstvenom šifrom na njihovom izvoru tako da se ne otkrije identitet pojedinih osoba čiji se podaci obrađuju. Farmaceutska poduzeća koja sponzoriraju takva istraživanja ne dobivaju šifru. Jedinstvenu šifru ima samo istraživač, tako da može identificirati sudionika istraživanja u posebnim okolnostima (npr. ako je potrebno praćenje liječenja). Da li prijenos tako šifriranih podataka iz EU-a u Sjedinjene Američke Države predstavlja prijenos osobnih podataka koji podliježe načelima „sigurne luke"?*

7. O: Ne. Ovo ne predstavlja prijenos osobnih podataka koji bi podlijegao načelima.

ČESTO POSTAVLJANO PITANJE 15 – Javne evidencije i javno dostupne informacije

P: *Moraju li se načela obavijesti, mogućnosti izbora i daljnjeg prijenosa primjenjivati na informacije iz javne evidencije ili na javno dostupne informacije?*

O: Načela obavijesti, mogućnosti izbora i daljnjeg prijenosa ne moraju se primjenjivati na podatke iz javne evidencije ako oni nisu pomiješani s podacima iz nejavne evidencije i ako se poštuju uvjeti za savjetovanje koje je utvrdilo nadležno tijelo.

Također, općenito nije potrebno primjenjivati načela obavijesti, mogućnosti izbora i daljnjeg prijenosa na javno dostupne podatke osim ako europski prenositelj navede da takvi podaci podliježu ograničenjima koja zahtijevaju da organizacija primjenjuje ova načela za namjeravane uporabe. Organizacije neće biti odgovorne za to kako takve podatke koriste oni koji ih dobiju iz objavljenih materijala.

Ako se utvrdi da je organizacija namjerno objavila osobne podatke suprotno načelima kako bi ona ili ostali izvukli koristi od tih iznimaka, više neće imati pravo na pogodnosti „sigurne luke”.

PRILOG III.

Pregled provedbe „sigurne luke”

Federalne i državne ovlasti s obzirom na „nepoštene i prijevarne radnje” i privatnost

Ovaj memorandum opisuje ovlast Federal Trade Commission (FTC) sukladno s odjeljkom 5. Federal Trade Commission Act-a (15 U.S.C. §§ 41-58, s izmjenama) za poduzimanje mjera protiv onih koji ne štite privatnost osobnih podataka u skladu s njihovim izjavama i/ili obvezama da to čine. Također govori o iznimkama u vezi s tim ovlaštenjem i mogućnostima ostalih saveznih i državnih agencija da poduzimaju mjere ako FTC nema ovlast ([1]).

Ovlast FTC-a u vezi s nepoštenim i prijevarnim radnjama

Odjeljak 5. Federal Trade Commission Act-a proglašava „nepoštene ili prijevarne radnje ili postupke u trgovini ili one koji utječu na trgovinu” nezakonitima. 15 U.S.C. § 45(a)(1). Odjeljak 5. daje FTC-u neograničenu ovlast da sprečava takve radnje i postupke. 15 U.S.C. § 45(a)(2). Sukladno s tim FTC može nakon završenog službenog saslušanja izdati „nalog o zabrani” da bi prekinuo kažnjivo ponašanje. 15 U.S.C. § 45(b). Ako bi to bilo u javnom interesu, FTC također može od okružnog suda SAD-a zatražiti privremenu sudsku zabranu ili privremenu ili trajnu mjeru. 15 U.S.C. § 53(b). U slučajevima kada su nepošteni ili prijevarni postupci ili radnje jako rašireni ili ako je već izdao nalog za zabranu neke pojave, FTC može donijeti upravni propis o spomenutim radnjama ili postupcima. 15 U.S.C. § 57a.

Svatko tko ne poštuje nalog FTC-a može biti kažnjen iznosom i do 11 000 USD, s tim da svaki sljedeći dan kršenja predstavlja novo kršenje ([2]). 15 U.S.C. § 45(1). Isto tako, svakome tko svjesno krši pravilo FTC-a može se izreći kazna od 11 000 USD za svako kršenje. 15 U.S.C. § 45(m). Odgovarajući postupak može pokrenuti Department of Justice ili ako ono odbije, FTC. 15 U.S.C. § 56.

Ovlast FTC-a i privatnost

Koristeći svoje ovlasti iz odjeljka 5., FTC zastupa stajalište da lažno prikazivanje razloga za prikupljanje podataka o potrošaču ili načina korištenja podataka predstavlja prijevarni postupak ([3]). Na primjer FTC je 1998. podnio tužbu protiv društva GeoCities radi otkrivanja podataka koje je prikupio na svojoj internetskoj stranici trećim stranama da bi privukli korisnike i to bez prethodnog dopuštenja, unatoč svojim izjavama o suprotnom ([4]). FTC-ovo osoblje je također potvrdilo da prikupljanje osobnih podataka od djece, te prodaja i otkrivanje tih podataka bez pristanka roditelja može biti prijevarni postupak ([5]).

([1]) Ovdje se ne raspravljaju svi različiti savezni propisi koji se bave privatnošću u specifičnim kontekstima ni propisi država i common law koji bi se mogli primjenjivati. Propisi na saveznoj razini koji reguliraju komercijalno prikupljanje i korištenje osobnih podataka uključuje Cable Communications Policy Act (47 U.S.C. § 551), Driver's Privacy Protection Act (18 U.S.C. § 2721), Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), Electronic Funds Transfer Act(15 U.S.C. §§ 1693, 1693m), Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.), Telephone Consumer Protection Act (47 U.S.C. § 227) i Video Privacy Protection Act (18 U.S.C. § 2710), među ostalima. Mnoge države imaju analogne zakone na tim područjima. Vidjeti npr., Mass. Gen. Laws ch. 167B, § 16 (koji zabranjuje financijskim ustanovama da otkrivaju financijske podatke o klijentima trećoj osobi bez klijentova pristanka ili sudskog postupka), N.Y. Pub. Health Law § 17 (koji ograničuje korištenje i otkrivanje podataka o zdravstvenom ili duševnom stanju pacijenata i daje pacijentima pravo pristupa istima).

([2]) Kod takvog postupanja, okružni sud Sjedinjenih Američkih Država može također izdati sudski nalog i pravičnu naknadu prikladnu za provedbu naloga FTC-a. 15 U.S.C. § 45(1).

([3]) „Prijevarni postupak” definira se kao izjava, propust ili praksa za koju je vjerojatno da će zavarati razumne potrošače.

([4]) Vidjeti www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) Vidjeti dopis osoblja za Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Osim toga, Children's Online Privacy Protection Act iz 1998. daje FTC-u specifičnu zakonsku ovlast da regulira prikupljanje osobnih podataka od djece putem internetskih stranica i pružatelja internetskih usluga. Vidjeti 15 U.S.C. §§ 6501-6506. Zakon osobito zahtijeva od pružatelja internetskih usluga da obavijeste roditelje i ishode njihov pristanak prije prikupljanja korištenja ili otkrivanja osobnih podataka djece i koji se može provjeriti. Ibid., § 6502(b). Taj zakon također daje roditeljima pravo pristupa i pravo da odbiju dati dozvolu za nastavak korištenja informacija. Ibid.

U pismu glavnom direktoru Europske komisije, Johnu Moggu, predsjedatelj FTC-a Pitofsky naveo je ograničenja u ovlasti FTC-a da zaštiti privatnost ako nije bilo lažnog prikazivanja (ili nikakve izjave) u vezi s korištenjem prikupljenih podataka. Pismo predsjedatelja FTC-a Pitofskyog Johnu Moggu (23. rujna 1998.). Međutim, trgovačka društva koja žele iskoristiti predloženu „sigurnu luku" moraju potvrditi da će zaštiti podatke koje prikupe u skladu s propisanim smjernicama. Shodno tome, ako trgovačko društvo potvrdi da će zaštititi privatnost podataka a onda to ne učini, takva će radnja predstavljati lažno prikazivanje i „prijevarni postupak" u smislu odjeljka 5.

Kako FTC-ova nadležnost obuhvaća nepoštene ili prijevarne postupke ili radnje „u trgovini ili one koji utječu na trgovinu", FTC neće biti nadležan za prikupljanje i korištenje osobnih podataka u nekomercijalne svrhe, na primjer, prikupljanje sredstava u dobrotvorne svrhe. Vidjeti pismo Pitofskyja, str. 3. Međutim, korištenje osobnih podataka u nekoj poslovnoj transakciji zadovoljit će ovu pravnu osnovu. Tako bi na primjer, poslodavčeva prodaja osobnih podataka o svojim zaposlenicima poduzećima koja se bave izravnim marketingom bila transakcija u području primjene odjeljka 5.

Iznimke propisane odjeljkom 5.

Odjeljak 5. utvrđuje iznimke u ovlasti FTC-a nad nepoštenim ili prijevarnim postupcima ili radnjama s obzirom na:

— financijske ustanove, uključujući banke, štedno-kreditne ustanove te kreditne unije,

— telekomunikacijske operatore i javne prijevoznike u međudržavnom prijevozu,

— zračne prijevoznike, te

— proizvođače mesnih prerađevina i trgovce stokom.

Vidjeti 15 U.S.C. § 45(a)(2). U nastavku teksta govori se o svim iznimkama i regulatornom tijelu koje preuzima njegovo mjesto.

Financijske institucije ([6])

Prva se iznimka primjenjuje na „banke, štedne i kreditne institucije opisane u odjeljku 18. točki (f) podtočki (3) [15 U.S.C. § 57a(f)(3)]" i „savezne kreditne unije opisane u odjeljku 18. točki (f) podtočki (4) [15 U.S.C. § 57a(f)(4)]" ([7]). Te financijske institucije pak podliježu propisima koje je izdao Federal Reserve Bord, Office of Thrift Supervision, ([8]), odnosno National Credit Union Administration Board. Vidjeti 15 U.S.C. § 57a(f). Te su regulatorne agencije dobile upute da donesu propise potrebne za sprečavanje nepoštenih i prijevarnih radnji tih financijskih institucija ([9]) i da osnuju zaseban odjel koji će se baviti pritužbama potrošača. 15 U.S.C. § 57a(f)(1). Konačno, ovlast za provedbu proizlazi iz odjeljka 8. Federal Deposit Insurance Act-a (12 U.S.C. § 1818), za banke i štedne i kreditne institucije, te odjeljaka 120 i 206 Federal Credit Union Act-a, za savezne kreditne unije. 15 U.S.C. §§ 57a(f)(2)-(4).

([6]) 12. studenoga 1999. Predsjednik Clinton potpisao je kao zakon Gramm-Leach-Bliley Act (Pub. L. 106-102, codified at 15 U.S.C. § 6801 et seq.). Taj Zakon ograničuje financijske ustanove u otkrivanju osobnih podataka svojih klijenata. Zakon traži od financijskih ustanova da, između ostaloga, obavijeste sve klijente o svojim politikama privatnosti i praksom u pogledu otkrivanja osobnih podataka svojim povezanim i nepovezanim društvima. Ovaj Zakon ovlašćuje FTC savezna bankarska tijela i ostala tijela da donose propise za provedbu zaštite privatnosti u skladu sa zakonom. Agencije su u tu svrhu izdale predložene propise.

([7]) Prema vlastitim odlukama ova se iznimka ne primjenjuje na sektor vrijednosnih papira. Stoga brokeri, dileri i ostali koji posluju s vrijednosnim papirima podliježu istodobnoj nadležnosti Securities and Exchange Commission i FTC-a u pogledu nepoštenih ili prijevarnih postupaka i radnji.

([8]) Iznimka u odjeljku 5. izvorno se odnosila na Federal Home Loan Bank Board kojeg je ukinuo Financial Institutions Reform, Recovery and Enforcement Act iz kolovoza 1989. Njegove su funkcije prenijete na Office of Thrift Supervision and to the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, and the Housing Finance Board.

([9]) Ukidajući nadležnost FTC-a nad financijskim ustanovama, odjeljak 5. također određuje da kad FTC objavi neko pravilo o nepoštenim ili prijevarnim postupcima i radnjama, financijski regulatorni odbori trebaju usvojiti paralelne propise u roku od 60 dana. Vidjeti 15 U.S.C. § 57a(f)(1).

Iako sektor osiguranja nije izričito uključen u popis iznimaka u odjeljku 5., McCarran-Ferguson Act (15 U.S.C. § 1011 et seq.) općenito prepušta regulaciju osiguravajuće djelatnosti svakoj državi pojedinačno ([10]). Nadalje, sukladno s odjeljkom 2. točkom (b) McCarran-Ferguson Act-a, niti jedan savezni zakon neće ukinuti, narušiti ili zamijeniti državne propise „osim ako se takav zakon izričito odnosi na djelatnost osiguranja". 15 U.S.C.§ 1012(b). Međutim, odredbe FTC Act-a primjenjuju se na sektor osiguranja „u onoj mjeri u kojoj njihovo poslovanje nije regulirano državnim zakonom." ibid. Treba također napomenuti da McCarran-Ferguson Act daje prednost državnim zakonima samo u odnosu na „djelatnost osiguranja". Stoga FTC zadržava preostali dio ovlasti nad nepoštenim ili prijevarnim radnjama osiguravajućih društava u aspektima poslovanja koji se ne odnose na osiguranje. To na primjer može uključivati slučajeve kada osiguravatelji prodaju osobne podatke o nositeljima njihovih polica poduzećima koja se bave izravnim marketingom proizvoda koji nisu proizvodi osiguranja ([11]).

Javni prijevoznici

Druga iznimka iz odjeljka 5. obuhvaća one javne prijevoznike koji podliježu „zakonima koji reguliraju trgovinu" 15 U.S.C. § 45(a)(2). U ovom se slučaju „zakoni koji reguliraju trgovinu" odnose na podnaslov IV. glavu 49. United States Code-a i to Communications Act-a iz 1934. (47 U.S.C. § 151 et seq.) (Communications Act). Vidjeti 15 U.S.C. § 44.

49 U.S.C. podnaslov IV. (međudržavni prijevoz) obuhvaća prijevoznike u željezničkom, automobilskom i vodenom prometu, posrednike, špeditere i poduzeća koja se bave prometom cjevovodima, 49 U.S.C. § 10101 et seq. Ti različiti javni prijevoznici podliježu regulaciji od strane Surface Transportation Board-a, neovisne agencije u sklopu Department of Transportation., 49 U.S.C. §§ 10501, 13501 i 15301. U svakom slučaju, prijevozniku je zabranjeno otkrivati podatke o vrsti, odredištu i ostalim aspektima svog tereta koji bi se mogli iskoristiti na pošiljateljevu štetu. Vidjeti 49 U.S.C. §§ 11904, 14908 i 16103. Ističemo da se te odredbe odnose na podatke koji se tiču pošiljateljeva tereta i stoga se ne čini da obuhvaćaju osobne podatke o pošiljatelju koji nisu vezani za dotičnu pošiljku.

Što se tiče Communications Act-a, on predviđa regulaciju „međudržavne trgovine i trgovine s inozemstvom žičnom i radijskom komunikacijom" od strane Federal Communications Commission (FCC). Vidjeti 47 U.S.C. §§ 151 i 152. Osim na javna telekomunikacijska poduzeća, Communications Act također se primjenjuje na trgovačka društva kao što su televizijske i radio postaje i pružatelji kabelskih usluga koji nisu javni operateri. Ova potonja trgovačka društva kao takva ne ispunjavaju uvjete za iznimku sukladno s odjeljkom 5. FTC Act-a. Tako FTC ima nadležnost istraživati nepoštene i prijevarne radnje u tim trgovačkim društvima, dok je FCC ravnopravno nadležan za provođenje svoje neovisne ovlasti na tom području kao što je opisano u nastavku.

Sukladno sa Communications Act-om, „svaki telekomunikacijski operater", uključujući i lokalne telefonske centrale, ima dužnost zaštititi privatnost privatnih mrežnih podataka o korisniku ([12]), 47 U.S.C. § 222(a). Osim ove opće ovlasti za zaštitu privatnosti, Communications Act je bio izmijenjen Cable Communications Policy Act iz 1984. („Cable Act"), 47 U.S.C. § 521 *et seq*., kako bi izričito propisao da kabelski operateri moraju zaštititi privatnost „informacija koje omogućavaju identitificiranje osobe" o pretplatnicima kabelske mreže, 47 U.S.C. § 551 ([13]). Cable Communications Policy Act ograničuje kabelske operatore u prikupljanju osobnih podataka i zahtjeva da obavijeste pretplatnika o vrsti prikupljenih informacija i kako će se one koristiti. Cable Communications Policy Act daje pretplatnicima pravo pristupa vlastitim podacima i pravo zahtjeva kabelskim operaterim za uništenje tih podatke kada ih više ne budu trebali.

Communications Act ovlašćuje FCC da provede te dvije odredbe o privatnosti, bilo na vlastitu inicijativu ili kao odgovor na vanjsku pritužbu ([14]), 47 U.S.C. §§ 205, 403; ibid. § 208. Ako FCC utvrdi da je telekomunikacijski operater (uključujući i kabelskog operatera) prekršio odredbe o privatnosti iz odjeljka 222. ili odjeljka 551., postoje tri osnovne mjere

([10]) „Djelatnost osiguranja i svaka osoba koja se njome bavi podliježe zakonima nekoliko država koji se odnose na regulaciju ili oporezivanje te djelatnosti", 15 U.S.C. § 1012(a).

([11]) FTC je koristio nadležnost nad osiguravajućim društvima u različitim kontekstima. U jednom je slučaju FTC poduzeo mjere protiv jednog društva radi lažnog oglašavanja u državi u kojoj nije imala dozvolu za rad. FTC-ova nadležnost je bila potpomognuta činjenicom da nije bilo učinkovite državne regulacije jer je društvo u stvarnosti bilo izvan dosega države. Vidjeti FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Što se tiče država, 17 ih je usvojilo nacrt „Insurance Information and Privacy Protection Act-a" kojeg je sastavilo National Association of Insurance COmmissioners (NAIC). Propis uključuje odredbe o obavješćivanju, korištenju i otkrivanju, te pristupu. Gotovo sve države usvojile su NAIC-ov predložak „Unfair Insurance Practices Act", koji je izričito usmjeren na nepoštene trgovinske prakse u sektoru osiguranja.

([12]) Pojam „privatnih mrežnih podataka o korisniku" podrazumijeva informacije koje se odnose na korisnikovu „količinu, tehničku konfiguraciju, vrstu, namjenu i vrijednost telekomunikacijskih usluga koje koriste" te informacije o telefonskom obračunu, 47 U.S.C. § 222(f)(1). Međutim, pojam ne uključuje informacije o popisu pretplatnika. *Ibid*.

([13]) Zakonodavstvo ne definira izričito „informacije koje omogućavaju identitificiranje osobe".

([14]) Ova ovlast obuhvaća prava na pravnu zaštitu zbog kršenja privatnosti, i prema odjeljku 222. Zakona o komunikacijama ili, kada se radi o kablovskim pretplatnicima, prema odjeljku 551. Zakona o kabelskim komunikacijama kao izmjena Zakona. Vidjeti također 47 U.S.C. § 551(f)(3) (građanski postupak na
Saveznom okružnom sudu nije isključivi pravni lijek, koji se nudi „pored nekog drugog zakonitog pravnog lijeka koji stoji na raspolaganju kablovskim pretplatnicima").

koje može poduzeti. Prvo, nakon saslušanja i utvrđivanja kršenja, povjerenstvo može narediti operateru da plati novčanu odštetu ([15]), 47 U.S.C. § 209. Umjesto toga FCC može narediti operateru da prestane s kažnjivim postupanjem ili propuštanjem, 47 U.S.C. § 205(a). I konačno, povjerenstvo može također narediti operateru koji čini prekršaj da „se uskladi i poštuje (neki) propis ili postupak" koji mu FCC može propisati. *ibid.*

Fizičke osobe koje vjeruju da je telekomunikacijski ili kabelski operator prekršio određene odredbe Communications Act-a ili Cable Communications Policy Act-a, mogu podnijeti tužbu FCC-u ili pokrenuti postupak pred saveznim okružnim sudom, 47 U.S.C. § 207. Tužitelj koji uspije u sporu pred saveznim sudom protiv telekomunikacijskog operatera zbog propusta da zaštititi privatne podatke korisnika u smislu odjeljka 222. Communications Act-a može dobiti naknadu stvarne štete i troškove odvjetnika. 47 U.S.C. § 206. Tužitelju koji podnese tužbu zbog kršenja privatnosti prema odjeljku 551. Cable Act-a koji se odnosi na kabelske operatere, mogu se osim stvarne štete i troškova zastupanja također dosuditi kaznena odšteta i razumni parnični troškovi. 47 U.S.C. § 551(f).

FCC je donio detaljna pravila za provedbu odjeljka 222. Vidjeti 47 CFR 64.2001-2009. Ta pravila propisuju određene zaštitne mjere od neovlaštenog pristupa vlasničkim mrežnim podacima o korisnicima. Propisi traže od telekomunikacijskih operatera da:

— razviju i uvedu računalne sustave koji „prikazuju" obaviještenost i odobrenje korisnika za korištenje njegovih podataka kada se prvi put na ekranu pojavi korisnikov dosje,

— vode elektronički „revizijski trag" kako bi se pratio pristup korisnikovom računu, uključujući podatke o tome kada je korisnikov dosje otvaran, tko ga je otvarao i u koju svrhu,

— osposobljavaju svoje osoblje za ovlašteno korištenje vlasničkih mrežnih informacija o korisnicima, uz uvedene odgovarajuće disciplinske postupke,

— uvedu postupak kontrolne provjere kako bi osigurali usklađenosti pri vanjskom marketingu, i

— svake godine potvrđuju FCC-u kako poštuju te propise.

Zračni prijevoznici

Zračni prijevoznici iz SAD-a i strani zračni prijevoznici koji podliježu Federal Aviation Act-u iz 1958. također su izuzeti od odjeljka 5. FTC Act-a. Vidjeti 15 U.S.C. § 45(a)(2). Ovo uključuje sve koji obavljaju međudržavni ili inozemni prijevoz robe ili putnika, ili koji avionom prevoze poštu. Vidjeti 49 U.S.C. § 40102. Zračni prijevoznici su pod nadležnošću Department of Transportation-a. U tom je pogledu Secretary of Transportation ovlašten poduzimati mjere koje „sprečavaju nepoštene, prijevarne, predatorske postupke ili protutržišna djelovanja u zračnom prijevozu". 49 U.S.C. § 40101(a)(9). Secretary of Transportation može ispitati je li zračni prijevoznik iz SAD-a ili inozemstva, ili agent koji prodaje karte, sudjelovao u nepoštenim ili prijevarnim radnjama, ako je to u javnom interesu. 49 U.S.C. § 41712. Nakon saslušanja Secretary of Transportation može izdati nalog za prekid nezakonitog postupka, ibid. Koliko nam je poznato, Secretary of Transportation nije iskoristio ovu ovlast kako bi pokrenuo pitanje zaštite privatnosti osobnih podataka korisnika zračnog prijevoza ([16]).

Postoje dvije odredbe koje štite privatnost osobnih podataka i primjenjuju se na zračne prijevoznike u određenim kontekstima. Prvo, Federal Aviation Act štiti privatnost kandidata za pilote. Vidjeti 49 U.S.C. § 44936(f). Dok omogućava zračnim prijevoznicima da dobiju kandidatovu radnu knjižicu, daje kandidatu pravo na obavijest da je knjižica zatražena, da odobri zahtjev, da ispravi netočne podatke i da pokaže knjižicu samo onima koji su uključeni u donošenje odluke o zapošljavanju. Drugo, uredbe DOT zahtijevaju da se očite informacije o putnicima prikupljene za vladine potrebe u slučaju avionske katastrofe „čuvaju kao povjerljive i otkriju samo US Department of State, National Transportation Board-u (na zahtjev NTSB-a) i U.S. Department of Transportation". 14 CFR dio 243, § 243.9(c) (dopunjen 63 FR 8258).

([15]) Međutim, nepostojanje izravne štete za tužitelja nije razlog da se tužba odbaci. 47 U.S.C. § 208(a).

([16]) Shvaćamo da postoje napori unutar ove gospodarske grane da se riješi pitanje privatnosti. Predstavnici ove grane su razgovarali o predloženim načelima zaštite i njihovoj mogućoj primjeni na zračne prijevoznike. Rasprava je obuhvatila prijedlog da se usvoji politika zaštite privatnosti unutar ove grane, prema kojoj bi se tvrtke sudionice stavile pod izričitu nadležnost DOT-a.

Proizvođači mesnih prerađevina i trgovci stokom

S obzirom na Packers and Stockyards Act iz 1921. (7 U.S.C. § 181 *et seq.*), zakon proglašava nezakonitim da „proizvođač mesnih prerađevina, s obzirom na stoku, meso, mesne prerađevine ili stočne proizvode u neprerađenom obliku, ili za trgovce živom peradi, obzirom na živu perad, sudjeluje u nepoštenim, nepravedno diskriminirajućim ili prijevarnim postupcima ili sredstvu, ili iste primjenjuje". 7 U.S.C. § 192(a); vidjeti također 7 U.S.C. § 213(a) (koji zabranjuje „bilo kakav nepošten, nepravedno diskriminirajući ili prijevarni postupak ili sredstvo" u odnosu na stoku). Secretary of Agriculture ima primarnu odgovornost provoditi ove odredbe, dok FTC zadržava nadležnost nad maloprodajnim transakcijama i onima koje se odnose na peradarstvo. 7 U.S.C. § 227(b)(2).

Nije jasno hoće li Secretary of Agriculture tumačiti propust proizvođača mesnih prerađevina ili trgovaca stokom da zaštititi privatnost u skladu s navedenom politikom kao postupak „prijevare" prema Packers and Stockyards Act-u. Međutim, iznimka iz odjeljka 5. primjenjuje se na osobe, partnerstva ili korporacije samo „u mjeri u kojoj podliježu Packers and Stockyards Act-u". Stoga, ako zaštita osobnih podataka nije pitanje iz područja primjene Packers and Stockyards Act-a, tada se iznimka iz odjeljka 5. ne mora primjenjivati, pa bi proizvođači mesnih prerađevina i trgovci stokom bili pod nadležnošću FTC-a u tom pogledu.

Ovlasti država nad „nepoštenim i prijevarnim radnjama"

Prema analizi koju je napravilo osoblje FTC-a, „svih 50 država te District of Columbia, Guam, Puerto Rico i Djevičanski otoci usvojili su zakone koji su više ili manje slični Federal Trade Commission Act-u ('FTCA') radi sprečavanja nepoštene ili prijevarne trgovačke prakse". Informativni list FTC-a, prenijet u „Komentar, Zaštita potrošača: Praktična učinkovitost državnih zakona o nepoštenim trgovinskim praksama", 59 Tul, L. Rev. 427 (1984). U svim slučajevima, agencija za provedbu ima ovlast „provoditi istrage korištenjem sudskih poziva pod prijetnjom kazne ili građanskih zahtjeva za istragu, tražiti uvjerenja o dobrovoljnom pridržavanju, izdavati sudske naloge o zabrani ili ishoditi sudske naloge za sprečavanje primjene nepoštenih, nesavjesnih ili prijevarnih trgovačkih praksi, *ibid.* U 46 jurisdikcija, zakon dopušta privatne tužbe za stvarnu, dvostruku, trostruku ili kaznenu odštetu, a u nekim slučajevima i naknadu troškova i troškova zastupanja. *Ibid.*"

Deceptive and Unfair Trade Practices Act Floride, na primjer, ovlašćuje javnog tužitelja da istražuje i pokreće građanske postupke protiv „nepoštenih načina tržišnog natjecanja, nepoštenih, nesavjesnih ili prijevanih trgovačkih praksi", uključujući lažno ili zavaravajuće reklamiranje, obmanjujuće prilike za *franchise* ili poslovanje, lažni telemarketing i piramidalne sheme. Vidjeti također Opći poslovni zakon New Yorka § 349 (koji zabranjuje nepoštene postupke i prijevarne radnje tijekom obavljanja djelatnosti).

Anketa koju je ove godine proveo National Association of Attorneys General (NAAG) potvrđuje ove rezultate. Od 43 države koje su sudjelovale, sve imaju „mini-FTC" propise ili ostale propise koji osiguravaju sličnu zaštitu. Također, prema anketi NAAG-a, 39 država navelo je da bi imale ovlast voditi postupak kojeg je pokrenula osoba koja nema boravište u dotičnoj državi. S obzirom na privatnost potrošača, 37 od 41 države koje su odgovorile navelo je da bi reagirale na pritužbe koje navode da trgovačko društvo pod njihovom nadležnošću ne poštuje vlastitu politiku o privatnosti koju je samo objavilo.

PRILOG IV.

Odštete za kršenje privatnosti, zakonske ovlasti te spajanja i preuzimanja prema pravu SAD-a

Ovo je odgovor na zahtjev Europske komisije za objašnjenje prava SAD-a u odnosu na (a) zahtjeve za odštetu zbog kršenja privatnosti, (b) „izričite ovlasti" u pravu SAD-a za uporabu osobnih podataka na način koji je u skladu s načelima „sigurne luke", te (c) utjecaj spajanja i preuzimanja na obveze preuzete sukladno načelima „sigurne luke".

A. **Odštete zbog kršenja privatnosti**

Nepoštovanje načela „sigurne luke" može dovesti do brojnih privatnih tužbi ovisno o danim okolnostima. Organizacije potpisnice načela „sigurne luke" mogu se smatrati odgovornima za lažno prikazivanje svoga nepridržavanja politike zaštite privatnosti za koju su naveli da je se pridržavaju. *Common law* također omogućava privatne razloge za pokretanje postupka za naknadu štete zbog kršenja privatnosti. Mnogi savezni i državni propisi o privatnosti također predviđaju naknadu štete fizičkim osobama zbog tog kršenja.

Pravo na naknadu štete zbog narušavanja privatnosti jasno je utvrđeno prema common law-u SAD-a.

Korištenje osobnih podataka koje nije u skladu s načelima „sigurne luke" može biti razlogom pravne odgovornosti prema nizu različitih pravnih teorija. Na primjer i nadzornik podataka koji se prenose i pogođeni pojedinci mogu tužiti organizacije potpisnice načela „sigurne luke" koje ne ispunjavaju svoje obveze zaštite za lažno prikazivanje. Prema Restatement of the Law, Second, Torsts ([1]), vrijedi sljedeće:

> Onaj tko s namjerom prijevare lažno prikaže činjenicu, mišljenje, namjeru ili zakon da bi potakao drugog da nešto poduzme ili ne poduzme oslanjajući se na to, odgovoran je osobi dovedenoj u zabludu nadoknaditi novčani gubitak koji mu je izazvao njegovim opravdanim oslanjanjem na lažno prikazano.

Restatement, § 525. Lažno prikazivanje ima „prijevarnu namjeru" ako je učinjeno svjesno ili u uvjerenju da je netočno. *Ibid.*, § 526. Općenito, osoba koja lažno prikazuje s namjerom prijevare potencijalno je odgovorna svakome prema kome ima namjeru ili očekuje od njega da se pouzda u lažno prikazivanje za svaki novčani gubitak koji može pretrpjeti kao posljedicu. *Ibid.* 531. Nadalje, strana koja se lažno prikazuje drugima s namjerom prijevare može biti odgovorna trećoj osobi ako počinitelj štete ima namjeru ili očekuje da njegovo lažno prikazivanje bude ponovljeno trećoj osobi i da ona postupa na temelju istoga. *Ibid.*, § 533.

U smislu „sigurne luke", pravno relevantan prikazivanje je javna izjava organizacije da će se pridržavati načela „sigurne luke". Jednom kad se na to obveže, svjesno nepridržavanje načela može za one koji se oslone na lažno prikazivanje predstavljati osnovu za podizanje tužbe zbog lažnog prikazivanja. Budući da se opredjeljenje za poštivanje načela objavljuje široj javnosti, pojedinci koji su nositelji tih podataka, kao i nadzornik podataka u Europi za prijenos osobnih podataka organizacijama iz SAD-a mogu imati razloge za podizanje tužbe protiv organizacija iz SAD-a zbog lažnog prikazivanja ([2]). Štoviše, organizacija iz SAD-a ostaje odgovorna prema njima za „nastavak lažnog prikazivanja" dokle god se oni oslanjaju na lažno prikazivanje na vlastitu štetu. Kodifikacija, § 535.

([1]) Restatement of the Law, Second, Torts/Druga kodifikacija, građanski delikti; Američki pravni institut (1997).

([2]) Ovo bi mogao biti slučaj, na primjer, ako su se pojedinci oslonili na opredjeljenje organizacije iz SAD-a za načela zaštite podataka kada su dali svoj pristanak nadzorniku podataka da prenese njihove osobne podatke u Sjedinjene Američke Države.

Oni koji se oslanjaju na lažno prikazivanje s namjerom prijevare imaju sukladno Restatement- u pravo na naknadu štete.

Primatelj lažnog prikaza s namjerom prijevare ima pravo na naknadu štete u postupku zbog prijevare protiv osobe koja mu je prouzročila novčani gubitak, a čiji je pravni razlog lažno prikazivanje.

Restatement, § 549. Štete koje se priznaju uključuju stvarni izravni gubitak, kao i izgubljenu „povoljnu priliku" u poslovnoj transakciji. *Ibid.*; *vidjeti, npr.*, Boling protiv Tennessee National Bank, 890 S.W.2d 32 (1994) (banka odgovorna zajmoprimcima za 14 825 USD odštete za otkrivanje osobnih podataka i poslovnih planova zajmoprimaca predsjedniku banke koji je imao suprotan interes).

Budući da lažno prikazivanje s namjerom prijevare zahtijeva ili stvarno znanje ili barem uvjerenje da je izjava netočna, odgovornost se može također pripisati za lažni iskaz. Sukladno s Kodifikacijom, tko god da lažnu izjavu dok obavlja svoju djelatnost, zvanje ili posao ili u nekoj novčanoj transakcija može biti odgovoran „ako ne pokaže izvjesnu brigu ili stručnost pri dobivanju ili prosljeđivanju informacija". Kodifikacija, § 552(1). Za razliku od lažnih prikaza s namjerom prijevare, odštete za lažni iskaz ograničene su na izravni gubitak. *Ibid.*, § 552B(1).

U jednom je nedavnom slučaju na primjer Viši sud u Connecticutu smatrao da to što elektrodistribucijsko poduzeće nije otkrilo svoje evidencije o korisnikovim uplatama nacionalnim kreditno-informacijskim uredima podržava temelj za podizanje tužbe zbog lažnog prikazivanja. Vidjeti Brouillard protiv United Illuminating Co., 1999. Conn. Super. LEXIS 1754. U tom je slučaju tužitelju bio uskraćen kredit jer je tuženik prijavio uplate koje nije primio u roku od trideset dana od ispostavljanja računa kao „kašnjenje". Tužitelj je izjavio da nije bio informiran o ovoj politici kad je otvorio račun za električne usluge kod tuženika. Sud je izričito smatrao da se „tužba zbog lažnog iskaza utemeljena zbog tuženikova propusta da se izjasni kada je imao obvezu to učiniti". Ovaj slučaj također pokazuje da svjesnost krivog postupanja ili namjera prevare nisu nužni elementi za podizanje tužbe za lažni iskaz. Tako organizacija iz SAD-a koja nesavjesno ne otkrije u potpunosti kako će koristiti osobne podatke primljene u skladu s načelima zaštite privatnosti može biti odgovorna za lažno prikazivanje.

Ako kršenje načela zaštite privatnosti obuhvaća zlouporabu osobnih podataka, osoba čiji se podaci obrađuju može podnijeti prigovor za prekršaj kršenja privatnosti prema običajnom pravu. Američko pravo već dugo priznaje razloge za parnicu koji se odnose na kršenje privatnosti. U slučaju iz 1905. ([3]), vrhovni sud države Georgia je zaključio u slučaju građanina čiju je fotografiju osiguravajuće društvo koristilo bez njegovoga pristanka ili znanja u svom reklamnom oglasu, da je pravo na privatnost ukorijenjeno u načelima prirodnog prava i običajnog prava. Izlažući sada poznate teme u američkoj pravnoj teoriji o privatnosti, sud je odlučio da je uporaba fotografije bila „zlonamjerna", „nepravedna" i da je željela „izvrgnuti tužitelja ruglu pred svijetom" ([4]). Temelji odluke u slučaju *Pavesich* su prevladale te uz manje promjene postale temelj američkog zakona u ovom području. Državni su sudovi, u skladu s time, prihvaćali razloge za podizanje tužbe u području kršenja privatnosti i barem 48 država sada sudski priznaje neke od takvih razloga za podizanje tužbe ([5]). Štoviše, barem 12 država ima ustavne odredbe koje jamče svojim građanima pravo na zaštitu privatnog života ([6]), koje se u nekim slučajevima mogu odnositi na zaštitu od ometanja od strane nevladinih organizacija. *Vidjeti npr.*, Hill protiv NCAA, 865 P.2d 633 (Ca. 1994); vidjeti također S. Ginder, Izgubljen i nađen u kibernetičkom prostoru: Informacijska privatnost u doba Interneta, 34 S.D.L. Rev. 1153 (1997.) („Ustavi nekih država uključuju zaštitu privatnosti koja nadilazi zaštitu privatnosti u Ustavu SAD-a. Aljaska, Arizona, Kalifornija, Florida, Havaji, Illinois, Louisiana, Montana, Južna Karolina i Washington imaju širu zaštitu privatnosti".)

Second Restatement of Torts daje mjerodavan pregled zakona iz ovog područja. Odražavajući običajnu sudsku praksu, Restatement objašnjava da „pravo na privatnost" obuhvaća četiri različita temelja za podizanje tužbe zbog delikta unutar tog okvir. *Vidjeti* Kodifikaciju, § 652A. Prvo, postoji temelj za podizanje tužbe za „ometanje intimne sfere" protiv tuženika koji namjerno, fizički ili na drugi način, ometa intimu ili izdvojenost druge osobe ili se miješa u njegove privatne poslove

([3]) Pavesich protiv New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).
([4]) *Ibid.*, 69.
([5]) Elektroničkim pretraživanjem Westlaw baze podataka pronađeno je 2 703 prijavljenih slučajeva građanskih postupaka pred državnim sudovima koji se odnose na „privatnost" od 1995. Prethodno smo poslali rezultate ovog pretraživanja Komisiji.
([6]) *Vidjeti npr.* Alaska Constitution, Art. 1 Sec. 22; Arizona, Art. 2, Sec. 8; California, Art. 1, Sec. 1; Florida, Art. 1, Sec. 23; Hawaii, Art. 1, Sec. 5; Illinois, Art. 1, Sec. 6; Louisiana, Art. 1, Sec. 5; Montana, Art. 2, Sec. 10; New York, Art. 1, Sec. 12; Pennsylvania, Art. 1, Sec.1; South Carolina, Art. 1, Sec. 10; and Washington, Art. 1 Sec. 7.

ili interese ([7]). Drugo, slučaj „prisvajanja" postoji kada netko prisvoji ime ili sliku drugoga za vlastitu uporabu ili korist ([8]). Treće, „objava privatnih činjenica" je kažnjiva kada bi objavljena stvar bila izrazito uvredljiva za razumnu osobu i nije od zakonitog interesa za javnost ([9]). I zadnje, tužba zbog „predstavljanja u krivom svjetlu" je prikladna kada tuženik svjesno ili bezobzirno predstavi drugoga javnosti u krivom svjetlu, što bi bilo vrlo uvredljivo za razumnu osobu ([10]).

U smislu načela zaštite privatnosti „ometanje intimne sfere" može obuhvaćati neovlašteno prikupljanje osobnih podataka budući da neovlašteno korištenje osobnih podataka u poslovne svrhe može dovesti do tužbe zbog prisvajanja. Slično bi i otkrivanje osobnih podataka koji su netočni predstavljalo delikt „prikazivanja u krivom svjetlu" pod uvjetom da su te informacije vrlo uvredljive za razumnu osobu. Konačno, kršenje privatnosti koje rezultira objavljivanjem ili otkrivanjem osjetljivih osobnih podataka može biti temelj za podizanje tužbe za „objavljivanje privatnih činjenica". (*Vidjeti* primjere dolje navedenih slikovitih slučajeva).

U pogledu odštete, kršenje privatnosti daje oštećenoj strani pravo na naknadu štete za:

(a) štetu njegovoj privatnoj sferi koja proizlazi iz kršenja;

(b) duševnu bol za koju je dokazano da ju je propatio, ako je ona takve vrste kakva obično je posljedica takvog kršenja; i

(c) posebnu štetu čiji je pravni uzrok kršenje.

Restatementa, § 652H. S obzirom na opću primjenjivost deliktnog prava i mnogostruke razloge za podizanje tužbe koji pokrivaju različite aspekte prava na poštovanje privatnosti, novčana je odšteta vjerojatan nadomjestak onima čija se privatnost naruši kao posljedica nepridržavanja načela zaštite privatnosti.

Državni su sudovi zaista prepuni slučajeva navodnog ometanja privatnosti u sličnim situacijama. *Ex Parte* AmSouth Bancorporation et al., 717 So. 2d 357, na primjer, je jednostrano pokrenula zajedničku tužbu u kojoj je navela da je tuženik „iskoristio novac ulagatelja stavljen u banku, otkrivajući povjerljive podatke o bankovnim ulagateljima i njihovim računima" kako bi omogućio društvu kćeri banke da preproda otvorene investicijske fondove i druge vrijednosne papire. U takvim se slučajevima često dodjeljuju odštete. U Vassiliades protiv Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.Apstr. 1985.), prizivni je sud preinačio presudu nižeg suda i odlučio da je uporaba fotografija tužitelja „prije" i „poslije" plastične operacije u prezentaciji u robnoj kući predstavljala kršenje privatnosti objavljivanjem privatnih činjenica. U slučaju Candebat protiv Flanagana, 487 So.2d 207 (Miss. 1986.) tuženo je osiguravajuće društvo iskoristilo nesreću u kojoj je tužiteljeva supruga bila ozbiljno ozlijeđena u reklamnoj kampanji. Tužitelj ga je tužio zbog kršenja privatnosti. Sud je presudio da tužitelj može nadoknaditi štetu duševne boli i prisvajanja identiteta. Parnice za lažno protupravno prisvajanje mogu se voditi čak i ako tužitelj nije poznat. *Vidjeti npr.*, Staruski protiv Continental Telephone Co., 154 Vt. 568 (1990.) (tuženik je ostvario poslovnu korist koristeći zaposlenikovo ime i fotografiju u novinskom oglasu). U Pulla protiv Amoco Oil Co., 882 F.Supstr. 836 (S.D Iowa 1995.) poslodavac je ometao privatni život tužitelja kao svoga zaposlenika time što je naredio drugom zaposleniku da provjeri njegov ispis s kreditne kartice da bi provjerio njegovu odsutnost s posla zbog bolovanja. Sud je podržao presudu porote od 2 USD stvarne odštete i 500 000 USD kaznene odštete. Jedan drugi poslodavac je proglašen odgovornim za objavljivanje priče u internim novinama poduzeća o zaposleniku koji je dobio otkaz zbog navodnog krivotvorenja svoje radne knjižice. *Vidjeti* Zinda protiv Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.Apstr. 1987.). Priča je narušila tužiteljevu privatnost objavljivanjem privatne stvari jer su novine bile u optjecaju u Zajednici. I kao zadnji slučaj, fakultet koji je testirao studente na HIV nakon što im je rekao da je analiza krvi bila za rubeolu bio je odgovoran samo za ometanje privatnosti. *Vidjeti* Doe protiv High-Tech Institutea, Inc., 972 P.2d 1060 (Colo.Apstr. 1998.). (Za ostale prijavljene slučajeve *vidjeti* Kodifikaciju, § 652H, Dodatak.)

Sjedinjene Američke Države često se kritizira kao previše sklone parničenju, ali to također znači da pojedinci stvarno i mogu i koriste pravna sredstva kada vjeruju da im je učinjena nepravda. Mnogi aspekti pravosudnog sustava olakšavaju

([7]) *Ibid.*, u poglavlju 28, odjeljku 62B.
([8]) *Ibid.*, u poglavlju 28, odjeljku 652C.
([9]) *Ibid.*, u poglavlju 28, odjeljku 652D.
([10]) *Ibid.*, u poglavlju 28, odjeljku 652E.

tužiteljima da ulažu tužbe, bilo pojedinačno ili grupno. Broj odvjetnika koji je relativno veći nego u većini drugih država čine pravno zastupanje lako dostupnim. Tužiteljev zastupnik koji zastupa pojedince u privatnim tužbama obično obračunava svoje troškove zastupanja prema postotku postignute odštete, omogućavajući čak i siromašnim tužiteljima da traže pravnu zaštitu. Ovo ukazuje na jedan bitan faktor - u Sjedinjenim Američkim Državama svaka strana obično snosi svoje odvjetničke troškove i ostale troškove. To je u suprotnosti s prevladavajućim pravilom u Europi gdje strana koji izgubi mora nadoknaditi troškove druge strane. Bez ulaženja u relativne prednosti ovih dvaju sustava, manja je vjerojatnost da bi pravilo SAD-a destimuliralo zakonite tužbe pojedinaca koji ne bi mogli platiti troškove obiju strana ako bi izgubili.

Pojedinci mogu tužiti za obeštećenje čak i ako su njihove tužbe relativno male vrijednosti. Većina, ako ne sva pravosudna tijela SAD-a, imaju sudove za sporove male vrijednosti koji obavljaju pojednostavljene i jeftinije postupke za sporove s vrijednošću ispod zakonske granice ([11]). Mogućnost kaznene odštete također nudi financijsku naknadu pojedincima koji su doživjeli manju izravnu štetu da podnesu tužbu za nedopustivo ponašanje. Konačno, pojedinci kojima je nanesena nepravda na isti način mogu udružiti svoja sredstva i svoje tužbe kako bi podnijeli zajedničku tužbu.

Dobar primjer mogućnosti pojedinaca da podnose tužbe da bi dobili naknadu je spor koji se vodi protiv Amazon.com-a zbog kršenja privatnosti. Amazon.com, veliko internetsko maloprodajno poduzeće, meta je zajedničke tužbe, u kojoj tužitelji tvrde da nisu bili informirani i da nisu pristali na prikupljanje vlastitih osobnih podataka dok su koristili softverski program pod nazivom „Alexa" u vlasništvu Amazona. U ovom su se slučaju tužitelji pozvali na kršenje Computer Fraud and Abuse Act zbog nezakonitog pristupa njihovim pohranjenim obavijestima i na (Electronic Communications Privacy Act zbog nezakonitog presretanja njihove elektroničke i telefonske komunikacije. Također navode kršenje privatnosti prema *common law*-u. Ovo proizlazi iz tužbe koju je podnio stručnjak za internetsku sigurnost u prosincu. Zatražena je odšteta od 1 000 USD za svakog člana skupine tužitelja, te plaćanje odvjetničkih troškova i dobit ostvarena kao rezultat kršenja zakona. S obzirom da broj članova skupine može dosezati i nekoliko milijuna, odštete mogu iznositi milijarde dolara. FTC također istražuje optužbe.

Savezno i državno zakonodavstvo o privatnosti često osigurava privatne razloge za podizanje tužbe za novčanu odštetu.

Osim što je temelj građanskopravne odgovornosti prema deliktom pravu, nepoštovanje načela zaštite privatnosti može također kršiti neki od stotinu saveznih i državnih zakona o privatnosti. Mnogi od ovih zakona, koji se odnose na postupanje i vlade i privatnog sektora prema osobnim podacima, omogućavaju pojedincima da tuže radi naknade štete kada dođe do kršenja. Na primjer:

Electronic Communications Privacy Act iz 1986. ECPA zabranjuje neovlašteno presretanje poziva mobitelom i prijenose podataka s računala na računalo. Kršenje može imati za posljedicu građanskopravnu odgovornost odštete koja ne iznosi manje od 100 USD za svaki dan kršenja. Zaštita prema ECPA-i također obuhvaća neovlašteni pristup ili otkrivanje pohranjenih elektroničkih poruka. Kršitelji su odgovorni za pretrpljene štete ili im se oduzima dobit ostvarena kršenjem.

Telecommunications Act iz 1996. Prema odjeljku 702. vlasnički mrežni podaci o korisniku (CPNI) ne mogu se koristiti u bilo koju drugu svrhu osim pružanja telekomunikacijskih usluga. Pretplatnici mogu uložiti pritužbu Federal Communications Commission-uili podnijeti tužbu pred Saveznim okružnim sudom radi naknade štete i troškovi zastupanja.

Consumer Credit Reporting Reform Act iz 1996. Zakon iz 1996. izmijenio je Fair Credit Reporting Act (FCRA) iz 1970. kako bi zahtijevao bolju obaviještenost i pravo pristupa subjektima kreditnog izvješća. Reform Act također je nametnuo nova ograničenja o prodavateljima podataka o kreditnoj sposobnosti potrošača. Potrošači mogu dobiti odštetu i sudske troškove zbog kršenja.

([11]) Ranije smo poslali Komisiji informacije o sporovima male vrijednosti.

Državni zakoni također štite privatnost u većem broju situacija. Područja u kojima su države poduzele mjere uključuju bankovne ispise, pretplate za kabelsku televiziju, kreditne izvještaje, radne knjižice, vladine evidencije, genetske podatke i zdravstvene kartone, spise o osiguranju, školske evidencije, elektronske komunikacije i posudbe video filmova ([12]).

B. **Izričita zakonska ovlaštenja**

Načela zaštite privatnosti sadrže iznimku ako zakon, propis ili sudska praksa dovode do „proturječnih obveza ili izričitih ovlaštenja, pod uvjetom da pri korištenju takvog ovlaštenja organizacija može pokazati da je njezino nepoštivanje načela ograničeno u mjeri potrebnoj da bi ispunila više zakonske interese koje podupire takvo ovlaštenje". Jasno je da ako pravo SAD-a nameće proturječne obveze, organizacije iz SAD-a bez obzira na to jesu li u „sigurnoj luci" ili nisu, moraju poštovati zakon. Dok je namjera načela „sigurne luke" premostiti razlike između američkog i europskog režima zaštite privatnosti, u pogledu izričitih ovlaštenja dužni smo poštovati posebna zakonska prava naših izabranih zakonodavaca. Ograničeno odstupanje od strogog pridržavanja načela „sigurne luke" usmjereno je na postizanje ravnoteže da bi se zadovoljili zakonski interesi obiju strana.

Iznimka je ograničena na slučajeve kada postoji izričito ovlaštenje. Stoga kad se radi o graničnom slučaju, određeni zakon, propis ili sudska odluka mora odobriti određeno ponašanje organizacija potpisnica sigurnosnih načela ([13]). Drugim riječima, iznimka se ne primjenjuje ako zakon šuti o tome. Osim toga, iznimka se primjenjuje samo kad bi izričito ovlaštenje bilo proturječno s pridržavanjem načela „sigurne luke". Čak i tada, iznimka „je ograničena u onoj mjeri koja je to potrebna da bi se ispunili viši zakonski interesi koje podupire takvo ovlaštenje". Primjera radi, ako zakon posebno ovlašćuje trgovačko društvo da proslijedi osobne podatke vladinome tijelu, iznimka se ne primjenjuje. I obrnuto, ako zakon izričito ovlašćuje trgovačko društvo da proslijedi osobne podatke vladinoj agenciji bez pojedinčeva pristanka, to bi predstavljalo „izričito ovlaštenje" da postupi na način suprotan „sigurnoj luci". Isto tako, određena odstupanja od pozitivnih zahtjeva za obavješćivanje i pristanak bila bi iznimka (budući da je to jednakovrijedno posebnom odobrenju da se podaci otkriju bez obavijesti i pristanka). Na primjer, zakon kojim se ovlašćuje liječnike da daju zdravstvene kartone svojih pacijenata na uvid zdravstvenim službama bez pacijentova prethodnog pristanka mogao bi odobriti izuzeće od načela obavijesti i mogućnosti izbora. Ovo ovlaštenje ne bi dozvoljavalo liječniku da iste zdravstvene kartone da na uvid organizacijama za očuvanje zdravlja ili komercijalnim farmaceutskim istraživačkim laboratorijima, jer bi to prelazilo namjere zakonskog odobrenja i stoga bilo izvan područja primjene iznimke ([14]). Ova konkretna zakonska ovlast može biti „samostalno" ovlaštenje da se postupi na određeni način s osobnim podacima, ali, kao što dolje navedeni primjeri pokazuju, veća je vjerojatnost da to bude iznimka od nekog šireg zakona koji zabranjuje prikupljanje, korištenje ili otkrivanje osobnih podataka.

Telecommunications Act iz 1996.

U većini su slučajeva ovlaštenja za korištenje u skladu sa zahtjevima Direktive i načelima, ili bi korištenje dopustila jedna od drugih dozvoljenih iznimaka. Na primjer, odjeljak 702. Telecommunications Act-a (kodificiranog pod 47 U.S.C. § 222) nameće dužnost telekomunikacijskim operaterima da čuvaju tajnost osobnih podataka do kojih dođu tijekom pružanja svojih usluga korisnicima. Ova odredba izričito dozvoljava telekomunikacijskim operaterima da:

1. koriste korisničke podatke za pružanje telekomunikacijskih usluga, uključujući i objavljivanje imenika s pretplatničkim brojevima;

2. daju korisničke podatke ostalima na pisani zahtjev korisnika; te

3. daju korisničke podatke kao cjelinu.

([12]) Nedavno elektroničko pretraživanje baze podataka Westlaw otkrilo je 994 prijavljena slučaja država koji su se odnosili na odštete i kršenje privatnosti.

([13]) Samo radi objašnjenja, određeno zakonsko tijelo ne mora se izričito pozivati se na načela „sigurne luke".

([14]) Slično tome, liječnik se u ovom primjeru ne bi mogao osloniti na to da zakonska ovlast ima prednost pred pojedinčevim korištenjem mogućnosti odustajanja od izravnog marketinga koju nudi često postavljano pitanje 12. Okvir svake iznimke s „izričitim dopuštenjem" nužno je ograničeno na područje primjene ovlaštenja sukladno s određenim zakonom.

Vidjeti 47 U.S.C. § 222(c)(1)-(3). Zakon također omogućava telekomunikacijskim operaterima da iznimno koriste korisničke podatke:

1. kako bi započeli, pružali, obračunali i naplatili svoje usluge;

2. kako bi pružili zaštitu od neiskrenog ili nezakonitog ponašanja i zloupotrebe; i

3. kako bi pružali telemarketinške, prateće ili administrativne usluge tijekom poziva koji je uputio korisnik ([15]).

Ibid., § 222(d)(1)-(3). Konačno, od telekomunikacijskih operatera se traži da izdavačima telefonskih imenika daju podatke o pretplatnicima, koji mogu uključivati samo imena, adrese, telefonske brojeve i zanimanje poslovnih korisnika. *Ibid*., § 222(e).

Iznimka za „izričito ovlaštenje" mogla bi doći u obzir kada telekomunikacijski operateri koriste privatne mrežne podatke o korisniku za sprečavanje prijevare ili ostalih oblika nezakonitog ponašanja. Čak i ovdje bi se takve parnice mogle smatrati onima „od javnog interesa" i biti dozvoljene u skladu s načelima iz tog razloga.

Pravila koje je predložio Department of Health and Human Services

Department of Health and Human Servicespredložilo je pravila o standardima za privatnost zdravstvenih podataka koji omogućavaju identitificiranje osobe. *Vidjeti* 64 Fed.Reg. 59.918 (2. studeni 1999.) (koji će biti kodificiran pod 45 C.F.R. točke 160-164). Ta bi pravila uvela zahtjeve s obzirom na privatnost iz Health Insurance Portability iz 1996., Pub. L. 104-191. Predložena pravila općenito bi zabranjivala pokrivenim organizacijama (tj. zdravstveni programi, institucije za prikupljanje podataka o zdravstvenoj skrbi i pružatelji zdravstvenih usluga koji prenose zdravstvene podatke u elektroničkom obliku) da koriste ili otkrivaju zaštićene zdravstvene podatke bez pojedinčevog dopuštenja. *Vidjeti* predloženi 45 C.F.R. § 164.506. Predložena pravila bi zahtijevala otkrivanje zaštićenih podataka o zdravlju samo u dvije svrhe: 1. da dozvole pojedincima da pregledaju i kopiraju vlastite zdravstvene podatke, *vidjeti ibid*. § 164.514; i 2. da provedu pravila, *vidjeti ibid*. § 164.522.

Predložena bi pravila dozvolila korištenje ili otkrivanje zaštićenih zdravstvenih podatka bez izričitog ovlaštenja pojedinca u ograničenim okolnostima. To bi, na primjer, uključivalo nadzor nad sustavom zdravstvene zaštite, provedbu zakona i hitne slučajeve. *Vidjeti ibid*. § 164.510. Predložena pravila detaljno navode ograničenja pri takvom korištenju i otkrivanju. Štoviše, dopuštena korištenja i otkrivanja zaštićenih zdravstvenih podataka bila bi ograničena na najmanju potrebnu količinu podataka. *Vidjeti ibid*. at § 164.506.

Dozvoljeni oblici uporabe, koje izričito omogućavaju predloženi propisi, općenito su u skladu s načelima zaštite ili su dopušteni nekom drugom iznimkom. Na primjer, kazneni progon i sudski postupci su dopušteni, kao i medicinska istraživanja. Ostale upotrebe, kao što je nadzor nad zdravstvenim sustavom, djelovanje javnog zdravstva i vladini sustavi zdravstvenih podataka služe javnom interesu. Otkrivanje za izvršavanje plaćanja zdravstvene skrbi i premija potrebno je radi pružanja zdravstvene skrbi. Uporaba u hitnim slučajevima, radi savjetovanja s osobama u srodstvu oko liječenja, ako se pacijentov pristanak „ne može dobiti jer je to neizvedivo ili nerazumno", ili radi utvrđivanja identiteta ili uzroka smrti preminuloga, štiti životne interese osoba čiji se podaci obrađuju i ostalih. Korištenje za upravljanje aktivnim vojnim jedinicama i ostalim posebnim skupinama pojedinaca pomaže pri pravilnom izvršenju vojne misije ili sličnih neizbježnih situacija. U svakom slučaju, takvo će se korištenje slabo ili nikako odnositi na potrošače općenito.

Tako ostaje samo korištenje osobnih podataka u zdravstvenim institucijama kako bi se napravili imenici pacijenata. Iako se takvo korištenje ne bi moglo podići na razinu „životnog" interesa, imenici su korisni kako pacijentima, tako i njihovim

([15]) Područje primjene ove iznimke je vrlo ograničeno. Sukladno s vlastitim uvjetima, telekomunikacijski operater može koristiti privatne mrežne podatke o korisniku samo tijekom poziva koji je uputio korisnik. Nadalje, FCC nas je upozorio da telekomunikacijski operater ne može koristiti privatne mrežne podatke o korisniku za distribuciju usluga izvan okvira korisnikova upita. Konačno, budući da korisnik mora odobriti uporabu privatnih mrežnih podataka o korisniku u ovu svrhu, ova odredba zapravo uopće nije „iznimka".

prijateljima i rodbini. Okvir i ove ovlaštene upotrebe je sam po sebi ograničavajući. Stoga, oslanjanje na iznimku od načela za korištenje koje je „izričito dozvoljeno" zakonom za ovu svrhu predstavlja minimalni rizik za privatnost pacijenata.

Fair Credit Reporting Act

Europska komisija je izrazila zabrinutost da bi iznimka uz „izričito ovlaštenje" „u stvarnosti predstavljala zaključak o primjerenosti" za Fair Credit Reporting Act(FCRA). To ne bi bio slučaj. U nedostatku određenog zaključka o primjerenosti za FCRA, one organizacije iz SAD-a koje bi se inače oslonile na takav zaključak, morale bi obećati da će se pridržavati načela zaštite privatnosti u svim aspektima. To znači da ako zahtjevi iz FCRA-a prelaze razinu zaštite utemeljenu u načelima, organizacije iz SAD-a trebaju poštovati samo FCRA. I obrnuto, ako bi FCRA bio nedovoljan, te bi organizacije trebale uskladiti svoje postupanje prema podacima s načelima. Iznimka ne bi promijenila ovu temeljnu ocjenu. Prema vlastitim odredbama, iznimka se primjenjuje samo ako određeni zakon izričito odobrava ponašanje koje bi bilo u suprotnosti načelima „sigurne luke". Iznimka se ne bi proširivala na područje u kojem zahtjevi FCRA-a jednostavno ne zadovoljavaju načela „sigurne luke" ([16]).

Drugim riječima, nije nam namjera da izuzeće znači da je sve što se ne traži stoga „izričito dopušteno". Nadalje, iznimka se primjenjuje samo kada je ono što je izričito dopušteno prema zakonu SAD-a proturječno zahtjevima načela „sigurne luke". Dotični zakon mora ispunjavati oba ova elementa prije nego što nepoštivanje načela bude dopušteno.

Odjeljak 604. FCRA-a, na primjer, izričito ovlašćuje agencije za izvješćivanje o potrošačima da izdaju izvješća o potrošačima u različitim navedenim situacijama. *Vidjeti* FCRA, § 604. Ako time odjeljak 604. ovlašćuje kreditne registre da postupaju suprotno načelima „sigurne luke", tada bi se kreditni registri trebali osloniti na iznimku (osim, naravno, ako se ne primjenjuju neke druge iznimke). Kreditni registri moraju poštovati sudske odluke i naloge velike porote, a korištenje kreditnog izvješća od strane vladinih tijela koja provode izdavanje dozvola, socijalnu skrb i alimentaciju služi javnoj svrsi. *Ibid*., § 604(a)(1.), (3.)(D), i (4.). Sukladno s tim, kreditni registar ne bi se morao za te svrhe oslanjati na iznimku uz „izričito dopuštenje". Ako postupa u skladu s pismenim napucima potrošača, agencija za izvješćivanje o potrošačima u potpunosti bi poštivala načela zaštite privatnosti. *Ibid*., § 604(O)(2). Isto tako se kreditni izvještaji o potrošačima mogu nabaviti u svrhe zapošljavanja samo uz potrošačevo pisano dopuštenje. (*ibid*., §§ 604(a)(3)(B) i (b)(2)(a)(ii)), a za kreditno poslovanje ili osiguranje koje nije pokrenuo potrošač, samo ako se potrošač nije ogradio od takve prodaje (*ibid*., § 604(c)(1)(B)). FCRA također zabranjuje kreditnim registrima da daju zdravstvene podatke u svrhe zapošljavanja bez pristanka potrošača. *Ibid*., § 604(g). Takvi oblici uporabe su u skladu s načelima obavijesti i mogućnosti izbora. Ostale namjene dozvoljene u odjeljku 604. obuhvaćaju transakcije koje uključuju potrošača i iz tog bi razloga bile dopuštene prema načelima. *Vidjeti ibid*., § 604(a)(3)(A) i (F).

Drugo korištenje „dopušteno" u odjeljku 604. odnosi se na sekundarna kreditna tržišta. *Ibid*., § 604(a)(3)(E). Nema proturječja između korištenja izvješća o potrošačima za ovu svrhu i načela zaštite privatnosti samih po sebi. Istina je da FCRA ne zahtijeva od kreditnih registara, na primjer, da pošalju obavijest i ishode pristanak od potrošača kada objavljuju izvješća s ovom svrhom. Međutim, ponavljamo činjenicu da nepostojanje zahtjeva ne podrazumijeva „izričito dopuštenje" postupanja na drugačiji način nego što je predviđeno. Na sličan način odjeljak 608. dozvoljava kreditnim registrima da daju neke osobne podatke vladinim agencijama. Ovo „dopuštenje" ne bi opravdalo kreditni registar što zanemaruje svoje obveze poštivanja načela „sigurne luke". Ovo se razlikuje od naših ostalih primjera u kojima izuzeće od zahtjeva za obavješćivanje i mogućnošću odabira ima učinak izričitog dopuštenja da se osobni podaci koriste bez obavijesti i mogućnosti izbora.

Zaključak

Čak i iz našeg ograničenog pregleda ovih zakona očito proizlazi sljedeće:

— „Izričito dopuštenje" u zakonu općenito dopušta uporabu ili otkrivanje osobnih podataka bez pojedinčeva prethodnog odobrenja; tako bi iznimka bila ograničena na načela obavijesti i mogućnosti izbora

([16]) Ovo naše razmatranje ne treba shvatiti kao potvrdu da FCRA ne pruža primjerenu zaštitu. Svaka procjena FCRA-e mora razmotriti zaštitu koju pruža zakon u cijelosti, a ne se samo usredotočiti na iznimke kao što to mi ovdje činimo.

— U većini slučajeva, iznimke odobrene zakonom su usko namijenjene primjeni u određenim situacijama za određene svrhe. U svim slučajevima zakon inače zabranjuje neovlašteno korištenje ili otkrivanje osobnih podataka koje ne pripada tim ograničenjima;

— U većini slučajeva, s obzirom na njihovu zakonitu prirodu, ovlašteno korištenje ili otkrivanje služi javnom interesu;

— U gotovo svim slučajevima ovlaštene upotrebe su ili potpuno u skladu s načelima zaštite privatnosti ili pripadaju jednoj od ostalih mogućih iznimaka.

Zaključak je da će iznimka uz „izričito dopuštenje" zakonom, po svojoj prirodi, vjerojatno imati prilično ograničeno područje primjene.

C. **Spajanja i preuzimanja**

Radna skupina iz članka 29. je izrazila zabrinutost u vezi sa situacijama kada organizaciju koja je potpisnica načela „sigurne luke" preuzima ili pripaja poduzeće koje se nije obvezalo primjenjivati načela „sigurne luke". Čini se, međutim, da je radna skupina pretpostavila da preživjelo poduzeće ne bi moralo primjenjivati načela „sigurne luke"na osobne podatke koje čuva preuzeto poduzeće, ali to nije nužno slučaj prema pravu SAD-a. Opće pravilo u Sjedinjenim Američkim Državama o spajanjima i preuzimanjima kaže da trgovačko društvo koje stječe glavne dionice drugog poduzeća općenito preuzima obveze i odgovornosti stečene tvrtke. *Vidjeti* 15 *Fletcher Cyclopedia of the Law of Private Corporations* § 7117 (1990.); *vidjeti također Model Bus. Corp. Act* § 11.06(3) (1979.) („preživjelo trgovačko društvo ima sve odgovornosti svakog pripojenog društva"). Drugim riječima, tvrtka koja nastane spajanjem ili preuzimanjem organizacije potpisnice načela „sigurne luke" prema ovoj bi metodi bila obvezana obvezama ove potonje.

Štoviše, čak i ako je spajanje ili preuzimanje izvršeno stjecanjem imovine, odgovornosti kupljenog poduzeća mogu svejedno obvezivati tvrtku stjecatelja u određenim okolnostima. 15 Fletcher, § 7122. Čak i kad odgovornosti ne bi nadživjele spajanje, važno je napomenuti da ne bi preživjele spajanje čak ni ako su podaci prenijeti iz Europe u skladu s ugovorom – jedinom održivom alternativom zaštiti privatnosti za prijenose podataka u Sjedinjene Američke Države. Osim toga, dokumenti o „sigurnoj luci" koji su pregledani sada zahtijevaju od svake organizacije potpisnice načela da obavijesti Department of Commerce o preuzimanju i dozvoljavaju nastavak prenošenja podataka u nasljednu organizaciju samo ako nasljedna organizacija pristupi načelima „sigurne luke". *Vidjeti često postavljeno pitanje 6*. Sjedinjene Američke Države su sada preinačile okvir „sigurne luke" tako da zahtijevaju od organizacija iz SAD-a da u ovakvoj situaciji obrišu podatke koje su primile u sklopu okvira „sigurne luke", ako se njihove obveze zaštite neće nastaviti ili ako nisu uvedene druge odgovarajuće zaštite.

PRILOG V.

14. srpnja 2000.

John Mogg
Direktor, DG XV.
Europska Komisija
Ured C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles

Poštovani gospodine Mogg,

Svjestan sam da su iskrsnula mnogobrojna pitanja vezana za moje pismo koje sam Vam uputio 29. ožujka 2000. Da pobliže objasnim naše ovlasti u onim područjima za koja su vezana postavljena pitanja, šaljem Vam ovo pismo koje se, zbog budućeg lakšeg snalaženja, nastavlja na prethodno i daje kratki pregled teksta prethodnog pisma.

Za vrijeme Vaših posjeta našim uredima i u Vašim dopisima postavili ste nekoliko pitanja o ovlastima Federal Trade Commission SAD-a (FTC) u području privatnosti pri korištenju Interneta. Smatram da bi bilo korisno dati sažet prikaz mojih prethodnih odgovora vezanih za aktivnosti FTC-a u ovom području, kao i dodatne informacije o nadležnosti agencije u području pitanja vezanih za zaštitu privatnosti potrošača koja postavljate u Vašem zadnjem pismu. Vi konkretno pitate: 1. je li FTC nadležan za prijenos podataka vezanih uz radni odnos ako je izvršen uz kršenje načela zaštite; 2. je li FTC nadležan za neprofitne programe s „pečatom" kao jamstvom zaštite privatnosti; 3. da li se Zakon o FTC-u jednako primjenjuje na svijet izvan i unutar Interneta; i 4. što se događa kada se nadležnost FTC-a preklapa s nadležnošću drugih tijela izvršavanja.

Primjena FTC Act-a na zaštitu privatnosti

Kao što znate, u proteklih pet godina, FTC je preuzeo vodeću ulogu u podupiranju nastojanja industrije SAD-a i potrošačkih skupina da razviju cjelovit odgovor na pitanja vezana za zaštitu potrošača, uključujući i prikupljanje i korištenje osobnih podataka na internetu. Javnim radionicama i stalnim savjetovanjima s predstavnicima industrije, potrošača i našim kolegama iz Departement of Commerce-a i iz cijele Vlade SAD-a, uspjeli smo utvrditi ključna pitanja politike i izraditi odgovarajuća rješenja.

Zakonska ovlast koju ima Federal Trade Commission u ovom području nalazi se u odjeljku 5. Federal Trade Commission Act („FTC Act") koji zabranjuje „nepoštene i prijevarne radnje i postupke" u trgovini ili koje utječu na trgovinu ([1]). Prijevarni postupak je definiran kao predstavljanje, propust ili postupak koji će vjerojatno znatno dovesti u zabludu razborite potrošače. Postupak je nepošten ako uzrokuje ili će vjerojatno uzrokovati značajnu štetu potrošačima, a koja se ne može izbjeći razboritošću i koju ne nadvladava protuteža koristi za potrošača ili konkurenciju ([2]).

Određeni postupci prikupljanja informacija lako mogu kršiti FTC Act. Npr. u slučaju da internetska stranica lažno tvrdi da poštuje navedenu politiku zaštite privatnosti ili skup samoregulirajućih smjernica, odjeljak 5. FTC Act-a pruža pravnu osnovu za smatranje takvog lažnog predstavljanja prijevarnim postupkom. Zaista smo uspješno provodili zakon kako bismo uspostavili ovo načelo ([3]). Osim toga, Komisija je zauzela stav da može imenovati posebno loše postupke prema privatnosti kao nepoštene sukladno odjeljku 5. ako takvi postupci uključuju djecu ili korištenje vrlo osjetljivih podataka, kao što su financijski podaci ([4]) i zdravstveni kartoni. Federal Trade Commission provodila je i nastavit će provoditi takve aktivnosti provedbe zakona putem aktivnog nadgledanja i istraživanja, te rješavanjem primjedaba koje dobijemo od samoregulirajućih organizacija i drugih, uključujući i države članice Europske unije.

([1]) 15 U.S.C. § 45. Fair Credit Reporting Act također bi se primjenjivao na prikupljanje i prodaju podataka na Internetu koji zadovoljavaju zakonsku definiciju „izvješća o potrošačima" i „kreditnih registara".
([2]) 15 U.S.C. § 45 (n).
([3]) Vidjeti: GeoCities, Docket No. C-3849 (Konačno rješenje 12. veljače 1999.) (nalazi se na stranici www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No. C-3891 (Konačno rješenje 12. kolovoza 1999.) (nalazi se na stranici www.ftc.gov/opa/1999/9905/younginvestor.htm). Vidjeti također: Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Dio 312 (nalazi se na stranici www.ftc.gov/opa/1999/9910/childfinal.htm). Pravilo COPPA-e koje je stupilo na snagu prošlog mjeseca zahtjeva od operatera internetskih stranica namijenjenih djeci ispod 13 godina ili koji svjesno prikupljaju osobne podatke od djece mlađe od 13 godina da primjenjuju standarde poštenih postupaka informiranja proglašene u Pravilu.
([4]) Vidjeti FTC v. Touch Tone, Inc., Građanska parnica broj 99-WM-783 (D.Co.) (uložena 21. travnja 1999.) na stranici www.ftc.gov/opa/1999/9904/touchtone.htm. Pismo mišljenja osoblja od 17. srpnja 1997. izdano kao odgovor na peticiju koju je uložio Center for Media Education, na stranici: www.ftc.gov/os/1997/9707/cenmed.htm.

FTC-ova podrška samoregulaciji

FTC već dugo podržava napore industrije u razvijanju učinkovitih samoregulirajućih programa koji bi osigurali zaštitu privatnosti potrošača na Internetu. Međutim, da ti napori uspiju, članovi industrije moraju sudjelovati u njima u velikom broju. Istodobno samoregulacija mora biti podržana provedbom zakona. Zbog tih će razloga FTC dati prednost primjedbama o nepridržavanju smjernica samoregulacije primljenima od organizacija kao što su BBOnline i TRUSTe. Ovaj će pristup biti u skladu s našom dugogodišnjom suradnjom s National Advertising Review Board (NARB) u okviru Better Business Bureau, koji upućuje žalbe na reklame FTC-u. National Advertising Division (NAD) pri NARB-u rješava žalbe vezane za nacionalno oglašavanje putem pravosudnog postupka. Kad stranka odbije pridržavati se odluke NAD-a, predmet se upućuje FTC-u. Zaposlenici FTC-a pregledavaju sporno oglašavanje po načelu prioriteta da utvrde krši li se Zakon o FTC-u i često uspijevaju zaustaviti sporno ponašanje ili uvjeriti stranke da nastave sudjelovati u postupku NARB-a.

Slično, FTC će dati prednost obavijestima o nepridržavanju načela „sigurne luke" od država članica EU-a. Kao i u slučaju obavijesti od samoregulirajućih organizacija iz SAD-a, naši će zaposlenici uzeti u obzir sve informacije koje dokazuju krši li postupak na koji je uložena žalba odjeljak 5. Zakona o FTC-u. Ova obaveza može se pronaći i u načelima zaštite pod često postavljanim pitanjem (često postavljana pitanja 11) o provedbi.

GeoCities: FTC-ov prvi slučaj zaštite privatnosti na Internetu

Prvi slučaj zaštite privatnosti na Internetu s kojim se susrela Federal Trade Commission, GeoCities, temeljio se na ovlastima Komisije prema odjeljku 5 ([5]). U tom je slučaju FTC tvrdio da je GeoCities pogrešno prikazivao odraslima i djeci kako će se koristiti njihovi osobni podaci. FTC-ov je prigovor tvrdio da je GeoCities pogrešno naveo da će određene osobne identifikacijske podatke koje je prikupio na svojoj internetskoj stranici koristiti isključivo u interne svrhe ili da potrošačima dostavi određene reklamne ponude i proizvode ili usluge koje su tražili, te da se određeni dodatni „neobavezni" podaci neće nikome prenijeti bez potrošačeve dozvole. Zapravo su ovi podaci otkriveni trećim osobama koje su ih koristile za pridobivanje članova za ono na što član nije pristao. Prigovor je dakle teretio GeoCities za sudjelovanje u prijevarnim radnjama vezanim uz prikupljanje podataka od djece. Sukladno FEC-ovom prigovoru, GeoCities je naveo da sam upravlja segmentom svoje internetske stranice za djecu i da podatke koje se tamo prikuplja vodi isključivo GeoCities. Zapravo su ta područja na internetskoj stranici vodile treće strane koje su prikupljale i čuvale podatke.

Nagodba zabranjuje društvu GeoCities pogrešno prikazivanje svrhe za koju prikuplja ili koristi osobne identifikacijske podatke potrošača ili o potrošačima, uključujući i djecu. Odluka zahtjeva od GeoCitiesa da javno objavi na svojoj internetskoj stranici jasnu i istaknutu „obavijest o zaštiti privatnosti" u kojoj se potrošačima navodi koji se podaci prikupljaju i u koju svrhu, kome će se otkriti i kako potrošači mogu imati pristup podacima i ukloniti ih. Da se osigura roditeljski nadzor, prema nagodbi GeoCities također mora dobiti dopuštenje roditelja prije prikupljanja osobnih identifikacijskih podataka od djece do 12 godina starosti. Prema odluci GeoCities mora obavijestiti svoje članove i pružiti im priliku da obrišu svoje podatke iz baza podataka GeoCitiesa i svih trećih osoba. Nagodba posebno zahtijeva da GeoCities obavijesti roditelje djece do 12 godina starosti da izbrišu svoje podatke, osim ako roditelj da pristanak da se oni zadrže i koriste. Konačno, GeoCities također mora kontaktirati i treće osobe kojima je prethodno otkrio podatke i zahtijevati da i one isto tako izbrišu te podatke ([6]).

ReverseAuction.com

Nedavno je ova agencija pokrenula postupak kojim se upućuje prigovor povodom navodnog kršenja zaštite privatnosti od strane nekog drugog internetskog društva. U siječnju 2000. Komisija je odobrila tužbu protiv, i Ugovor o suglasnosti sa, ReverseAuction.com, internetskom stranicom za aukcije koja je navodno dobila osobne identifikacijske podatke potrošača s konkurentne stranice (eBay.com) i tada je slao prijevarne, samoinicijativne poruke elektroničkom poštom onim potrošačima koji su pretraživali njihovu poslovnu djelatnost ([7]). Naša tužba je tvrdila da je društvo ReverseAuction prekršilo

([5]) GeoCities, Docket No. C-3849 (Konačno rješenje 12. veljače 1999.) (nalazi se na stranici www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([6]) Komisija je naknadno riješila drugi predmet koji je uključivao prikupljanje osobnih podataka od djece na Internetu. Društvo Liberty Financial Companies, Inc. upravljalo je web stranicom „Young Investor" namijenjenoj djeci i tinejdžerima, a bavila se tematikom vezanom za novac i ulaganje. Komisija je tvrdila da je internetska stranica lažno navela da se osobni podaci prikupljeni od djece putem ankete čuvaju anonimno i da će se sudionicima poslati e-mail glasnik, kao i nagrade. Zapravo su osobni podaci o djetetu i financijama njegove obitelji bili čuvani na način koji se može utvrditi, a e-mail glasnik i nagrade nisu poslane. Ugovor o suglasnosti zabranjuje takva lažna prikazivanja u budućnosti i zahtijeva od Liberty Financiala da objavi obavijest o zaštiti privatnosti na internetskim stranicama za djecu i da mora dobiti dopuštenje roditelja koje se može provjeriti prije prikupljanja osobnih identifikacijskih podataka od djece. Liberty Financial Cos., Docket No. C-3891 (Konačno rješenje 12. kolovoza 1999.) (nalazi se na stranici www.ftc.gov/opa/1999/9905/younginvestor.htm).

([7]) Vidjeti ReverseAuction.com, Inc., Tužba br. 000032 (D.D.C.) (uložena 6. siječnja 2000.) (priopćenje za tisak i odgovor na tužbu nalaze se na www.ftc.gov/opa/2000/01/reverse4.htm).

odjeljak 5. Zakona o FTC-u prikupljanjem osobnih identifikacijskih podataka koji su uključivali internetske adrese i osobne korisničke identifikacijske nazive („korisničke lozinke") korisnika eBay-a i slanjem prijevarnih elektroničkih poruka.

Kao što je opisano u tužbi, ReverseAuction se prije prikupljanja podataka registrirao kao korisnik eBaya i prihvatio da će se pridržavati eBay-evog ugovora o korištenju i politike zaštite privatnosti. Ugovor i politika štite privatnost klijenata tako što sprečavaju korisnike eBay-a u prikupljanju i korištenju osobnih identifikacijskih podataka u neslužbene svrhe, kao što je slanje samoinicijativnih komercijalnih elektroničkih poruka. Stoga je naša tužba prvo tvrdila da je društvo ReverseAuction lažno navela da će se pridržavati eBay-evog ugovora o korištenju i politike zaštite privatnosti, što čini prijevarni postupak sukladno odjeljku 5. Kao alternativa, u tužbi se tvrdi da je ReverseAuction koristio podatke u svrhu slanja samoinicijativnih komercijalnih elektroničkih poruka, pri čemu se krši ugovor o korištenju i politika zaštite privatnosti, što je predstavljalo nepoštenu trgovačku praksu sukladno odjeljku 5.

Kao drugo, tužba je tvrdila da su elektroničke poruke namijenjene potrošačima sadržavale prijevaran naziv poruke kojim se potrošače informiralo da će im korisničke lozinke „uskoro isteći". Konačno, u tužbi je navedeno da su elektroničke poruke lažno predstavljale da je eBay izravno ili neizravno pružao društvu ReverseAuction podatke o osobnim identifikacijskim podacima potrošača ili na neki drugi način sudjelovao u širenju samoinicijativnih elektroničkih poruka.

Nagodba koju je FTC izborio zabranjuje društvu ReverseAuction da čini ovakve prekršaje u budućnosti. Ona također zahtijeva od društva ReverseAuction da obavijesti potrošače koji su se registrirali ili će se registrirati kod društva ReverseAuction zbog primitka elektroničke poruke od društva ReverseAuction. Obaviješću se obavješćuje te potrošače da njihove korisničke lozinke na eBayu ne istječu i da eBay nije znao niti ovlastio ReverseAuction za slanje samoinicijativnih elektroničkih poruka. Obavijest također pruža tim potrošačima mogućnost da otkažu registraciju kod društva ReverseAuction i da im se osobni identifikacijski podaci izbrišu iz njihove baze podataka. Osim toga, odluka zahtijeva od društva ReverseAuction da izbriše i da ne koristi ili otkriva osobne identifikacijske podatke članova eBay-a koji su primili elektroničku poštu ReverseAuctiona, ali koji se nisu registrirali kod njih. Konačno, sukladno s prethodnim odlukama o zaštiti privatnosti koje je ostvarila ova agencija, nagodba zahtijeva od društva ReverseAuction da objavi svoju politiku čuvanja privatnosti na svojoj internetskoj stranici, te sadrži opsežne odredbe o vođenju evidencije koje omogućuju FTC-u praćenje njezinog pridržavanja.

Slučaj društva ReverseAuction pokazuje da se FTC posvetio korištenju provedbe zakona u svrhu podupiranja napora industrije za samoregulacijom u području zaštite privatnosti korisnika Interneta. Zaista, ovaj slučaj je izravno osporio ponašanje koje potkopava politiku čuvanja privatnosti i ugovor o korištenju koji štiti privatnost potrošača i koji je mogao potkopati povjerenje potrošača u mjere zaštite privatnosti koje su poduzela online trgovačka društva. Budući da je ovaj slučaj uključivao pronevjeru podataka o potrošačima koji su bili zaštićeni politikom zaštite privatnosti jednog društva od strane drugog društva, on bi također mogao biti od posebnog značaja za rješavanje zabrinutosti zbog zaštite privatnosti uzrokovane prijenosom podataka između trgovačkih društava u raznim zemljama.

Neovisno o akcijama provedbe Zakona o FTC-u u društvima GeoCities, Liberty Financial Cos. i ReverseAuction, ovlasti agencije u nekim područjima online privatnosti su nešto više ograničene. Kao što je gore navedeno, kako bi prikupljanje i korištenje osobnih podataka bez pristanka potpadalo pod Zakon o FTC-u, ono mora uključivati prijevarne ili nepoštene trgovačke postupke. Stoga se Zakon o FTC-u vjerojatno ne može primijeniti na postupke internetske stranice koja je prikupljala osobne identifikacijske podatke od potrošača, ali nije lažno prikazivala svrhu za koju su ti podaci bili prikupljani i korišteni ili koja je otkrivala podatke na način koji će vjerojatno uzrokovati značajnu štetu potrošačima. Isto tako ne mora biti u okviru FTC-ove ovlasti da općenito zahtijeva da se tijela koja prikupljaju podatke na Internetu moraju pridržavati politike zaštite privatnosti ili bilo koje određene politike zaštite privatnosti ([8]). Međutim, kao što je gore navedeno, ako se trgovačko društvo ne pridržava navedene politike zaštite privatnosti to vjerojatno predstavlja prijevarni postupak.

([8]) To je razlog zašto je Federal Trade Commission u svom obraćanju Kongresu navela da je vjerojatno potrebno dodatno zakonodavstvo koje bi naložilo da se sve komercijalne internetske stranice u SAD-u koje su usmjerene prema potrošačima pridržavaju navedenih poštenih postupaka vezanih uz prikupljanje podataka. „Consumer Privacy on the World Wide Web". Pred Subcommittee on Telecommunications, Trade and Consumer Protection, House Committee on Commerce United States House of Representatives, 21. srpnja 1998. (obraćanje se može naći na www.ftc.gov/os/9807/privac98.htm) FTC je odgodio poziv na donošenje takvog zakonodavstva kako bi dao priliku samoregulacijskim naporima da pokažu široku prihvaćenost pravednih postupaka prikupljanja podataka na web stranicama. U FTC-ovom izvješću „Privacy Online: A Report to Congress", lipanj 1998. (izvješće se može naći na www.ftc.gov/reports/privacy3/toc.htm), FTC je preporučio da zakonodavstvo zahtijeva da komercijalne internetske stranice prvo dobiju dopuštenje roditelja prije prikupljanja osobnih identifikacijskih podataka od djece mlađe od 13 godina. Vidjeti bilješku na dnu stranice 3 supra. Prošlogodišnje izvješće Komisije „Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress" iz srpnja 1999. (izvješće se može pronaći na www.ftc.gov/os/1999/9907/index.htm#13,) vidjeti značajan napredak u samoregulaciji i stoga je FTC odlučila da trenutno ne preporuči to zakonodavstvo. Komisija će sljedećih tjedana podnijeti izvješće Kongresu o napretku samoregulacije.

Nadalje, nadležnost FTC-a u ovom području obuhvaća nepoštene ili prijevarne postupke samo ako su oni „unutar trgovačke djelatnosti ili na nju utječu". Prikupljanje podataka od strane komercijalnih tijela koja promoviraju proizvode ili usluge, uključujući prikupljanje i korištenje podataka u komercijalne svrhe, vjerojatno će zadovoljiti preduvjet „trgovačke djelatnosti". S druge strane, mnogi pojedinci ili tijela mogu prikupljati podatke na Internetu u nekomercijalne svrhe i stoga mogu biti izvan nadležnosti Savezne trgovinske komisije. Primjer takvog ograničenja uključuje „chat rooms" ako njima upravljaju nekomercijalna tijela, npr. dobrotvorne organizacije.

Konačno, postoji nekoliko potpunih ili djelomičnih izuzetaka od FTC-ove osnovne nadležnosti nad trgovačkim postupcima koji ograničavaju FTC-ovu sposobnost pružanja cjelovitog odgovora na probleme privatnosti na Internetu. Oni uključuju izuzetke za mnoge poslovne aktivnosti potrošača u kojima se izmjenjuju brojne informacije kao što su bankovno poslovanje, poslovanje s osiguravajućim društvima i zrakoplovnim kompanijama. Kao što znate, ostale bi federalne ili državne agencije imale nadležnost nad tim tijelima, kao što su savezne bankovne agencije ili Department of Transportation.

U slučajevima u kojima je FTC nadležan, FTC prihvaća i ako mu to sredstva dozvoljavaju odgovara na pritužbe potrošača koje prima poštanskim ili telefonskim putem u Consumer Response Center („CRC") te odnedavno na svojoj internetskoj stranici ([9]). CRC prihvaća pritužbe od svih potrošača, uključujući i onih koji imaju prebivalište u državama članicama Europske unije. FTC Act pruža Federal Trade Commission nepristranu moć dobivanja pravne zaštite protiv budućih kršenja Zakona o FTC-u kao i naknadu za potrošače koji su oštećeni. Mi bismo, međutim, provjerili je li trgovačko društvo pokazalo obrazac nepoštenog ponašanja, jer ne rješavamo pojedinačne sporove potrošača. U prošlosti je Federal Trade Commission pružala naknadu građanima iz SAD-a i iz ostalih zemalja ([10]). FTC će nastaviti nametati svoj autoritet u odgovarajućim slučajevima da bi osigurala naknadu građanima drugih zemalja koji su oštećeni prijevarnim postupcima koji potpadaju pod njezinu nadležnost.

Podaci o radnom odnosu

U Vašem najnovijem pismu tražili ste dodatno objašnjenje vezano uz nadležnost FCT-a u području podataka o radnom odnosu. Prvo ste postavili pitanje bi li FTC mogao poduzeti mjeru prema odjeljku 5. protiv društva koje tvrdi da se pridržava načela zaštite privatnosti SAD-a, ali prenosi ili koristi podatke vezane za radni odnos na način koji krši ova načela. Jamčimo Vam da smo pažljivo pregledali zakonodavstvo koje ovlašćuje FTC, za to vezane dokumente i relevantnu sudsku praksu, te smo zaključili da FTC ima jednaku nadležnost za podatke vezane za radni odnos kao što bi općenito imao sukladno s odjeljkom 5. Zakona o FTC-u ([11]). To znači, ako bi slučaj zadovoljavao naše sadašnje kriterije (nepoštenje ili prijevaru) za postupak provedbe mjere vezane za zaštitu privatnosti, mogli bismo pokrenuti postupak u situaciji kada su podaci vezani za radni odnos.

Također želimo raspršiti sumnje u to da je sposobnost FTC-a da poduzme mjere za provedbu zaštite privatnosti ograničena isključivo na situacije kada društvo prevari potrošače kao pojedince. Zapravo, kao što to jasno predočava najnoviji postupak Komisije vezan za ReverseAuction ([12]), FTC će poduzeti mjere za provedbu zaštite privatnosti u situacijama koje uključuju prijenos podataka između društava, tamo gdje je jedno društvo navodno postupilo nezakonito prema drugom društvu, što vodi do moguće štete potrošačima i društvima. Očekujemo da će se u toj situaciji najvjerojatnije postaviti pitanje radnog odnosa, jer se podaci o radnom odnosu Europljana prenose iz europskih društava u američka društva koja su se obavezala da će se pridržavati načela „sigurne luke".

Međutim, želimo naglasiti jednu okolnost u kojoj bi FTC-ova mjera bila ograničena. To bi se dogodilo u situacijama u kojima se spor već počeo rješavati pri Nacionalnom odboru za radne odnose u tradicionalnom kontekstu rješavanja radnopravnog spora, najvjerojatnije vezano za arbitražu u slučaju pritužbi, ili pritužbu na nepravedno postupanje na radnom mjestu.

([9]) Vidjeti: http://www.ftc.gov/ftc/complaint.htm za FTC-ov internetski obrazac za pritužbe.

([10]) Na primjer, u nedavnom slučaju koji uključuje internetsku piramidalnu shemu, Komisija je primila odštete za 15 622 potrošača u ukupnom iznosu od cca. USD 5,5 milijuna. Potrošači su imali prebivalište u SAD-u i 70 stranih zemalja. Vidjeti: www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([11]) Osim ako je posebno izuzeta temeljem statua o FTC-ovim ovlastima, nadležnost FTC-a sukladno sa Zakonom o FTC-u u postupcima „u trgovini ili koja utječe na trgovinu" preklapa se s konstitucionalnim ovlastima Kongresa prema Klauzuli o trgovini, Sjedinjene Američke Države protiv American Building Maintenance Industries, 422 U.S. 271, 277, n. 6 (1975.). Nadležnost FTC-a stoga obuhvaća praksu vezanu uz radni odnos u trgovačkim društvima i industrijama u međunarodnoj trgovini.

([12]) Vidjeti „Online Auction Site Settles FTC Privacy Charges", FTC-ovo izvješće za medije (6. siječnja 2000.) – nalazi se na stranici http://www.ftc.gov/opa/2000/01/reverse4.htm.

Ovo bi se moglo dogoditi ako se npr. neki poslodavac obvezao u kolektivnom pregovaračkom ugovoru vezanom za korištenje osobnih podataka, a zaposlenik ili sindikat tvrdi da je poslodavac prekršio taj ugovor. Komisija bi vjerojatno prihvatila mišljenje tog tijela ([13]).

Nadležnost nad programima s „pečatom"

Drugo, pitate bi li FTC imao nadležnost nad programima s „pečatom" koji upravljaju mehanizmima rješavanja sporova u SAD-u koji su lažno predstavili svoju ulogu u provedbi načela zaštite i u rješavanju pritužbi pojedinaca, čak i kad su ta tijela tehnički bila „neprofitna". Pri utvrđivanju imamo li nadležnost nad tijelom koje se naziva neprofitnim, Komisija detaljno analizira da li to tijelo, dok ne stvara dobit za sebe, povećava profit svojih članova. Komisija je uspješno nametnula svoju nadležnost nad takvim tijelima i nedavno je 24. svibnja 1999. Vrhovni sud Sjedinjenih Država u slučaju California Dental Association protiv Federal Trade Commission jednoglasno potvrdio nadležnost FTC-a nad dobrovoljnim neprofitnim udruženjem lokalnih stomatoloških udruga u predmetu za suzbijanje zlouporabe monopolskog položaja. Vrhovni sud je odlučio:

Zakon o FTC-u ne štedi truda uključiti ne samo tijela „organizirana da provode poslovne aktivnosti za svoju dobit" 15 U.S.C. § 44, već i ona koja provode poslovne aktivnosti za dobit „svojih članova". …Teško bi bilo za pretpostaviti da je Kongres tako usko shvatio pojam skrivenih podupirućih organizacija i time stvorio mogućnost zaobilaska nadležnosti tamo gdje bi namjene Zakon o FTC-u očito trebale nametnuti tu nadležnost.

Ukratko, određivanje treba li nametnuti nadležnost nad određenim „neprofitnim" tijelom provodeći program s „pečatom" zahtijeva činjenični pregled opsega u kojem je to tijelo osiguravalo ekonomsku korist svojim „profitnim" članovima. Ako bi takvo tijelo upravljalo svojim pečatnim programom tako da bi osiguralo ekonomsku korist svojim članovima, FTC bi vjerojatno nametnuo svoju nadležnosti. Osim toga, FTC bi vjerojatno imala nadležnost nad prijevarnim programom s „pečatom" koji lažno prikazuje svoj status kao neprofitno tijelo.

Privatnost u svijetu izvan interneta

Treće, primjećujete da je naša prethodna korespondencija bila usmjerena na privatnost u svijetu interneta. Dok je online privatnost glavna briga FTC-a kao kritična komponenta za razvoj elektroničkog trgovanja, Zakon o FTC-u datira iz 1914. godine i jednako se primjenjuje i na svijet van Interneta. Stoga možemo goniti trgovačka društva koja se ne bave internetskim poslovanjem, a koja se upuštaju u nepoštene ili prijevarne trgovinske postupke obzirom na privatnost potrošača ([14]). Zapravo u slučaju kojeg je Komisija pokrenula prošle godine, FTC protiv TouchTone Information, Inc. ([15]) „informacijski burzovni mešetar" je optužen da je ilegalno primao i prodavao privatne financijske podatke potrošača. Komisija je tvrdila da je TouchTone primio podatke o potrošačima „pod izlikom". Ovaj su izraz skovali privatni istražitelji da opišu praksu dobivanja osobnih podataka o drugima pod lažnim navodima, obično telefonom. Slučaj, koji je arhiviran 21. travnja 1999. na Saveznom sudu u Koloradu, traži sudsku zabranu i svu nezakonito stečenu dobit.

Preklapanje sudske nadležnosti

Konačno postavljate pitanje međudjelovanja FTC-ove nadležnosti i nadležnosti ostalih agencija za provedbu zakona, posebno u slučajevima kad postoji preklapanje nadležnosti.

([13]) Određivanje je li određeno ponašanje „nepravedan radni postupak" ili kršenje kolektivnog pregovaračkog ugovora tehničke prirode i obično je li rezerviran za stručne sudove za radne sporove koji će saslušati prigovore, kao što su arbitri ili NRLB.

([14]) Kao što znate iz prethodnih rasprava, Fair Credit Reporting Act također daje ovlaštenje FTC-u da zaštiti financijsku privatnost potrošača u sklopu područja primjene Zakona i Komisija je nedavno izdala odluku u vezi s tim predmetom. Vidjeti predmet Trans Union, broj djelovodnika 9255 (1. ožujka 2000.) (izvješće za medije i mišljenje se nalaze na www.ftc.gov/os/2000/03/index.htm#1).

([15]) Građanski postupak 99-WM-.783 (D.Colo.) (nalazi se na adresi http://www.ftc.gov/opa/1999/9904/touchtone.htm) (odluka o načelnoj suglasnosti još nije donesena).

Razvili smo blisku suradnju s mnogobrojnim drugim agencijama za provedbu zakona, uključujući savezne bankovne agencije i državne tužitelje. Vrlo često usklađujemo istraživanja da bismo što bolje iskoristili svoja sredstva u slučajevima preklapanja nadležnosti. Također često upućujemo predmete odgovarajućoj saveznoj ili državnoj agenciji na istraživanje.

Nadam se da će Vam ovaj pregled biti od pomoći. Molim Vas da me obavijestite ako su Vam potrebne neke dodatne informacije.

S poštovanjem,

Robert Pitofsky

PRILOG VI.

John Mogg
Direktor, DG XV.
Europska Komisija
Ured C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles

Poštovani glavni direktore Mogg,

Pišem Vam ovo pismo na zahtjev Department of Commerce SAD-a da objasnim ulogu Department of Transportation u zaštiti privatnosti potrošača u odnosu na podatke koje im dostavljaju zrakoplovne tvrtke.

Department of Transportation potiče samoregulaciju kao najmanje nametljivo i najučinkovitije sredstvo za osiguranje privatnosti podataka koje korisnici daju zrakoplovnim tvrtkama, te stoga podržava uspostavu režima „sigurne luke" koji bi omogućio zrakoplovnim tvrtkama da poštuju zahtjeve Direktive Europske unije o privatnosti s obzirom na prijenosa izvan EU-a. Međutim, Department priznaje da je za funkcioniranje samoregulacije potrebno da se zrakoplovne tvrtke koje se obvežu na načela privatnosti utvrđena režimom „sigurne luke" doista i pridržavaju istih. U tom se pogledu samoregulaciju treba podržati provedbom zakona. Stoga, koristeći svoju postojeću zakonsku ovlast za zaštitu potrošača, Departement će osigurati da zrakoplovne tvrtke poštuju obveze zaštite privatnost koje su preuzele prema javnosti, te će prosljeđivati napomene o navodnom nepoštivanju koje je primilo od samoregulatornih organizacija i ostalih, uključujući i države članice Europske unije.

Ovlast Department-a da poduzima provedbene mjere u ovom području proizlazi iz 49 U.S.C. 41712 koji zabranjuje prijevozniku „nepoštene ili prijevarne postupke, ili nelojalan način konkurencije" u prodaji zračnoga prijevoza, koji uzrokuju ili mogu izazvati štetu potrošaču. Odjeljak 41712 je sastavljeno po uzoru na odjeljak 5. Federal Trade Commission Act-a (15 U.S.C. 45). Međutim, zračni prijevoznici su na temelju 15 U.S.C. 45(a)(2) izuzeti od propisa Federal Trade Commission-a iz odjeljka 5.

Moj ured istražuje i tuži slučajeve sukladno s 49 U.S.C. 41712. (Vidjeti npr. propise Department of Transportation 99-11-5, 9. studenoga 1999.; 99-8-23, 26. kolovoza 1999.; 99-6-1, 1. lipnja 1999.; 98-6-24, 22. lipnja. 1998.; 98-6-21, 19. lipnja 1998.; 98-5-31, 22. svibnja 1998. i 97-12-23, 18. prosinca 1997.). Takve slučajeve pokrećemo na temelju vlastitih istraga, kao i službenih i neslužbenih pritužbi koje primimo od pojedinaca, putničkih agencija, zrakoplovnih tvrtki, te vladinih agencija iz SAD-a i inozemstva.

Želio bih istaknuti da prijevoznikovo nečuvanje privatnosti podataka koje dobije od putnika ne bi samo po sebi bilo kršenje odjeljka 41712. Međutim, jednom kad se prijevoznik službeno i javno obveže da će sukladno načelu zaštite privatnosti čuvati privatnost podataka o potrošaču koje dobije, Department bi bio ovlašten koristiti zakonske ovlasti iz odjeljka 41712 da osigura poštovanje tih načela. Stoga, jednom kada putnik da podatke prijevozniku koji se obvezao poštovati načela „sigurne luke", svako nepridržavanje istih bi vjerojatno nanijelo štetu potrošaču i predstavljalo bi kršenje odjeljka 41712. Moj ured bi dao veliku prednost istrazi takve navodne radnje i gonjenju svakog slučaja koji dokazuje takvu radnju. Također ćemo savjetovati Department of Commerce SAD-a o ishodu svakog takvog slučaja.

Kršenje odjeljka 41712 može dovesti do izdavanja sudskih naloga za suspenziju i izricanja građanskih kazni zbog kršenja ovih naloga. Iako nemamo ovlast za dodjelu odšteta ili novčanih naknada tužiteljima pojedincima, imamo ovlast potvrditi nagodbe kojima se zaključuju istrage i tužbe podnijete Department-u, a koje osiguravaju predmete od vrijednosti potrošačima, bilo kao olakšavajuće okolnosti, bilo kompenzacije za novčane kazne koje bi se inače naplatile. To smo činili u prošlosti, a možemo i činit ćemo to i u kontekstu načela zaštite kada to okolnosti dozvoljavaju. Ako bi neka zrakoplovna tvrtka iz SAD-a više puta kršila odjeljak 41712, također bi se postavilo pitanje o spremnosti zrakoplovne tvrtke na poštivanje, što bi moglo u vrlo ozbiljnim situacijama, dovesti do zaključka da zrakoplovna tvrtka više nije

sposobna obavljati djelatnost i stoga bi izgubila dozvolu za obavljanje svoje djelatnosti. (Vidjeti propise Department of Transportation-a 93-6-34, 23. lipnja 1993. i 93-6-11, 9. lipnja 1993. Iako se ovaj postupak nije doticao odjeljka 41712, imao je za posljedicu povlačenje dozvole prijevoznika za rad zbog potpunog neuvažavanja odredbi Federal Aviation Act-a, bilateralnog sporazuma te pravila i propisa Department-a.)

Nadam se da će Vam ova informacija biti od koristi. Ako imate kakvih pitanja ili trebate daljnje informacije, slobodno me možete kontaktirati.

S poštovanjem,

Samuel Podberesky

Pomoćnik glavnog savjetnika za provedbu
načela i pravnih postupaka u zrakoplovstvu

PRILOG VII.

U odnosu na članak 1. stavak 2. točku (b), vladina tijela u Sjedinjenim Američkim Državama koja su ovlaštena da istražuju pritužbe i osiguraju pravnu zaštitu protiv nepoštenih ili prijevarnih radnji, kao i naknadu za pojedince, bez obzira na državu u kojoj žive ili državljanstvo, u slučaju nepoštivanja načela provedenih u skladu s često postavljanim pitanjima su:

1. Federal Trade Commission; i

2. Department of Transportation SAD-a.

Federal Trade Commission djeluje na temelju svoje ovlasti iz odjeljka 5. Federal Trade Commission Act-a. Nadležnost Federal Trade Commission-a na temelju odjeljka 5. ne odnosi se na banke, štedno-kreditne ustanove i kreditne unije; telekomunikacije i javne prijevoznike u međudržavnom prijevozu, zračne prijevoznike, te proizvođače mesnih prerađevina i trgovce stokom. Iako osiguravajuća društva nisu izričito uvrštena u popis iznimaka u odjeljku 5., McCarran-Ferguson Act-a ([1]) prepušta regulaciju osiguravajuće djelatnosti svakoj državi pojedinačno. Međutim, odredbe Zakona o FTC-u primjenjuju se na osiguravajuća društva u onoj mjeri u kojoj njihovo poslovanje nije regulirano državnim zakonom. FTC zadržava preostali dio ovlasti nad nepoštenim ili prijevarnim radnjama osiguravajućih društava kada se ne bave poslovima osiguranja.

Ministarstvo prometa SAD-a djeluje na temelju svoje ovlasti iz glave 49., odjeljka 41712 United States Code. Department of Transportation SAD-a pokreće slučajeve na temelju vlastitih istraga, kao i službenih i neslužbenih pritužbi koje primi od pojedinaca, putničkih agencija, zrakoplovnih tvrtki te vladinih agencija iz SAD-a i inozemstva.

([1]) 15 U.S.C. § 1011 *et seq.*