

29 STRAIPSNIO duomenų apsaugos darbo grupė

**10107/05/EN
WP 105**

Darbinis dokumentas duomenų apsaugos klausimais kai naudojama RDID technologija

2005 m. sausio 19 d.

Ši Darbo grupė buvo sudaryta pagal 95/46/EC Direktyvos 29 straipsnį. Ji yra Europos savarankiška patariamoji duomenų apsaugos ir privatumo institucija. Jos tikslai nubrėžti 95/46/EC Direktyvos 30 straipsnyje ir 2002/58/EC Direktyvos 15 straipsnyje.

Sekretariatas yra išlaikomas Europos Komisijos E direktorato (paslaugos, autoriaus teisės, pramoninė nuosavybė ir duomenų apsauga), Vidaus rinkos pagrindinis direktoratas, B-1049 Briuselis, Belgija, įstaigos Nr. C100-6/136.

Tinklapis: www.europa.eu.int/comm/privacy

DARBO GRUPĖ DĖL ASMENŲ APSAUGOS TVARKANT ASMENS DUOMENIS sudaryta pagal Europos Parlamento ir Tarybos 95/46/EB Direktyvą 1995¹,

atsižvelgdama į aukščiau nurodytos Direktyvos 29 straipsnį, 30(1)(c) straipsnį ir 30(3) straipsnį,

atsižvelgdama į jos tvarkos nurodymus ir ypač į 12 ir 14 straipsnius,

PRIĖMĖ ŠĮ darbinį dokumentą:

1. ĮVADAS

Radio dažnių indentifikacijos (vadinamosios „RDID technologija“) naudojimas įvairiems tikslams ir paskirčiai gali padėti verslininkams, asmenims ir visuomeninėms tarnyboms (taip pat vyriausybėms). Šiame dokumente iliustruojama, kaip RDID padeda mažmenininkams valdyti jų prekių atsargas, stiprinti vartotojų pirkimo patyrimą, pagerinti vaistų saugumą, taip pat leidžia asmenims geriau kontroliuoti ribojamas sritis.

Nors RDID technologijos naudojimo privalumai akivaizdūs, tačiau paplitusi tokios technologijos sklaida ir naudojimas taip pat išryškina galimus trūkumus. Duomenų apsaugos srityje, 29 straipsnio darbo grupė reiškia susirūpinimą, kad naudojant RDID gali būti pažeistas žmogaus orumas ir teisės į duomenų apsaugą. Susirūpinimą pagrįstai kelia tai, kad verslininkai ir vyriausybės gali pasinaudoti galimybe kištis į privačią asmenų sritį. Atsiradusi galimybė slapta rinkti įvairius duomenis apie tą patį asmenį; sekti asmenis viešose vietose (oro uostuose, geležinkelių stotyse, parduotuvėse); padidinti profilius, pirkėjų elgseną stebint parduotuvėse; skaityti dėvimų drabužių ir aksesuarų etiketes bei pirkėjų nešiojamus su savim vaistus - visi šie RDID technologijos naudojimo atvejai kelia susirūpinimą dėl privatumo. Padėtį dar labiau apsunkina tas faktas, jog dėl palyginti mažos tokios technologijos kainos, ji taps prieinama ne tik svarbiausių vaidmenų atlikėjams, bet ir eiliniams veikėjams ir atskiriems piliečiams.

Suvokdama šią naują grėsmę, 29 straipsnio darbo grupė priversta ištirti privatumo ir kitų pagrindinių teisių apsaugos reikšmę, taikant RDID technologijas. Be kita ko, siekdama šio tikslo, 29 straipsnio darbo grupė tarėsi su suinteresuotomis šalimis, įskaitant gamintojus ir tokios technologijos skleidėjus, naudotojus bei privatumo šalininkus. 29 straipsnio darbo grupės atlikto tyrimo pagrindu buvo priimtas šis darbinis dokumentas, turintis du pagrindinius tikslus: pirmas yra teikti RDID skleidėjams ir naudotojams rekomendacijas dėl pagrindinių principų, nustatytų Europos Komisijos direktyvose, laikymosi, ypač atsižvelgiant į Duomenų apsaugos direktyvą² ir Direktyvą dėl privatumo ir elektroninio ryšio apsaugos³, ir antras - šiuo priimtu darbinio dokumentu 29 straipsnio darbo grupė nori teikti rekomendacijas tokios technologijos gamintojams (RDID žymenis, skaitytuvus ir aparatus) bei RDID standartizavimo tarnyboms dėl jų atsakomybės už privatumo apsaugos reikalavimus atitinkančių technologijų kūrimą, kad tokios technologijos skleidėjai ir naudotojai galėtų vykdyti prievoles, nustatytas Duomenų apsaugos direktyvoje.

Atsižvelgdama į palyginti nedidelę RDID technologijos naudojimo patirtį, 29 straipsnio darbo grupė šį dokumentą laiko pirmuoju situacijos įvertinimu. Darbo grupė ir toliau tirs situaciją ir

¹ Official Journal L 281, 23.11.1995, p.31, gaunamas:

http://europa.eu.int/comm/internal_market/privacy/law-fr.htm

² 95/46/EB 1995 m. spalio 24 d. Direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

³ 2002/58/EB 2002 m. liepos 12 d. Direktyva dėl asmenų duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje.

sukaupti patirtį teiks rekomendacijas ateityje. Jų svarba išaugs, jei RDID technologija ateityje taps, kaip tikimasi, vienu iš informacinės aplinkos kertinių akmenų ateityje. Iš esmės, šis dokumentas yra pradinis ir 29 straipsnio darbo grupė ir toliau nagrinės šį klausimą.

2. RADIO DAŽNIŲ IDENTIFIKACIJOS TECHNOLOGIJA: TECHNOLOGIJOS IR JOS NAUDOJIMO APŽVALGA⁴

2.1. Radijo dažnių identifikacijos technologijos pagrindai

Pagrindiniai radijo dažnių identifikacijos technologijos elementai *arba* infrastruktūra yra *žymuo* (t.y. mikroschema) ir *skaitytuvas*. Žymenį sudaro elektroninė grandinė, kaupianti duomenis, ir antena, perduodanti duomenis radijo bangomis. Skaitytuvas susideda iš antenos ir modulatoriaus, kuris pakeičia įeinančią analoginę radijo ryšio informaciją skaitmeniniais duomenimis. Ši skaitmeninė informacija tada gali būti apdorojama kompiuteriu.

Kaip matyti iš kitų skirsnių, RDID technologija gali veikti įvairiais būdais priklausomai nuo žymenų ir skaitytuvų tipų. Naudojantieji tokią technologiją turės pasirinkti, kokias naudoti technines galimybes pagal savo poreikius. Naudotojai privalės nuspręsti, ar naudoti aktyvius, ar pasyvius žymenis. „Pasyvieji“ žymenis neturi savarankiško energijos šaltinio (baterijų) ir todėl gali būti sužadinti praėjus dešimtmečiams po jų pagaminimo. Žymuo įjungiamas radijo signalu. RDID skaitytuvas siunčia radijo signalus, kurie sužadina žymenį per nuotolį, skatindamas perduoti jame sukauptą informaciją. „Aktyviuosiuose“ žymenyse esanti baterija trumpina jų veikimo trukmę. Jie arba perduoda juose esančią informaciją be skaitytuvo užklauso, arba laukia, kol spragtelės skaitytuvas.

2.2 Įvairus taikymas skirtinguose sektoriuose - Pavyzdžiai

RDID technologija pradedama diegti įvairiuose *sektoriuose* (pvz., sveikatos apsaugos, aviacijos, transporto). Be to, daugėja RDID žymenų veikimo skirtinguose sektoriuose ypatumų ir jų galimybės tik pradeda atsiskleisti. Šiame skyriuje siekiama apibūdinti pagrindines RDID technologijos veikimo galimybes ir jos pritaikymą skirtinguose sektoriuose, t.y. transporto ir sveikatos apsaugos. Nors kai kurie RDID taikymo atvejai, aprašyti žemiau, tebėra testuojami, tačiau keletas veikia realiai, kartais duomenų subjektui to nežinant.

Transportavimas/Išdėstymas. RDID sistemos puikiai tinka kai kuriais transportavimo atvejais. Tinkamai išdėstius RDID skaitytuvus, transporto priemonės su žymenų įtaisais gali būti sekamos pakeliui iki galutinės paskirties vietos. Daugelyje visuomeninio transporto bilietų jau įdiegta RDID technologija. Kaip teigia pramonės šaltiniai, pasaulinėje praktikoje milijonuose automobilių raktų yra įdiegta RDID.

Aviacija. RDID technologija gali būti taikoma bagažo valdymo tikslais. Bagažo registravimo vietoje, prie bagažo bus pritvirtinti žymenis ir įvairiuose oro uosto skyriuose sumontuoti skaitytuvai seks bagažo kelionę iš vieno oro uosto į kitą kaip ir pačiame oro uoste. Yra projektų, kaip įrengti įsodinimo korteles su žymenimis, leidžiančiais nustatyti vėluojančių keleivių buvimo vietą.

Sveikatos apsauga. RDID sistemos yra taikomos farmacijos pramonėje, kad būtų lengviau sekti vaistus ir užkirsti kelią klastotėms bei išvengti nuostolių dėl vagysčių transportavimo metu. Tai galima pasiekti gamintojams patalpinus žymenis į kiekvienus vaistus, taip patvirtinant jų kilmę. Vaistinėse ar vaistus parduodančiose parduotuvėse bus įtaisyti skaitytuvai, kurie patikrins ir

⁴ Išsamesnis RDID technologijos ir jos taikymo aprašymas pateiktas šio dokumento priede.

patvirtins, jog vaistai priklauso rodomam gamintojui. Jungtinių Valstijų MVA agentūra jau yra išleidusi rekomendacijas dėl RDID naudojimo vaistų pakuotėje sekimui ir vengiant klaidų.⁵ Ligoninėse taip pat pritvirtinant žymenis prie tam tikrų elementų, RDID pagerina paciento saugumą ir leidžia ligoninėms taupyti tais atvejais, kai, pavyzdžiui, sumažinama rizika palikti kokį elementą paciento viduje baigiant operaciją. RDID žymenis dar galima pritvirtinti prie pačių pacientų, kad būtų nustatyta jų tapatybė, buvimo vieta ir tikslūs veiksmai, kokių reikėtų imtis medicinos personalui. Ligoninės personalą taip pat galima sekti ir būtiniausiu atveju yra lengva aptikti jo buvimo vietą. MVA neseniai davė sutikimą kompanijos prašymui (VeriChip), kad RDID žymuo būtų įvestas atliekant poodines injekcijas, nurodantis paciento medicininės bylos numerį, kuris būtų panaudotas esant nenumatytiems atvejams.⁶

Saugumo ir prieigos kontrolė. RDID sistemos leidžia sekti vertingo įrenginio judėjimą, kadangi žymenis perduoda informaciją skaitytuvams apie jo buvimo vietą tam tikru atstumu. Pavyzdžiui, automobilių pramonėje RDID jau yra naudojamas kaip automobilio stabdymo sistemos elementas. Vartotojų ir mažmenininkų sektoriuje gali būti naudojami specialūs RDID žymenis, užtikrinantys prekės kilmę. Tokiu būdu galima patikrinti, ar neklastojamos labai vertingos prekės. Viena iš svarbiausių mokslinių tyrimų temų per pastaruosius keletą metų buvo piniginių banknotų apsauga taikant RDID.

Remiantis darbu, atliktu TCAO⁷, RDID bus taikomas pasuose⁸. Asmenų priėjimas prie draudžiamųjų sričių taip pat gali būti reguliuojamas, pritvirtinus prie jų RDID žymenį arba suteikus jiems mažesnės gebos ryšio korteles, tokias kaip Aukščiausiojo lygio pasitarimui apie informacinės visuomenės kūrimą arba Kinijos komunistų partijos suvažiavimui.

Naudojimas mažmeninėje prekyboje. Keletas didesnių mažmenininkų paprašė gamintojų sudėti žymenis ant jų gaminių. Mažmenininkai produktų pažymėjimo naudą patiria keliais atžvilgiais. Pavyzdžiui, RDID mažmenininkams leidžia pagerinti prekių sandėliavimo tvarkymą. Kadangi kiekvienas atskiras produktas yra identifikuojamas įvairiose stadijose (t.y., atgabenus jį į sandėlį, parduotuvę, jam patekus ant lentynos, pardavimo vietoje), RDID suteikia mažmenininkui parankų įrankį kontroliuoti ir valdyti produktus, esančius parduotuvėje ir sandėlyje. RDID leidžia pagerinti parduotuvėje esančių produktų naudingumą, teikiant naudą tiek mažmenininkui, tiek ir galimiems vartotojams. Pavyzdžiui, įrengus skaitytuvus išėjimo tikrinimo zonose, jos apeinamos ir taip pirkėjas sutaupo laiko apsipirkimui parduotuvėje. RDID gali padėti produktų sekimo srityje, efektyviau tokius produktus, kurie yra nesaugūs arba jų galiojimo terminas jau yra pasibaigęs, išimti iš apyvartos.

Kalbant apie RDID mažmeninės prekybos sektoriuje, svarbu išdėmėti standartizavimo darbą, atliktą EPC Global, kuriant „Elektroninius produktų kodus“, kurie nustatys atskirus produktus⁹.

⁵ Radijo dažnių identifikavimo įgyvendinimo tyrimai ir bandomosios vaistų programos; Patarimai MVA personalui ir pramonei; Suderinamumo strategijos programa; Sec.400.210; Radijo dažnių identifikavimo įgyvendinimo tyrimai ir bandomosios vaistų programos; 2004 m. lapkritis.

⁶ Sveikatos apsaugos ir žmonių aptarnavimo departamentas; Maisto ir vaistų administravimas; 21 CFR 880 dalis; Rejstras Nr.2004N-0477; išspausdinta Federaliniame registre / t.69, Nr.237 /penktadienis, 2004 m. gruodžio 10 d. / Taisyklės ir nuostatai.

⁷ Tarptautinė civilinės aviacijos organizacija

⁸ 2003 TCVO nustatė techninius RDID technologijos, naudojamos elektroniniuose pasuose, reikalavimus. Tie reikalavimai išspausdinti TCAO Doc 9303.

⁹ Papildomos informacijos apie EPK Global rasite skyrelyje 5.2.

3. Duomenų apsauga ir privatumo apsaugos sąsajos

Nors kai kurie RDID taikymo atvejai nekelia duomenų apsaugos sunkumų, tačiau, kaip iliustruojama žemiau, daugelis sukelia. Šiame skirsnyje apžvelgiami pagrindiniai duomenų apsaugos aspektai, atsirandantys dėl RDID technologijos naudojimo.

3.1 RDID naudojimas informacijos, susijusios su asmens duomenimis, rinkimui

Pirmasis rūpestį keliantis dalykas dėl duomenų apsaugos atsiranda tada, kai RDID technologija naudojama informacijai rinkti, kuri tiesiogiai ar netiesiogiai susijusi su asmens duomenimis. Pirmiausia reikia atsižvelgti į tą atvejį, kai produkto(gaminio) RDID žymens numeris yra susijęs su įrašu apie jį nupirkusį pirkėją. Pavyzdžiui, elektronikos parduotuvė savo prekes gali pažymėti unikaliais kodais, kuriuos mažmenininkas sistemingai jungia su pirkėjų pavardėmis, surenkamomis apmokant kredito kortelėmis, ir vėliau susieja juos su to mažmenininko pirkėjų duomenų baze. Tai gali būti atliekama, garantijos tikslais. Kitas pavyzdys, į kurį tenka atsižvelgti, yra tas atvejis, kai prekybos centrai seka lojalumo korteles arba panašias priemones, nustatančias asmenų tapatybę pagal jų pavardes pirkėjų įpročiams išsiaiškinti ir registruoti jiems esant parduotuvėje, įskaitant laiką, sugaištą konkrečiame prekybos centro skyriuje, siekiant nustatyti, kiek kartų pirkėjas lankėsi prekybos centre nieko nepirkdamas, ir t.t..

Nurodytais dviem atvejais tiek, kiek informacija, surinkta naudojant RDID technologiją, yra susijusi su asmens duomenimis, privatumo apsaugos reikšmė itin akivaizdi. Greta padidėjusios egzistuojančios galimybės išsiaiškinti vartotojo įpročius ir gauti asmens atvaizdą pagal lojalumo korteles, RDID technologija atveria galimybes tiesioginei rinkodarai žymenimis ženklinant atskiras prekes, kadangi asmenys gali būti atpažįstami įeidami į parduotuvę ir jų įpročiai kontroliuojami parduotuvėje. Be to, susirūpinimą kelia ir tai, jog platus tokios technologijos taikymas lems, kad įvairiausi valdytojai tvarkys vis daugiau duomenų (įvairaus pobūdžio ir apimties).

3.2. RDID naudojimas kaupti asmens duomenims kiekviename žymenyje

Dar vienas privatumo apsaugos aspektas išryškėja tada, kai asmens duomenys kaupiami RDID žymenyse. Vienas iš tokių pavyzdžių galėtų būti transporto bilietai. Galima paanalizuoti spėjama atvejį, kai organizacija nusprendžia įgyvendinti bekontaktę nuolatinių bilietų sistemą, pagrįstą RDID technologija, kai bilieto savininko pavardė ir kontaktiniai duomenys yra integruoti žymenyje. Tai reikštų, jog organizacijai leidžiama žinoti, kur nustatytas asmuo važinėja visą laiką. Tai, akivaizdžiai turės poveikį asmens privatumo saugumui. Be šios organizacijos, turinčios tokią informaciją, tokią pat informaciją slapta gali gauti ir trečioji šalis, kadangi bet kas gali nustatyti tam tikrų RDID žymenų buvimo vietą su įprastiniu skaitytuvu. Reikia pabrėžti ir tai, kad RDID sistemos yra labai jautrios įsibrovimams. Kadangi jos veikia be nematomos linijos ir be kontaktinio ryšio, įsibrovėlis gali veikti per nuotolį ir pasyvusis skaitytuvas nebus pastebimas.

3.3. RDID naudojimas sekimui be „tradicinių“ identifikatorių

Trečiasis duomenų apsaugos aspektas atsiranda, kai naudojantis RDID technologija, sekamas asmuo ir gaunama prieiga prie asmens duomenų. Keletas žemiau išvardintų pavyzdžių rodo, kaip RDID technologija gali pažeisti asmens privatumą.

Pavyzdžiui, vieno tinklo bakalėjos krautuvė gali išduoti pirkėjams prietaisus su žymenimis (pvz., žetonus, talonus), leidžiančiais naudotis prekių vežimėliais, kuriuos pirkėjai naudoja kaskart apsilankę parduotuvėje. Šis mechanizmas leistų sudaryti bylą parduotuvei pagal identifikavimo

numerį, saugomą paženklintame žymeniu prietaise, kuris padėtų stebėti, kokius produktus asmuo (nustatytas pagal žetoną ar taloną) perka, kaip dažnai vartojami tokie produktai ir kuriuose vieno tinklo bakalėjos parduotuvėse vartotojas juos perka. Parduotuvė galėtų daryti išvadas, prielaidas apie asmens pajamas, sveikatos būklę, gyvenseną, pirkimo įpročius ir t.t. Tokia informacija galėtų būti panaudota įvairiems sprendimams priimti, pavyzdžiui, tokiems, kaip rinkodara, tikslai arba net dinamiškas kainų nustatymas. Kadangi prietaisas nustatytų asmenį kaskart jam/jai atėjus į parduotuvę, pirkėjas galėtų būti aptarnaujamas, atsižvelgiant į įrašus apie jo vartojimo įpročius. Be parduotuvės, galinčios rinkti aukščiau išvardintą informaciją, praktiškai tokią informaciją gali gauti ir trečioji šalis. Tokiu būdu tampa įmanomi visokie sprendimai apie tokį identifikuotą asmenį be jo ar jos aiškaus sutikimo. Gali taip nutikti, kad valgant sausainukus „on-line“ aplinkoje, netgi jeigu asmuo ne iškart ir netiesiogiai identifikuojamas prekės informacijos lygmenyje, jis gali būti identifikuotas bendrame lygmenyje dėl esančios galimybės identifikuoti jį be sunkumų, pasinaudojant jį supančia informacija ar informacija, sukaupta apie jį. Be to, duomenys, surinkti iš jo, gali turėti įtakos, kaip tas asmuo bus vertinamas ir kaip bus su juo elgiamasi. Šis RDID taikymas taip pat yra svarbus duomenų apsaugos aspektu.

Dar vienas pavyzdys galėtų būti tas, kai naudojant RDID žymenis tvarkomi asmens duomenys, netgi, jei RDID technologija neapima kitų aiškių identifikatorių naudojimo. Pasitelkime tokią hipotezę, kai asmuo Z užėina į parduotuvę C su krepšiu, kuriame yra prekės, pažymėtos RDID žymenimis, iš parduotuvių A ir B. Parduotuvė C nuskaito jo krepšį ir prekės jame (tiksliau, krūva skaičių) atskleidžiamos. Parduotuvė C saugo skaičių įrašus. Kai asmuo Z kitą dieną grįžta į tą pačią parduotuvę, jis dar kartą nuskenuojamas. Prekę Y, nuskaityta prieš dieną, išaiškinama šiandien - skaičius (numeris) reiškia laikrodį, kurį jis visuomet segi. Parduotuvė C sudaro rinkmeną, pritaikydama prekės Y numerį kaip „raktą“. Tai leidžia jiems sekti, kada asmuo Z įeina į parduotuvę, naudodami laikrodžio RDID numerį kaip jo informacinį numerį. Tai leidžia parduotuvei C sudaryti profilį asmens Z (kurio pavardės jie nežino) ir sekti, ką jis turi savo krepšyje kitais kartais jam apsilankius parduotuvėje C. Šitaip elgdamasi parduotuvė C tvarko asmens duomenis, nepažeisdama duomenų apsaugos įstatymo.

Pagalčiau, imkime žymenų naudojimą ant tam tikrų objektų, apimančių objekto pobūdį atskleidžiančią informaciją. Tai, kas priklauso asmeniui, yra asmeniška ir apima informaciją, kurios žinojimas trečių šalių reikštų privatumo asmens, to objekto savininko pažeidimą. Kiti pavyzdžiai iliustruoja šią hipotezę. Pagalvokite apie atvejį, kai kiekvienas, turintis skaitytuvą, gali aptikti banknotus, knygas, vaistus ar vertingus praeivių daiktus. Trečiųjų šalių žinojimas apie tai pažeis privatumą asmens, kuriam tie daiktai priklauso. Tokio pat pobūdžio nerimą kelia ir teroristai, gebantys nustatyti konkrečių tautybių žmones minioje. Dar dramatiškesnis kišimasis atsirastų tada, kaip apibūdinta aukščiau, kai pačiame prietaise būtų svarbi asmeninė informacija, prilygstanti paso duomenims arba informacijai, kuri yra itin slapta.

Kaip rodo šie pavyzdžiai, didžiausią susirūpinimą dėl duomenų apsaugos ir privatumo naudojant RDID technologiją kelia slapta atliekamas, nepageidaujamas asmens sekimas, vykdamas neteisėtą prieigą prie žymens atskleistos informacijos ar atminties.

Iš kituose skirsnuose pateiktų apibūdinimų aiškėja, jog svarbu pateikti rekomendacijas, kaip taikyti EK direktyvose nubrėžtus pagrindinius principus, ypač Duomenų apsaugos direktyvoje, aukščiau išvardintų duomenų tvarkymui.

4. ES duomenų apsaugos įstatymų taikymas informacijai, surenkamai naudojant RDID technologiją

4.1. Rekomendacijos dėl Duomenų apsaugos direktyvos taikymo duomenų rinkimui ir tolesniam tvarkymui naudojant RDID technologiją

Kalbant apie taikymo sritį, Duomenų apsaugos direktyva taikoma visų asmens duomenų tvarkymui. Direktyvoje pateiktas platus „asmens duomenų“ apibrėžimas, apimantis „bet kurią informaciją, susijusią su asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta“. Kyla klausimas, ar tai reiškia, jog Duomenų apsaugos direktyva neišvengiamai apima duomenų rinkimą naudojant RDID technologiją. Atsakymas priklausytų apskritai nuo konkrečių, specifinių RDID technologijos taikymo atvejų, ypač nuo to, ar tokiais specifiniais RDID taikymo atvejais ja tvarkomi asmens duomenys, kaip apibrėžta pagrindinėje DA direktyvoje.

Vertindami klausimą, ar Duomenų apsaugos direktyvoje atsispindi asmens duomenų rinkimas naudojant RDID, privalome apibrėžti (a) koku mastu tvarkomi duomenys *susiję* su asmeniu ir, (b) ar tokie duomenys susiję su asmeniu, kurio tapatybė yra *nustatyta* arba *gali būti nustatyta*. Duomenys laikomi susijusiais su asmeniu, jeigu jie nurodo tapatybę, būdingus bruožus ar asmens elgseną, arba jei tokia informacija yra naudojama elgesiui su asmeniu ar jo vertinimui nustatyti ar paveikti. Vertinant, ar informacija liečia asmenį, kurio tapatybė gali būti nustatyta, reikia remtis Duomenų apsaugos direktyvos Konstatuojamosios dalies 26 skirsniu, kuris nustato, jog „reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti“.

Atsižvelgiant į tai, kas išdėstyta aukščiau, nors akivaizdu, kad ne visas duomenų rinkimas naudojant RDID technologiją pateks į Duomenų apsaugos direktyvos taikymo sritį, tačiau tampa aišku, kad galimi daugelis atvejų, kai RDID technologiją naudojant surinktos asmeninės informacijos tvarkymui bus taikoma Duomenų apsaugos direktyva.

Ketinantis naudotis informacija, surinkta naudojant RDID technologiją, privalės prieš tai įvertinti, ar tokia informacija yra laikoma „asmens duomenimis“ pagal Duomenų apsaugos direktyvą. Jeigu RDID neapima nei asmeninės informacijos, nei yra susijusi su asmens duomenimis, kaip apibūdinta aukščiau, vadinasi Duomenų apsaugos direktyvos nuostatos netaikytinos. Iš tikrųjų, jeigu žymens informacija nėra derinama su kita identifikavimo medžiaga, pavyzdžiui, kieno nors nuotrauka arba pavardė ir adresu, arba su pasikartojančiu nuorodos numeriu, tada Duomenų apsaugos direktyva netaikytina.

3 skirsnyje apibūdintiems trimis variantams Duomenų apsaugos direktyvos nuostatos taikytinos. Pirmuoju atveju taip yra todėl, kad prekės lygmens informacija, surinkta naudojant RDID technologiją, yra tiesiogiai susijusi su asmens duomenimis, esančiais arba kreditinėje, arba lojalumo kortelėse. Antruoju atveju Duomenų apsaugos direktyva ima veikti iškart, kai asmens informacija – pavardė įrašoma į RDID žymenis. Pagaliau, RDID technologijos naudojimas individo judėjimo sekimui, kuris, atsižvelgiant į didžiulį duomenų kiekį, kompiuterio atmintį bei apdorojimo galimybes, vis vien bus nustatytas, todėl taip pat pagrindžia duomenų apsaugos Direktyvos taikymą.

4.2. Rekomendacijos dėl duomenų apsaugos reikalavimų suderinimo

Duomenų valdytojai dėl duomenų, surinktų naudojant RDID technologiją, bus įpareigojami vykdyti prievoles, numatytas Duomenų apsaugos direktyvoje (šiuo dokumente tai dažnai apibūdinama kaip „technologijos skleidėjai“). Kadangi nėra įmanoma nustatyti, kaip šie reikalavimai tinka kiekvienam RDID atvejui, pateikiama bendros gairės, kuriomis duomenų valdytojai gali pasinaudoti pritaikydami pagal aplinkybes, susijusias su duomenų tvarkymu. Žemiau, 5 skirsnyje aprašoma, kad gamintojai yra tiesiogiai atsakingi kad būtų užtikrinta privatumo apsaugą atitinkanti technologija, kuri padėtų valdytojams vykdyti jų prievoles, numatytas Duomenų apsaugos direktyvoje ir palengvintų asmens teisių įgyvendinimą.

Principai:

Darbo grupė siekia pažymėti, kad RDID technologijos ir bet kurios kitokios technologijos taikymo struktūra yra nubrėžta Duomenų apsaugos direktyvos 2 Konstatuojamosios dalies punkte, kuris skelbia, kad „*duomenų tvarkymo sistemos skirtos tarnauti žmogui; duomenys turi būti tvarkomi nepaisant jų tautybės, gyvenamosios vietos, gerbiant žmogaus teises ir laisves, ypač privatumo teisę, taip pat remiant ekonominę ir socialinę pažangą, prekybos plėtrą bei žmonių gerovę.*“

Principai, susiję su duomenų kokybe: Duomenų valdytojai, renkantys duomenis taikydami RDID, privalo laikytis kelių **duomenų apsaugos principų**, įskaitant šiuos:

Naudojimo ribojimo principą (tikslų principą): Šis principas iš dalies suformuluotas 6 (1)(b) straipsnyje Duomenų apsaugos direktyvos, draudžia tolesnį tvarkymą, nesuderinamą su rinkimo tikslu.

Duomenų kokybės principas: Šis Direktyvos principas reikalauja, kad asmens duomenys būtų renkami tik numatytam tikslui ir nebūtų pertekliniai. Taigi, tikslo neatitinkantys duomenys neturi būti renkami, o jeigu yra surinkti, privalo būti sunaikinti (Straipsnis 6.1.c). Jis taip pat reikalauja, kad duomenys būtų tikslūs ir nuolat atnaujinami.

Saugojimo principas: Šis principas reikalauja, kad asmens duomenys būtų saugomi ne ilgiau nei reikalinga tam tikslui, kuriam duomenys buvo renkami ar toliau tvarkomi.

Teisinis duomenų tvarkymo pagrindas: Remiantis Duomenų apsaugos direktyvos 7 straipsniu, asmens duomenys gali būti tvarkomi tik tada, kai yra bent vienas teisinis duomenų tvarkymo pagrindas¹⁰.

Daugeliu RDID technologijos naudojimo atvejų, individų sutikimas bus vienintelis įstatymu paremtas teisinis pagrindas duomenų valdytojams teisėtai rinkti informaciją. Pavyzdžiui, prekybos centrams, tvirtinantiems žymenis ant lojalumo kortelių, prireiks arba aiškių sutarties nuostatų, arba asmens sutikimo, kad susietų asmens informaciją, gaunamą išsigyjant lojalumo kortelę, su informacija, surinktą naudojant RDID technologiją. Beje, sutikimas ne visuomet yra tinkamas asmens duomenų tvarkymo teisinis pagrindas, kai duomenys renkami naudojant RDID sistemas. Pavyzdžiui, ligoninėms, naudojančioms RDID chirurginiams instrumentams, kad būtų išvengta rizikos palikti tam tikrą instrumentą ar daiktą paciento viduje, pasibaigus operacijai, paciento sutikimo gali neprireikti; šis tvarkymas bus teisėtas, nes ginami paties duomenų subjekto gyvybiniai

¹⁰ 7 straipsnis išvardina tokius įstatyminius, duomenų tvarkymą įteisinančius, pagrindus: (i) duomenų subjektas yra nedviprasmiškai davęs sutikimą; (ii) tvarkyti reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš šalių; (iii) tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui; (iv) tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus; (v) tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui; (vi) tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai tokių interesų bei duomenų subjekto, kuriam pagal 1 straipsnio 1 dalį reikalinga apsauga, teisės ir laisvės yra viršesnės.

¹¹ 29 straipsnio darbo grupė pažymi, jog tinkamiausias teisėtas pagrindas, numatytas Duomenų apsaugos direktyvos 7 straipsnyje, duomenų tvarkymo priklausys nuo tokio tvarkymo konkrečių aplinkybių.

¹² Informacija apie duomenų gavėjus, pareiga atsakyti ir priėjimo ir teisės gauti informaciją ir pataisyti duomenis buvimas turi būti užtikrintas, kiek tai būtina atsižvelgus į ypatingas aplinkybes, kuriomis renkami duomenys, siekiant garantuoti sąžiningą tvarkymą duomenų subjekto naudai.

interesai, o tai yra vienas teisėtas pagrindas, numatytas Duomenų apsaugos direktyvos 7 straipsnyje.¹⁰

Naudojant sutikimą, remiantis Direktyvos 2 straipsniu ir 7(a) straipsniu, jis privalo atitikti nustatytus reikalavimus: (i) jis turi būti savanoriškas, t.y., be „apgaulės ir prievartos“; (ii) jis turi būti konkretus, kitaip tariant, jis turi atitikti tam tikrą tikslą; (iii) sutikimas privalo rodyti individo veiksmingą valią; (iv) sutikimas privalo būti žinomas. Pagaliau, sutikimas privalo būti „nedviprasmiškas“, kitaip tariant, toks sutikimas, kuris gali turėti daugiau nei vieną reikšmę, nebūtų laikomas sutikimu.

Reikalavimai informacijai: Remiantis Duomenų apsaugos direktyvos 10 straipsniu, duomenų valdytojai, tvarkantys informaciją naudojant RDID technologiją, privalo pateikti duomenų subjektams tokią informaciją: valdytojo tapatybę, tvarkymo tikslus, informaciją apie duomenų gavėjus ir teisės į prieigą įrodymą¹². Pagal šį įpareigojimą, 4 atvejo kontekste mažmeninės prekybos parduotuvei teks duomenų subjektams pateikti mažiausiai tokią aiškia informaciją apie:

- (i) RDID žymenų buvimą ant prekių arba jų pakuočių ir skaitytuvų buvimą;
- (ii) pasekmes tokio žymenų bei skaitytuvų buvimo ir su tuo susijusį informacijos kaupimą; duomenų valdytojai ypač aiškiai turi informuoti asmenis, jog tokie prietaisai leidžia žymenims perduoti informaciją, šiame procese visai nedalyvaujant pačiam asmeniui;
- (iii) informacijos panaudojimo ketinamus tikslus, įskaitant (a) duomenų tipą, su kuriuo RDID informacija bus siejama, ir (b) ar šia informacija bus leista pasinaudoti trečiosioms šalims ir,
- (iv) valdytojo tapatybę.

Priklausomai nuo tam tikrų RDID naudojimo atvejų, duomenų valdytojas privalės papildomai informuoti asmenis: (v) kaip pašalinti, sugadinti ar nuimti žymenis nuo prekių, gaminių, ir tokiu būdu užkirsti kelią tolesniam informacijos atskleidimui, ir (vi) kaip įgyvendinti teisę gauti informaciją. Pavyzdžiui, tokia informacija bus būtina 3.1 skyreliuose aprašytais atvejais. Nors tokios pastabos, siūlytos EPK Global, kurios turėtų būti pateiktos plataus vartojimo prekėms, atitinka (i) vardintą informacijos pateikimo tikslą, tai turėtų būti papildyta kita dokumentacija, pridedant aukščiau aprašytą informaciją.¹³

Sąžiningo duomenų tvarkymo principas, nustatytas Duomenų apsaugos direktyvos 6 straipsnyje, reikalauja pateikti informaciją duomenų subjektui aiškia ir suprantama forma.

Pagaliam, teikiant aukščiau apibūdintą informaciją, Darbo grupė mano, kad ypač reikšminga yra pabrėžti, jog duomenų subjektas turėtų gauti pakankamai informacijos, kad lengvai suprastų RDID taikymo poveikį.

Duomenų subjekto teisė gauti informaciją: Duomenų apsaugos direktyvos 12 straipsnis suteikia duomenų subjektams galimybę patikrinti duomenų tikslumą ir užtikrinti, kad jie būtų atnaujinami. Šios teisės visiškai taikomos asmens duomenų rinkimui su RDID technologija. Jeigu prisiminsime pavyzdį su prekybos centrais, kurie deda žymenis ant lojalumo kortelių, toks teisės gauti

¹³ Žr. skirsnį 5.1 EPC Global veiklos apžvalga.

informaciją įgyvendinimas apims atskleidimą *visos* informacijos, susijusios su asmeniu, ir tai gali apimti asmens apsilankymų parduotuvėje skaičių, pirktas prekes ir t.t.

Jeigu RDID žymenyse yra asmens informacija, kaip nurodyta 3.2, asmenys privalėtų žinoti tą informaciją, esančią žymenyje, ir atlikti taisymus, pasinaudodami lengvai prieinamomis priemonėmis.

Saugumo reikalavimai: Duomenų apsaugos direktyvos 17 straipsnis nustato reikalavimą duomenų valdytojams įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užkirstas kelias atsitiktiniam arba neteisėtam asmens duomenų naikinimui, ar neįgaliotam atskleidimui. Priemonės gali būti organizacinės ar techninės. Šis reikalavimas, išaiškintas skirsnyje 5, paskirtame RDID ir būtinam privatumo stiprinimo technologijos naudojimui.

5. Techniniai ir organizaciniai reikalavimai, užtikrinantys tinkamą duomenų apsaugos principų įgyvendinimą

Aukščiau išvardintų principų, kaip ir duomenų minimizavimo principo, suformuluotų Duomenų apsaugos direktyvos 6.1 straipsnyje laikymasis yra svarbiausias dalykas tiems, kurie skleidžia RDID technologiją.

29 straipsnio Darbo grupė yra tos nuomonės, jog technologija gali atlikti pagrindinį vaidmenį užtikrinant asmens duomenų apsaugos principų laikymąsi, asmens duomenis renkant RDID. Pavyzdžiui, RDID žymenų, RDID skaitytuvų ir RDID programų projektavimas, skatinamas standartizavimo iniciatyvų, gali turėti įtakos mažinimui asmens duomenų, kaupimo ir naudojimo, taip pat užkertant kelią neteisėtoms tvarkymo formoms, panaikinant technines galimybes neįgaliotiems asmenims naudotis asmens duomenimis.

Šioje situacijoje Darbo grupė nori pabrėžti, kad nors RDID naudotojai ir skleidėjai yra tiesiogiai atsakingi už asmens duomenų rinkimą, naudojantis svarstomąja technologija, RDID technologijos gamintojai ir standartizavimo tarnybos yra atsakingos už tai, kad užtikrintų duomenų apsaugos ir privatumo reikalavimus atitinkančios RDID technologijos perdavimą tiems, kas tokią technologiją skleidžia. Mechanizmas privalo būti išvystytas taip, kad praktinėje veikloje būtų taikomi tokie standartai ir jų laikomasi. Ypač reikalingi RDID privatumo apsaugą atitinkantys standartai, leidžiantys duomenų valdytojams, tvarkantiems duomenis naudojant RDID technologiją, turėti būtinus įrankius įgyvendinimui reikalavimų, nustatytų Duomenų apsaugos direktyvoje. Todėl Darbo grupė ragina RDID žymenų, skaitytuvų ir RDID programų gamintojus ir standartizavimo tarnybas atsižvelgti į pateikiamas rekomendacijas.

5.1. Standartizavimo ir sąveikos įtaka duomenų apsaugos principų įgyvendinimui

Svarstant bet kurią technologiją, standartizacijos procesas paprastai yra pagrindinis veikimo sąveikos įrankis, kuris yra svarbus sėkmingam naujų technologijų įsisavinimui ir įdiegimui. Standartizavimas taip pat gali padėti įsisavinti duomenų apsaugos ir privatumo reikalavimus.

Visi RDID sistemos elementai yra arba bus standartizuoti, pvz., žymens ir skaitytuvo dizainas, žymenyje užfiksuoti duomenys, ryšių protokolas (oro sąsaja) tarp skaitytuvo ir žymens, skaitytuvu surinktų duomenų valdymas, kita. Standartizavimo tarnybos ir kitos grupės jau yra pradėjusios tam tikrą darbą RDID srityje. Reikia paminėti, jog RDID standartizavimas turės įtakos kai kurioms rinkoms ypač paveikdamos su prekėmis susijusias operacijas.

Susikūrusi kaip atsakas į karvių pasiutligės krizę, Tarptautinė Standartizacijos Organizacija (ISO) išplėtojo sektorių specifinius standartus (Krovinių gabenimo konteinerių, Transporto priemonių,

gyvūnų, ir t.t.) RDID žymenims ir bendresnius oro sąsajai (ISO 18000 serijos) ir prekių vadybai (ISO/IEC 15963:2004).

„EPCglobal Inc“¹⁴, bendra „EAN International“ ir „Uniform Code Council“ (UCC) įmonė, yra valdoma „EPCglobal“ Valdytojų tarybos, kuri sudaryta iš pirmaujančių įmonių. Ši organizacija kuria „Elektroninius produktų kodus“ („EPK“), kurie identifikuos atskiras prekes. Kiekvienas produktas turės pritvirtintą žymenį, rodantį produkto, prie kurio jis yra pritvirtintas, numerį. Tokios sistemos pirmtakas yra „Universalus Produkto kodas“ („UPK“) arba brūkšninė kodo sistema, kurią EPK numato pakeisti. Šių dviejų sistemų skirtumas yra tas, kad UPK nustato produkto tipą nenumėruojant kiekvienos atskiros prekės. Be to, „EPK Global Network“ kuria standartus, kaip sujungti serverius, saugančius informaciją apie prekes, nustatomas pagal EPK numerius. Serveriai, vadinami EPK informacijos tarnybomis arba EPK informacinėmis sistemomis, yra prieinami per internetą ir sujungti, įgalinti ir pasiekiami, naudojant tinklo paslaugų rinkinį¹⁵.

Dauguma RDID standartizavimo iniciatyvų numato galimybę įtraukti duomenų apsaugos sąlygas į technines sąlygas. Pavyzdžiui, neseniai buvo pasiūlyta¹⁶ pritaikyti standartą „skaitytuvų žymuo“ protokolą, suformuluotą ISO, kad būtų įtrauktas sąžiningos informacijos taikymas, suformuluotas „OECD“¹⁷.

Pastaruoju metu Europos elektroninių ryšių standartų institutas (EESI) pritarė naujam Europos standartui dėl RDID sistemų naudojimo didinant leidžiamą skaitytuvo galingumą ir turimų dažnių skaičių ultraaukšto dažnio bangą, vieno iš perspektyviausių mažmeninės prekybos sektoriuje nustatant prekę. Tokia raida ypač praplės skaitymo lauką nuo skaitytuvo iki žymens¹⁸. RDID sistemų veikimo sąveika (techninė įranga, programinė įranga ir gauti duomenys) logiškai išplaukia iš standartizavimo proceso. Žvelgiant iš verslo perspektyvos, RDID sistemų veikimo sąveika yra teigiama. Iš tikrųjų, dėl palaikomo verslo modelio, mažmenininkas turėtų vengti būtinybės įrengti keletą skirtingų žymenų skaitytuvų, kad nuskaitytų žymenis, pagamintus įvairių gamintojų. Sprendžiant iš duomenų apsaugos perspektyvos, nors veikimo sąveika ir gali pagerinti techninę duomenų kokybę ir prisidėti prie suderinamumo su Direktyvos 6(1) (d) straipsniu, vis dėlto RDID veikimo sąveika gali tuo pačiu turėti neigiamų šalutinių poveikių duomenų apsaugai, nebent būtų imtasi atitinkamų priemonių. Pavyzdžiui, tikslo ar paskirties apribojimo principą būtų kur kas sunkiau įgyvendinti ir kontroliuoti. Be to, prieigos teisių, susijusių su privatumu, reguliavimas galėtų tapti kritiniu, kadangi išaugtų skaičius asmenų, manipuliuojančių duomenimis.

¹⁴ <http://www.epcglobalinc.org/>

¹⁵ Iki šiol Europos Sąjungos susirūpinimas nebuvo akcentuotas šiose iniciatyvose, kurias daugiausia palaiko JAV pramonės tarpininkai. Taip pat tebėra neaišku, ar kinų rinka priims vieną iš cituotų standartų, ar įsives savuosius.

¹⁶ Christian Floerkemeier, Roland Schneider, Marc Langheinrich; Skenuoti tikslingai - Sąžiningos Informacijos Principų palaikymas RDIDD protokoluose. 2-as tarptautinis simpoziumas apie naudojimosi kompiuteriu sistemų paplitimą (NKSP 2004), Lapkričio 8-9, Tokijas, Japonija.

¹⁷ ISO 18000 6 dalis A tipas

¹⁸ Atstumas iki skaitytuvo ir jo galingumas gali turėti įtakos konkrečiau RDID pritaikymo kišimosi į privatumą invaziškumui.

5.2. Techninės ir organizacinės priemonės informavimui apie RDID buvimą, matomumą ir aktyvacijos būseną

Kaip nurodyta 4 skirsnyje, iš RDID technologijos naudotojų ir skleidėjų reikalaujama pateikti duomenų subjektams informaciją ne tik apie duomenų tvarkymo tikslus, bet *taip pat* apie RDID prietaisų buvimą, bei laikytis tokių reikalavimų:

Pirma, asmenys turi būti informuojami apie RDID tipo ar aktyvuotų RDID skaitytuvų buvimą. Tam reikalui naudotinos žinomos, pasaulinėje praktikoje plačiai taikomos standartinės piktogramos ir kitos informacinės priemonės. Aprūpinimas tokio tipo informacija yra labai svarbus, kad būtų užkirstas kelias neteisėtam ir slaptam asmens duomenų rinkimui naudojantis RDID technologija. Pavyzdžiui, jei parduotuvė ar ligoninė yra aktyvavusios žymenis, asmenys turėtų būti apie tai informuoti.

Antra, dėl tų pačių, aukščiau išvardintų, priežasčių (slapto asmens duomenų rinkimo vengimo) pranešimas apie *RDID aparatų buvimą* šalia asmens (pavyzdžiui, drabužiuose ir objektuose) yra atskiras reikalavimas, nes dėl savo dydžio RDID aparatas gali būti nepastebimas. Būdai įvykdyti šį reikalavimą gali būti įvairūs: gali būti standartinės pranešimų formos, tačiau tai gali būti atliekama techninėmis priemonėmis.

Trečia, faktiškai nepakanka informuoti asmenis vien tik apie RDID prietaisų buvimą, nes, remiantis Duomenų apsaugos direktyva, asmenys turi gauti informaciją apie aktyvinimą arba *tikrąjį RDID prietaisų aktyvavimo laiką*. Taigi, reikalingos taip pat įprastos vaizdinės nuorodos apie aktyvavimą ar aktyvacijos būklę. Informacija apie PET technologijos buvimą ir pobūdį (t.y. laikinas sugadinimas, fizinis žymens nuėmimo pobūdis, kita) kaip ir organizacinės priemonės konkrečioje aplinkoje turėtų būti lengvai prieinama.

29 straipsnio Darbo grupė pažymi, jog dėl šių trijų informacijos pateikimo sąlygų visoms šalims teks nuolat remtis R&D (*angl.* Research & Development), „Tyrimai ir plėtra“.

5.3. Techninės ir organizacinės teisės į informacijos gavimą, duomenų taisymą ir naikinimą įgyvendinimo priemonės

Kaip apibūdinama žemiau, metodas, kuriuo diegiama RDID technologija, gali turėti didžiulę įtaką užtikrinant veiksmingą teisių gauti informaciją, taisyti ir naikinti duomenis įgyvendinimą, kaip numato Duomenų apsaugos direktyvos 12 straipsnis.

a) Priėjimas prie žymens turinio (Duomenų apsaugos direktyva, 12 straipsnis)

Pagal technologijos pobūdį, informacijos apie žymens turinį gavimas įmanomas tada, kai skaitytuvas veikia pagal žymens protokolą ir asmuo gauna vaizdą ekrane. Tačiau daugeliu naudojimo atvejų, žymuo turi tik tapatybės duomenis, kurio semantika gali paaiškėti tik pritaikius visą IT programą. Mūsų žiniomis, tik nedidelis RDID žymenų skaičius turi semantinę informaciją (apibūdinančią objektą, duomenų valdytojo identifikatorių, duomenų rinkimo pabaigą, t.t.), o tai irgi sudaro sunkumų asmenims gauti informaciją apie turinį.

Viena galimybė padidinti informacijos vertę yra nustatyti semantinius standartus naudojant, pavyzdžiui, XML. Kad ir kokios formos jie būtų, tokie semantiniai apibūdinimai vis dar sudaro prieigos sunkumų neįgaliotoms trečiosioms šalims. (žr. 3 skyrelį viršuje).

b) Turinio taisymas (Duomenų apsaugos direktyvos 12 b straipsnis)

Skirtingai nuo prieigos prie turinio, taisymas reikalauja, kad skaitytuvas veiktų su žymens protokolu ir sąveikaujančia IT sistema, leidžiančia asmeniui valdyti turinio skaitymą ir turinio keitimą.

Ši galimybė siūlo sukurti žymenyje savybę, kuri ištrintų arba sumaišytų prekės serijos numerį ir pateiktų tik visą ar dalį prekės klasės apibūdinimą (atvirkštinis variantas taip pat yra įmanomas, tačiau su skirtingomis privatumo reikšmėmis).

c) Turinio ištrynimasis (Duomenų apsaugos direktyvos 12 a straipsnis)

Ar žymenų gadinimo priemonės turėtų būti įdiegtos, kad asmenys galėtų sustabdyti asmens duomenų tvarkymą tuo metu, kai žymuo patenka į skaitytuvo lauką, ar ne, priklauso nuo teisinio pagrindo, reglamentuojančio asmens duomenų tvarkymą. Pavyzdžiui, toks diegimas nebūtų priimtinas tais atvejais, kai RDID žymenys yra pasuose, o duomenų apsaugos atžvilgiu tokios priemonės tampa būtinos, kai RDID žymenys tvirtinami prie vartojimo prekių. Ši tema buvo nagrinėjama Sidnėjuje vykusioje Duomenų apsaugos ir privatumo įgaliotinių konferencijoje, kuri atspindėta Sidnėjaus deklaracijoje dėl RDID¹⁹.

Per pastaruosius kelerius metus buvo siūlomi įvairūs sprendimai. Vienas iš siūlymų buvo naikinimo komandos įdiegimas. Tai reiškia, žymuo gali būti ilgam laikui ar laikinai deaktyvuotas pasiuntus „sunaikinti“ komandą. Ilgalakis deaktyvavimas gali būti atliktas pasinaudojus saugikliu, sujaukiant atmintį ar nuimant žymenį. Laikini deaktyvuoti galima mechaniškai arba taikant programinės įrangos užraktą. Šio metodo trūkumas yra tas, kad prarandamas RDID gebos privalumas atnaujinti veikimą už parduotuvės ribų. Taigi buvo siūlomi kiti metodai.

Aukščiau siūlytame variante numatoma pakeisti saugomus duomenis RDID žymenyje nuliais. Žymuo išlieka aktyvuotas, tačiau užklausus grąžina tik nulius vietoj skaičiaus. Ši sistema iš tikrųjų „nesugadina“ RDID. Žymuo tebereaguoja ir perduoda informaciją, kad asmuo neša žyminį vieneta, ir tai gali turėti tokias pasekmes. Pirma, kol RDID žymenys, grąžinantys tik nulius, dar nėra labai paplitę, vien tik egzistavimas tokio žymens sudaro vertingą informaciją. Ji rodo, kad asmuo yra nusipirkęs kažką iš parduotuvės, kuri žymi prekes. Išmananti šiuos dalykus kompanija gali atspėti. Antra, paaiškėja, kad iš pradžių RDID žymenys ketinami naudoti tik vertingoms prekėms. Keletą metų vien tik RDID žymens buvimas (netgi jeigu jis rodo tik nulius ar nesuprantamus duomenis) padės vagims, ieškantiems vertingų daiktų rūbinėse ir parkavimo vietose. Pagaliau, pagausėjus RDID žymenų, parduotuvės nemėgs tokių žymenų, kurie į užklausą atsako niekam tikusiais duomenimis.

Dar vienas siūlomas būdas yra fizinis žymens skydas, kurį tikriausiai mielai naudos pirkėjai. Pavyzdžiui, gali būti naudojamos piniginės su skydu ir tada banknotai su žymenimis nebūtų susekti. Aliuminio plokštelė, įdėta į RDID paso viršelį, būtų pakankama apsaugos priemonė turiniui apsaugoti, išskyrus atvejus, kai pasas yra atverstas. Tačiau skydeliai tinka ne visiems atvejams. Pavyzdžiui, drabužiai su įtaisytais žymenimis negali būti pakuojami su skydine medžiaga, kol dėvimi. Be to, toks metodas, regis, būtų pernelyg sunki našta tiems asmenims, kurie yra tiesiogiai atsakingi už žymens duomenų atskleidimo prevenciją.

Apibrėžiant, kaip žymenų neveiksmingumo, sugadinimo įrankiai turėtų veikti, be to, kas jau aptarta, standartizavimo institucijos, gamintojai ir RDID technologijos platintojai bei naudotojai turėtų atsižvelgti į tai, kad asmenys, nusprendę pašalinti žymenį, nebūtų baudžiami jokiomis priemonėmis.

Kaip ir prieš tai, 29 straipsnio darbo grupė pabrėžia, jog aptariant šias sąlygas, visos šalys turėtų nuolat remtis R&D (angl. Research and Development) - „Tyrimai ir plėtra“.

¹⁹ Rezoliucija dėl Radijo dažnių identifikavimo, priimta 25-oje Duomenų apsaugos ir privatumo įgaliotinių konferencijoje, 2003 Sidnėjuje, <http://www.privacyconference2003.org> teigia: „...kai RDID žymenis turi asmenys, jie privalo turėti galimybę ištrinti duomenis ir sustabdyti žymenų veikimą arba sunaikinti juos“.

5.4. Teisinis duomenų tvarkymo pagrindas

Žymenų išjungimas: Greta žymenų veikimo sustabdymo poreikio, aprašyto 5.3 skyriaus kontekste, kitos Duomenų apsaugos direktyvos nuostatos reikalauja šios funkcijos (atjungti žymenį). Iš tikrųjų, kai remiantis Duomenų apsaugos direktyva sutikimas yra vienintelis įstatymu pagrįstas teisėtas asmens duomenų rinkimas naudojant RDID technologiją (žr. skirsnį 4.2), asmenys bet kada gali atsiimti sutikimą, duotą dėl asmens duomenų tvarkymo (ankstesnis 7 a straipsnis). Jeigu asmuo neturi jokios priemonės žymens veikimo sustabdymui, toks asmuo, kuris nenori, kad žymuo testų informacijos teikimą su jo ar jos sutikimu, negalės pasinaudoti tokia teise. Kai asmens duomenys, sukaupti RDID žymens, buvo sukaupti kitu teisiniu pagrindu, o ne remiantis sutikimu, ne visada yra būtina tokiems žymenims turėti išjungimo priemones. Pavyzdžiui, kai asmens informacija, saugoma žymenyse, yra naudojama darbo kontekste dėl darbo reguliavimo, gali būti nereikalinga, kad žymenyse būtų stabdymo priemonės, jei duomenų tvarkymas remiasi darbo santykiais.

Kai kuriais atvejais taikant RDID technologiją, pavyzdžiui, kai asmuo turi teisę atsiimti jo ar jos sutikimą ar prieštarauti dėl duomenų tvarkymo (ankstesnis 14 a straipsnis) ir vėliau teisę sugadinti žymenį, tiek gamintojai, tiek RDID technologijos platintojai ir naudotojai privalo užtikrinti, kad tokį žymens sugadinimo (atjungimo) veiksmą būtų nesudėtinga atlikti. Kitaip tariant, duomenų subjektui atjungti žymenį turi būti lengva.

5.5. Duomenų saugumas

Šifruočių naudojimas žymenims ir pritaikymas: Kai RDID žymenys apima asmens duomenis, laikantis Duomenų apsaugos direktyvos 17 straipsnio nurodymų juose privalo būti įrengtos techninės priemonės, apsaugančios nuo neteisėto duomenų atskleidimo. Kol tokių priemonių nėra įrengta, bet kas, turintis skaitytuvą, galėtų „sužadinti“ žymenį ir gauti jame esančią informaciją. Tokios priemonės taip pat yra būtinos pagal Duomenų apsaugos direktyvos ankstesnį 6.1.d straipsnį, kad užtikrintų duomenų, saugomų žymenyje, integralumą, vengiant neteisėtų pakeitimų.

Techninių priemonių tipas priklausys nuo duomenų pobūdžio. Pagal žemiau pateiktą pavyzdį, daugeliu atvejų šiems žymenims prireiks duomenų šifruotės ir skaitytuvo autentiškumo paliudijimo, kad būtų užkirstas kelias trečiosioms šalims, turinčioms skaitytuvus, nuskaityti informaciją. Atsižvelgiant į atvejį, kai RDID žymenyje nurodoma paciento tapatybė, atsakingasis gydytojas ir ligoninės personalo atliekamos reikalingos procedūros, nesunku suprasti ligoninės įsipareigojimą užtikrinti, kad tokios informacijos negalėtų nuskaityti trečiųjų šalių skaitytuvai, ir poreikį pritaikyti tokias technines priemones, kaip šifruotė, kad būtų tam užkirstas kelias.

Paprasčiausias ir saugus būdas yra taikyti standartinius autentiškumo liudijimo protokolus (pvz., ISO/IEC 9798). Jie jau yra plačiai taikomi tinklalapiuose arba jautrioms kortelėms. Šiuose standartizuotuose protokoluose naudojamos elementarios šifruotės. Dėl simetrinių autentiškumo liudijimo metodų, o tai reiškia, jog siuntėjo ir gavėjo raktai yra vienodi, naudojami PAK (pranešimų autentiškumo nustatymo kodai) ar simetriniai šifruočių algoritmai (pvz., DES, AES). Asimetriniams šifruočių algoritmams (pvz., RSA, ECC) yra naudojamos parašų schemas.

Kai kurie šifruočių tipo autentiškumo liudijimo metodai yra įdiegti automobiliuose ar įėjimo kontroliavimo sistemose, tačiau juose dažnai naudojami patentuoti algoritmai, kadangi juos paprasčiau ir pigiau įdiegti negu standartinius algoritmus. Vis dėlto sustiprintam saugumui, kurio gali prireikti ypatingiems duomenims, turėtų būti įdiegti standartiniai algoritmai ir protokolai. Šių protokolų ir algoritmų privalumas yra tas, kad jie jau yra plačiai naudojami, taigi patikrinti ir išbandyti daugelio skirtingų šalių. Šiuo atžvilgiu jie yra laikomi saugiais.

Spaudoje pasirodė straipsnių, teigiančių, jog simetriniai algoritmai (tokie kaip AES) tinka RDID žymenims²⁰. Viena problema, naudojant simetrinius autentiškumo liudijimo algoritmus, yra ta, kad

²⁰Feldhofer M., Dominikus S., Wolkerstorfer J., „Simetrinių autentiškumo liudijimo algoritmų (AES) privalumai RDID sistemoms“. Pasitarimo apie šifruočių techninę įrangą ir įtvirtintas sistemas protokolai (CHES 2004, rugpjūčio 11-13, 2004, Bostonas, JAV), Mokslo apie kompiuterius paskaitų konspektai (LNCS) t. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, p. 357-370.

rakto įvedimas ir rakto valdymas yra sudėtingas. Asimetriniai metodai išvengia šios problemos, tačiau yra brangesni nei simetriniai.

6. Išvados

Atsižvelgdama į augantį RDID technologijos taikymą įvairiems tikslams ir įvairų panaudojimą, įskaitant didžiulę duomenų apsaugos svarbą, Darbo grupė laiko būtinu dalyku šiame etape išleisti šį Darbinį dokumentą ir teikti pagalbą svarstant su RDID susijusius klausimus. Darbo grupė tikisi, jog šio dokumento turinys bus naudinga parama svarstant RDID ir kviečia visus su tuo susijusius laikytis šiame dokumente minimų principų.

Šis Darbinis dokumentas yra parengtas remiantis turima informacija, atsižvelgiant į tokios technologijos plėtojimo padėtį ir ypač jos dabartinį diegimą daugelyje sektorių. Vis dėlto Darbo grupė supranta, jog RDID plėtotė tebevyksta: taikymo sritis nuolat tobulinama ir, augant patirčiai, auga žinios dėl svarstomų klausimų. Dėl šios priežasties Darbo grupė yra išipareigojusi tęsti technologijų plėtojimo šioje srityje monitoringą, bendradarbiaudama su suinteresuotomis šalimis. Keletas klausimų, iškeltų šiame Darbiniame dokumente, gali reikalauti peržiūrėjimo įgijus didesnę patirtį. Be to, priklausomai nuo RDID technologijos raidos ir jos taikymo, vėlesniame etape Darbo grupė gali nuspręsti išsamiau nagrinėti specifines sritis, teikdama papildomas rekomendacijas ypatingų taikymo atvejų klausimais.

PRIEDAS

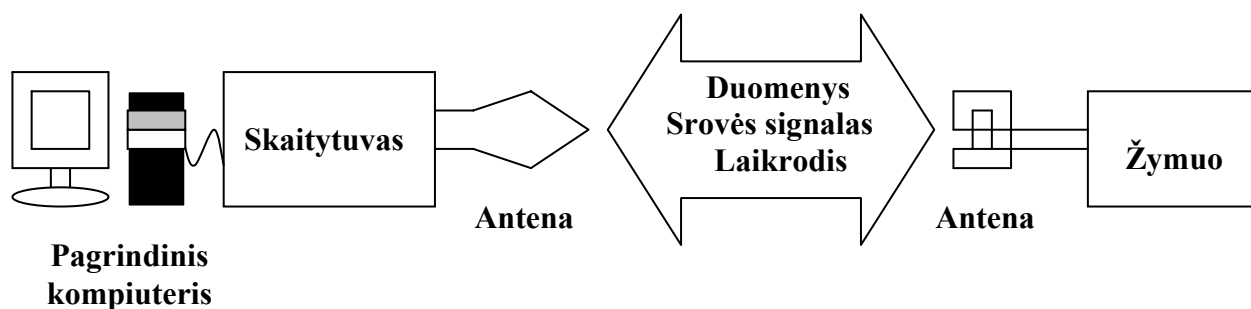
RDID TECHNOLOGIJA

Radio ryšys yra kylanti, perspektyvi technologija ir mūsų laikais jos taikymo sritys smarkiai plečiamos. Prie tokių sričių priskirtinas ir radio ryšio vietos tinklų (WLAN) ar žemo dažnio bangų radio ryšio įrengimas įvairiems prietaisams, pvz., nešiojamam kompiuteriui, delninukui, PDA, judriojo ryšio telefonams ir kitiems (Bluetooth).

Pastaraisiais metais naujoji technologija tampa vis populiareesnė. Ji vadinama RDID (anglų k. - RFID), ir reiškia Radio dažnių identifikavimą. Pagrindinė mintis, diegiant šią technologiją, buvo suteikti kiekvienam objektui, turinčiam pritrivintą žymenį, unikalią tapatybę, kuri gali būti perduota skaitytuvui radio dažniais. Ji leidžia naudotis įvairiais prietaisais tiekimo grandyje ir kitose pramonės šakose. Pradžioje RDID žymenis buvo planuojama naudoti vietoj brūkšninių kodų. Jų privalumai tarpo akivaizdūs: tokiems įrenginiams nebereikia užslėptos eilutės ir todėl registravimo procesas atliekamas automatiškai. Mūsų laikais, spartėjant technologinei pažangai, tampa įmanomos subtilesnės tokio ryšio technologijos pritaikymo galimybės. Prieš aptardami galimus taikymo atvejus, apžvelkime šią technologiją.

Paprasčiausią RDID sistemą sudaro du elementai: žymuo, pritrivintas prie objekto, ir skaitytuvas, gebantis išrinkti duomenis iš žymens. Šie du elementai yra sujungti radio ryšiu. Ir žymuo, ir skaitytuvas turi po anteną ir demoduliatorių (analoginį siuntėjas-gavėjas). Šis siuntėjas-gavėjas „verčia“ įeinančią analoginę informaciją iš radio ryšio į skaitmeninius duomenis. Šiuos duomenis apdoroja toliau skaitmeninė skaitytuvo dalis arba žymuo.

Žymens lygmenyje skaitmeninis tvarkymas atliekamas arba naudotojo sukurta technine įranga arba mikroprocesoriumi. Tam, kad duomenys, išrinkti iš žymenų, būtų tvarkomi, naudojamas pagrindinis kompiuteris, prijungtas prie skaitytuvo. Į pagrindinį kompiuterį reikia įvesti specialią žymens duomenis naudojančią programą. Piešinyje pavaizduota šiuolaikinė RDID sistema.



Paveikslas: RDID sistemos struktūra

Konkrečią RDID sistemą apibūdina įvairūs technologijos parametrai. Priklausomai nuo parametru, galimos įvairios RDID sistemos programos.

- *Aktyvieji/pasyvieji RDID žymenys.* Pagrindiniai žymenys, veikiantys pasyviai, gauna srovės ir laikrodžio signalą, tvarko bei siunčia duomenis skaitytuvo elektromagnetiniu lauku. Šio lauko intensyvumas ribojamas nacionaliniais ir tarptautiniais reglamentais. Taigi, žymens energijos naudojimas turi būti ribojamas, kad būtų užtikrintas taisyklingas veikimas. Lauko stiprumas mažėja priklausomai nuo atstumo iki skaitytuvo, todėl kuo mažiau sunaudojama žymens energijos, tuo platesnis skaitytuvo veikimo diapazonas, t.y. skaitytuvas ir žymuo geba palaikyti ryšį per didelį atstumą. Aktyvieji žymenys perduoda duomenis netgi jei nėra skaitytuvo ar jis nenustatytas. Tam juose yra baterijos. Tiksliau apibūdinant, žymenys gali turėti testerius arba matavimo prietaisus, fiksuojančius vertes, kaip, pavyzdžiui, termometras, kad būtų nustatomi lūžimai šaltojoje grandinėje, ir šiuo konkrečiu atveju baterija taip pat reikalinga, tačiau ji neturi tiesioginio poveikio aktyviam/pasyviam žymens pobūdžiui.

- *Veikiantys dažniai.* RDID sistemos gali veikti įvairiais dažniais, diapazonais ir būti įvairių sujungimo tipų. Šie parametrai dažnai labai priklausomi vieni nuo kitų. Dažniai įvairuoja nuo 135 kHz iki 5.8 GHz. Šiuo atžvilgiu labai reikšmingi yra tarptautiniai ribojimai ir fizinės savybės. Jungimas gali būti elektros, magnetinis ar elektromagnetinis. Sujungimo tipas turi įtakos veikimo diapazonui, kuris kinta nuo kelių milimetrų iki 15 m ir daugiau. Tiksliau apibrėžti galima išskiriant tokius požymius:

- Artimo sujungimo sistemos, kurioms reikalingi žymenys, veikiantys nedidelės apimties - iki vieno centimetro, diapazonu. Jos veikia tarp nuolatinės srovės ir 30 MHz dažniais ir privalo būti skaitytuvo viduje arba ant jo, kad susidarytų ryšys. Tokioms sistemoms būdingos didelės energijos sąnaudos ir spartus duomenų perdavimas.
- Nuotolinio sujungimo sistemos, veikiančios apytikriai vieno metro diapazonu. Daugelyje RDID sistemų naudojamas nuotolinis sujungimas ir veikimo dažniai yra nuo 135 kHz iki 13.56 MHz.
- Plataus diapazono sistemos, kurių diapazonas apima daugiau negu vieną metrą. Jos veikia nuo 868 MHz iki 5.8 GHz.

RDID sistemos gali kliudyti kitiems radijo ryšio įrenginiams. Todėl ypač svarbu tai, kad jos naudotų kitokius dažnius negu radijas, televizija ar judriojo radijo ryšio tarnybos. Svarbiausi dažniai naudojami RDID sistemose yra nuo 0 iki 135 kHz, o pramoniniai-moksliniai-medicinos (ISM) dažniai yra 6.78 MHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 869.0 MHz, 2.45 GHz, 5.8 GHz ir 24.125 GHz.

- *Skaitymo/rašymo gebėjimas.* RDID sistemų sudėtingumas įvairuoja. Jį dažnai riboja žymens gebėjimai.

- Mažo galingumo sistemose žymenys tik nuskaitymi. Skaitytuvas gali nuskaityti tik žymens turinį, o tai, apskritai kalbant, tėra serijos numeris su keliais baitais. Tokie paprasti žymenys dažnai naudojami dėl mažos kainos ir nedidelio mikroschemos užimamo ploto. Jos gali būti naudojamos vietoj brūkšnių kodų sistemų, kai reikia identifikuoti objektus, paprastai prekių sandėliavimui ir srauto reguliavimui gamybos procese. Dar tokie žymenys gali būti pritaikomi gyvūnams sekti.
- Vidurinėsios klasės RDID sistemų žymenys gali turėti rašytinę atmintį. Atminties talpa šiuo metu svyruoja nuo keleto baitų iki keleto dešimčių ar šimtų kilobaitų EEPROM²¹ pasyviuosiuose žymenyse iki SRAM²² aktyviuosiuose. Šiame diapazone jutikliai (temperatūros, slėgio...) taip pat gali būti integruoti į žymenis, pavyzdžiui, nustatantys aplinkosaugos nelaimes. Tokie žymenys vėliau gali būti pritaikyti prieigos kontrolei. Dar vienas veikiantis ir išbandytas pavyzdys - lagaminų sekimas oro uostuose. Galutinė lagamino paskirties vieta gali būti įrašoma į žymens atmintį ir maršrutas bus nustatytas automatiškai. Dar ši sistema sėkmingai veikia sveikatos apsaugos sektoriuje. Tokie žymenys gali būti naudojami ligoninėse, užrašant paciento gydymo detales, arba kontroliuojant keletą paciento būklės rodiklių.
- Bekontaktės jautrios kortelės su mikroprocesoriumi ir veikiančia sistema yra vadinamosios didelio galingumo sistemos. Jose taip pat yra tam tikra atminties talpa, kuri iš esmės didesnė negu taikoma vidutinio galingumo RDID žymenims. Kortelėse galima diegti sudėtingas funkcijas. Programos gali būti saugomos žymens atmintyje ir po to vykdomos mikroprocesoriumi. Dėl didelio tokių kortelių energijos vartojimo, tokių sistemų veikimo laukas mūsų dienomis yra tik keli centimetrai. Tokiose kortelėse gali būti įdiegti dar sudėtingesni įrenginiai. Jos gali būti pritaikytos ten, kur reikia tipinės jautrios kortelės, kaip antai prieigos kontrolė. Be to, jas galima naudoti kaip tapatybės liudijimą arba sveikatos draudimo kortelę. Kelionės dokumentai su ICC²³ (anglų k. Integrated Circuit Chip – mikroschema; lustas), kuriuos apibrėžia ICAO, ar viza ir leidimas gyventi užsienyje su ICC, akivaizdžiai įrodo RDID sistemų privalumus ir žada joms puikią perspektyvą.

Atlikta Briuselyje 2005 m. sausio 19 d.

Darbo grupės vardu
Pirmininkas
 Peter SCHAAR

²¹ Elektra ištrinama programuojama nuskaitymo atmintis

²² Statinė operatyvinė atmintis

²³ Mikroschema; lustas