31.03.2015

II sesija
Drošība un privātums kibertelpā

Tehnoloģiju piedāvāto iespēju rezultātā ir radušies dažādu līmeņu jautājumi saistībā ar drošību un privātumu. Kibertelpu var izmantot, lai nodarbotos ar krāpniecību, noziedzīgi iegūtu līdzekļus vai legalizētu tos, ielauztos datortīklos ar mērķi nozagt datus vai komercnoslēpumus, vai iznīcināt dokumentus. Šie izaicinājumi var skart valstu drošības aspektus, privātpersonu pilsonisko tiesību, tostarp privātās dzīves, aizsardzību, vai arī uzņēmumu un valstu ekonomisko attīstību un konkurētspēju.

No **valstu drošības** viedokļa jauns risks ir iespēja attālināti apdraudēt valsts kritiskās infrastruktūras objektus, tādējādi iespaidojot, piemēram, elektroenerģijas nodrošināšanu vai cilvēku drošību. Plašākā kontekstā uz valstu drošību attiecas arī valstu e-identifikācijas sistēmu droša darbība, kā arī iespējamu elektronisku un attālinātu vēlēšanu sistēmu nodrošināšanas jautājumi.

2013. gada 22. jūlija ES Padomes secinājumi apraksta Eiropas Savienības (ES) vispārējo kiberdrošības stratēģiju. Īpaša nozīme ir paredzama 2013. gada 12. augusta Direktīvai 2013/40/ES par uzbrukumiem informācijas sistēmām, kura dalībvalstīm ir jāpārņem līdz 2015. gada 4. septembrim. Šobrīd notiek darbs pie Direktīvas par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā ES (NIS direktīva).

Arvien aktuālāki kļūst **privātās dzīves aizsardzības jautājumi** – gan privātpersonu attiecībās ar valsti, gan privātpersonu savstarpējās attiecībās, kā arī, privātpersonu datu kā ekonomikas resursa izmantošanā. Valsts drošības interešu līdzsvarošana ar privātās dzīves aizsardzību var būt sarežģīta, jo mūsdienu tehnoloģiju attīstība ļauj realizēt, līdz šim nepieredzētu masveida uzraudzību. Privātpersonu savstarpējās attiecībās jaunus izaicinājumus regulējumam rada tādi izgudrojumi kā, piemēram, *Google glass* un pieaugošā tiešsaistes sociālo tīklu izplatība. Var sadurties dažādu valstu regulējums un atšķirīgas izpratnes par privātumu; praksē var būt grūti vai pat neiespējami pārkāpumu apturēt pie kādas valsts robežas.

Ar ES Tiesas Virspalātas 2014. gada 13. maija spriedumu lietā C-131/12 *Google/Spānija* tika nostiprinātas tiesības prasīt interneta meklētājprogrammas pakalpojuma sniedzējam savu datu dzēšanu. Tomēr šādu tiesību efektīva nodrošināšana rada jaunas izmaksas un virkni praktisku grūtību meklētājprogrammu pakalpojumu sniedzējiem, kuriem jāmeklē tehniski un administratīvi risinājumi pieteikumu saņemšanai, izskatīšanai un informācijas dzēšanai. Spriedumam var būt arī iespaids uz vienoto digitālo tirgu, jo, vienota regulējuma neesamības gadījumā, uzņēmumiem var būt atšķirīgi pienākumi dažādās dalībvalstīs.

2012. gada sākumā Eiropas Komisija ierosināja visaptverošu reformu ES 1995. gadā izstrādātajiem noteikumiem par datu aizsardzību, lai nostiprinātu privātuma tiesības tiešsaistē un veicinātu Eiropas digitālās ekonomikas attīstību. Komisija izstrādāja paziņojumu "Privātuma nodrošināšana

saistītā pasaulē Eiropas datu aizsardzības regulējums 21. gadsimtam" un priekšlikumus ietvara regulai un direktīvai par personas datu aizsardzību. Galvenās izmaiņas paredz, pirmkārt, vienotu datu aizsardzības noteikumu kopumu visā ES, novēršot pārmērīgas administratīvās prasības, otrkārt, personas datu apstrādātāju pienākumu un pārskatatbildības palielināšanu, treškārt, privātpersonām vienkāršāku pieeju saviem datiem, ceturtkārt, "tiesības tikt aizmirstam", piektkārt, principu, ka ES noteikumi būs jāpiemēro, ja personas datus ārvalstīs apstrādā uzņēmumi, kas darbojas ES tirgū un sniedz pakalpojumus ES pilsoņiem. Ar direktīvu tiek paredzēts, ka vispārīgie datu aizsardzības principi un noteikumi būs piemērojami policijas un tiesu iestāžu sadarbībai krimināllietās.

Vēl viens sarežģīts aspekts ir **digitālās ekonomikas iespēju izmantošanas iespaids uz drošumu un privātumu**. No globālās konkurētspējas viedokļa ES no, piemēram, Amerikas Savienotajām Valstīm un Indijas, atšķir tās nostāja attiecībā uz nodrošināmajām privātuma garantijām. Vienlaikus ir svarīgi, lai attiecīgie kritēriji būtu vienādi visā ES, ļaujot ES uzņēmumiem izmantot vienotā digitālā tirgus priekšrocības, nevis apgrūtinot to darbību.

Liela nozīme ir tam, vai pastāv pārliecība, ka veikt darījumus kibertelpā ir droši un ka pastāv regulējums, kas ļauj efektīvi atrisināt strīdus vai atgūt savus līdzekļus krāpniecības gadījumā. Tas veicina attiecīgo ekonomisko pakalpojumu sniegšanas un saņemšanas popularitātes paplašināšanos un attiecīgi izmaksu samazinājumu.

No privātuma viedokļa, privātpersonas arvien retāk spēj pilnvērtīgi izvērtēt to, kādai savu datu izmantošanai tās piekrīt, un pat saprast, kur un kā tiks izmantoti viņu dati. Privātpersonas bieži nemaz nevar izvērtēt iespējamos riskus, piemēram, to, kādā veidā darbojas datu brokeri, kuri vāc patērētāju informāciju no liela avotu skaita un pēc tam pārdod tos tālāk citiem uzņēmumiem. Datu brokeri lielākoties informāciju apkopo bez privātpersonu piekrišanas, turklāt nereti sasaistot tiešsaistē iegūtos datus un "fiziskajā pasaulē" iegūtos datus. Notiekot datu noplūdei no šāda datu brokera, ir gandrīz neiespējami noskaidrot noplūdes avotu un ir ļoti grūti veikt darbības, lai mazinātu kaitējumu, kas tādējādi nodarīts personai. Situāciju vēl vairāk sarežģī apstāklis, ka ir pazudusi robežšķirtne starp to, kas ir "privātie" vai "personu identificējošie" dati, jo, sapludinot lielu skaitu datu punktu, kas katrs par sevi netiktu uzskatīti par "privātiem", ir iespējams atvasināt personas identitāti.

Personas datu izmantošana ES ir atkarīga no tā dēvētās informētās piekrišanas. Nereti pakalpojumu sniedzēji informē par detalizētiem noteikumiem un nosacījumiem pakalpojuma izmantošanai un par to, kā tiks izmantota iegūtā informācija, taču lietotāji vienkārši deklarē savu piekrišanu. Iespējams, visos līmeņos ir jādomā par lietotāju izglītošanu par šādiem riskiem, kā arī par datu privātuma un drošības vienkāršotu pašdeklarēšanu.

Visbeidzot, tehnoloģiju un to sniegto iespēju ātrā attīstība nereti nozīmē, ka patērētāji pat īsti neapzinās, kādas sekas var būt tam, ka viņi atsakās no kādiem sava privātuma elementiem. Ir sagaidāms, ka nākotnē arvien raksturīgāks būs piedāvājums atklāt kādus privātuma elementus ar mērķi saņemt nelielu labumu no pakalpojuma sniedzēja. Apkopojot lielu apjomu šādas informācijas uzņēmējam var rasties jaunas uzņēmējdarbības iespējas, taču patērētājs var pat neapzināties iespējamo iespaidu nākotnē.

Iespējamie jautājumi diskusijai:

- Kā veicināt sabiedrības izglītošanos un uzticēšanos digitālajai videi, kā īstenot publisko-privāto sadarbību kiberdrošības uzlabošanai un pētniecību digitālās drošības jomā, stiprinot ES drošības pozīcijas?
- Kāda ir labā prakse personas datu aizsardzības un kibertelpas aizsardzības kompetento iestāžu sadarbībā? Kādi ir veiksmīgākie praktiskās sadarbības piemēri un dalībvalstu tiesiskā regulējuma piemēri?
- Kas ir "privātie dati" lielo datu laikmetā? Kā panākt sabiedriskā labuma maksimizēšanu, atverot datus, vienlaikus izskaužot datu masveida analītikas un šķērskorelēšanas (*cross corelation*) radītos riskus indivīdu privātumam?
- Kā aizsargāt personu identitāti ārpus eIDAS Regulas tvēruma? Kā ieviest principu "*safety sells*", it īpaši mazajos un vidējos uzņēmumos? Kā nodrošināt, lai mazie un vidējie uzņēmumi, veidojot elektroniskos pakalpojumus un lietotnes, izprastu un rūpētos par lietotāju drošību, nevis mēģinātu pēc iespējas ātrāk "palaist lietotni"?