Nordisk Administrativt Tidsskrift

ISSN: 2246-1310 Vol 97, No 1 (2020), e4095 https://doi.org/10.7577/nat.4095

Fagartikkel

Observationer om personuppgiftsskydd i offentlig förvaltning

Tarja Hautamäki*

Nycelord: Personuppgiftsskydd, offentlig förvaltning, digitalisering, automatiserad beslutprocess, biometrisk identifiering

Teknologins samhälleliga betydelse och en kraftig betoning av individens rättigheter och friheter har under det här årtusendet växt med tilltagande fart. I en verksamhetsmiljö som håller på att digitaliseras har det vid sidan om människans fysiska identitet uppstått en s.k. digital identitet, vilken i allt högre grad utgör grunden för individens rättigheter och möjligheter till påverkan samt för beslutsfattande och övervakning som riktar sig mot individen. Människor behöver digitala profiler för olika ärenden och profilerna innehåller personuppgifter som, om de hamnar i fel händer, kan äventyra integriteten och personuppgiftsskyddet. När man i den nya digitaliserade miljön behöver tolka gamla rättsnormer, kan det visa sig bli en rättslig utmaning att samtidigt optimera både den digitala utvecklingen och individens rättigheter och friheter.[1]

Den digitala hanteringen av personuppgifter i finländsk myndighetsverksamhet regleras i allmänna ordalag i ramverket om informationshantering som grundar sig på lagen om offentlighet i myndigheternas verksamhet (21.5.1999/621) och omfattar lagen om tillhandahållande av digitala tjänster (15.3.2019/306), lagen om elektronisk kommunikation i myndigheternas verksamhet (24.1.2003/13), lagen om informationshantering inom den offentliga förvaltningen (18.3.2019/906), arkivlagen (23.9.1994/831), förvaltningslagen (6.6.2003/434) och lagen om förvaltningens gemensamma stödtjänster för e-tjänster (29.6.2016/571). När det gäller skyddet av personuppgifter utgör EU:s allmänna

1 Korja 2016: 56–59, 453–454; Pedersen 2017: 27–29.

*Epost: tarja.hautamaki@obotnia.fi
Tarja Hautamäki, Dr. i förvaltningsvetenskap, fil. mag, Österbottens förbund.

dataskyddsförordning,[2] direktivet om skydd av personuppgifter som behandlas i brottsbekämpningssyfte[3] samt den nationella dataskyddslagen (5.12.2018/1050) den centrala författningshelheten, som bör tolkas och tillämpas tillsammans med andra lagar i ramverket i enlighet med andan i offentlighetslagen.

Påföljder för bristande efterlevnad av skyldigheterna i fråga om dataskydd

Trots att EU:s allmänna dataskyddsförordning ska tillämpas enhetligt i alla medlemsstater har det lämnats ett nationellt manöverutrymme när det gäller bestämmelser om sanktioner för bristande efterlevnad. I artikel 58 i förordningen föreskrivs att tillsynsmyndigheterna har rätt att ålägga den registeransvarige och personuppgiftsansvarige administrativa sanktionsavgifter eller andra påföljder för bristande efterlevnad av skyldigheterna i dataskyddsförordningen. Beroende på överträdelsens art kan sanktionsavgifterna uppgå till högst 20 miljoner euro eller, när det gäller ett företag, 4 % av den totala årliga globala omsättningen under det föregående budgetåret, beroende på vilket som är störst.

Den finska översättningen “hallinnollinen sakko” (“administrativa böter”) av begreppet “administrativa sanktionsavgifter” i dataskyddsförordningen har kritiserats och till och med ansetts vara misslyckad, liksom många andra ordval i den finska översättningen av dataskyddsförordningen. Termen “sakko” har traditionellt syftat på en straffrättslig påföljd. Administrativa påföljder som räknats i pengar utanför det straffrättsliga systemet har kallats för “rikemaksu” (“ordningsavgift”) eller “seuraamusmaksu” (“påföljdsavgift”) och har inte förståtts som utövande av domsrätt.[4] Titeln på 24 § i dataskyddslagen innehåller begreppet “hallinnollinen seuraamusmaksu” ("administrativa påföljdsavgifter") som är mer specifikt för den finländska rättsordningen, men i bestämmelsens första moment används ändå båda begreppen. I sitt yttrande ansåg grundlagsutskottet att det misslyckade begreppet “hallinnollinen sakko” (“administrativa böter”) i dataskyddsförordningen bör ingå i form av

[2] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[3] Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[4] Koillinen 2016: 575; Korpisaari, Pitkänen & Warma–Lehtinen 2018: 535–536.

ett informativt komplement till dataskyddslagen[5].

Dataskyddsförordningen gav medlemsstaterna möjligheten att införa egna regler om huruvida offentliga organ kan åläggas administrativa sanktionsavgifter och i vilken utsträckning de kan åläggas, dock utan att begränsa tillsynsmyndighetens befogenheter enligt artikel 83 i förordningen (DSF artikel 83). I Finland betraktades det som ett främmande förfarande för vårt rättssystem att ålägga offentliga organ administrativa sanktionsavgifter. Utgångspunkten är att myndigheterna redan är bundna av förvaltningens legalitetsprincip och måste följa den allmänna förvaltningslagstiftningen, samt att den som arbetar för en myndighet har som tjänsteplikt att behandla personuppgifter i enlighet med lagen.[6] Enligt grundlagsutskottet skulle dessutom en administrativ sanktionsavgift som åläggs myndigheterna vara problematisk i systemet för grundläggande rättigheter som helhet, eftersom det skulle ge ett mycket starkt skydd för en enskild grundläggande rättighet[7].

Även om ingen enighet nåddes i frågan[8] skrev man in i 24 § i dataskyddslagen att administrativa sanktionsavgifter inte får åläggas statliga myndigheter, statliga affärsverk, kommunala myndigheter, oberoende offentligrättsliga institutioner, parlamentariska organ, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland och ortodoxa kyrkan i Finland samt deras kyrkor, församlingar och andra organ, det vill säga de myndigheter som avses i 2 § i förvaltningslagen och inte heller statliga affärsverk. Universiteten anses också vara oberoende offentligrättsliga institutioner som inte kan bli föremål för administrativa sanktionsavgifter.

Offentliga och privata aktörer i Finland befinner sig följaktligen i en ojämlik situation när det gäller sanktionsavgifter, vilket är särskilt relevant när en offentlig och privat aktör konkurrerar om att tillhandahålla tjänster på samma marknad. Sett till tjänstemannens ansvar ligger den offentliga sektorns ansvar ytterst hos den enskilde tjänsteman som försummar sin tjänsteplikt och sanktionen är då straffrättslig. Inom den privata sektorn bärs ansvaret av en organisation som kan få en ekonomisk sanktion för försummelsen i form av en administrativ sanktionsavgift.[9] Vid utarbetandet av den nationella dataskyddslagen

5 GrUU 14/2018 rd s. 9.
6 RP 9/2018 rd. s. 105–196.
7 GrUU 14/2018 s. 20.
8 Se Betänkande av arbetsgruppen för genomförande av EU:s allmänna dataskyddsförordning (TATTI) 2017: 23–24; FvUB 13/2018 rd., FvUB 14/2018 rd.; LaUU 5/2018 rd.; GrUU 14/2018 rd.; GrUU 24/2018 rd.; GrUU 26/2018 rd.; Utlåtande av rådet för bedömning av lagstiftningen om utkastet till regeringens proposition till riksdagen med förslag till allmän lagstiftning som kompletterar EU:s allmänna dataskyddsförordning 8.2.2018.
9 Lång & Haavikko 2019: 5–6.

identifierades eventuella problem till följd av ojämlikheten och i regeringens förslag konstaterar man att effektiviteten hos påföljderna för myndigheters brott mot dataskyddsförordningen måste följas upp, i synnerhet när det gäller påverkan på konkurrensen[10].

I Sveriges lagstiftning har man å andra sidan kommit fram till en reglering som kraftigt betonar den grundläggande rätten till personuppgiftsskydd. 6 kap 2 § i lagen som kompletterar den allmänna dataskyddsförordningen (SFS 2018:218) gav tillsynsmyndigheten rätt att ålägga även en statlig eller kommunal myndighet administrativa sanktionsavgifter, som inte får överstiga 20 miljoner kronor. Samtidigt hävdes påföljden med fängelsestraff som funnits i personuppgiftslagen utifrån det så kallade förbudet mot dubbel bestraffning. Samma förseelse kan inte leda till både en hög sanktionsavgift och ett fängelsestraff. I Sverige ansåg man att det fanns starka skäl för att påföljderna för brott mot personuppgiftsskyddet skulle vara likadana för privata juridiska personer som för myndigheter eftersom hanteringsprocesserna för personuppgifter till stor del är likadana i privat och offentlig sektor samt att personuppgiftsskyddet i Europarätten är en grundläggande rättighet som måste respekteras på samma sätt i såväl privat som offentlig sektor.[11]

Om en offentlig förvaltnings verksamhet i Finland är klandervärd när det gäller dataskydd och de råd, varningar, anmärkningar eller bestämmelser som tillhör tillsynsmyndighetens korrigerande befogenheter (artikel 58 i DSF) inte har någon önskvärd effekt, kan man som en sista utväg ingripa i verksamheten med straffrättsliga medel i domstol. I strafflagen regleras brott mot dataskydd (SL 38:9 §), kränkning av kommunikationshemlighet (SL 38:3-4), dataintrång (SL 38:8-8a), brott mot sekretess och tjänstehemlighet (SL 38:1-2, 40:5). Ett allmänt skadeståndsansvar i enlighet med skadeståndslagen (3:2, 4:1–2) kan också vara aktuellt för skador som orsakats av fel eller underlåtenhet vid myndighetsutövning. Utifrån dessa författningar kan en tjänsteman i Finland till och med dömas till fängelse beroende på dataskyddsbrottets allvar.

Personuppgifter och digitaliserad offentlig förvaltning

Våren 2020 verkar all form av statlig verksamhet till följd av coronaviruspandemin flytta sig i

10 RP 9/2018 rd. s. 57.
11 SOU 2017:39: 281–297; Wedleby & Wetterberg 2018: 324–326.

en allt snabbare takt till digitala nätverksmiljöer, där det för ärendebehandling eller för att utöva olika funktioner är nödvändigt att behandla data om en person och identifiera personen elektroniskt. Härnäst granskas frågor som kan ha att göra med myndigheters automatiserade beslutsprocesser och biometrisk identifiering.

Automatiserade beslutsprocesser

Genom automatisering av rutinmässiga beslutsprocesser och massbehandling av uppgifter söker många myndigheter större effektivitet och ändamålsenlighet samt kostnadsbesparingar inom den offentliga sektorn. Till exempel har man ibehandlingen av skatteuppgifter och beräkningen av skattebeslut använt automatisering i enlighet med de lagändringar om beskattningsförfarandet som antogs år 2005. På Folkpensionsanstalten fattar robotar beslut om studiestöd och man planerar att testa automatiserat beslutsfattande om det allmänna bostadsbidraget. De mest synliga lösningarna med artificiell intelligens för kunder är förmodligen virtuella tjänsterådgivare dvs. chatbots.[12]

I artikel 22 i dataskyddsförordningen regleras det angående automatiserade individuella beslut inklusive profilering, att en person har rätt att inte bli föremål för ett beslut som enbart grundar sig på automatiserad behandling, såsom profilering, och som har rättsverkningar på personen eller påverkar personen på motsvarande betydande sätt. När det gäller myndighetsutövning har dock den enskilde sällan eller aldrig verklig valfrihet i beslutsprocessen. Även om myndigheter enligt motiveringen till lagen om digitala tjänster utöver andra möjligheter till ärendehantering är skyldiga att organisera digitala tjänster och e-tjänster som rör personers status, rättigheter och skyldigheter och att säkerställa lämplig tillgång till alternativa kanaler och tjänstevägar,[13] så kan det ändå vara så svårt att nå icke-automatiserade förfaranden (t.ex. telefontjänster eller tjänster på myndighetens kontor) att utövandet av den rättighet som föreskrivs i artikel 22 i dataskyddsförordningen till och med kan ifrågasättas. Riksdagens justitieombudsman har därför ansett att det är problematiskt att ha ett förfarande där en myndighet motiverad av effektivisering och behovet av arbetskraft endast erbjuder elektronisk ärendehantering. Förfarandet uppfyller inte principerna om god förvaltning och tjänsteprincipen som är bindande för myndigheten.[14]

Den biträdande justitieombudsmannen har ansett att skatteförvaltningens automatiserade beslutsförfarande är olagligt eftersom det inte grundar sig på lämplig och exakt lagstiftning som borde ta hänsyn till grundlagens krav på korrekt genomförande av god förvaltning och

12 Folkpensionsanstalten, Verksamhetsberättelse och bokslut 2017: 12; Uutinen 26.11.2019.; Tapio 2019.
13 RP 60/2018 rd. s. 66.
14 EOAK 31.12.2015 Dno 4653/4/14.

rättssäkerhet samt tjänsteplikten. På lagnivå bör det fastställas hur ärenden väljs ut för automatiserat beslutsfattande och hur offentlighet uppnås när det gäller algoritmerna för automatiserat beslutsfattande. Regleringen av vad en algoritm innebär i automatiserat beslutsfattande måste vara avgränsad och exakt. Förtroendeskyddet som är en av grunderna i god förvaltning förutsätter öppen information och rådgivning. Mot bakgrund av skadeståndsansvaret och den straffrättsliga legalitetsprincipen i 8 § i grundlagen går det vid automatiserat beslutsfattande inte att härleda något exakt tjänsteansvar och inte heller dess innehåll och omfattning.[15] I Sverige har rättssäkerheten i automatiserade processer inom den offentliga förvaltningen stärkts genom lagändringar som gör det möjligt att lämna information till enskilda om innehållet i algoritmer och datorprogram som påverkar beslut om medborgare.[16]

Enligt biträdande justitieombudsmannen och grundlagsutskottet berör det automatiserade beslutsfattandet ett mycket brett spektrum av specifika rättsliga frågor gällande grundläggande rättigheter och utövande av offentlig makt som bör bedömas utifrån behovet av att utveckla den allmänna lagstiftningen. Med enskilda lagstiftningsförslag om användningen av spelrummet i dataskyddsförordningen kan man inte bortse från förverkligandet av grundlagens krav på grundläggande rättigheter och begränsningar och ansvar i utövandet av offentlig makt. Grundlagsutskottet betonar att regleringen av dataskyddsförordningen när det kommer tillskydd av personuppgifter inte ger tillräcklig grund för automatiserat beslutsfattande med tanke på principerna om god förvaltning och förvaltningens rättssäkerhetssystem.[17]

Såväl biträdande justitieombudsmannen som grundlagsutskottet betonar vikten av att utreda regleringen som rör automatiserat beslutsfattande. Den biträdande justitieombudsmannens och grundlagsutskottets åsikter sammanfaller också med Hirvonens slutsatser: enbart dataskyddsförordningen och dess bestämmelser om automatisk databehandling löser inte problemen med automatiserat beslutsfattande. Enligt Hirvonen är förändringen i förfarandet dessutom mycket mer omfattande än bara en fråga om personuppgifter. Det är även fråga om allvarliga rättssäkerhetsaspekter.[18]

Datorer eller artificiell intelligens kan inte hållas straffrättsligt ansvariga eller sanktioneras.

---

15 EOAK 20.11.2019 Dno 3379/2018. Jmfr. Den utredning som justitiekanslern på eget initiativ begärt om automatiseringen av beslutsfattandet om socialskydd vid FPA. (OKA 24.10.2019. Dno OKV/21/50/2019.)
16 SOU 2018:25: 19–21.
17 GrUU 7/2019 rd. s. 8–12.
18 Hirvonen 2018: 310.

Ur ansvarssynpunkt är det viktigt vem och vilka som ansvarar för den automatiserade driften och i vilken utsträckning den tjänsteansvariga eller annan person som ansvarar för verksamheten ansvarar för datorns beslut och funktioner. Pöysti sätter samarbetet mellan yrkesverksamma inom olika områden i centrum. Han efterlyser att utformningen av digitala tjänster och system från början, vid sidan av teknikexperter, ska involvera experter på verksamhetens innehåll från den sektor där den tekniska lösningen ska användas. Det är också nödvändigt med förebyggande rättslig planering och rättslig kvalitetssäkring av digitala tjänster och system i linje med krav på grundläggande rättigheter, mänskliga rättigheter och god förvaltning.[19]

Automatiserat beslutsfattande förefaller omfatta ett antal frågor som inte regleras av den allmänna förvaltningslagstiftningen: hur regleringen av automatiserade förvaltningsprocesser och beslutsfattande uppfyller förvaltningens rättsliga principer, offentlighetsprincipen och de förvaltningsprinciper som utgör en del av grunden i god förvaltning, samt hur den säkerställer rättssäkerhet och ett korrekt genomförande av det offentliga ansvaret.[20] Justitieministeriets förstudie som klargör viktiga rättsliga frågor färdigställdes i februari 2020. Där lade ministeriet också fram ett förslag om att gå vidare med utredningen.[21]

Biometrisk identifiering av en person

Traditionellt baseras identifieringen av en person på vad personen känner till (t.ex. lösenord och koder) eller vad personen äger (t.ex. passerkort och nycklar). Biometrisk identifiering baseras på vad en person är när det kommer till en fysiologisk egenskap eller beteendemässig egenskap. Identifieringen kan också ske automatiskt på en dator med hjälp av olika enheter och programvara, utan att en person utför identifieringen.[22] Enligt artikel 4 i dataskyddsförordningen avses med biometriska uppgifter alla personuppgifter som erhållits genom teknisk behandling av en fysisk persons fysiska och fysiologiska egenskaper eller beteende, såsom ansiktsbilder eller fingeravtrycksuppgifter, som gör det möjligt att identifiera eller verifiera den fysiska personen.

Biometrisk identifiering har ökat explosionsartat under 2000-talet. Orsakerna är det politiska klimatet i början av millenniet, de minskade kostnaderna för biometrisk identifiering och samhällets krav på enkel, effektiv och mer tillförlitlig identifiering i den nya digitala miljön.

19 Pöysti 2019.
20 GrUU 62/2018 rd s. 9; GrUU 70/2018 rd. s. ; GrUU 78/2018 rd. pp. 5–6; GrUU 7/2019 rd. pp. 8–12.
21 Se Automaattiseen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeet (2020).
22 Korja 2016: 139–141.

Terrorattackerna den 11 september 2001 ledde till en snabb utvidgning av införandet i Förenta staterna och även i Europa med säkerhet som motivering.[23]

Vid den biometriska identifiering som används i myndighetsverksamhet kan det uppstå en konflikt mellan intresset hos den myndighet som ansvarar för registret med personuppgifter och i slutändan det samhällsnyttiga syftet å ena sidan, och den registrerades rättigheter å andra sidan. Den 20 augusti 2019 ålade Datainspektionen i Sverige de första administrativa sanktionsavgifterna för brott mot dataskyddsförordningen åt Skellefteå gymnasienämnd, som på prov hade använt ansiktsigenkänning med kamera för att säkerställa gymnasieelevers närvaro i klassrummen. Enligt nämnden tar det 10 minuter av lektionstid att kontrollera närvaron med den traditionella metoden. Med hjälp av närvarokontroll genom ansiktsigenkänningsteknik uppskattade nämnden att gymnasieskolan skulle spara in totalt 17 280 timmar i arbetstid per år.

Datainspektionen ansåg att förfarandet var oförenligt med fyra artiklar i dataskyddsförordningen. Ansiktsigenkänningen hade utförts i strid med de principer för behandling av personuppgifter som fastställs i artikel 5 i förordningen. Kameraövervakningen hade i onödigt stor omfattning kränkt elevernas privatliv i deras vardagliga miljö. Närvarokontroll är möjlig på sätt som inte kränker privatlivet i den utsträckningen. De uppgifter som samlas in genom ansiktsigenkänning är biometriska uppgifter som tillhör särskilda kategorier av personuppgifter i enlighet med artikel 9, vars behandling alltid kräver ett särskilt skäl. Enligt Datainspektionen uppfyllde inte det samtycke som gymnasienämnden begärt kriterierna för frivillig, individualiserad, medveten och otvetydig viljeyttring som krävs enligt förordningen, eftersom det finns ett beroendeförhållande mellan eleverna och den registeransvariga nämnden. Nämnden hade också underlåtit att uppfylla de skyldigheter som föreskrivs i artiklarna 35 och 36 om konsekvensbedömning och samråd med myndigheten.

Den sanktionsavgift som Datainspektionen ålade Skellefteå gymnasienämnd var 200 000 kronor. Dess storlek berodde bland annat på att det handlade om en myndighet och ett test som pågick under en begränsad tidsperiod, som varade i tre veckor och gällde 22 elever. Den maximala sanktionsavgift som myndigheten kunde ha ålagts var 10 miljoner kronor. I enlighet med artikel 58.2 i dataskyddsförordningen fick nämnden dessutom en varning om risker för framtida överträdelser, eftersom den hade meddelat att den skulle fortsätta med

23 Korja 2016: 148.

ansiktsigenkänning för att kontrollera elevernas närvaro.[24]

Biometriska uppgifter bör behandlas som särskilda personuppgifter i enlighet med dataskyddslagstiftningen, men behovet av specifik lagreglering av biometri kan ändå anses vara uppenbart på grund av biometriska uppgifters oföränderlighet. Om du förlorar unika biometriska data kan de inte bytas ut mot nya[25]. Användningen av identifieringsredskap berör frågor om integritet, rättssäkerhet och andra grundläggande rättigheter för vilka grundlagen kräver reglering. Detta har delvis redan genomförts genom att den befintliga lagstiftningen om skydd av personuppgifter anpassats till kraven i nya verksamhetsmiljöer.

I sin avhandling anser Korja att skyddet av personuppgifter för biometrisk identifiering bör regleras av en allmän lag som vid behov kan kompletteras med uppförandekoder. Om en särskild lag skulle antas om biometrisk identifiering skulle det finnas en risk för att den "drunknar i floden av regler om personuppgiftsskydd" och förbigår den vanliga medborgarens medvetenhet, och att lagens mål inte skulle uppnås.[26] Regleringen av biometrisk identifiering ligger nu på nivå med allmän lag, men ovan nämnda beslut om Skellefteå gymnasienämnd visar att det inte garanterar att lagens mål uppnås.

Slutligen

Som nämnts ovan är det möjligt att digitalisera även myndighetsverksamhet, till exempel genom att automatisera beslutsprocessen och använda biometrisk identifiering. Utgångspunkten för vårt rättssystem är dock att uppgifter med rättsverkningar på enskilda utförs av andra individer och juridiska personer. Vår förordning erkänner inte tekniska lösningar som juridiska aktörer som också skulle kunna hållas ansvariga för sina handlingar. Det är nödvändigt att utveckla lagstiftningen på ett sådant sätt att de rättsliga konsekvenserna av tekniska lösningar, som till följd av samhällets snabba digitalisering har uppstått vid sidan av fysiska miljöer, bedöms och beaktas i förordningen.

Nu när EU:s allmänna dataskyddsförordning har tillämpats i ett par år är det för tidigt att dra slutsatser om huruvida dess tillämpning i den offentliga förvaltningens digitaliserade miljöer har varit framgångsrik. Utformningen av innehållet i regleringen av dataskydd kräver tid och den konkretiseras när tillsynsmyndigheterna och domstolarna har fällt avgöranden i tillräckligt många ärenden samt när det till följd av avgörandena har färdigställts nya

24 DI-2019-2221. 2019-08-20.
25 Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) 2010: 99.
26 Korja 2016: 438–447.

kommentarer och anvisningar. Det är också viktigt att samla erfarenheter från de som tillämpar reglerna. Till det förpliktigar redan artikel 97 i dataskyddsförordningen som föreskriver att Europakommissionen regelbundet måste överlämna rapporter om tillämpningen och översynen av förordningen till Europaparlamentet senast den 25 maj 2020 och därefter vart fjärde år. Rapporterna kommer att producera material som säkerligen också kommer att tjäna forskningen. I skrivande stund pågår åtgärder för att begränsa coronaviruspandemins spridning och myndigheters verksamhet har överförts till digitala nätmiljöer snabbare än planerat. Effekterna av detta skeende på behandlingen av personuppgifter bör också undersökas. En empirisk studie av dataskyddsförfaranden som tillämpas vid undantagsförhållanden skulle ge värdefull information för det framtida lagstiftningsarbetet.

Källor

Automaattiseen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeet (2020). Esiselvitys 14.2.2020. Oikeusministeriö. Hämtad 2020-02-16 https://api.hankeikkuna.fi/asiakirjat/ff3444f4-24c9-4ee8-8c9d-7bc581c0021a/796dac3f-4527-45c0-a7b8-d63024345ac8/JULKAISU_20200214084153.pdf

DI-2019-2221. 2019-08-20. Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktigenkänning för närvarokontroll av elever.

EOAK 14.3.2019. Dnro 923/2018. Henkilötunnusten merkitseminen Tuomas-järjestelmästä tulostettuun lausumapyyntöön. (Att antecka personnummer i en utsaga som skrivits ut i Tuomas-systemet.)

EOAK 20.11.2019. Dnro 3379/2018. Verohallinnon automatisoitu päätöksentekomenettely ei täytä perustuslain vaatimuksia. (Skatteförvaltningens automatiserade beslutsförfarande uppfyller inte grundlagens krav.)

EOAK 31.12.2015. Dnro 4653/4/14. Yrittäjien rakentamisilmoitukset vain sähköisesti – AOA Sakslin: Verohallinto unohti asiakkaan oikeudet. (Företagare måste lämna bygganmälan elektroniskt – BJO Sakslin: Skatteförvaltningen förbisåg klienternas rättigheter.)

EU :n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö (2017). Oikeusministeriön julkaisuja 35/2017. Lönnberg Print & Promo : Oikeusministeriö. Hämtad 2019-11-25 https://julkaisut.valtioneuvosto.fi/handle/10024/80098

FvUB 13/2018 rd. Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

FvUB 14/2018 rd. Regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten och till vissa lagar som har samband med den.

GrUU 14/2018 rd. Grundlagsutskottets utlåtande till förvaltningsutskottet. Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

GrUU 24/2018 rd. Grundlagsutskottets utlåtande till förvaltningsutskottet. Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

GrUU 7/2019 rd. Grundlagsutskottets utlåtande till förvaltningsutskottet. Regeringens proposition till riksdagen med förslag till lag om behandling av personuppgifter i migrationsförvaltningen och till vissa lagar som har samband med den.

GrUU 70/2018 rd. Grundlagsutskottets utlåtande till social- och hälsovårdsutskottet. Regeringens proposition till riksdagen med förslag till patientförsäkringslag och till vissa lagar som har samband med den.

GrUU 78/2018 rd. Grundlagsutskottets utlåtande till social- och hälsovårdsutskottet Regeringens proposition till riksdagen med förslag till ändring av socialtrygghets- och försäkringslagstiftningen med anledning av EU:s allmänna dataskyddsförordning.

Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) (2010). Työryhmän loppuraportti. Sisäasiainministeriön julkaisut 32/2010. Helsinki: Sisäasiainministeriö. Hämtad 2019-12-29 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79876/sm_322010.pdf

Hirvonen, Hanne (2018): Automatisoitu päätöksenteko julkisella sektorilla. Oikeus 3/2018, 302–310.

Kansaneläkelaitos. Toimintakertomus ja tilinpäätös 2017. Hämtad 2019-11-30 https://www.kela.fi/documents/10180/0/Kelan+toimintakertomus+2017+%28pdf%29/7c92b093-4fa4-447e-9895-fece68654aa8

Koillinen, Mikael (2016): Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. Defensor Legis N :o 4/2016, 571–586.

Korja, Juhani (2016): Biometrinen tunnistaminen ja henkilötietojen suoja. Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. Acta Universitatis Lapponiensis 325. Hansaprint Oy: Lapin yliopisto. Oikeustieteiden tiedekunta.

Korpisaari, Päivi, Olli Pitkänen & Eija Warma-Lehtinen (2018): Tietosuojalainsäädöntö. BALTO Print Liettua: Lakimiesliiton kustannus.

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi yleiseksi lainsäädännöksi 8.2.2018. Dnro: VNK/133/32/2018.

LaUU 5/2018 rd. Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

Lång, Jukka & Tuomas Haavikko (2019): Mitä muutoksia uusi kansallinen tietosuojalaki tuo käytännössä? Hämtad 2019-11-29 www.edilex.fi/artikkelit/19271

OKA 24.10.2019. Dnro OKV/21/50/2019. Selvityspyyntö (Begäran om utredning).

Pedersen, Morten Jarlbæk (2017): Digitaliseringsparat lovgivning: Ved vi, vhad vi talar om? Nordisk administrativ tiedsskrift 3/2017, 25–29.

Pöysti, Tuomas (2019): Digitalisaation vastuukysymykset työterveyshuollossa. Hämtad 2019-12-03 https://www.okv.fi/fi/tiedotteet-ja-puheenvuorot/517/oikeuskansleri-poysti-digitalisaation-vastuukysymykset-tyoterveydenhuollossa-kuka-vastaa-terveydenhuollon-palveluiden-digitaalisesta-tuotekehyksesta-ja-mitka-ovat-roolit-vastuut-ja-oikeusturvajarestelyt-siina/

RP 2/2020 rd. Regeringens proposition till riksdagen med förslag till lagar om ändring av vissa bestämmelser om behandling av personuppgifter inom justitieministeriets förvaltningsområde.

RP 60/2018 rd. Regeringens proposition till riksdagen med förslag till lag om tillhandahållande av digitala tjänster och lag om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet.

RP 9/2018 rd. Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s allmänna dataskyddsförordning.

Sankari, Valtteri & Matti Wiberg (2019): GDPR ei toimi: Tietosuojakäytännöt eivät noudata asetusta. Yhteiskuntapolitiikka 84:3, 340–346. Hämtad 2019-11-29 http://urn.fi/URN:NBN:fi-fe2019061220180

SOU 2017:39. Ny dataskydsslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Betänkande av Dataskyddsutredningen. Hämtad 2019-11-01 https://www.regeringen.se/49a184/contentassets/e98119b4c08d4d60a0a2d0878990d5ec/ny-dataskyddslag-sou-201739

SOU 2018:25. Juridik som stöd till förvaltningens digitalisering. Betänkande av Digitaliseringsrättsutredningen. Hämtad 2019-11-01 https://www.regeringen.se/495f60/contentassets/e9a0044c745c4c9ca84fef309feafd76/juridik-som-stod-for-forvaltningens-digitalisering-sou-201825.pdf

Tapio, Ilari (2019): Oikeuskansleri otti Kelan päätösrobotin tutkintaan – kyse on samantapaisesta automatiikasta kuin verottajalla. Länsi-Suomi 27.11.2019. Hämtad 2019-11-20 https://ls24.fi/lannen-media/oikeuskansleri-otti-kelan-paatosrobotin-tutkintaan-kyse-on-samantapaisesta-automatiikasta-kuin-verottajalla

Tähti Aarre (2019): Euroopan Unionin yleiseen tietosuoja-asetukseen ja Suomen tietosuojalakiin liittyvistä oikeudellisista ongelmista. Defensor Legis 3/2019, 324–338.

Uutinen 26.11.2019. Apulaisoikeusasiamies: automatisoidun päätöksenteon sääntelytarpeet tulee selvittää viipymättä. Hämtad 2019-11-30 https://www.vero.fi/tietoa-verohallinnosta/uutishuone/uutiset/uutiset/2019/apulaisoikeusasiamies-automatisoidun-p%C3%A4%C3%A4t%C3%B6ksenteon-s%C3%A4%C3%A4ntelytarpeet-tulee-selvitt%C3%A4%C3%A4-viipym%C3%A4tt%C3%A4/