FÖRVALTNINGSRÄTTEN I STOCKHOLM

Avdelning 34

DOM
2021-09-30
Meddelad i Stockholm

Mål nr
4756-21

KLAGANDE
Polismyndigheten

MOTPART
Integritetsskyddsmyndigheten

ÖVERKLAGAT BESLUT
Integritetsskyddsmyndighetens beslut 2021-02-10, se bilaga 1

SAKEN
Sanktionsavgift enligt brottsdatalagen

FÖRVALTNINGSRÄTTENS AVGÖRANDE

Förvaltningsrätten avslår överklagandet.

Postadress	Besöksadress	Telefon	Telefax	Expeditionstid
115 76 Stockholm	Tegeluddsvägen 1	08-561 680 00 **E-post**: avd34.fst@dom.se www.domstol.se/forvaltningsratten-i-stockholm/	-	måndag–fredag 08:00–16:00

YRKANDEN M.M.

Integritetsskyddsmyndigheten (IMY) beslutade den 10 februari 2021 att påföra Polismyndigheten en sanktionsavgift om 2 500 000 kr för överträdelser av 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen (2018:1177) genom användande av applikationen Clearview AI under perioden hösten 2019 till och med den 3 mars 2020. IMY beslutade även att förelägga Polismyndigheten att vidta utbildningsåtgärder och övriga organisatoriska åtgärder som krävs för att säkerställa att de rutiner som finns når hela organisationen och att myndigheten därmed kan visa och säkerställa att all behandling av personuppgifter är författningsenlig. IMY beslutade vidare att förelägga Polismyndigheten att informera de registrerade vars personuppgifter myndigheten matat in i Clearview AI samt att vidta möjliga och relevanta åtgärder för att de personuppgifter som den matat in i Clearview AI raderas från applikationen. Skälen för beslutet och tillämpliga bestämmelser framgår av bilaga 1.

Polismyndigheten överklagar beslutet i den del det avser påförande av sanktionsavgift och yrkar i första hand att någon sanktionsavgift inte ska tas ut och i andra hand att den påförda sanktionsavgiften ska sättas ned.

IMY anser att överklagandet ska avslås.

SKÄLEN FÖR AVGÖRANDET

Vad målet gäller

Den första frågan som förvaltningsrätten har att ta ställning till är om Polismyndigheten har behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen. Om förvaltningsrätten kommer fram till att så är fallet måste därefter prövas om IMY haft grund för sitt

ingripande i form av en sanktionsavgift. Om förvaltningsrätten kommer fram till att IMY haft fog för sitt beslut även i denna del måste slutligen sanktionsavgiftens storlek prövas.

Har IMY gjort sin bedömning utifrån ett bristfälligt underlag?

Polismyndigheten gör gällande att IMY inte har ställt några frågor om vilka skyddsåtgärder i form av riktlinjer, utbildningar, kommunikationskanaler etcetera som Polismyndigheten har tagit fram i enlighet med kraven i 3 kap. 2 § brottsdatalagen.

Förvaltningsrätten kan i denna del konstatera att IMY den 14 december 2020 skickat en kommunicering till Polismyndigheten enligt vilken myndigheten informerats om att IMY överväger att besluta om att överträdelse av bl.a. 3 kap. 2 § brottsdatalagen skett. Polismyndigheten har getts en svarsfrist till och med den 11 januari 2021 för att komma in med eventuell ytterligare dokumentation, vilket enligt förvaltningsrättens mening får anses vara en skälig tidsfrist. Förvaltningsrätten bedömer mot denna bakgrund att IMY inte kan anses ha brustit i sin utrednings- eller kommuniceringsskyldighet enligt förvaltningslagen (2017:900). Det saknas därmed skäl att angripa beslutet på denna grund.

Har Polismyndigheten behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen?

Har lämpliga tekniska och organisatoriska åtgärder vidtagits?

Polismyndigheten har i denna del anfört i huvudsak följande. Det har vidtagits lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de personuppgiftsbehandlingar som vidtas inom myndigheten är författningsenliga och att de registrerades rättigheter skyddas. Av riktlinjer

för processägares instruktioner om personuppgiftsbehandling framgår bl.a. att en processägare som utgångspunkt är ansvarig för myndighetens personuppgiftsbehandling inom sitt ansvarsområde. För att säkerställa detta krävs att processägaren eller den som är ansvarig för personuppgiftsbehandlingen ger instruktioner om hur personuppgifter ska behandlas samt fördelar arbetsuppgifter till en eller flera medarbetare. Riktlinjerna reglerar i vilka situationer som processägaren behöver ge instruktioner om personuppgiftsbehandling genom styrdokument och när det är tillräckligt att det sker genom exempelvis dokumentation över personuppgiftsbehandling i myndighetens förteckning. Riktlinjerna reglerar även hur styrdokument, i de fall det behövs, ska utformas. Det framgår även att processägare i styrdokumentet uttömmande ska reglera vilka IT-system och/eller lagringsytor eller motsvarande som ska eller får användas för personuppgiftsbehandlingen samt vilka som regelmässigt ska eller får använda uppgifterna som omfattas av behandlingen.

Polismyndigheten har även tagit fram riktlinjer för dataskydd vid verksamhetsutveckling, för samordning av personuppgiftsfrågor, för särskild registervård av personuppgiftsbehandlingar, avseende informationsbehandling med stöd av IT samt för mobil elektronisk utrustning. Av den sistnämnda framgår bl.a. att endast mobiltelefoner, surfplattor och motsvarande som tillhandahålls av arbetsgivaren får användas i tjänsten. Det framgår även att användning av mobil IT-utrustning i strid med riktlinjerna kan leda till att arbetsgivaren vidtar disciplinära åtgärder.

Samtliga anställda vid Polismyndigheten genomgår en obligatorisk utbildning i informationssäkerhet, som fokuserar på frågor kopplade till IT-utrustning och hur den får användas. Polismyndigheten har även tagit fram flera särskilda utbildningar på olika nivåer avseende dataskydd. Samtliga dessa utbildningar är tillgängliga för alla inom myndigheten och i vissa fall

har processägare angett att genomgången utbildning är en förutsättning för att få behörighet till särskilda IT-stöd. Dessutom har det nyligen tagits fram en ny introduktionsutbildning och Polismyndigheten har redan påbörjat en översyn av den nya utbildningen i syfte att uttryckligen förklara att externa applikationer inte får laddas ner och användas utan en föregående bedömning. På Polismyndighetens intranät finns också omfattande och övergripande information om personuppgiftsbehandling. Att ett fåtal av cirka 33 000 anställda har behandlat personuppgifter i strid med framtagna riktlinjer och utbildningar fråntar inte myndigheten sitt personuppgiftsansvar men bör inte innebära en presumtion för att myndigheten inte har vidtagit lämpliga organisatoriska och tekniska åtgärder enligt 3 kap. 2 § brottsdatalagen. Det är inte rimligt att det ska krävas att hundra procent av de anställda ska göra hundra procent rätt vid varje behandlingsåtgärd för att myndigheten ska anses ha uppfyllt kraven. Det föreligger inga systematiska brister. Spridningen av dataskyddsombudets rekommendation inom myndigheten i nu aktuell fråga är ett tydligt och verksamt exempel på att myndigheten har förmåga att sprida information rörande dataskyddsfrågor inom myndigheten eftersom behandlingen upphörde omedelbart därefter och sedan inte återupptagits.

Förvaltningsrätten gör i denna del följande bedömning.

Inledningsvis instämmer förvaltningsrätten i IMY:s bedömning att Polismyndigheten är personuppgiftsansvarig för den i målet aktuella behandlingen, oaktat att Polismyndigheten inte tillhandahållit den ifrågavarande applikationen eller sanktionerat användandet av densamma.

Vilka tekniska och organisatoriska åtgärder som den personuppgiftsansvarige bör vidta får avgöras i varje enskilt fall beroende på vilken verksamhet det rör sig om och beroende på vilka personuppgifter som ska behandlas. Organisatoriska åtgärder som avses i nu aktuell bestämmelse är

bl.a. att anta interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av IT-system, behandlingar och vidtagna åtgärder och teknisk spårbarhet genom loggning och logguppföljning. Skyldigheten att vidta lämpliga åtgärder är inte knuten till en viss tidpunkt, utan något som den personuppgiftsansvarige ständigt ska ha för ögonen. Åtgärder som har vidtagits måste därför kontinuerligt revideras och vid behov förändras (prop. 2017/18:232 s. 173–174 och 453).

Förvaltningsrätten kan konstatera att Polismyndigheten kommit in med dokumentation om ett antal riktlinjer och information om utbildningsåtgärder som inte var kända för IMY vid tidpunkten för det överklagade beslutet. Förvaltningsrätten anser att den dokumentation som Polismyndigheten gett in i samband med överklagandet i och för sig visar att tekniska och organisatoriska åtgärder har vidtagits, exempelvis har det antagits riktlinjer för mobil elektronisk utrustning. Bestämmelsen i 3 kap. 2 § brottsdatalagen innebär dock att den personuppgiftsansvarige ska säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Att en åtgärd vidtas, exempelvis framtagandet av en riktlinje, kan således inte per automatik anses innebära att den aktuella bestämmelsen är uppfylld. Åtgärdens lämplighet och effekt sett till syftet måste också bedömas.

Den nu aktuella behandlingen av biometriska uppgifter är av känslig art och innebär särskilda risker, vilket medför höga krav på tekniska och organisatoriska åtgärder för att kunna säkerställa en författningsenlig behandling. I de inlämnade riktlinjerna finns inte någon närmare information om behandling av biometriska uppgifter eller ansiktsigenkänning. Det som framgår är att fotografier som går att identifiera utgör personuppgifter och att dessa ska hanteras i enlighet med numera upphävda personuppgiftslagen

(1998:204) och polisdatalagen (2010:361). Frågan berörs således inte specifikt i riktlinjerna. Inte heller har Polismyndigheten visat att information har lämnats på annat sätt om och i så fall hur biometriska uppgifter ska hanteras för att anses ha behandlats författningsenligt. Den omständigheten att polismyndigheten påbörjat en översyn av den nya utbildningen i syfte att uttryckligen understryka att externa applikationer inte får användas utan en föregående rättslig bedömning i sig talar för att myndighetens tidigare utbildnings- och informationsinsatser varit bristfälliga i detta avseende. Mot bakgrund av det nu sagda instämmer förvaltningsrätten i IMY:s bedömning att Polismyndigheten inte har kunnat visa att myndigheten genom lämpliga tekniska och organisatoriska åtgärder har säkerställt att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Polismyndigheten har således behandlat personuppgifter i strid med 3 kap. 2 § brottsdatalagen.

Har Polismyndigheten haft laglig grund för behandling av biometriska uppgifter?

Polismyndigheten vidgår att dessa frågor inte har utretts inför den behandling som enstaka medarbetare utfört genom att testa den aktuella applikationen. Det ska dock framhållas att det vid utredning av specifika fall av sexuella övergrepp mot barn eller för att identifiera individer kopplade till grov organiserad brottslighet kan vara en absolut nödvändig utredningsåtgärd att göra en biometrisk jämförelse. Polismyndigheten har därför inte behandlat personuppgifter i strid med 2 kap. 12 § brottsdatalagen.

Förvaltningsrätten anser i denna del att det inte har kommit fram skäl att frångå den bedömning som IMY har gjort i det överklagade beslutet. Avsaknaden av en föregående rättslig bedömning från Polismyndighetens sida och knapphändig information om hur de biometriska uppgifterna i detalj har använts i applikationen, exempelvis hur länge de har sparats, gör

att det inte går att dra slutsatsen att Polismyndighetens användning av biometriska uppgifter varit absolut nödvändig för ändamålet med behandlingen. Polismyndigheten har därmed överträtt 2 kap. 12 § brottsdatalagen.

Har Polismyndigheten underlåtit att genomföra en konsekvensbedömning?

Användandet av applikationen har inte varit sanktionerad av Polismyndigheten utan det har varit fråga om att några få medarbetare, under en begränsad tid, testat en gratis applikation utan att dessförinnan ha informerat eller frågat sina chefer. Som en följd av att Polismyndigheten inte känt till applikationen har några rättsliga bedömningar inte kunnat göras. Under sådana förhållanden anser Polismyndigheten att den inte kan klandras särskilt för att någon konsekvensbedömning inte har genomförts.

Förvaltningsrätten har bedömt att Polismyndigheten inte har kunnat visa att myndigheten genom lämpliga tekniska och organisatoriska åtgärder har säkerställt att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Förvaltningsrätten bedömer att varken lagstiftningen eller dess förarbeten medger ett undantag från Polismyndighetens skyldighet att i det nu aktuella fallet genomföra en konsekvensbedömning innan behandlingen påbörjas. Det är ostridigt att någon sådan bedömning inte gjorts. Förvaltningsrätten bedömer därmed att Polismyndigheten har överträtt även 3 kap. 7 § brottsdatalagen.

Har IMY haft grund för att påföra Polismyndigheten en sanktionsavgift?

Förvaltningsrätten bedömer således att Polismyndigheten har behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 och 7 §§

brottsdatalagen. Förvaltningsrätten har därmed att ta ställning till om IMY haft grund för sitt ingripande i form av en sanktionsavgift.

Polismyndigheten har i denna del anfört i huvudsak följande. Det framgår uttryckligen av förarbetsuttalanden att det inte är rimligt att ålägga en myndighet sanktionsavgift om någon i ett enstaka fall behandlat en personuppgift felaktigt, även om det kan vara djupt kränkande. Det har inte varit fråga om ett systematiskt eller av Polismyndigheten sanktionerat agerande. Behandlingen har dessutom omfattats av vissa skyddsåtgärder som minskat risken för de registrerade. Bland annat har bilder beskurits så att eventuella utomstående inte kunnat få någon information om sammanhanget, vilket minskar risken för de registrerade. I detta fall är det inte heller fråga om att Polismyndigheten inte hörsammat tillsynsmyndighetens tidigare förelägganden. Polismyndigheten har vidtagit en mängd förebyggande åtgärder för att säkerställa korrekt hantering och så snart myndigheten fick kännedom om användningen av Clearview AI vidtogs åtgärder.

Förvaltningsrätten bedömer att den nu aktuella behandlingen av biometriska uppgifter i sig är av känslig art och innebär särskilda risker, vilket medför höga krav på tekniska och organisatoriska åtgärder för att kunna säkerställa en författningsenlig behandling. Det har i det aktuella fallet varit fråga om integritetskänsliga uppgifter som utan en föregående rättslig bedömning använts i en extern applikation. Det har vidare inte kunnat klarläggas vad som hänt med de använda personuppgifterna. Förvaltningsrätten anser att de potentiella skadeverkningarna bör bedömas som stora, inte minst med hänsyn till att behandlingen inneburit att biometriska uppgifter matchats mot stora mängder av personuppgifter som hämtats utan filtrering på det öppna internet. Detta ska beaktas vid val av ingripande. Förvaltningsrätten anser att de omständigheter som Polismyndigheten har lyft fram, exempelvis att det inte varit fråga om uppsåtliga överträdelser eller att det varit fråga om

överträdelser trots tidigare ingripanden från IMY, i och för sig är sådana omständigheter som ska beaktas i förmildrande riktning vid val av ingripande. Förvaltningsrätten bedömer dock att överträdelsens svårighetsgrad och den fara som överträdelsen inneburit väger tyngre än de omständigheter som Polismyndigheten har lyft fram som förmildrande. Förvaltningsrättens sammantagna bedömning är således att IMY haft fog för att påföra Polismyndigheten en sanktionsavgift.

Sanktionsavgiftens storlek

Förvaltningsrätten kan konstatera att de omständigheter som redogjorts för i ovanstående stycke är omständigheter som ska beaktas inte bara vid bestämmande av val av ingripande utan även vid bestämmande av storleken på sanktionsavgiften. Enligt förvaltningsrättens mening framstår den påförda sanktionsavgiften som välavvägd och avskräckande i enlighet med bestämmelsens syfte (prop. 2017/18:232 s. 328). Möjligheten att helt eller delvis sätta ned sanktionsavgiften är en undantagsbestämmelse som enligt förvaltningsrättens uppfattning bör tillämpas restriktivt. Vid en sammantagen bedömning anser förvaltningsrätten att det inte har kommit fram skäl att helt eller delvis sätta ned den påförda sanktionsavgiften.

FÖRVALTNINGSRÄTTENS SLUTSATSER

Förvaltningsrätten bedömer sammanfattningsvis att Polismyndigheten genom användande av applikationen Clearview AI under perioden hösten 2019 till och med den 3 mars 2020 har behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen. IMY har haft grund för att påföra en sanktionsavgift och sanktionsavgiften framstår som väl avvägd. Överklagandet ska alltså avslås i dess helhet.

FÖRVALTNINGSRÄTTEN I STOCKHOLM **DOM**

HUR MAN ÖVERKLAGAR

Detta avgörande kan överklagas. Information om hur man överklagar finns i bilaga 2 (FR-03).

Anna Önell
Chefsrådman

Nämndemännen Åsa Fallqvist, Maria Holm och Mattias Östholm har också deltagit i avgörandet.

Förvaltningsrättsfiskalen Martin Une-Larsson har varit föredragande.

Integritetsskydds myndigheten

Polismyndigheten
Skickas endast per e-post
registrator.kansli@polisen.se

Diarienummer:
DI-2020-2719

Ert diarienummer:
A126.614/2020

Datum:
2021-02-10

Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetens användning av Clearview AI

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Polismyndigheten har behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 § och 7 § första stycket brottsdatalagen genom att använda applikationen Clearview AI under perioden hösten 2019 till och med 3 mars 2020.

Integritetsskyddsmyndigheten beslutar med stöd av 6 kap. 1 § brottsdatalagen att Polismyndigheten ska betala en sanktionsavgift på 2 500 000 (två miljoner femhundra tusen) kronor.

Integritetsskyddsmyndigheten förelägger Polismyndigheten enligt 5 kap. 7 § första stycket 2 brottsdatalagen att vidta utbildningsåtgärder och övriga organisatoriska åtgärder som krävs enligt 3 kap. 2 § brottsdatalagen för att säkerställa att de rutiner som finns når hela organisationen och att myndigheten därmed kan visa och säkerställa att all behandling av personuppgifter är författningsenlig. Åtgärderna ska ha vidtagits senast den 15 september 2021.

Integritetsskyddsmyndigheten förelägger med stöd av 5 kap. 7 § första stycket 2 brottsdatalagen Polismyndigheten att enligt 4 kap. 2 § brottsdatalagen informera de registrerade, vars personuppgifter Polismyndigheten matat in i Clearview AI, i den utsträckning skyldigheten att lämna information inte är begränsad enligt 4 kap. 5 § brottsdatalagen. Informationen ska ha lämnats senast den 15 september 2021.

Integritetsskyddsmyndigheten förelägger med stöd av 5 kap. 7 § första stycket 2 brottsdatalagen Polismyndigheten att vidta möjliga och relevanta åtgärder för att de personuppgifter som Polismyndigheten matat in i Clearview AI raderas från applikationen. Sådana åtgärder ska ha vidtagits den 15 september 2021.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen, uppmärksammades i februari 2020 genom uppgifter i media på att brottsbekämpande myndigheter i Sverige kunde ha använt sig av applikationen Clearview AI. IMY inledde mot bakgrund av uppgifterna omgående en granskning där Polismyndigheten ombads besvara om myndigheten använt sig av applikationen samt med vilket rättsligt stöd behandling i så fall skett. Av yttranden från Polismyndigheten under våren 2020 framgick att applikationen använts av några anställda inom myndigheten vid ett antal tillfällen utan att myndigheten tillhandahållit applikationen till de anställda. IMY inledde därför en fördjupad granskning av Polismyndighetens användning av Clearview AI.

Clearview AI är en applikation tillhandahållen av ett amerikanskt företag som erbjuder en ansiktsigenkänningstjänst där användaren, efter att ha laddat ner applikationen på en digital enhet, laddar upp en bild som genom biometri matchas mot ett mycket stort antal bilder som skrapats från det öppna internet.[1] Användaren får sedan ett resultat i form av ett antal webbadresser där eventuella matchningar finns.[2]

Polismyndighetens användning av applikationen Clearview AI

Polismyndigheten har uppgett att applikationen Clearview AI använts vid ett antal tillfällen under perioden hösten 2019 till och med 3 mars 2020.

Det är medarbetare vid den Nationella Operativa Avdelningen (NOA) samt region Syd som har använt sig av Clearview AI. Vid NOA har applikationen använts av totalt sex medarbetare varav fem använt applikationen i operativ verksamhet, bl.a. för att identifiera målsäganden i misstänkta sexualbrott mot barn samt i spanings-verksamheten för att försöka identifiera okända personer vid spaning av grov organiserad brottslighet. Vid polisregion Syd har applikationen använts vid utredning av sexualbrott mot barn samt testats av medarbetare mot bilder i Polismyndighetens s.k. OBS-portal.[3] När Polismyndighetens användning av Clearview AI blev känd genom uppgifter i media gick myndighetens dataskyddsombud ut med en rekommendation om att Nationellt Forensiskt Centrum och NOA skulle klargöra och sprida att sådan användning inte var tillåten.

Motivering av beslutet

Polismyndighetens ansvar för anställdas behandling av personuppgifter inom den brottsbekämpande verksamheten

Polismyndigheten är en stor organisation med ett särskilt uppdrag att upprätthålla lag och ordning. Polismyndigheten styrs därtill av tydlig lagstiftning kring hur personuppgifter ska behandlas, särskilt inom den brottsbekämpande verksamheten. Den stora mängd personuppgifter, även känsliga sådana, som myndigheten behandlar samt de långtgående maktbefogenheter Polismyndigheten har gör att myndigheten har ett särskilt ansvar för att personuppgifter behandlas korrekt.

[1] Webbtjänsten uppger att de samlat tre miljarder ansiktsbilder från Facebook, YouTube och miljoner andra webbplatser. IMY rapport 2021:1; Integritetsskyddsrapport 2020 – redovisning av utvecklingen på it-området när det gäller integritet och ny teknik, sid. 70.
[2] https://clearview.ai, 2020-11-25.
[3] it-stöd inom Polismyndigheten där underrättelseuppgifter förmedlas till den brottsbekämpande verksamheten.

Polismyndigheten är, som personuppgiftsansvarig, ansvarig för all personuppgiftsbehandling som sker under myndighetens ledning eller på myndighetens vägnar enligt 3 kap. 1 § brottsdatalagen. Det innebär att all personuppgiftsbehandling som utförs vid myndigheten faller under Polismyndighetens personuppgiftsansvar, även den behandling personuppgiftsbiträden, anställda, personer som är att jämställa med anställda (t.ex. inhyrd personal) eller uppdragstagare utför.[4] Även av 2 kap. 1 § lagen (2018:1693) om polisens behandling inom brottsdatalagens område (PBDL) framgår att Polismyndigheten är ansvarig för den personuppgiftsbehandling som utförs vid myndigheten. Det innebär att det är Polismyndighetens skyldighet att tillse att all behandling som sker inom myndigheten har bl.a. en rättslig grund, ett berättigat ändamål och att tillräckliga skyddsåtgärder är på plats genom lämpliga tekniska och organisatoriska åtgärder. Polismyndigheten ska tillse att det finns tydliga riktlinjer och rutiner avseende de it-verktyg som de anställda får använda och att de anställda är tillräckligt utbildade och informerade om hur personuppgifter får behandlas.[5]

Enligt Polismyndigheten är det ett fåtal anställda som använt Clearview AI utan att myndigheten tillhandahållit applikationen till de anställda. Behandlingen har dock skett vid utförande av de anställdas arbetsuppgifter på myndigheten. Behandlingen har dessutom utförts med personuppgifter hämtade från aktuella utredningar och vid majoriteten av tillfällena under pågående brottsutredningar, dvs. under myndighetsutövning. Att det skett utan att myndigheten tillhandahållit Clearview AI eller godkänt användningen av it-verktyget fråntar därmed inte Polismyndigheten det ansvar som myndigheten har som personuppgiftsansvarig.

IMY konstaterar mot denna bakgrund att Polismyndigheten är ansvarig för de anställdas behandling av personuppgifter vid användningen av Clearview AI.

Polismyndighetens skyldighet att genom tekniska och organisatoriska åtgärder säkerställa och visa att myndighetens personuppgiftsbehandling är författningsenlig

Som personuppgiftsansvarig har Polismyndigheten enligt 3 kap. 2 § brottsdatalagen en skyldighet att, genom tekniska och organisatoriska åtgärder, säkerställa och kunna visa att myndighetens behandling av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Det ska i varje enskilt fall bedömas vilka sådana åtgärder som behövs med beaktande av bl.a. vilka personuppgifter som behandlas.[6] Organisatoriska åtgärder kan bl.a. vara att anta interna strategier för dataskydd, informera och utbilda anställda samt säkerställa en tydlig ansvarsfördelning.[7] Åtgärder som kan vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av it-system, behandlingar och vidtagna åtgärder m.m.[8]

Polismyndigheten har i ärendet lämnat in en intern rutin för personuppgiftsbehandling inom myndigheten. Något ytterligare styrdokument för de anställdas behandling av personuppgifter har inte lämnats in. Inte heller något underlag kring hur utbildning av anställda eller hur den interna rutinen ska nå hela organisationen har lämnats in eller redogjorts för. Det saknas också uppgift om att någon utbildning eller motsvarande aktivitet faktiskt har genomförts inom myndigheten. Att anställda vid två olika

[4] Prop. 2017/18:232 s. 171 f., 319 och 452.
[5] Se vidare nedan under rubriken Polismyndighetens skyldighet att genom tekniska och organisatoriska åtgärder säkerställa och visa att myndighetens personuppgiftsbehandling är författningsenlig.
[6] Prop. 2017/18:232 s. 172 f.
[7] Sandén, H-O, 2019, SFS 2018:1177 Lagkommentar, Norstedts juridik.
[8] Prop 2017/18:232, s. 453.

organisatoriska enheter använt sig av Clearview AI i strid med gällande reglering visar att rutinen inte fått tillräckligt genomslag inom myndigheten. Polismyndigheten har mot denna bakgrund inte kunnat visa att det finns tillräckliga organisatoriska åtgärder, i form av t.ex. interna strategier eller utbildning, på plats för att säkerställa att behandlingen är författningsenlig.

IMY konstaterar att Polismyndigheten inte har vidtagit lämpliga organisatoriska åtgärder för att säkerställa och kunna visa att myndighetens behandling av personuppgifter varit författningsenlig. Polismyndigheten har därmed överträtt 3 kap. 2 § brottsdatalagen.

Polismyndighetens behandling av biometriska uppgifter i samband med användningen av Clearview AI

Enligt Polismyndighetens uppgifter har bilder på personer, som sedan omvandlats till biometriska uppgifter, i pågående operativa ärenden lästs in i Clearview AI vid ett flertal tillfällen.

Polismyndigheten har inte redogjort för hur de biometriska uppgifterna som lästs in i Clearview AI behandlas i applikationen, t.ex. om och i så fall hur länge uppgifterna sparas, hur matchningen av biometriska uppgifter går till, om uppgifterna överförs till tredjeland eller om uppgifterna lämnas ut till andra i samband med användningen. Det beror enligt uppgifter från Polismyndigheten på att inga rättsliga bedömningar har gjorts före användningen av Clearview AI.

Biometriska personuppgifter är känsliga personuppgifter och får enligt 2 kap. 12 § brottsdatalagen endast behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen. Av 2 kap. 4 § PBDL framgår att Polismyndigheten får behandla biometriska uppgifter om användningen är absolut nödvändig för ändamålet med behandlingen.

Användningen av en tjänst som Clearview AI innebär att enskildas biometriska personuppgifter matchas mot stora mängder personuppgifter som ofiltrerat inhämtats från det öppna internet. Enligt IMY:s bedömning kan en brottsbekämpande myndighets behandling av personuppgifter vid användning av en sådan tjänst sannolikt inte uppfylla det strikta krav på nödvändighet som följer av brottsdatalagen och det bakomliggande brottsdatadirektivet.[9] Europeiska dataskyddsstyrelsen har gett uttryck för en liknande uppfattning.[10]

Den behandling av biometriska uppgifter som skett vid Polismyndighetens användning av Clearview AI har utförts utan någon kontroll eller kunskap från Polismyndigheten om hur uppgifterna hanteras av Clearview AI. Någon bedömning av om behandlingen varit absolut nödvändig enligt 2 kap. 12 § brottsdatalagen har inte skett. Genom den information som lämnats in i ärendet har Polismyndigheten inte visat att myndighetens behandling av biometriska uppgifter i tjänsten Clearview AI varit absolut nödvändig för ändamålet för behandlingen.

[9] Artikel 10 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 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.
[10] EDPB response to MEPs Sophie in ‘t Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI.

IMY konstaterar att Polismyndighetens behandling av biometriska uppgifter har skett i strid med 2 kap. 12 § brottsdatalagen.

Skyldighet att genomföra en konsekvensbedömning

Enligt 3 kap. 7 § första stycket brottsdatalagen är en personuppgiftsansvarig skyldig att genomföra en konsekvensbedömning innan påbörjan av en ny behandling som kan antas medföra särskild risk för intrång i den registrerades personliga integritet.

Av förarbetena till brottsdatalagen och det bakomliggande brottsdatadirektivet framgår att vid bedömningen av om en konsekvensbedömning behövs ska behandlingens omfattning, art, sammanhang och art beaktas. Särskilt ska beaktas om behandlingen innefattar någon ny teknik.[11]

De personuppgifter som har behandlats i applikationen är biometriska uppgifter och dessa får, som redovisats ovan, endast behandlas om det är särskilt föreskrivet och absolut nödvändigt med hänsyn till ändamålet med behandlingen. Eftersom användningen av Clearview AI har inneburit behandling av biometriska uppgifter, som omfattar ansiktsigenkänning, med ny teknik tillhandahållen av en extern aktör i tredjeland kan behandlingen antas ha inneburit en särskild risk för intrång i registrerades personliga integritet. En konsekvensbedömning skulle därför ha genomförts innan behandlingen påbörjades. Användningen av applikationen Clearview AI påbörjades dock utan att några rättsliga överväganden eller beaktande av risker för intrång i de registrerades personliga integritet ägde rum.

Polismyndigheten har inte använt applikationen systematiskt i sin verksamhet och applikationen har inte rekommenderats av myndigheten. Som IMY konstaterat ovan är dock Polismyndigheten ansvarig för den behandling anställda utfört vid användningen av Clearview AI. Bristen på organisatoriska åtgärder har medfört att anställda använt applikationen utan att dessförinnan genomföra en konsekvensbedömning, trots att det krävs enligt 3 kap. 7 § brottsdatalagen.

IMY konstaterar att Polismyndigheten i strid med 3 kap. 7 § första stycket brottsdatalagen underlåtit att genomföra en konsekvensbedömning före användningen av Clearview AI.

Val av ingripande

Av 5 kap. 7 § brottsdatalagen följer de korrigerande befogenheter IMY har att tillgå vid överträdelser av nämnda lag. Dessa utgörs av bl.a. förelägganden, förbud mot behandling samt utfärdande av sanktionsavgift.

Av 6 kap. 1 och 2 §§ brottsdatalagen följer att IMY kan utfärda sanktionsavgift vid överträdelse av bl.a. bestämmelserna i 2 kap. 12 § samt 3 kap. 2 och 7 §§ brottsdatalagen. Sanktionsavgiften ska uppfylla de krav som ställs i brottsdatadirektivet på att sanktioner ska vara proportionella, avskräckande och effektiva.[12]

Vid bedömningen av om en sanktionsavgift ska tas ut och sanktionsavgiftens storlek ska särskild hänsyn tas till de omständigheter som anges i 6 kap. 4 § brottsdatalagen, dvs. om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller

[11] Prop. 2017/18:232 s.181 f.
[12] Prop. 2017/18:232 s. 309 f.

kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet, vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen, och om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

IMY konstaterar att Polismyndigheten brustit i flera avseenden i sitt personuppgiftsansvar vid användningen av Clearview AI. Polismyndigheten har inte vidtagit tillräckliga organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter i det aktuella fallet varit författningsenlig, behandlat biometriska uppgifter i strid med brottsdatalagen samt underlåtit att genomföra en konsekvensbedömning.

Som IMY konstaterat ovan innebär detta att Polismyndigheten behandlat personuppgifter i strid med 2 kap. 12 § samt 3 kap. 2 § och 7 § första stycket brottsdatalagen.

Det har inte kunnat utredas om de registrerade lidit någon faktiskt skada vid Polismyndighetens användning av Clearview AI. Detta är dock inte avgörande för om sanktionsavgift ska tas ut, utan det faktum att risk för skada förelegat är enligt förarbetena tillräckligt för detta.[13] Genom användningen av Clearview AI har anställda vid Polismyndigheten fått tillgång till integritetskänsliga uppgifter om ett stort antal registrerade. EU-domstolen har uttalat att tillgång till stora mängder av personuppgifter av en myndighet måste ses som ett särskilt intrång, oavsett om de enskilda lidit någon skada av behandlingen eller inte.[14] Även de uppgifter som Polismyndigheten matat in i applikationen har varit av integritetskänsligt slag och det har inte kunnat klarläggas vad som hänt med dessa personuppgifter efter inmatningen. Med anledning av vad som nu anförts bedömer IMY risken för skada för de registrerade som hög i det aktuella fallet.

Polismyndigheten har behandlat personuppgifter utan rättsliga överväganden och utan någon kontroll över eller bedömning av behandlingens intrång i enskildas personliga integritet. Vad avser användningen av Clearview AI har Polismyndigheten inte kunnat redogöra för vad som skett med de personuppgifter myndigheten matat in i applikationen samt med det resultat man erhållit. Det kan förutsättas att de uppgifter som matats in i applikationen ofta omfattats av någon form av sekretess, t.ex. 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), och Polismyndigheten har inte presenterat någon sekretessbrytande grund som kunnat motivera utlämnande av uppgifterna. Dessa omständigheter innebär att det finns skäl att se allvarligt på överträdelserna.

Också omfattningen och varaktigheten av behandlingen ska beaktas vid bestämmandet av sanktionsavgiftens storlek. En förmildrande omständighet är att det endast är ett fåtal registrerade vars personuppgifter delats med Clearview AI. Användningen av Clearview AI har dock sammanlagt skett under några månaders tid, och upphörde först sedan Integritetsskyddsmyndighetens granskning påbörjats. Dessutom har Polismyndigheten genom användningen av Clearview AI fått tillgång till ett stort antal personuppgifter och det är oklart hur länge de inmatade personuppgifterna och de uppgifter som erhållits genom matchningen behandlats.

Det får vidare anses försvårande att de registrerades uppgifter matchats mot en applikation med personuppgifter från hela det öppna internet samt att Polismyndigheten inte har någon kunskap om vad som hänt med de uppgifter som

[13] Prop. 2017/18:232 s. 483.
[14] Eu-domstolens domar i målen C-594/12 punkt 35 samt C-623/17 punkt 70.

matats in. Det faktum att det varit biometriska, dvs. känsliga personuppgifter, som behandlats och att uppgifterna använts för ansiktsigenkänning gör därutöver att det finns skäl att se allvarligt på överträdelsen.[15]

Sammanfattningsvis medför de redovisade omständigheterna att en sanktionsavgift ska tas ut och att en förhållandevis kännbar sanktionsavgift är motiverad.

Sanktionsavgiftens storlek

Enligt 6 kap. 5 § brottsdatalagen får en sanktionsavgift sättas ned helt eller delvis om överträdelsen varit ursäktlig eller att det vore oskäligt att utfärda sanktionsavgift. Den omständigheten att den personuppgiftsansvariga inte känt till regler eller haft bristfälliga rutiner är inte en anledning att sätta ned sanktionsavgiften.[16] IMY konstaterar att det inte heller i övrigt framkommit skäl för att sätta ned sanktionsavgiften enligt 6 kap. 5 § brottsdatalagen.

Av 6 kap. 3 § första stycket brottsdatalagen följer att en sanktionsavgift för överträdelse av 3 kap. 7 § samma lag högst får uppgå till fem miljoner kronor. Av andra stycket följer att för en överträdelse av bl.a. 2 kap. 12 § och 3 kap. 2 § brottsdatalagen får en sanktionsavgift uppgå till högst tio miljoner kronor. Det högsta beloppet som kan fastställas är således tio miljoner kronor.

IMY bestämmer utifrån en samlad bedömning att Polismyndigheten ska betala en sanktionsavgift på 2 500 000 kronor.

Förelägganden

Polismyndigheten ska föreläggas att vidta utbildningsåtgärder och övriga organisatoriska åtgärder som krävs enligt 3 kap. 2 § brottsdatalagen för att säkerställa att de rutiner som finns når hela organisationen och att myndigheten därmed kan visa och säkerställa att all behandling av personuppgifter är författningsenlig. Åtgärderna ska ha vidtagits senast den 15 september 2021.

Enligt 4 kap. 2 § brottsdatalagen ska den personuppgiftsansvarige i ett enskilt fall lämna viss information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter. Informationen ska bl.a. omfatta den rättsliga grunden för behandlingen, kategorier av mottagare av personuppgifterna och hur länge personuppgifterna får behandlas. Av förarbetena framgår att bestämmelsen är tillämplig t.ex. i fall där den registrerade riskerar att lida rättsförlust om han eller hon inte får del av informationen eller om det av annat skäl är viktigt för honom eller henne att känna till behandlingen för att kunna tillvarata sina rättigheter. Ett annat exempel som tas upp i förarbetena är att känsliga personuppgifter har behandlats i strid med 2 kap. 11 § om känsliga personuppgifter.[17]

Informationsskyldigheten enligt 4 kap. 2 § brottsdatalagen gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut bl.a. av hänsyn till intresset av att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, att andra rättsliga utredningar eller undersökningar inte

[15] Prop 2017/18:232 s. 485.
[16] Prop 2017/18:232 s.465
[17] Prop. 2017/18:232 s. 465

hindras, eller att någon annans rättigheter och friheter skyddas (4 kap. 5 § brottsdalagen).

Som IMY konstaterat har det inte kunnat klarläggas vad som hänt med de personuppgifter som Polismyndigheten matat in i Clearview AI. Det är därför viktigt att de registrerade får kännedom om behandlingen för att kunna tillvarata sina rättigheter, särskilt som det är fråga om känsliga personuppgifter som behandlats i strid med 2 kap. 11 § BDL. IMY bedömer därför att Polismyndigheten har en skyldighet att lämna information enligt 4 kap. 2 § BDL. Under utredningen har Polismyndigheten inte framfört något om att de registrerade ska ha informerats om användningen.

Polismyndigheten ska mot denna bakgrund föreläggas att lämna information till de registrerade, vars personuppgifter Polismyndigheten matat in i Clearview AI, enligt 4 kap. 2 § brottsdatalagen med de begränsningar som följer av 4 kap. 5 § samma lag. Informationen ska ha lämnats senast den 15 september 2021.

Som IMY konstaterat har Polismyndigheten matat in känsliga personuppgifter i Clearview AI. Då det saknas information om vad som skett med de personuppgifter som delats med Clearview AI och om dessa ännu lagras hos applikationen ska Polismyndigheten slutligen föreläggas att vidta möjliga och relevanta åtgärder för att tillse att de personuppgifter som matats in i Clearview AI raderas från applikationen. Sådana åtgärder ska ha vidtagits senast den 15 september 2021.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Elena Mazzotti Pallard. Vid handläggningen har även juristen Frida Orring och processägaren för tillsynsprocessen Katarina Tullstedt deltagit. Vid den slutliga handläggningen har rättschefen David Törngren och enhetschefen Charlotte Waller Dahlberg medverkat.

Lena Lindgren Schelin, 2021-02-10 (Det här är en elektronisk signatur)

Bilaga:
Hur man betalar sanktionsavgift.

Kopia för kännedom till:
Dataskyddsombudet: dataskyddsombud@polisen.se

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.

SVERIGES DOMSTOLAR

Hur man överklagar

FR-03

Vill du att beslutet ska ändras i någon del kan du överklaga. Här får du veta hur det går till.

Överklaga skriftligt inom 3 veckor

Tiden räknas oftast från den dag som du fick del av det skriftliga beslutet. I vissa fall räknas tiden i stället från beslutets datum. Det gäller om beslutet avkunnades vid en muntlig förhandling, eller om rätten vid förhandlingen gav besked om datum för beslutet.

För en part som företräder det allmänna (till exempel myndigheter) räknas tiden alltid från den dag domstolen meddelade beslutet.

Observera att överklagandet måste ha kommit in till domstolen när tiden går ut.

Vilken dag går tiden ut?
Sista dagen för överklagande är samma veckodag som tiden börjar räknas. Om du exempelvis fick del av beslutet måndagen den 2 mars går tiden ut måndagen den 23 mars.

Om sista dagen infaller på en lördag, söndag eller helgdag, midsommarafton, julafton eller nyårsafton, räcker det att överklagandet kommer in nästa vardag.

Så här gör du

1. Skriv förvaltningsrättens namn och målnummer.
2. Förklara varför du tycker att beslutet ska ändras. Tala om vilken ändring du vill ha och varför du tycker att kammarrätten ska ta upp ditt överklagande (läs mer om prövningstillstånd längre ner).
3. Tala om vilka bevis du vill hänvisa till. Förklara vad du vill visa med varje bevis. Skicka med skriftliga bevis som inte redan finns i målet.
4. Lämna namn och personnummer eller organisationsnummer.

   Lämna aktuella och fullständiga uppgifter om var domstolen kan nå dig: postadresser, e-postadresser och telefonnummer.

   Om du har ett ombud, lämna också ombudets kontaktuppgifter.
5. Skicka eller lämna in överklagandet till förvaltningsrätten. Du hittar adressen i beslutet.

Vad händer sedan?

Förvaltningsrätten kontrollerar att överklagandet kommit in i rätt tid. Har det kommit in för sent avvisar domstolen överklagandet. Det innebär att beslutet gäller.

Om överklagandet kommit in i tid, skickar förvaltningsrätten överklagandet och alla handlingar i målet vidare till kammarrätten.

Har du tidigare fått brev genom förenklad delgivning kan även kammarrätten skicka brev på detta sätt.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05

Prövningstillstånd i kammarrätten

När överklagandet kommer in till kammarrätten tar domstolen först ställning till om målet ska tas upp till prövning.

Kammarrätten ger prövningstillstånd i fyra olika fall.

- Domstolen bedömer att det finns anledning att tvivla på att förvaltningsrätten dömt rätt.
- Domstolen anser att det inte går att bedöma om förvaltningsrätten dömt rätt utan att ta upp målet.
- Domstolen behöver ta upp målet för att ge andra domstolar vägledning i rättstillämpningen.
- Domstolen bedömer att det finns synnerliga skäl att ta upp målet av någon annan anledning.

Om du *inte* får prövningstillstånd gäller det överklagade beslutet. Därför är det viktigt att i överklagandet ta med allt du vill föra fram.

Vill du veta mer?

Ta kontakt med förvaltningsrätten om du har frågor. Adress och telefonnummer hittar du på första sidan i beslutet.

Mer information finns på www.domstol.se.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05