

Juridiska fakultetskansliet

Finansdepartementet

Remiss: Förbättrade möjligheter för polisen att använda kamerabevakning (Ds 2024:11)

Sammanfattning

Juridiska fakultetsnämnden vid Stockholms universitet tillstyrker förslagen som helhet, men finner att förslagen bör kompletteras med tydligare regler kring myndighetsinterna och externa kontroller av andra myndigheter för hur användningen av kamerabevakning, ANPR-teknik och system för biometrisk fjärridentifiering hanteras. Som ett led i detta är det av betydelse att tydligt reglera krav på dokumentation av sådan användning. Juridiska fakultetsnämnden finner inte att de brister och risker som sådan teknologianvändning är behäftade med har redovisats i promemorian i tillräckligt stor utsträckning.

Synpunkter och kommentarer på promemorian

Juridiska fakultetsnämnden finner som helhet att förslagen i promemorian är väl avvägda. Det är rimligt att Polismyndigheten och Säkerhetspolisen har möjlighet att på ett ändamålsenligt sätt använda teknologier som har potentialen till att bidra till en mer effektiv brottsbekämpning.

Icke desto mindre finner Juridiska fakultetsnämnden att förslagen inte i alla delar är helt väl underbyggda. Analysen framstår som tämligen snäv och synes inte beakta vidden av de rättigheter som användningen av kamerabevakning, ANPR-teknik och system för biometrisk fjärridentifiering kan komma i konflikt med. Detta utvecklas närmare nedan.

Vidare skulle förslagen i viss mån behöver kompletteras med tydligare reglering om hur användningen av dessa teknologier ska kontrolleras och dokumenteras, vare sig det sker i förväg eller i efterhand, och utvärderas, både i förhållande till den interna verksamheten och externt i förhållande till granskande myndigheter. Detta ligger också i linje med AI-förordningen.¹

¹ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Förslaget i förhållande till behovet av koherens och konsistens i rättssystemet

Juridiska fakultetsnämnden vill särskilt lyfta frågan om koherensen och samstämmigheten i pågående lagstiftningsarbete på området. Parallellt med detta utredningsarbete har en annan utredning pågått som lämnade sitt betänkande i april i år, SOU 2024:27, *Kamerabevakning i offentlig verksamhet – lättnader och möjligheter*. Det gör det svårt att överblicka helheten över de sammantagna konsekvenserna av de lagändringar som föreslås inom området. Det hade därför varit en fördel om dessa utredningar hade kunnat redovisas tillsammans. Dataskyddslagstiftningen är överhuvudtaget svåröverskådlig, vilket också innebär svårigheter när det gäller att få en överblick över vidden av de rättighetsinskränkande lagändringar som sker på grund av intresset av en mer effektiv brottsbekämpning. Förslaget synes därmed inte bidra till en ökad koherens och samstämmighet i rättssystemet.

”Surveillance Creep” och behovet av motvikter i den aktuella lagstiftningen

Den massövervakning som utökade möjligheter till kamerabevakning, biometrisk fjärridentifiering m.m. innebär behöver också analyseras utifrån riskerna med vad som kan betecknas som *surveillance creep*, d.v.s. att det sker en målförskjutning och expansion av övervakningsåtgärderna.² Lagförslag som lämnar förslag till olika ingripande övervakningsåtgärder som det förevarande, bör därför med beaktande av detta, tydliggöra vilka motvikter som behöver finnas i systemet, för att förhindra överanvändning och missbruk av sådana övervakningsmöjligheter. Detta handlar inte endast om olika begränsningar i lag, såsom dataskyddslagstiftningen, utan även om interna rutiner inom myndigheterna och särskild extern granskning av t.ex. tillsynsmyndigheter och domstolar.

Evidensbaserad och teoretisk underbyggnad

Förslaget grundas i stor utsträckning på olika behovsbeskrivningar av de brottsbekämpande myndigheterna. Det är positivt att möten och intervjuer har ägt rum med företrädare för brottsbekämpande myndigheter såväl i Sverige som i vissa andra länder för att utröna vilka behov som finns av att använda dessa teknologier. Det redovisas emellertid inte att andra berörda aktörer såsom andra myndigheter (t.ex. Integritetsskyddsmyndigheten och Diskrimineringsombudsmannen), relevanta organisationer inom det civila samhället eller forskare har hörts i dessa frågor. Detta innebär att det underlag som ligger till grund för behovsanalysen är tämligen begränsat och ensidigt.

Den europeiska utblick som företas i kapitel 4 ger viss information om hur kamerabevakning, ANPR-teknik och biometriska system för fjärridentifikation regleras i ett antal europeiska länder. Jämförelser mellan länders lagstiftning kan tjäna som både inspiration och ett viktigt analysverktyg beträffande det egna systemet. Denna europeiska utblick är emellertid mycket kortfattad och det är oklart hur urvalet har gjorts och i vilken mån den har beaktats. Det är svårt att få inblick i för- och nackdelar med respektive system samt vilka erfarenheter som gjorts. När det gäller användning av teknologier för

² Marx, Gary T., *Surveillance Studies*, International Encyclopedia of the Social & Behavioral Sciences, andra upplagan, 2015 s. 738.

ansiktsgenkänning, gångigenkänning m.m. hade det varit lämpligt att söka sig utanför Europa, t.ex. USA för att få fler exempel från demokratiska länder där detta används mer aktivt än i Sverige samt vad det har för följder, såväl positiva som negativa. Det hade säkerligen varit möjligt att göra intervjuer även med forskare i andra länder inom olika områden som forskar om dessa teknologier och deras konsekvenser för samhället, t.ex. inom forskningsfältet ”surveillance studies”.

Det förekommer överhuvudtaget ingen redogörelse för forskning rörande kamerabevakning, ANPR-teknik, ansiktsgenkänning m.fl. metoder som kan användas för brottsbekämpning. I viss mån görs en sådan redogörelse i SOU 2024:27, men det framgår inte att dessa utredningar ska läsas tillsammans eftersom de redovisas separat. I SOU 2024:27 saknas vidare genomgång av forskning rörande t.ex.

ansiktsgenkänningsteknologi som behandlas i promemorian. Det hade varit lämpligt att forskningsresultat m.m. skulle ha en självständig genomgång i den aktuella promemorian, i synnerhet vad gäller biometrisk system för fjärridentifiering. Det framgår i vart fall inte om och i så fall hur vetenskaplig forskning har beaktats i promemorian.

Juridiska fakultetsnämnden kommenterade den redogörelse för forskningen kring kamerabevakning för framför allt brottsbekämpning som gjordes i SOU 2024:27 i sitt remissyttrande över detta förslag. Härvid framkom att det finns relativt lite forskning och få utvärderingar om kamerabevakning som brottsbekämpande metod och kameraövervakning i andra sammanhang.³ Den forskning som finns på området är emellertid inte helt entydig vad gäller sådana åtgärders effektivitet. Det framstår t.ex. som om effekterna av kamerabevakning är *situationsspecifik* och synes fungera bättre i förhållande till t.ex. egendomsbrott än till t.ex. terrorism.⁴

En annan viktig aspekt är att även om det sker en minskning av brott inom det kamerabevakade området, kan detta innebära att brottsligheten förflyttas till andra icke bevakade platser i närliggande områden. Riskerna för detta kan också behöva utvärderas närmare.⁵

I SOU 2024:27 redogjordes vidare för att det förekommer forskning som visar att kamerabevakning kan uppvisa att brottsligheten har minskat i ett område som kameraövervakas, men att det inte alltid går att bevisa att det är just kamerabevakningen som har lett till minskningen. Det framgår t.ex. genom att detta inte alltid återspeglas i den bevisning som åklagare för fram beträffande de lagförda brott som omfattas.

Det föreligger enligt den forskning som redovisas i SOU 2024:27 skillnader då kamerabevakning sker i kombination med att andra brottsbekämpande åtgärder vidtas, såsom ökad polisnärvaro, sociala insatser eller förbättrad belysning.⁶ De aktuella forskningsresultaten visar också sammantaget på att det finns en betydande skillnad när kamerabevakningen sker via aktiva system, där en operatör övervakar bilderna i realtid i förhållande till passivt övervakade system.⁷

³ SOU 2024:17, *Kamerabevakning i offentlig verksamhet – lättnader och möjligheter*, s. 227.

⁴ Stuzer, Alois och Zehnder, Michael, *Is camera surveillance an effective measure of counterterrorism?* Defence and Peace Economics Vol. 24, No 1, 2013, s. 10.

⁵ Alexandrie, Gustav, *Surveillance cameras and crime: a review of randomized and natural experiments*, Journal of Scandinavian Studies in Criminology and Crime Prevention, 18:2, 2017, s. 214.

⁶ SOU 2024:27, s. 144.

⁷ SOU 2024:27, s. 144. Norris framhåller att: “if a camera is mounted on a wall, coupled to a monitor and a video recorder, we have a CCTV system. But if no one notices the camera, and nobody looks at either the monitor or the tapes, its social and criminological impact is almost zero.” Det är därför viktigt att förstå att kamerövervakningssystem inte bara är tekniska system utan socio-tekniska system. För att förstå hur dessa fungerar inom ramen för en brottsbekämpningsstrategi är det nödvändigt att beakta att det befinner sig i en särskild organisatorisk miljö och att detta kommer att ha en betydande effekt på hur

Sammanfattningsvis råder det inte enighet om hur effektivt kamerabevakning i realiteten är. Det betyder emellertid inte att det inte ska vara en metod som ska vara tillgänglig för polisen, men det innebär att viss försiktighet måste iaktas när kamerabevakning används.

När det gäller ansiktsgenkänningsteknologi finns en tämligen omfattande forskning som visar på problem med precisionen hos dessa system och som påtalades redan på ett tidigt stadium i denna teknikutveckling. En av pionjörerna inom ansiktsgenkänningsteknologi Woodrow Bledsoe uttalade redan 1966 följande:

“This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations.”⁸

Bledsoes reflektioner är i viss utsträckning alltså av relevans. Sådana system kan producera falskt positiva träffar, d.v.s. att en person felaktigt identifieras i systemet eller falskt negativa träffar, det vill säga att en person felaktigt inte identifieras av systemet. I dag är precisionen betydligt bättre när tekniken används under gynnsamma förhållanden. Den amerikanska standardmyndigheten NIST (National Institute of Standards and Technology) kom t.ex. fram till att ett system som användes för ombordstigning på flygplan på flygplatser uppvisade mycket hög precision, vilket innebär att 99,5 procent av de resande kunde gå ombord flyget utan extra kontroller.⁹ Ett antagande är emellertid att det inte alltid råder gynnsamma förhållanden när polisen använder sådana teknologier, vilket kan komplicera användningen.

Senare forskning av t.ex. Buolamwini och Gebru har vidare visat på andra mycket allvarliga brister vad gäller precisionen avseende dessa teknologier, vilket särskilt gäller kön och ras.¹⁰ Precisionen är som sämst när det gäller svarta kvinnor, vilket till stor del hänger samman med att systemen framför allt tränas på bilder av vita män.¹¹ Detta har senare även bekräftats i undersökningar av NIST rörande demografiska faktorer.¹² Dessvärre har detta bidragit till negativa konsekvenser i praktiken. Det finns flera

systemet kommer att användas. Se Norris, Clive, *There's No Success Like Failure and Failure's No Success at all: Some critical reflections on understanding the global growth of CCTV surveillance* i Doyle, Aaron, Lippert, Randy, Lyon, David, *Eyes Everywhere: The global growth of camera surveillance*, Routledge 2012 (e-bok) s. 44. Se även Alexandrie, s. 217.

⁸ Ballantyne, Michael, Boyer, Robert S., Hines, Larry, *Woody Bledsoe – His Life and Legacy*, The AI Magazine, p. 10-11 with reference to Bledsoe, W.W. 1966a. *Man-Machine Facial Recognition: Report on Large-Scale Experiment*, Technical Report PRI 22, Panoramic Research, Inc., Palo Alto, California.

⁹ NISTIR 8381, *Face Recognition Vendor Test (FRVT), Part 7: Identification for Paperless Travel and Immigration* by Grother, Patrick, Hom, Austin, Ngan, Mei, Hanaoka, Kayee, National Institute of Standards and Technology, US Department of Commerce, July 2021, p. 3.

¹⁰ Buolamwini, Joy, Gebru, Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* in Friedler, Sorelle A., Wilson, Christo (eds.), *Proceedings of Machine Learning Research* 81:1-15, 2018.

¹¹ Buolamwini & Gebru 2018.

¹² NISTIR 8280, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* by Grother, Patrick, Ngan, Mei, Hanaoka, Kayee, NIST, U.S. Department of Commerce 2019.

exempel på afroamerikanska personer som felaktigt har arresterats eller åtalats på felaktiga grunder på grund av användning av ansiktsgenkännings-teknologi.¹³ Ett tämligen nyligt och uppmärksammat exempel på detta var en gravid svart kvinna som felaktigt arresterades i Detroit inför sina minderåriga barn för bl.a. rån.¹⁴

Det finns sådana risker även för svenskt vidkommande om dessa teknologier inte används med tillräckligt stor försiktighet. Här är det emellertid inte en fråga enbart om dataskydd utan också om skyddet mot diskriminering. Sistnämnda har inte särskilt analyserats i förslaget. Förtroendet för polisen kan vidare allvarligt undermineras som en följd härav.

Detta kan också innebära problem i förhållande till bevisvärderingen, i den mån resultatet av användningen av dessa teknologier används som bevis i en senare rättsprocess. En annan problematik handlar om överskottsinformation.

Det är av stor betydelse att denna teknologianvändning blir tillfredsställande belyst när det handlar om att införa nya möjligheter använda rättighetsinskränkande teknologier. Det gäller för lagstiftaren att visa att det finns goda belägg och goda skäl att anta att kamerabevakning och bruk av biometriska system för fjärridentifiering kommer att vara effektiva.

Behov av särskilda kontrollmekanismer och dokumentation

Det aktuella förslaget ger inte närmare information om hur tillfredsställande mekanismer för att motverka överanvändning, missbruk m.m. ska säkerställas. Det skulle vidare ha varit lämpligt om problem med överskottsinformation hade fått en bättre genomlysning.

För att motverka de inneboende brister som föreligger vid kamerabevakning och bruk av biometriska system för fjärridentifiering i förhållande till såväl rättssäkerheten som mänskliga rättigheter i form av skyddet för personuppgifter och skyddet mot diskriminering, behövs särskilda kontrollfunktioner. Det handlar om krav på interna kontrollmekanismer, såsom särskilda beslutsfattare och särskilda förfaranden inom myndigheterna. Vidare är det av betydelse att skapa en struktur för en effektiv extern kontroll och hur denna ska genomföras. Vilken/vilka myndigheter har kompetens och resurser att genomföra sådana inspektioner? Är det tillräckligt med de myndigheter som redan finns eller behövs en särskild myndighet för detta?

För att kontrollen ska fungera krävs också att användningen dokumenteras på ett tillfredsställande sätt, vare sig det sker i förväg eller i efterhand. Dokumentationen är också av betydelse för att skapa ett statistiskt underlag för att effektivt kunna utvärdera polisens användning av de aktuella teknologierna. Mot den bakgrunden får det därför anses nödvändigt med en specifik dokumentationsskyldighet i denna del.

En annan viktig fråga handlar om att säkerställa kvaliteten i de system som används och inte minst om datakvaliteten. Dessa aspekter behandlas inte särskilt i promemorian annat än

¹³ Se t.ex. Hill, Kashmir, *Wrongfully accused by an algorithm*, The New York Times 2 July 2020; se även Hill, Kashmir, *Your Face Belongs to Us – The Secretive Startup Dismantling Your Privacy*, Simon Schuster 2023.

¹⁴ Se t.ex. Sahouri, Andrea May, *Lawsuit filed after facial recognition tech causes wrongful arrest of pregnant woman*, USA Today, 8 augusti 2023.

genom hänvisningar till AI-förordningen. I det sammanhanget är det också nödvändigt att diskutera vilken minimikvalitet på den utrustning som ska användas för dessa ändamål ska ha. Detta kan få avgörande betydelse i bevishänseende. En annan viktig fråga är om det finns det tillräckligt tydliga standarder för användningen av sådan teknologi, vilket i synnerhet är av betydelse rörande de aktörer med vilka Polismyndigheten samverkar. Om deras utrustning och deras system inte håller måttet, så kan polisen gå miste om viktig information eller kvalitativ bevisning.

Remissvaret har på fakultetsnämndens uppdrag beslutats av dekanus, professor Jane Reichel. Yttrandet har beretts av docent Katarina Fast Lappalainen. Föredragande har varit utredare Karolina Alveryd. Yttrandet har expedierats av Juridiska fakultetskansliet.

Jane Reichel

Karolina Alveryd