ATT ÖVERVAKA FRAMTIDEN

MARIE ENEMAN OCH JAN LJUNGBERG

Sammanfattning
Samtida polisarbete förändras i takt med att nya digitala och AI-baserade tekniker införs i kombination med rättsliga mandat som ger polisen utökade möjligheter att använda övervakning. Kapitlet undersöker svenska medborgares perspektiv på övervakning och integritet i en tid där polisens befogenheter utökas och övervakning utvecklas från att identifiera vad som har hänt till att förutse vad som kan komma att hända. I Sverige har två särskilt långtgående metoder nyligen införts, hemlig dataavläsning och DNA-baserad släktforskning, samtidigt som ansiktsigenkänning i realtid införs i juli 2026. Med utgångspunkt i SOM-undersökningen analyserar kapitlet medborgares inställning till övervakning, uppfattningar om integritet samt uttryckta fördelar och nackdelar. Resultaten visar ett brett men villkorat stöd för polisens användning av övervakning, samtidigt som en stor andel anger att deras integritet varken påverkas negativt eller positivt. Kapitlet problematiserar vad denna utveckling innebär för reglering, tillsyn, ansvarsutkrävande och legitimitet när övervakning i allt större utsträckning kombineras.

Samtida polisarbete förändras i takt med att nya digitala och AI-baserade tekniker införs i kombination med nya rättsliga mandat som ger polisen utökade möjligheter att använda olika former av övervakning (Urquhart & Miranda, 2021). En central utveckling är att övervakning i allt större utsträckning används för att förutse och förebygga brott, och inte enbart för att utreda händelser i efterhand. Denna utveckling illustrerades som en framtidsvision i fiktionen *The Minority Report*, där misstanke inte grundas på vad som har hänt utan i sannolikhetsbaserade förutsägelser om framtida handlingar (Dick, 1956; filmatiserad av Spielberg, 2002). Traditionellt har övervakning främst handlat om att identifiera personer eller rekonstruera vad som redan har inträffat, exempelvis genom vittnesuppgifter, kamerabilder eller teknisk bevisning. I dag används övervakning i ökande grad för att upptäcka mönster, samband och risker innan brott begås. Fokus förskjuts därmed från att identifiera vad som har hänt till att, baserat på sannolikhetsbedömningar, förutse vad som kan komma att hända (Eneman m.fl., 2025). Denna utveckling innebär också att misstanke skapas genom indikationer, mönster och samband snarare än enbart genom konkreta handlingar eller identifierade personer. Övervakning blir därmed mer framåtblickande och inriktad på att identifiera risker i ett tidigt skede. Samtidigt kan polisiära insatser i vissa fall genomföras tidigare,

Eneman, Marie & Ljungberg, Jan (2026). Att övervaka framtiden. I Anders Carlander, Amanda Ramsälv, Björn Rönnerstrand & Patrik Öhberg (Red.), *Mot en tid som flytt.* SOM-institutet vid Göteborgs universitet.

innan ett brott har begåtts eller innan misstanken är fullt utvecklad (Amoore, 2020; Fussey m.fl., 2021; Crawford, 2021).

Utvecklingen handlar inte om enskilda nya teknologier. I stället växer mer omfattande *övervakningsassemblage* fram (Haggerty & Ericson, 2000), det vill säga sammanlänkade socio-tekniska arrangemang där teknologier, dataflöden, rättsliga mandat och institutionella praktiker kopplas samman. I sådana assemblage samlas information från olika källor in, kombineras och analyseras, vilket skapar nya möjligheter att identifiera mönster, samband och risker. Övervakningens konsekvenser uppstår därmed inte enbart genom enskilda teknologier, utan genom deras sammantagna användning och de nya former av analys och intervention som möjliggörs när olika system kopplas samman (Haggerty & Ericson, 2000; Fussey & Murray, 2025).

I Sverige har denna utveckling intensifierats genom att två särskilt långtgående metoder nyligen införts, *hemlig dataavläsning* och *DNA-baserad släktforskning*, samtidigt som *AI-baserad ansiktsigenkänning i realtid*, en ytterligare långtgående metod, införs i juli 2026 (Eneman, 2026).

Hemlig dataavläsning infördes som tillfällig lag 2020 men permanentades 1 april 2025 och ger polisen möjlighet att i hemlighet få tillgång till digitala enheter, ta del av kommunikation och i vissa fall aktivera mikrofoner och kameror. Att metoden även får användas i preventivt syfte innebär en genomgripande förändring.

Lagstiftningen om DNA-baserad släktforskning, som trädde i kraft den 1 juli 2025, innebär att polisen kan använda kommersiella släktforskningsdatabaser för att identifiera misstänkta genom genetiska kopplingar mellan personer och deras släktingar. Metoden möjliggör därmed indirekt identifiering genom släktskap, vilket kan bidra till att lösa grova brott men samtidigt innebär att personer som själva inte är misstänkta figurerar i brottsutredningar.

AI-baserad ansiktsigenkänning i realtid, som träder i kraft i juli 2026, förväntas ge polisen möjlighet att snabbare identifiera misstänkta gärningspersoner och potentiella offer vid vissa särskilt allvarliga brottstyper genom analys av kamerabilder. Samtidigt innebär tekniken risker för kontinuerlig identifiering i offentliga miljöer, där även personer utan koppling till brott kan omfattas, samt AI-baserade analyser med risk för bias och felaktiga identifieringar.

Var och en av dessa metoder innebär långtgående utvidgningar av polisens möjligheter att samla in och analysera information. Konsekvenserna blir särskilt tydliga när metoderna kombineras med varandra och med redan etablerade former av övervakning, såsom stationär kameraövervakning, kroppsburna kameror och andra digitala informationsflöden, vilket bidrar till mer sammanlänkade och omfattande övervakningsassemblage. Den sammantagna användningen skapar nya möjligheter att analysera stora och integrerade datamängder genom olika tekniker och datakällor, där misstanke i ökande grad formas genom sammanlänkade dataflöden och sannolikhetsbaserade analyser (Amoore, 2020; Fussey & Murray, 2025; Murray, 2021).

Mot denna bakgrund presenterar vi i detta kapitel svenska medborgares inställning till övervakning och integritet i en tid där polisens befogenheter utökas och övervakning i ökande grad utvecklas från att identifiera och rekonstruera händelser till att förutse och förebygga brott, samtidigt som övervakningen integreras i växande övervakningsassemblage. Kapitlet visar medborgares inställning till olika former av övervakning, hur de uppfattar konsekvenser för integritet samt vilka fördelar och nackdelar de uttrycker i relation till ökad övervakning. Vidare problematiserar vi kring vad denna utveckling innebär för reglering, tillsyn, ansvarsutkrävande och legitimitet när olika övervakningsmetoder och teknologier i allt större utsträckning kombineras.

Det nya övervakningslandskapet: Från representation till prediktion

Två centrala perspektiv kännetecknar det framväxande övervakningslandskapet: utvecklingen från representation till prediktion, och övervakning som assemblage. Tillsammans gör dessa perspektiv det möjligt att analysera hur hemlig dataavläsning, DNA-baserad släktforskning och ansiktsigenkänning i realtid inte enbart innebär nya befogenheter för polisen, utan också förändrar hur misstanke uppstår, hur ingripanden motiveras samt vilka konsekvenser detta får för rättssäkerhet och demokratisk kontroll.

En central utveckling i samtida polisarbete är en förskjutning från representativa till prediktiva och sannolikhetsbaserade former av styrning, där fokus i allt högre grad ligger på att identifiera mönster, samband och risker, och där misstanke uppstår genom statistiska associationer och närhet till potentiell risk (Amoore, 2013, 2020; Rouvroy & Berns, 2013; Eneman m.fl., 2025).

Misstanke uppstår genom statistiska associationer och genom att individer eller situationer bedöms ligga nära en potentiell risk. Ingripanden kan därmed aktualiseras innan ett brott har begåtts eller innan misstanken är fullt utvecklad, i takt med att styrning alltmer sker genom förebyggande och sannolikhetsbaserade logiker (Rouvroy & Berns, 2013).

Denna utveckling beskrivs i forskningen ofta som approximation (Amoore, 2020). Begreppet syftar på hur beslut och misstankar formas genom likheter, sannolikheter och samband snarare än genom säker kunskap. Approximation påverkar hur kunskap produceras och används i polisarbete (Weiskopf & Hansen, 2023). Det som räknas som relevant information är inte längre begränsat till direkta observationer, vittnesuppgifter eller traditionell bevisning. I stället används allt oftare sannolikhetsbaserade analyser, riskbedömningar och klassificering. Polisarbete orienteras därmed inte enbart mot att rekonstruera det förflutna, utan också mot att agera i relation till möjliga framtida händelser (Amoore, 2020; Anderson, 2010; McCulloch & Wilson, 2017; Zedner, 2007).

Klassificering spelar en central roll i denna utveckling. Klassificeringspraktiker organiserar vad som kan identifieras och vad som framstår som riskfyllt. Kategorier, standarder och tröskelvärden beskriver inte bara verkligheten, utan formar också

handlingsutrymmet (Bowker & Star, 1999; Suchman, 1994). Klassificeringssystem fungerar därmed som styrningsmekanismer som gör vissa samband synliga och andra osynliga.

Som nämndes i inledningen används begreppet övervakningsassemblage för att förstå de sammantagna effekterna – både möjligheter och risker – av olika former av övervakning (Haggerty & Ericson, 2000; Eneman m.fl., 2025). Perspektivet är särskilt relevant när metoder som verkar inom olika områden kopplas samman i praktiken. Ansiktsigenkänning i realtid bygger direkt på AI-baserad analys, medan hemlig dataavläsning och DNA-baserad släktforskning genererar data som kan integreras i sådana analyser.

Begreppet assemblage tydliggör också att risker inte enbart uppstår genom enskilda tekniker, utan genom deras sammantagna användning. Fussey och Murray (2025) beskriver detta som sammansatta övervakningsrisker, där konsekvenserna uppstår genom flera system som samverkar över tid. Den analytiska frågan blir därmed inte enbart om enskilda metoder är proportionerliga, utan hur deras sammantagna användning förändrar förutsättningarna för polisarbete och vilka konsekvenser detta får för rättssäkerhet, ansvar och demokratisk kontroll.

Svenska medborgares perspektiv på övervakning och integritet

Tabell 1 visar variationer i hur respondenterna ställer sig till olika former av övervakning som används av polisen, men också ett tydligt mönster där en relativt hög andel är positiva till polisens användning av flera av dessa metoder. För samtliga metoder anser en majoritet att övervakningen alltid bör kunna användas eller användas i undantagsfall, medan andelen som motsätter sig metoderna helt är låg. Resultaten pekar därmed på ett relativt brett stöd för polisens användning av övervakning, även när metoderna innebär risk för omfattande informationsinsamling eller intrång i privatlivet.

Stödet är högst för visuella och etablerade former av övervakning. Inställningen är mest positiv till kroppsburna kameror, där 82 procent anser att dessa alltid bör kunna användas. Även fast kameraövervakning (71 procent) och fordonsburna kameror (73 procent) uppvisar relativt höga nivåer av stöd. Motståndet mot dessa former är begränsat, vilket skulle kunna tolkas som att kamerabaserad övervakning i stor utsträckning framstår som en etablerad och relativt okontroversiell del av polisens arbete. För andra former av övervakning är inställningen mer återhållsam, men fortfarande övervägande positiv. DNA-baserade släktforskningsdatabaser får stöd av 68 procent, medan en majoritet är positiva till ansiktsigenkänning både i efterhand (58 procent) och i realtid (53 procent). Samtidigt är andelen som motsätter sig ansiktsigenkänning i realtid något högre, vilket kan tyda på att kontinuerlig identifiering i offentliga miljöer uppfattas som mer ingripande.

Hemlig dataavläsning har lägst stöd bland de undersökta formerna av övervakning. Samtidigt anser 37 procent att metoden alltid bör kunna användas, medan ytterligare 49 procent anser att den bör kunna användas i undantagsfall. Trots att

hemlig dataavläsning innebär ett långtgående intrång i privatlivet kan resultaten tolkas som att även mer ingripande och dolda former av övervakning får ett relativt omfattande stöd när de kopplas till brottsbekämpning och säkerhet.

Detta skulle kunna förklaras med Lyons (2018) resonemang kring övervakningens dubbla karaktär, där övervakning både kan uppfattas som trygghetsskapande och kontrollskapande. Den relativt positiva inställningen kan också förstås i relation till den samtida samhällskontexten. Grov organiserad brottslighet, skjutningar och sprängningar har under senare år fått stort utrymme i den offentliga debatten, vilket kan bidra till att mer långtgående övervakningsåtgärder framstår som mer motiverade (Lyon, 2003). Resultaten kan även relateras till det generellt höga förtroendet för polisen i Sverige. SOM-undersökningar visar återkommande att polisen tillhör de institutioner som åtnjuter högst förtroende bland medborgarna. Detta institutionella förtroende, ibland beskrivet som det ”nordiska guldet” (Holmberg & Rothstein, 2020), kan bidra till att mer långtgående övervakningsåtgärder möter ett bredare stöd. Samtidigt har frågor om övervakning och integritet i perioder varit mer kontroversiella i den offentliga debatten, vilket pekar på att sådana attityder kan variera över tid.

Sammantaget visar resultaten en differentierad men relativt bred positiv inställning till olika former av övervakning som används av polisen. Resultaten kan tolkas som att inställningen varierar beroende på hur etablerad och synlig övervakningen uppfattas, samtidigt som motståndet genomgående är begränsat. Resultaten pekar därmed på att många respondenter ser polisens användning av övervakning som motiverad, samtidigt som variationerna tyder på att stödet är villkorat.

Tabell 1 Bör brottsbekämpande myndigheter få använda följande övervakningsmetoder, 2025 (procent)

	Bör alltid kunna användas	Bör kunna användas men bara i undantagsfall	Bör aldrig kunna användas	Ingen uppfattning	Summa procent	Antal svarande
Fast kameraövervakning	71	25	2	2	100	1 805
Kroppsburna kameror	82	14	1	3	100	1 789
Fordonsburna kameror (från t.ex. drönare, helikopter eller bilar)	73	23	2	2	100	1 782
Hemlig dataavläsning (intrång i mobiler eller datorer för att läsa av information och aktivera mikrofon eller kamera)	37	49	11	3	100	1 778
Ansiktsigenkänning som sker i efterhand på redan insamlat material	58	34	4	4	100	1 779
Ansiktsigenkänning i realtid när personen befinner sig framför kameran	53	34	9	4	100	1 779
DNA-baserade släktforskningsdatabaser	68	23	5	4	100	1 778

Kommentar: Frågan löd *Tycker du svenska brottsbekämpande myndigheter (t.ex. polisen) bör få använda följande?*. Svarsalternativen framgår i tabellen. Procentbasen utgörs av dem som besvarat respektive delfråga.

Källa: Den nationella SOM-undersökningen 2025.

Tabell 2 visar hur respondenterna uppfattar att deras integritet påverkas av olika former av övervakning som används av polisen. Resultaten visar variationer mellan metoderna, men också ett tydligt mönster där negativa uppfattningar är relativt ovanliga. Samtidigt är den största enskilda svarskategorin genomgående att integriteten varken påverkas positivt eller negativt. För samtliga övervakningsformer ligger denna andel omkring 36–43 procent.

Den relativt stora andelen som anger att integriteten varken påverkas positivt eller negativt kan tolkas på flera sätt. Det kan spegla att respondenterna inte upplever någon tydlig påverkan på integriteten, men också att det kan vara svårt att bedöma konsekvenserna av vissa former av övervakning. För visuella och mer etablerade former av övervakning är andelen som uppfattar en positiv påverkan större än andelen som uppfattar en negativ påverkan. Detta gäller exempelvis kroppsburna kameror, där 53 procent anger en positiv påverkan och 6 procent en negativ. Ett liknande mönster framträder för fast kameraövervakning (49 procent positivt, 10 procent negativt) och fordonsburna kameror (49 procent positivt, 8 procent negativt). Resultaten pekar på att visuella och mer etablerade former av övervakning i större utsträckning uppfattas ha begränsad negativ påverkan på den personliga integriteten.

För mer ingripande och dolda former av övervakning framträder en mer blandad bild. Hemlig dataavläsning har den högsta andelen som anger negativ påverkan (28 procent), medan 36 procent anger att integriteten varken påverkas positivt eller negativt och 36 procent anger positiv påverkan. Även ansiktsigenkänning i realtid har en relativt hög andel som anger negativ påverkan (17 procent), samtidigt som 43 procent anger positiv påverkan och 40 procent att integriteten varken påverkas positivt eller negativt. Dessa resultat kan tolkas som att mer ingripande och mindre synliga former av övervakning i högre grad väcker frågor om integritet, även om negativa uppfattningar inte dominerar.

DNA-baserade släktforskningsdatabaser avviker delvis från detta mönster. Här anger 49 procent en positiv påverkan, medan 10 procent anger negativ påverkan och 41 procent anger att integriteten varken påverkas positivt eller negativt. En möjlig tolkning är att metoden, trots långtgående möjligheter till indirekt identifiering, i relativt begränsad utsträckning uppfattas påverka den personliga integriteten negativt. I kombination med resultaten i tabell 1, där stödet för polisens användning av övervakning var relativt högt, väcker detta frågor om hur integritet uppfattas i relation till polisens brottsbekämpande arbete.

Sammantaget visar resultaten att en stor andel respondenter anger att deras integritet varken påverkas positivt eller negativt av polisens användning av olika former av övervakning. För samtliga metoder ligger denna andel på omkring 40 procent, samtidigt som andelen som uppfattar en negativ påverkan är relativt begränsad, även för mer ingripande metoder såsom hemlig dataavläsning och ansiktsigenkänning i realtid.

Resultaten kan tolkas i relation till Nissenbaums (2010) begrepp *contextual integrity*, där integritet förstås som kontextberoende och som kan omförhandlas. När övervakning kopplas till polisens brottsbekämpande arbete och till frågor om grov organiserad brottslighet, skjutningar och sprängdåd kan vissa former av övervakningsåtgärder uppfattas som mindre problematiska i relation till integritet. En möjlig tolkning är att integritet omförhandlas i relation till upplevda hot, trygghet och inställningen till polisens brottsbekämpande arbete (Eneman & Ljungberg, 2025).

Samtidigt bör resultaten tolkas med viss försiktighet. Flera av metoderna rör komplexa och tekniskt avancerade former av långtgående övervakning, och det är oklart i vilken utsträckning respondenterna har kunskap om hur dessa teknologier fungerar i praktiken. Den relativt stora andelen som anger att integriteten varken påverkas positivt eller negativt kan också spegla svårigheter att ta ställning till svarsalternativen, även om detta inte kan fastställas utifrån resultaten.

Tabell 2 Påverkan på integritet vid användning av följande övervakningsmetoder, 2025 (procent)

	Mycket positivt	Ganska positiv	Varken positivt eller negativt	Ganska negativt	Mycket negativt	Summa procent	Antal svarande
Fast kameraövervakning	30	19	41	8	2	100	1 790
Kroppsburna kameror	33	20	41	4	2	100	1 778
Fordonsburna kameror (från t.ex. drönare, helikopter eller bilar)	30	19	43	6	2	100	1 771
Hemlig dataavläsning (intrång i mobiler eller datorer för att läsa av information och aktivera mikrofon eller kamera)	18	18	36	17	11	100	1 777
Ansiktsigenkänning som sker i efterhand på redan insamlat material	26	20	42	8	4	100	1 767
Ansiktsigenkänning i realtid när personen befinner sig framför kameran	25	18	40	10	7	100	1 760
DNA-baserade släktforskningsdatabaser	32	17	41	6	4	100	1 762

Kommentar: Frågan löd *Hur anser du att din integritet hade påverkats av att brottsbekämpande myndigheter (t.ex. polisen) använde följande?*. Svarsalternativen framgår i tabellen. Procentbasen utgörs av dem som besvarat respektive delfråga.

Källa: Den nationella SOM-undersökningen 2025.

Medborgarnas syn på fördelar och nackdelar med övervakning

Den öppna frågan i SOM-undersökningen ger en bild av hur medborgare resonerar kring övervakningens fördelar och nackdelar. Frågan formulerades som: Vad tycker du är de största nackdelarna/fördelarna med ökad övervakning i samhället?

Analysen av fritextsvaren genomfördes som en kvalitativ, tolkande och iterativ process inspirerad av etablerade kvalitativa analysansatser (Alvesson & Deetz, 2000;

Alvesson & Kärreman, 2011). I en första fas lästes samtliga svar igenom för att identifiera återkommande teman. I en andra fas genomfördes en mer systematisk kodning av materialet, med fokus på formuleringar kring upplevda fördelar och nackdelar med övervakning. Utifrån denna process identifierades tre övergripande teman: (1) övervakningens betydelse för trygghet, brottsbekämpning och förebyggande möjligheter, (2) risker för integritet, kontroll och missbruk samt (3) spänningen mellan effektivitet och rättssäkerhet. Resultaten visar återkommande teman kring upplevda möjligheter och risker med ökad övervakning.

Främsta fördelarna: trygghet, brottsbekämpning och förebyggande möjligheter
Den vanligaste fördelen som lyfts fram är övervakningens betydelse för brottsbekämpning och ökad trygghet. Respondenter betonar att övervakning kan bidra till att förebygga brott, identifiera misstänkta och underlätta utredningar, med återkommande formuleringar som ”minska kriminalitet”, ”öka tryggheten” och ”lättare att lösa brott”.

Flera framhåller också att övervakning kan underlätta polisens arbete, exempelvis genom snabbare identifiering eller bättre underlag i utredningar. Därtill betonar många möjligheten att upptäcka risker i ett tidigt skede, exempelvis genom att ”förebygga” eller ”stoppa brott innan de sker”. Detta skulle kunna tolkas som ett visst stöd för mer framåtblickande former av övervakning, där övervakning uppfattas som ett sätt att öka möjligheterna att förebygga och hantera brott.

Främsta nackdelarna: risker för integritet, kontroll och missbruk
Risker för integritet framträder som den mest återkommande nackdelen. Respondenter uttrycker oro för intrång i privatlivet, känslan av att vara övervakad och risken för ett mer kontrollerat samhälle. Formuleringar som ”integritetskränkning” och ”övervakningssamhälle” återkommer i materialet. Utöver integritet lyfts även risker för felaktig användning och maktmissbruk, exempelvis att oskyldiga kan bli föremål för misstanke eller att övervakning används oproportionerligt. Detta pekar på att frågor om rättssäkerhet, transparens och kontroll är viktiga för delar av respondenterna. Samtidigt uppger vissa respondenter att de inte ser några tydliga nackdelar. Svar som ”inga nackdelar” eller resonemang om att övervakning kan vara motiverad för att bekämpa brott förekommer i materialet, vilket skulle kunna tolkas som att övervakning i vissa fall uppfattas som ett motiverat inslag i arbetet med trygghet och brottsbekämpning.

Effektivitet vs. Rättssäkerhet
Respondenterna lyfter fram den välkända spänningen mellan effektivitet och rättssäkerhet som central. Övervakning beskrivs som ett sätt att stärka brottsbekämpningen och öka tryggheten, samtidigt som oro uttrycks för felaktig användning, bristande kontroll och konsekvenser för den personliga integriteten. Denna spänning kommer också till uttryck i respondenternas resonemang om

trygghet och integritet, där övervakning både framhålls som trygghetsskapande och som ett potentiellt intrång i privatlivet. Samtidigt varierar inställningen mellan respondenter, där vissa ser få nackdelar medan andra uttrycker mer övergripande farhågor om ett mer övervakat samhälle.

Att övervaka framtiden: konsekvenser för ansvar, reglering och legitimitet

Syftet med detta kapitel har varit att undersöka svenska medborgares perspektiv på övervakning och integritet i en tid där polisens befogenheter utökas och övervakning i ökande grad utvecklas från att identifiera och rekonstruera händelser till att förutse och förebygga brott. Resultaten visar en differentierad men relativt bred positiv inställning till flera av de former av övervakning som används av polisen. För samtliga metoder anser en majoritet att övervakningen alltid bör kunna användas eller användas i undantagsfall, medan andelen som motsätter sig metoderna helt är låg. Inställningen är mest positiv till visuella och etablerade former av övervakning, såsom kroppsburna kameror, fast kameraövervakning och fordonsburna kameror. Även mer ingripande metoder, såsom hemlig dataavläsning, får visst stöd från respondenterna, men i mer återhållsam utsträckning.

Samtidigt är andelen som anger att övervakningen påverkar den personliga integriteten negativt relativt låg för samtliga metoder, och en stor andel respondenter anger att integriteten varken påverkas positivt eller negativt. Detta kan tolkas på flera sätt, bland annat som att respondenterna inte upplever någon tydlig påverkan på integriteten, men också som att det kan vara svårt att ta ställning till konsekvenserna av mer komplexa och tekniskt avancerade former av övervakning i en enkät. Visuella och mer etablerade former av övervakning anges i större utsträckning ha en mer begränsad påverkan på integriteten, medan mer ingripande och mindre synliga metoder i högre grad väcker frågor om integritet, även om negativa inställningar inte dominerar. Sammantaget kan resultaten tolkas som att övervakning i relativt stor utsträckning uppfattas som motiverad i relation till polisens brottsbekämpande arbete, samtidigt som inställningen varierar beroende på metodernas karaktär.

Detta mönster kan förstås i relation till övervakningens dubbla karaktär, där övervakning både kan uppfattas som trygghetsskapande och kontrollskapande (Lyon, 2003, 2018). Den relativt positiva inställningen kan också förstås i relation till den samtida samhällskontexten, där grov organiserad brottslighet, skjutningar och sprängningar fått stort utrymme i den offentliga debatten. Resultaten kan även relateras till det generellt höga förtroendet för polisen i Sverige, vilket kan bidra till en mer positiv inställning.

Sammantaget pekar resultaten på en relativt bred positiv inställning till polisens användning av övervakning, samtidigt som variationerna visar att stödet är villkorat och påverkas av hur ingripande metoderna uppfattas. Detta aktualiserar frågan om hur nya övervakningsmetoder bör regleras och granskas i takt med att teknologin utvecklas.

Kriminella aktörer har få begränsningar i sin användning av ny teknologi, och det är naturligt att polisen kontinuerligt utvecklar sin användning av tekniska verktyg för att bekämpa brott. I ett demokratiskt samhälle är det samtidigt lika centralt att denna utveckling följs av reglering och tillsyn. Det som ofta förbises är att även organiseringen av denna tillsyn och reglering behöver utvecklas i takt med tekniken.

Detta blir särskilt tydligt i relation till de tre nya och långtgående mandaten: Hemlig dataavläsning, DNA-baserad släktforskning och AI-baserad ansiktsigenkänning i realtid.

Hemlig dataavläsning möjliggör hemlig tillgång till digital kommunikation och information från digitala enheter, vilket kan ge insyn i annars slutna miljöer med krypterad information. Samtidigt innebär metoden långtgående intrång i privatlivet och kan, särskilt när den används i preventivt syfte, aktualisera frågor om proportionalitet, rättssäkerhet och tillsyn (Oerlemans & van Toor, 2022; Eneman, 2026). DNA-baserad släktforskning möjliggör indirekt identifiering genom genetiska kopplingar mellan personer och deras släktingar. Metoden har visat stor potential, exempelvis i utredningen av dubbelmordet i Linköping, men innebär samtidigt att genetisk information från en individ kan få konsekvenser för andra inom samma släktnätverk, vilket aktualiserar frågor om proportionalitet och individens rättigheter (Guerrini m.fl., 2018; Tuazon m.fl., 2024). Ansiktsigenkänning i realtid möjliggör snabb identifiering genom AI-baserad analys av kamerabilder i kombination med fasta kameror, kroppsburna kameror eller drönare. Erfarenheter från bland annat Storbritannien visar att tekniken redan används operativt, samtidigt som behovet av tydligare rättsliga ramar och tillsyn har lyfts fram (Fussey & Murray, 2025). Den brittiska regeringen har också nyligen genomfört en offentlig konsultation om framtida reglering av biometriska och AI-baserade övervakningsteknologier, vilket ytterligare illustrerar behovet av att utveckla rättsliga ramar i takt med den tekniska utvecklingen.

Var och en av dessa metoder är långtgående i sig, men deras konsekvenser förändras när de förstås som en del av bredare övervakningsassemblage, där olika teknologier och datakällor kopplas samman. När data från flera källor integreras förändras inte bara polisens möjligheter att identifiera misstänkta, utan också hur misstanke uppstår. Denna utveckling kan förstås i relation till en bredare förskjutning från representativ till prediktiv övervakning (Amoore, 2020; Rouvroy & Berns, 2013; Eneman m.fl., 2025). Traditionellt har övervakning främst handlat om att identifiera personer eller rekonstruera händelser, medan vi idag ser en utveckling till att identifiera mönster, samband och risker i ett tidigt skede. Detta speglas också i respondenternas svar, där många lyfter värdet av att kunna förebygga brott och identifiera risker i ett tidigt skede.

En ytterligare aspekt är att många av de teknologier som används utvecklas och tillhandahålls av externa privata aktörer. Detta innebär att centrala delar av

polisens övervakningskapacitet i ökande grad är beroende av tekniska system som myndigheten inte själv utvecklar eller fullt ut kontrollerar. När institutioner som omgärdas av en hög grad av sekretess använder svårgranskade teknologiska system förstärks dessa utmaningar ytterligare, något som har beskrivits som en ”double black box”, där både teknologiska system och institutionella processer är svåra att granska (Pasquale, 2016; Burrell, 2016; Deeks, 2025; Black & Murray, 2019; Murray, 2024).

När övervakning i ökande grad sker genom sammanlänkade och sannolikhetsbaserade system förändras också förutsättningarna för ansvar och legitimitet. Ansvar kan i mindre utsträckning knytas till enskilda beslut eller aktörer och blir i stället fördelat över tekniska system, organisatoriska rutiner och rättsliga strukturer (Murray, 2021, 2024; Black & Murray, 2019). Samtidigt ökar komplexiteten med att granska beslutsprocesser när flera system och aktörer samverkar, vilket gör det svårare att förstå hur misstanke uppstår och varför ingripanden genomförs.

Denna utveckling påverkar också legitimiteten. I demokratiska rättsstater bygger legitimitet inte enbart på laglighet, utan också på att maktutövning är begriplig och möjlig att granska (Suchman, 1995; Tyler, 2025). När övervakning i ökande grad används för att identifiera framtida risker snarare än att utreda redan begångna brott förändras också villkoren för rättssäkerhet och demokratisk kontroll.

Frågan blir därmed inte bara vilka teknologier polisen bör få använda. Frågan blir vad som händer när misstanke inte längre grundas i konkreta handlingar, utan i sannolikheter. När individer inte identifieras utifrån vad de har gjort, utan genom datadrivna matchningar, sannolikhetsbaserade beräkningar och prediktiva bedömningar av framtida risk. När övervakning inte längre bara ser, utan förutser.

I takt med att övervakning blir mer prediktiv, sammanlänkad och datadriven förändras inte bara hur övervakning som del av polisarbete bedrivs, utan också grunden för statlig maktutövning. När framtida risker, snarare än begångna handlingar, blir utgångspunkt för intervention förskjuts också gränserna för när misstanke uppstår och när ingripanden anses legitima, samtidigt som upplevd effektivitet och framgång i brottsbekämpning kan bidra till att legitimera mer långtgående övervakningsåtgärder. Misstanke kan därmed uppstå genom sannolikheter, samband och prediktiva beräkningar snarare än genom konkreta handlingar. Frågan blir därför inte bara om våra institutioner är rustade att reglera dessa teknologier, utan hur demokratisk kontroll kan upprätthållas när misstanke i ökande grad produceras genom datadrivna och sannolikhetsbaserade system.

Detta väcker en angelägen fråga: när övervakning i ökande grad handlar om att identifiera potentiella framtider – vem avgör vad som räknas som risk, hur denna risk produceras, och vem som därmed blir föremål för misstanke?

Tackord

Denna forskning har finansierats av Forskningsrådet för hälsa, arbetsliv och välfärd (Forte). Författarna vill rikta ett stort tack för stödet som möjliggjort den här forskningen.

Referenser

Alvesson, M., & Kärreman, D. (2011). *Qualitative research and theory development: Mystery as method.* Sage Publications.

Alvesson, M., & Deetz, S. (2000). *Doing Critical Management Research*. London: SAGE.

Amoore, L. (2020). Cloud Ethics: Algorithms and the attributes of ourselves and others. Duke University Press.

Amoore, L. (2013). *The politics of possibility: risk and security beyond probability.* Duke University Press.

Anderson, B. (2010). Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography*, *34*(6), 777–798.

Black, J., & Murray, A. (2019). Regulating AI and machine learning: Setting the regulatory agenda. *European Journal of Law and Tech*nology, *10*(3).

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Soc*iety, *3*(1), 1–12.

Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (1 uppl.). Yale University Press.

Deeks, A. S. (2025). *The Double Black Box: National Security, Artificial Intelligence, and the struggle for Democratic Accountability*. Oxford University Press.

Dick, P. K. (1956). *The Minority Report*. *Fantastic Universe*, January 1956. King-Size Publications.

Eneman, M. (2026). The Surveillance Turn in Policing: Legitimacy in Tension. I W. Stol, L. Wacher Lentz, M. Naarttijärvi, I. M. Sunde, A. Jackson, L. Strikwerda & J. Jansen (Red.), *Opportunities and Challenges in Digital Policing; Theoretical and Practical Perspectives*. Boom.

Eneman, M., Ljungberg, J., Miranda, D., Urquhart, L., & Webster, W. (2025). The Ontological Shift in Surveillance: Revisiting the "Surveillant Assemblage" in the Age of Facial Recognition. *Surveillance & Society*, *23*(4), 498–504.

Eneman, M., & Ljungberg, J. (2025). Hur mycket övervakning tål det demokratiska samhället? I B. Rönnerstrand, A. Carlander, P. Öhberg & A. Bergström (Red.), *I rörelse* (s. 51–64). SOM-institutet vid Göteborgs universitet.

Eneman, M., Ljungberg, J., Raviola, E., & Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities. *Information Polity*, *27*(2), 219–232.

Fussey, P. & Murray, D. (2025). *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence.* Oxford University Press.

Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *British Journal of Crim*inology, *61*(2), 325–344.

Guerrini, C., Robinson, J., Petersen, D., & McGuire, A. (2018). Should police have access to genetic genealogy databases? Capturing the Golden State Killer and other criminals using a controversial new forensic technique. *PLoS Biology*, *16*(10)

Haggerty, K. D., & Ericson, R. V. (2006). *The new politics of surveillance and visibility*. University of Toronto Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622.

Holmberg, S., & Rothstein, B. (2020). *Social Trust – The Nordic Gold?* QoG Working Paper Series 2020:1. The Quality of Government Institute, Department of Political Science, University of Gothenburg.

Lyon, D. (2018). *Culture of Surveillance*. Polity Press.

Lyon, D. (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. Routledge.

McCulloch, J., & Wilson, D. (2017). *Pre-crime: Pre-emption, precaution and the futur*e. Routledge Frontiers of Criminal Justice.

Murray, A. (2024). Automated Public Decision Making and the Need for Regulation. *LSE Public Policy Review*, *3*(3), 1–10.

Murray, A. (2021). *Almost Human: Law and Human Agency in the Time of Artificial Intelligence* – Sixth Annual T.M.C. Asser Lecture. T.M.C. ASSER PRESS

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Oerlemans, J. J., & van Toor, D. A. G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law, and Criminal Justice*, *30*(3–4), 309–328.

Pasquale, F. (2016). *The Black Box Society*. Harvard University Press.

Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships? *Réseaux, 177*(1), 163–196.

Spielberg, S. (Director). (2002). *Minority Report* [Film]. 20th Century Fox.

Suchman, L. (1994). Do Categories Have Politics? *The Language/Action Perspective Reconsidered. Computer Supported Cooperative Work (CSCW) 2*(3): 177–190.

Suchman, M. (1995). Legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571–610.

Tuazon, O. M., Wickenheiser, R. A., Ansell, R., Guerrini, C. J., Zwenne, G.-J., & Custers, B. (2024). Law enforcement use of genetic genealogy databases in criminal investigations: Nomenclature, definition and scope. *Forensic Science International: Synergy*, 8, 100460.

Tyler, T. (2025). Legitimacy-based policing. *Criminology & Public Policy*, *24*, 165–187.

Urquhart, L., & Miranda, D. (2021). Policing faces: the present and future of intelligent facial surveillance. *Information & Communications Technology Law*, *31*(2), 194–219.

Weiskopf, R., & Hansen, H. K. (2023). Algorithmic governmentality and the space of ethics: Examples from 'People Analytics.' *Human Relations (New York)*, *76*(3), 483–506.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, *11*(2), 261–281. https://doi.org/10.1177/1362480607075851