VÄLKOMMEN TILL DET DIGITALA ÖVERVAKNINGSSAMHÄLLET

MARIE ENEMAN OCH JAN LJUNGBERG

Sammanfattning
Den ökande digitaliseringen i samhället och utvecklingen inom AI möjliggör kraftfull övervakning vi tidigare inte sett. Dessutom har både statliga och privata aktörer fått utökade befogenheter att använda övervakning. Detta motiveras av behovet av ökad effektivitet och säkerhet i samhället samtidigt som det väcker oro för att utvecklingen hotar grundläggande demokratiska rättigheter som integritet. Mot den här bakgrunden undersöker detta kapitel svenska medborgares inställning till olika aktörers användning av övervakning samt hur de uppfattar att deras integritet påverkas. Resultatet visar att medborgare är mer positivt inställda till övervakning som utförs av statliga aktörer jämfört med övervakning som utförs av privata aktörer och att medborgare inte verkar särskilt oroade över integritetsrisker i relation till brottsbekämpande myndigheters användning av övervakning.

I det digitala samhället har övervakning kommit att bli subtilt inbäddat i nästan alla områden av våra liv. Staten kontrollerar exempelvis medborgarnas aktiviteter med hjälp av stationära kameror i offentliga miljöer, genom polisens kroppskameror samt med drönare. Privata aktörer samlar in data om oss genom GPS och sensorer i mobiltelefoner och träningsklockor, och på sociala medier som Facebook och Instagram delar vi generöst allehanda data om oss själva och vad vi gör (Zuboff, 2019). Övervakning skall inte förstås som något vi endast är utsatta för utifrån (av externa aktörer) då vi lever i en övervakningskultur där vi har blivit en del av systemet (Lyon, 2018). Utvecklingen inom digitalisering och artificiell intelligens (AI) möjliggör övervakning i en omfattning och intensitet vi aldrig tidigare sett (Park & Jones-Jang, 2022; Eneman m.fl., 2022) förutom i dystopisk film och litteratur. Murray (2016) argumenterar att dagens övervakningsteknologier möjliggör mycket effektivare kontroll av medborgare än vad Orwell förutspådde i sin dystopiska klassiker *1984* (Orwell, 2008). Den tekniska utvecklingen i kombination med nya lagar och politiska förslag har gett statliga och privata aktörer i Sverige utökade befogenheter att använda olika typer av övervakningsteknologier. Detta skapar å ena sidan stora förväntningar på ökad effektivitet och säkerhet i samhället samtidigt som det å andra sidan väcker oro för att utvecklingen hotar grundläggande demokratiska rättigheter som integritet (Ball & Webster, 2019; Véliz, 2020). Mot den bakgrunden undersöker det här kapitlet svenska medborgares

Eneman, Marie & Ljungberg, Jan (2023). Välkommen till det digitala övervakningssamhället.
I Ulrika Andersson, Patrik Öhberg, Anders Carlander, Johan Martinsson & Nora Theorin (red) *Ovisshetens tid*.
Göteborg: SOM-institutet, Göteborgs universitet.

inställning till övervakning samt hur de uppfattar att deras integritet påverkas i det digitala samhället.

Övervakning överallt och hela tiden

Att staten övervakar sina medborgare är inget nytt, det har en lång tradition och är kopplat till utvecklingen av den byråkratiska staten med behov av att föra register över medborgarna (Boersma m.fl., 2014). Det som är nytt och en viktig skillnad är att staten idag förlitar sig alltmer på privata aktörer för att samla in, lagra, dela och analysera data om medborgare (Brayne, 2021). Begreppet övervakning refererar till systematisk och rutinmässig observation av människors beteende (Lyon & Murakami Wood, 2021). Den ökade digitaliseringen i samhället och utvecklingen inom artificiell intelligens (AI) har skapat nya möjligheter för kraftfulla former av övervakning (Kosta, 2022; Park & Jones-Jang, 2022). Dessa teknologier är mer dolda, sofistikerade, genomgripande och automatiserade än tidigare. Detta gör att många processer och uppgifter kan utföras samtidigt, och underlättar för storskalig insamling och lagring av data, samt möjliggör att data snabbt kan flöda inom och mellan olika system (Ball & Snider, 2019; Eneman & Ljungberg, 2023). Genom att individer i många situationer inte är medvetna om när de utsätts för övervakning förknippas denna utveckling med allvarliga hot mot individens integritet (Flyverbom, 2022). Insamlingen av data om medborgares förehavanden kan idag ske genom en mängd olika teknologier som fasta kameror, kroppsburna kameror, fordonsburna kameror (till exempel från drönare, helikoptrar och bilar), biometri genom exempelvis ansiktsigenkänning, digitala fingeravtryck, hemlig dataavläsning och ett spektrum av olika sensorer (Eneman & Ljungberg, 2023). En mycket stor mängd data tillgängliggörs dessutom från digitala plattformar och digitala tjänster såsom sociala medier och hälsoappar, smarta telefoner med GPS och mängder med andra digitala spår. Dessa tillgängliga data med ingående uppgifter om individer och deras aktiviteter används av både statliga och privata aktörer i olika övervakning, marknadsföring och påverkanskampanjer (Zuboff, 2019, 2022). Att övervaka och samla in tillgänglig data som användare genererar i det digitala samhället benämns i litteraturen som dataveillance (van Dijk, 2014; Buchi, Festic & Latzer, 2022). Till detta tillkommer utvecklingen inom AI och maskininlärning, där data kan analyseras såväl historiskt, i realtid samt för att förutsäga framtida aktiviteter och beteenden (Brayne, 2021; Kosta, 2022).

Under 2020 skedde flera viktiga ändringar av svensk lagstiftning som gav brottsbekämpande myndigheter ett ökat mandat att använda övervakning. En ändring är att Polismyndigheten nu själva internt får fatta beslut om och när de ska införa och använda kameraövervakning. Tidigare fick polisen vända sig till Integritetskyddsmyndigheten och söka tillstånd och motivera sitt intresse och även visa på tänkbara konsekvenser för individers integritet. En annan ändring är tillkomsten av den nya lagen om *Hemlig dataavläsning* (2020:62) (Eneman, Ljungberg & Rolandsson,

2022), som ger brottsbekämpande myndigheter lagligt stöd att vid misstanke om grov brottslighet 'hacka' sig in i en misstänkts dator och telefon genom att utnyttja sårbarheter i systemen. Något som t.ex. användes för att läsa av information från den krypterade chattjänsten Encrochat (Oerlemans & Van Toor, 2022). Svenska myndigheter har tidigare inte fått avlyssna krypterade data, men med den nya lagstiftningen kan de nu fånga upp och läsa av information från meddelanden och konversationer i krypterade applikationer och program. De kan också aktivera en kamera eller en mikrofon i en digital enhet (t.ex. i mobiltelefoner, datorer) för att fånga ljud eller bilder där den misstänkte befinner sig. Detta innebär en risk att även icke-misstänkta personer som befinner sig i miljön också blir övervakade. Den nya lagen motiverades med att den är ett viktigt redskap i kampen mot organiserad brottslighet, men lagen har också kritiserats på grund av dess långtgående risker för enskildas integritet och infördes därför med tidsbegränsning om fem år samt med bestämmelsen att den skall utvärderas innan beslut fattas om den ska permanentas. Nyligen har det skett ytterligare en utredning med titeln *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19) som bland annat föreslår att brottsbekämpande myndigheter skall kunna använda hemlig dataavläsning i preventivt syfte, det vill säga frikopplat från brottsmisstanke. Lagändringarna föreslås träda i kraft den 1 januari 2024 och motiveras med att de kommer bidra till att stävja organiserad brottslighet.

Den tekniska utvecklingen går snabbt i samhället, inte minst i relation till AI. Brottsbekämpande myndigheter har t.ex. stora förväntningar på att möjligheten att använda AI för att analysera stora datamängder skall leda till ökad effektivitet och säkerhet (Smyth, 2019; Park & Jones-Jang, 2022). Användningen av AI för övervakning är också förknippad med stor oro för risker för demokratiska värden som yttrandefrihet och integritet (Dencik m.fl., 2022). Europeiska kommissionen (2021) har definierat ansiktsigenkänning som en 'högrisk-teknologi'.

Ett aktuellt exempel på AI-baserad övervakning är den kontroversiella ansiktsigenkänningsapplikationen Clearview AI (Stahl, Schroeder & Rodrigues, 2023), som går långt utöver traditionella ansiktsigenkänningsteknologier. Företaget använder en automatiserad bildskrapa för att skrapa ansiktsbilder från det öppna Internet, till exempel från sociala medieplattformar som Facebook, Instagram och Twitter. Bilderna lagras i en enorm biometrisk databas med ansiktsfoton. Clearview säljer sedan åtkomst till databasen till brottsbekämpande myndigheter och privata säkerhetsföretag. Under en testperiod kan applikationen användas kostnadsfritt och ett antal svenska poliser laddade ner Clearviews applikation och använde den för ansiktsigenkänning i utredningsarbeten. Integritetsskyddsmyndigheten gjorde en formell tillsyn av polisens användning av Clearview AI och konstaterade att användningen var att betrakta som olaglig. Fallet med Clearview är ett intressant exempel på hur myndigheter kan lockas att använda kraftfulla och lättillgängliga tekniker som inte har sanktionerats av myndigheten, men där förväntningar om effektivisering av myndighetsarbetet blir drivande (Eneman m.fl., 2022). EU har

påpekat att Clearview AI:s förmåga att skydda data är mycket tveksam och dess säkerhetsnivå har ännu inte testats av oberoende part. Det kan därmed finnas stora risker med att miljontals EU-medborgare som delat personliga foton på sociala medieplattformar nu har sina porträtt i företagets databas.

Flera forskare (Zuboff, 2019, 2022; Kitchin, 2022) har också uppmärksammat hur privata aktörer och kommersiella företag övervakar medborgarna genom att samla in data från bland annat sociala medieplattformar. Studier pekar på deras förmåga att analysera exempelvis våra konsumentbeteenden, identifiera våra vanor, geo-positionering, sjukdomar eller politiska preferenser. Dessa privata aktörer, som vägleds av marknadslogik, har intresse av att sälja sådan data vidare till aktörer som är intresserade av att forma och påverka konsumentbeteenden. Zuboff (2019) har myntat termen ”övervakningskapitalism” för att beskriva detta aktuella fenomen. Dagens övervakningspraktiker involverar både privata och offentliga aktörer och det är därför viktigt att även studera det komplexa förhållandet mellan statliga och privata företag för att förstå de framväxande övervakningspraktikerna (Ball & Snider, 2019; Privacy International, 2022). I enlighet med detta har forskning pekat på vikten av ökade juridiska krav eftersom stora mängder information om individers beteende och personlig information samlas in och flödar mellan olika system (Black & Murray, 2019).

Vad är personlig integritet och hur ser det rättsliga skyddet ut?

Digitaliseringen av samhället med framväxande övervakningspraktiker innebär att allt mer personlig information samlas in, används och återanvänds, vilket sker på bekostnad av individens integritet (Hildebrandt, 2020; Véliz, 2020). Sedan publiceringen av den inflytelserika artikeln ’The right to privacy’ (Warren & Brandeis, 1890) har begreppet integritet varit flitigt omdiskuterat och föremål för olika tolkningar och definitioner. Begreppet har trots sitt politiska värde beskrivits som svårdefinierat och tvetydigt (Solove, 2006; Amoore, 2014). Definitionerna har sträckt sig från rätten att bli lämnad ifred och rätten till personlig utveckling till rätten att kontrollera information om sig själv (Wong, 2005). I det digitala samhället har personlig integritet beskrivits som den enskildes rätt till privatliv och självbestämmande (Integritetsskyddsmyndigheten, 2021). Därtill refereras privatliv till rätten att få vara ifred, kunna kommunicera med andra utan att bli kartlagd, spårad eller övervakad; och självbestämmande refererar till kontroll över person-uppgifter som rör en själv, hur informationen används och vilka som använder den, vilket blir särskilt viktigt när det t.ex. gäller känslig information. Nissenbaum (2010, 2015) hävdar att integritetsproblem inte enbart bör begränsas till att förstås som att det handlar om individens oro för kontroll över personlig information eftersom det som människor reagerar på när de uttrycker oro för integriteten inte är handlingen att dela information i sig, utan snarare det olämpliga insamlandet och användandet av information. Vidare argumenterar hon för att integritet

ständigt omförhandlas och är kontextberoende, vilket innebär att det kan få olika innebörd i olika kontexter. Det är främst två teoretiska skolor som har dominerat tolkningen av begreppet integritet (Westin, 1967; Wong, 2005). Ett perspektiv som framhåller att integritet inte är en unik rättighet och därför kan reduceras för andra samhällsvärden (t.ex. nationell säkerhet, andra individers rättigheter) och ett annat perspektiv som menar att integritet är unikt i sig själv som egen rättighet.

För att skydda individers integritet har ett antal lagar och förordningar på nationell nivå och EU-nivå skapats som reglerar hur data om individer får samlas in, lagras och användas (Integritetsskyddsmyndigheten, 2021). Det rättsliga skyddet regleras bland annat genom *Europakonventionen om de mänskliga rättigheterna* (ENG: European Convention on Human Rights), vilken gäller som lag i Sverige. Den personliga integriteten skyddas också genom svensk grundlag, *Regeringsformen*. (RF) 2 kap. 6§, med regler kring hemlig avlyssning och för andra intrång som riskerar ha långgående risker för den personliga integriteten och som innebär övervakning eller kartläggning av den enskildes privata sfär. Ytterligare exempel på det rättsliga skyddet är *Dataskyddsdirektive*t som specifikt reglerar hur personuppgifter får hanteras vid bland annat brottsbekämpning och *Dataskyddsförordningen* (GDPR). GDPR är en gemensam lagstiftning för hela EU och infördes 2018 i syfte att stärka individers grundläggande rättigheter och friheter, särskilt enskildas rätt till skydd av personuppgifter samt för att utgöra ett enhetligt skydd inom EU. Ett viktigt syfte med att skapa GDPR som gemensamt rättsligt skydd var att det skulle vara anpassat för dagens digitala samhälle där teknik utvecklas snabbt och används i alla samhällets sektorer för att samla in data om individer. Slutligen så skyddas den personliga integriteten även genom den svenska *Kamerabevakningslagen* (2018:1200) som kompletterar GDPR och syftar till att skydda individer mot otillbörligt intrång i den personliga integriteten vid kamerabevakning. Sammantaget kan vi konstatera att det finns ett antal olika rättsliga skydd som på olika sätt syftar till att skydda den personliga integriteten, men den snabba utvecklingen av sofistikerade övervakningsteknologier med bland annat AI kommer sannolikt ge upphov till nya risker för den personliga integriteten.

Svenska medborgares perspektiv på övervakning och integritet

Vi deltog i den svenska SOM-undersökningen 2022 och den första frågan var formulerad som: *Tycker du svenska brottsbekämpande myndigheter (t.ex. polisen) bör få använda följande?* Därefter presenterades sex olika övervakningsalternativ (se tabell 1 nedan). Resultatet i Tabell 1 visar att en majoritet av respondenterna ställer sig positiva till brottsbekämpande myndigheters användning av fast kameraövervakning av offentliga platser, användning av kroppsburna kameror och användning av fordonsburna kameror (från drönare, helikopter, bilar). Medborgarna uttrycker påfallande högt förtroende för att kroppsburna kameror, fast kameraövervakning av offentliga platser och fordonsburna kameror (från drönare, helikopter, bilar)

alltid skall kunna användas. Förvånande är att nästan hälften av respondenterna anger att de tycker att ansiktsigenkänning alltid bör kunna användas och att en dryg tredjedel uttrycker att hemlig dataavläsning alltid bör kunna användas, då detta är kraftfulla övervakningstekniker med långtgående risker för integriteten. Det bör även påpekas att relativt få respondenter uttryckte att de olika övervakningsalternativen aldrig bör få användas.

Tabell 1 Bör brottsbekämpande myndigheter få använda följande övervakningstekniker, 2022 (procent)

	Bör alltid kunna användas	Bör kunna användas men bara i undantagsfall	Bör aldrig kunna användas	Ingen uppfattning	Summa procent	Antal svarande
Fast kameraövervakning av offentliga platser	72	24	2	2	100	1 682
Kroppsburna kameror	73	21	2	4	100	1 654
Hemlig dataavläsning (dvs intrång i datorer, mobiler för att ta del av information)	34	55	8	3	100	1 655
Ansiktsigenkänning	48	36	9	7	100	1 644
Fordonsburna kameror (från drönare, helikopter, bilar)	59	34	3	4	100	1 653
Inhämtning av data från privata aktörer (sociala medier, Internetleverantörer)	41	45	9	5	100	1 657

Kommentar: Frågan lyder '*Tycker du svenska brottsbekämpande myndigheter (t.ex. polisen) bör få använda följande?',* Svarsalternativen framgår av figuren.

Källa: Den nationella SOM-undersökningen 2022.

Vår andra fråga var formulerad som: *Hur anser du att din integritet hade påverkats av att brottsbekämpande myndigheter (t.ex. polisen) använde följande?* Därefter presenterades sex olika övervakningsalternativ (se tabell 2 nedan). Ett överraskande resultat här är att 40–45 procent av respondenterna anser att deras integritet varken hade påverkats positivt eller negativt om brottsbekämpande myndigheter använde något av de sex möjliga övervakningsalternativen (tabell 2). När det gäller fast kameraövervakning av offentliga platser så anger drygt hälften av respondenterna

att de anser att deras integritet skulle påverkas mycket positivt eller ganska positivt och nästan hälften av respondenterna anger att kroppsburna kameror skulle påverka deras integritet mycket positivt eller ganska positivt. Förvånande resultat är att 19–23 procent av medborgarna anser att kontroversiella övervakningstekniker som ansiktsigenkänning, hemlig dataavläsning och inhämtning av data från privata aktörer skulle påverka deras integritet mycket positivt och mindre än 10 procent anger att de två teknikerna skulle ha en negativ påverkan på integriteten. Sammantaget visar resultatet i tabell 2 att fler medborgare tycker att användningen av dessa sex övervakningsalternativ har en högre positiv påverkan på den personliga integriteten än en negativ påverkan. Resultatet skiljer sig åt från vad som lyfts fram i tidigare forskning och bör tolkas med försiktighet.

Tabell 2 Påverkan på integritet när brottsbekämpande myndigheter använder följande övervakningstekniker, 2022 (procent)

	Mycket positivt	Ganska positivt	Varken positivt eller negativt	Ganska negativt	Mycket negativt	Summa procent	Antal svarande
Fast kameraövervakning av offentliga platser	34	17	40	7	2	100	1 656
Kroppsburna kameror	32	17	45	4	2	100	1 635
Hemlig dataavläsning (dvs intrång i datorer, mobiler för att ta del av information)	19	16	41	16	8	100	1 632
Ansiktsigenkänning	23	16	45	9	7	100	1 624
Fordonsburna kameror (från drönare, helikopter, bilar)	27	17	45	8	3	100	1 630
Inhämtning av data från privata aktörer (sociala medier, Internetleverantörer)	20	14	42	15	9	100	1 628

Kommentar: Frågan lyder '*Hur anser du att din integritet hade påverkats av att brottsbekämpande myndigheter (t.ex. polisen) använde följande?'.* Svarsalternativen framgår av figuren.

Källa: Den nationella SOM-undersökningen 2022.

Vår tredje fråga var formulerad som: *Hur stort förtroende har du för följande aktörers användning av övervakning i samhället?* Därefter presenterades sex olika alternativ med statliga och privata aktörer som bedriver övervakning i samhället (se tabell 3 nedan). Resultatet visar att respondenterna uttrycker ett stort förtroende för statliga aktörers användning av övervakning i samhället och att förtroendet för privata

aktörers användning av övervakning anges som betydligt lägre. Högst förtroende uttrycker respondenterna för Polismyndighetens användning av övervakning följt av ett högt förtroende även för andra brottsbekämpande myndigheters användning av övervakning. Mellan 30–40 procent av medborgarna anger att de har varken stort eller litet förtroende för den övervakning som sker av de privata aktörerna. Resultatet visar att medborgarna uttrycker lägst förtroende för den övervakning som sker av sociala medieplattformar, tätt följt av privata teknikföretag, privata säkerhetsföretag och internetleverantörer.

Tabell 3 Svenska medborgares förtroende för olika aktörers användning av övervakning, 2022 (procent)

	Mycket stort förtroende	Ganska stort förtroende	Varken stort eller litet förtroende	Ganska litet förtroende	Mycket litet förtroende	Summa procent	Antal svarande
Polismyndigheten	39	40	13	6	2	100	1 660
Andra brotts-bekämpande myndigheter	24	36	30	7	2	100	1 629
Sociala medie-plattformar	3	7	30	28	32	100	1 625
Internet-leverantörer	3	8	35	31	23	100	1 630
Privata teknik-företag	2	7	35	31	25	100	1 626
Privata säkerhets-företag	3	9	38	27	23	100	1 624

Kommentar: Frågan lyder '*Hur stort förtroende har du för följande aktörers användning av övervakning i samhället?'*. Svarsalternativen framgår av figuren.

Källa: Den nationella SOM-undersökningen 2022.

Vår fjärde och sista fråga var formulerad som: *Vilken är din åsikt om följande förslag?* Därefter presenterades fyra olika alternativ som respondenterna fick ta ställning till (se tabell 4 nedan). Resultatet visar ett starkt stöd för att öka kameraövervakning på allmänna platser och för att brottsbekämpande myndigheter ansvarar för övervakning i samhället. En tydlig majoritet av medborgarna anger ett mycket lågt stöd kring förslaget att information som privata aktörer samlar in på nätet ska få säljas vidare till andra företag, dvs. det som forskningen beskriver som övervakningskapitalism (Zuboff, 2019, 2022). Slutligen uttrycker medborgarna lågt stöd kring förslaget att låta privata aktörer ansvara för övervakning i samhället. Återigen kan vi notera en påtaglig skillnad kring medborgares förtroende gällande statliga och privata aktörers användning av övervakning i samhället.

Tabell 4 Svenska medborgares åsikt om följande förslag kring övervakning, 2022 (procent)

	Mycket bra förslag	Ganska bra förslag	Varken bra eller dåligt förslag	Ganska dåligt förslag	Mycket dåligt förslag	Summa procent	Antal svarande
Öka kamera-övervakningen på allmänna platser	60	25	8	5	2	100	1 663
Låta brottsbekämpande myndigheter ansvara för övervakning i samhället	46	35	14	3	2	100	1 640
Låta privata företag ansvara för övervakning i samhället	4	8	22	32	34	100	1 638
Information som privata aktörer samlar in om mig på nätet ska få säljas vidare till andra företag	1	2	6	15	76	100	1 639

Kommentar: Frågan lyder '*Vilken är din åsikt om följande förslag?'*. Svarsalternativen framgår av figuren.

Källa: Den nationella SOM-undersökningen 2022.

Balansen mellan säkerhet och integritet

Ett tydligt och genomgående resultat är att svenska medborgare uttrycker högre förtroende för att *statliga* aktörer som Polismyndigheten och andra brottsbekämpande myndigheter ansvarar för och använder övervakning i samhället jämfört med privata aktörers övervakning. Att medborgarna i vår studie anger högt förtroende för dessa myndigheter ligger väl i linje med flera andra studier (Rothstein & Holmberg, 2022; Nordiska Ministerrådet, 2017; Svenska Trender, 2022) som visar att svenska medborgare tillsammans med medborgare i andra nordiska länder generellt har en hög grad av social tillit och högt förtroende för publika institutioner som t.ex. Polismyndigheten. Resultatet visar också att medborgares inställning till olika typer av övervakning skiljer sig åt. En majoritet av svenska medborgare ställer sig positiva till polisens och andra brottsbekämpande myndigheters användning av fast kameraövervakning av offentliga platser, kroppskameror och fordonsburna kameror (från drönare, helikopter, bilar). Däremot ställer sig medborgarna mer negativa till användning av ansiktsigenkänning, hemlig dataavläsning och inhämtning av data från privata aktörer (sociala medier, Internetleverantörer). Resultatet kan tolkas som att det inte är de statliga aktörernas övervakning som i första hand uppfattas hota den personliga integriteten utan den som sker av privata aktörer

som t.ex. sociala medieplattformar, internetleverantörer samt privata teknik- och säkerhetsföretag (Solove, 2021; Oscarsson & Tipple, 2018).

Det mest förvånande resultatet i vår studie är att medborgarna inte uttrycker någon större oro kring eventuella risker för hur övervakningen kan komma att påverka den personliga integriteten. Faktum är att många medborgare uttrycker att deras integritet skulle påverkas positivt av mer övervakning. Störst negativ inverkan på integritet anses vara när brottsbekämpande myndigheter använder hemlig dataavläsning och inhämtar data från privata aktörer (sociala medier, internetleverantörer). Resultatet väcker viktiga frågor kring betydelsen av integritet i dagens digitala samhälle. Integritet kan, utöver det som beskrivs tidigare i kapitlet, även inkludera rätten att känna sig trygg och säker i samhället. Där kan övervakningskameror på offentliga platser bidra till en känsla av ökad trygghet, medan till exempel hemlig dataavläsning kan upplevas mer integritetskränkande. Integritet är en grundläggande demokratifråga som handlar om vilket samhälle vi vill ha.

Resultaten bör tolkas i den vidare samhällskontexten där media dagligen rapporterar om den eskalerande grova brottsligheten i form av gängkriminalitet, skjutningar och annan kriminalitet, vilket sannolikt kan ha påverkat respondenternas svar. I Svenska Trender (2022) ställdes bland annat frågan vad medborgare oroar sig mest för och en betydande majoritet svarade ’organiserad brottslighet’ vilket hamnade på andra plats efter ‘situationen i Ryssland’ (som hamnade på första plats 2022). Lyon (2018) betonar i sin forskning att rädsla spelar en central roll för att skapa och upprätthålla övervakning i samhället där t.ex. regeringar och media etc. vill förmedla att vi lever i en osäker värld, vilket gör medborgare mer benägna att acceptera olika former av övervakning. Sammantaget så framstår det som mycket troligt att medborgarnas oro och rädsla kring den aktuella samhällssituationen i Sverige påverkar deras inställning till övervakning och integritet.

Det råder just nu en stark politisk vilja att ge statliga och privata aktörer ytterligare befogenheter att använda övervakning motiverat av behovet att öka effektiviteten och säkerheten i samhället (Kitchin, 2022). Vilket leder till att nya kraftfulla förslag presenteras i snabb takt. Ett aktuellt förslag är EU-kommissionens förslag kring Chat control vilket enligt förslaget förväntas utgöra ett verktyg i kampen mot viss brottslighet genom omfattande massövervakning av medborgare som bygger på att privata aktörer som internetleverantörer, plattformsägare m.fl. skall övervaka all kommunikation som sker via deras tjänster med hjälp av Chat controls algoritmer. Ett annat aktuellt förslag är att svenska brottsbekämpande myndigheter skall få utökade möjligheter att använda hemlig dataavläsning i preventivt syfte, det vill säga frikopplat från brottsmisstanke. Som beskrevs tidigare har det nyligen skett en utredning i Sverige där lagändringarna föreslås träda i kraft den 1 januari 2024 och motiveras med att de kommer bidra till att stävja organiserad brottslighet. En sådan lagändring skulle utgöra ett paradigmskifte för rättssäkerheten i Sverige, med påtagliga risker att användningen kan bli godtycklig och oförutsägbar.

Den tekniska utvecklingen sker snabbt i samhället, inte minst i relation till AI. Brottsbekämpande myndigheter har stora förväntningar kring möjligheten att använda AI samtidigt som det är en stor utmaning att balansera teknologins potential för att öka effektiviteten och säkerheten i samhället samtidigt som demokratiska värden som integritet, yttrandefrihet och allas lika värde ska skyddas. Som nämndes tidigare så har EU definierat vissa kontroversiella övervakningsteknologier, bland annat ansiktsigenkänning, som högriskteknologi. Teknik utvecklas snabbt i samhället och reglering som syftar till att kontrollera hur ny teknik får användas tenderar att släpa efter (Black & Murray, 2019). Myndigheter kan också lockas till att använda kraftfulla och lättillgängliga teknologier som inte har sanktionerats av myndigheten, men där förväntningar om effektivisering av myndighetsarbetet blir drivande t.ex. som vid polisens användning av kontroversiella ansiktsigenkänningsapplikationen Clearview AI.

Ett ytterligare dilemma är att när kraftfulla övervakningsteknologier väl införts så finns det alltid risk för ändamålsglidning. Vidare bör det betonas att framväxande övervakningsteknologier inte ska förstås som individuella verktyg relaterade till vissa metoder utan som en växande, komplex sammansättning (assemblage) av enheter, infrastrukturer, praktiker och tjänster, utförda i ett komplext samspel mellan statliga och privata aktörer (Neil, 2017; Privacy International, 2022) som inte är under total kontroll av någon statlig aktör (Black & Murray, 2019). Viktigt här är att statlig övervakning blir alltmer intrasslad i den kommersiella privata sektorns marknadslogik, vilket ger upphov till olika utmaningar och dilemman, inte minst eftersom dessa statliga praktiker mobiliserar värden och logiker från både den offentliga och privata sektorn (Eneman & Ljungberg, 2023). Följaktligen flyter insamlad data om medborgare mellan den offentliga och den privata sektorn (Ball och Snider, 2019). Relationen mellan statliga och privata aktörer är här inte oproblematisk eftersom myndighetslogiken styrs av myndighetsuppdraget att öka tryggheten i samhället och marknadslogiken styrs av kommersiella intressen (Lyon & Murakami Wood, 2021).

Givet den samhällssituation vi har med allvarlig organiserad brottslighet så framstår det som fullt rimligt att brottsbekämpande myndigheter ska kunna utveckla sina arbetsmetoder och nyttja potentialen med ny teknologi för att mer effektivt kunna bekämpa den grova brottsligheten i samhället, men det behöver ske på ett ansvarsfullt sätt där riskerna kring användningen av de nya arbetsmetoderna och teknikerna noggrant beaktas och balanseras i relation till individers rätt till ett starkt integritetsskydd. Detta väcker ett antal grundläggande frågor som behöver diskuteras för att värna vår demokrati som t.ex. vilka aktörer som ska ha ansvar att fatta beslut om övervakning i vårt samhälle, vilka metoder och teknologier ska tillåtas och hur ska kontrollen av olika aktörers övervakning organiseras dvs. – *vem vakar över övervakarna i det digitala övervakningssamhället?*

Referenser

Amoore, Louise (2014). Security and the claim to privacy. *International political sociology,* 8(1): 108–112.

Ball, Kirstie & William Webster (2019). *Surveillance and Democracy in Europe*. Oxon, UK/New York: Routledge.

Ball, Kirstie & Laureen Snider (2019). *The Surveillance Industrial Complex: A political economy of surveillance*. Oxon, UK/New York: Routledge.

Black, Julia & Andrew Murray (2019). Regulating AI and Machine Learning: Setting the Regulatory Agenda. *European Journal of Law and Technology*, 10(3).

Boersma, Kees, van Brakel, Rosamunde, Fonio, Chiara & Pieter Wagenaar (2014). *Histories of State Surveillance in Europe and Beyond.* Oxon, UK/ New York: Routledge.

Brayne, Sarah (2021). *Predict and Surveil, Data, Discretion and the Future of Policing*. Oxford: Oxford University Press.

Büchi, Moritz, Festic, Noemi & Michael Latzer (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society,* 9(1).

Dencik, Lina, Hintz, Arne, Redden, Joanna & Emiliano Treré (2022). *Data Justice*. London: SAGE Publications Ltd.

van Dijck, José (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society,* 12: 197–208.

Eneman, Marie & Jan Ljungberg (2023). Organizing governmental surveillance practices in the age of AI: The complicated interplay between the state and the market. *Proceedings of the 39th European Group for Organizational Studies (EGOS) Colloquium*. Italy.

Eneman, Marie, Ljungberg, Jan, Raviola, Elena & Bertil Rolandsson (2022). The Sensitive Nature of Facial Recognition: Tensions between the Swedish police and regulative authorities. *Information Polity*, 27(2): 219–232.

Eneman, Marie, Ljungberg, Jan & Bertil Rolandsson (2022). Secret Data Interception' and its implications for privacy. 9thSurveillance Studies Network Conference. Rotterdam.

Eneman, Marie, Ljungberg, Jan, Rolandsson, Bertil & Dick Stenmark (2020). Governmental Surveillance - The balance between security and privacy. *Proceedings of the 25th UK Academy for Information Systems*, Oxford. Storbritannien.

European Commission (2021). *Proposal for a regulation of the European Parliament and of the council, Laying down harmonised rules on artificial intelligence and amending certain union legislative acts*, COM (2021) 206 final.

Hildebrandt, Mireille (2020). *Law for computer scientists and other folk*. Oxford University Press.

Integritetsskyddsmyndigheten (2021). *Integritetsskyddsrapporten*. https://www.imy.se/

Kitchin, Rob (2022). *The Data Revolution: A Critical Analysis of Big Data, Open Data & Data Infrastructure*s. SAGE Publications Ltd.

Kosta, Eleni (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*, 16: 212–224.

Lyon, David & David Murakami Wood (2021). *Big Data Surveillance and Security Intelligence, The Canadian case*. Vancouver: UBC Press.

Lyon, D (2018) *The Culture of Surveillance*, Cambridge, UK/Malden, USA: Polity Press.

Lyon, David (2015). *Surveillance after Snowden*. Cambridge, UK/Malden, USA: Polity Press.

Murray, Andrew (2016). *Information Technology Law: The Law and Society*. Oxford: Oxford University Press.

Nissenbaum, Helen (2015). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics,* 1–22.

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

Nordiska Ministerrådet (2017). *Tillit – Det nordiska guldet.* 2017:731.

Oerlemans, Jan-Jaap & Dave van Toor (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law, and Criminal Justice,* 30: 309–28.

Orwell, Georg (2008). *1984*. London: Penguin Books Ltd.

Oscarsson, Henrik & Frida Tipple (2018). Svenska folket allt mer positiva till övervakning. I Ulrika Andersson, Anders Carlander, Elina Lindgren & Maria Oskarson (red), *Sprickor i fasaden*. Göteborg: SOM-institutet vid Göteborgs universitet.

Park, Yong Jin & Mo Jones-Jang (2022). Surveillance, Security, and AI as Technological Acceptance. *AI & Society*.

Persson, Thomas & Sten Widmalm (2022). Politisk tolerans och självcensur i orostider. I Ulrika Andersson, Henrik Oscarsson, Björn Rönnerstrand & Nora Theorin (red), *Du sköra nya värld*. Göteborg: SOM-universitet vid Göteborgs universitet.

Privacy International (2022). *Challenging Public Private Surveillance Partnerships: A Handbook for Civil Society*, https://privacyinternational.org/sites/default/files/2022-06/Handbook%20PDF%20absolutely%20final.pdf

Rothstein, Bo & Sören Holmberg (2022). *Social tillit i höglitarlandet Sverige.* SOM-Institutets Temaserie 2022:1. Göteborg: SOM-institutet vid Göteborgs universitet.

Smyth, Sara (2019). *Biometrics, Surveillance and the Law: Societies of Restricted Access, Disciplines and Control*. Oxon, UK/New York: Routledge.

Solove, Daniel (2021). The Myth of the Privacy Paradox. *The George Washington Law Review,* 89: 1–51.

Solove, Daniel (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3): 477–564.

Stahl, Bernd Carsten, Schroeder, Doris & Rowena Rodrigues (2023). *Ethics of Artificial Intelligence*. Cham: Springer Nature.

Svenska trender (2022). *Svenska trender 1986–2021.* Göteborg: SOM-institutet vid Göteborgs universitet.

Véliz, Carissa (2020). *Privacy is Power*. London: Bantam Press.

Warren, Samuel & Louis Brandeis (1890). The Right to Privacy. *Harvard Law Review,* 4(5): 193–219.

Westin, Alan (1967). *Privacy and Freedom*. London: London Bodleey Head.

Wong, Rebecca (2005) Privacy: Charting its Development and Prospects. In Andrew Murrray (red), *Human Rights in the Digital Age*. Glasshouse Press.

Zuboff, Shosanna (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory,* 3(3): 1–79.

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London: Profile Books Ltd.