Tekniken i samhället, samhället i tekniken
specialnummer av *Arkiv. Tidskrift för samhällsanalys*, nr 18 (2025)

Digitala (o)trygghetsteknologier som sociotekniska system: föreställningar, materialitet och praktiker

Katarina Winter & Anne Kaun

SAMMANDRAG: Katarina Winter och Anne Kaun utvecklar i den här artikeln begreppet ”digitala trygghetsteknologier” för att beskriva nya digitala initiativ för att öka tryggheten i våra offentliga rum. Med avstamp i forskning om säkerhetisering och i teknik- och vetenskapsstudier (STS) visar de att även till synes ”mjuka” teknologier, som ofta presenteras som mindre ingripande och mer legitima, riskerar att normalisera och förstärka en logik där trygghet görs till en fråga om övervakning, kartläggning och kontroll. Den begreppsliga diskussionen illustreras empiriskt med material från tre fallstudier av olika typer av fenomen som faller under deras begrepp. Genom att introducera och problematisera begreppet digitala trygghetsteknologier vill Winter och Kaun möjliggöra analyser av teknologiers diskursiva, materiella och politiska implikationer för hur trygghet produceras, för vilka subjekt som målas upp som hot eller skyddsvärda, samt för hur ansvar förskjuts mellan offentliga och privata aktörer.

NYCKELORD: digitala trygghetsteknologier; säkerhetisering; trygghet; brottsprevention; övervakning; bevakning.

PUBLICERINGSHISTORIK: Originalpublicering.

KATARINA WINTER är docent och lektor i kriminologi samt doktor i sociologi vid Stockholms universitet.
E-POSTADRESS: katarina.winter@criminology.su.se

ANNE KAUN är professor i medie- och kommunikationsvetenskap vid Södertörns högskola.
E-POSTADRESS: anne.kaun@sh.se

FÖRSLAG PÅ KÄLLANGIVELSE:
Winter, Katarina & Anne Kaun (2025) ”Digitala (o)trygghetsteknologier som sociotekniska system: föreställningar, materialitet och praktiker”, i *Tekniken i samhället, samhället i tekniken*, specialnummer av *Arkiv. Tidskrift för samhällsanalys*, nr 18, s. 143–171. https://doi.org/10.13068/2000-6217.18.4

Arkiv. Tidskrift för samhällsanalys är en sakkunniggranskad vetenskaplig tidskrift för samhällsvetenskap och historia. Samtliga artiklar publiceras fritt tillgängliga på:

www.tidskriftenarkiv.se
Beständig länk: https://doi.org/10.13068/2000-6217

Den här artikeln finns tillgänglig i följande format:

PDF: via beständig länk, https://doi.org/10.13068/2000-6217.18.4
TRYCK: ingår i bokutgåva av numret, ISBN: 978 91 7924 400 2

Grafisk utformning och sidnumrering är identisk i pdf och tryck.

Samtliga artiklar i nr 18 (2025), *Tekniken i samhället, samhället i tekniken*,
nås via beständig länk, https://doi.org/10.13068/2000-6217.18

REDAKTÖR FÖR NUMRET: Majsa Allelin

Arkiv. Tidskrift för samhällsanalys
ISSN: 2000-6217 (för elektronisk resurs)
ISSN: 2000-6225 (för tryckta nummer)

ges ut av
Stiftelsen Arkiv för främjande och spridning
av samhällsvetenskaplig och historisk forskning

genom
Arkiv förlag & tidskrift
Box 1559
SE-221 01 Lund
BESÖK: Stora Gråbrödersgatan 17 a
TELEFON: 046-13 39 20
ARKIV FÖRLAG: arkiv@arkiv.nu · www.arkiv.nu
TIDSKRIFTEN ARKIV: red@tidskriftenarkiv.se · www.tidskriftenarkiv.se

Digitala (o)trygghetsteknologier som sociotekniska system: föreställningar, materialitet och praktiker

KATARINA WINTER & ANNE KAUN

Inledning

Den 4 februari 2025 ägde den dödligaste masskjutningen i Sveriges historia rum på komvuxskolan Campus Risbergska i Örebro. Totalt dödades elva personer inklusive gärningsmannen i skjutningen. Enligt medierapporteringen sköts två elever ihjäl efter att de hade följt uppmaningen i mobilapplikationen Cosafe att utrymma lokalerna i stället för att söka skydd genom så kallad inrymning (*Dagens Nyheter* 2025a). Syftet med denna mobilapplikation (hädanefter app) är just att varna och larma personal och elever under situationer av pågående dödlig våld. Genom förbättrad och förenklad kommunikation ska man kunna informera snabbt och effektivt och därmed rädda liv. Vid masskjutningen på Risbergska skolan skickades dock larmen både till fel mottagare – i det här fallet den kommunala ledningsgruppen som inte befann sig i området – samt uppmanade till olika handlingar till olika enheter: tre larm om inrymning och fyra larm om utrymning (*Dagens Nyheter* 2025b). I efterhand utredde Örebro kommun Cosafeappen. I utredningen konstaterades att utan appen hade ”utfallet av våldsdådet […] kunnat bli ännu värre” samtidigt som behovet av ”användandet av säkerhetsappen [behöver] omprövas” (Örebro kommun 2025). Appen är fortfarande i bruk i Örebro och andra kommuner och fler planerar att köpa in den just på grund av skjutningen på Risbergska.

Cosafes app är ett av många exempel på vad vi kallar digitala trygghetsteknologier. De syftar till ökad trygghet genom att förebygga brott, underlätta förfaranden i farliga situationer och i en del fall till och med rädda liv på offentliga och semioffentliga platser. I den här texten tittar vi närmare på detta framväxande fenomen genom tre fallstudier som tillsammans exemplifierar nya digitala initiativ för ökad trygghet. Utöver Cosafeappen har vi studerat Collactivates trygghetssensorer hos ett allmännyttigt bostadsbolag, som ersätter eller kompletterar övervakningskameror och spårar rörelsemönster på offentliga platser med argument om kostnadseffektivitet och integritetsskydd. Vi fördjupar oss också i Embrace, ett digitalt systemstöd för kommuners och andra organisationers rapportering och analys av otrygga aktiviteter och brottsförebyggande åtgärder. Dessa tre sorters digitala teknologier ter sig ganska olika från varandra när det gäller utformning och hur de kan användas. De har dock gemensamt att a) det är just ”kollektiv” trygghet som ska uppnås på offentliga eller halvoffentliga platser, b) de bygger på digital infrastruktur och c) är databaserade, det vill säga att trygghet sammankopplas med inhämtning, produktion och samkörning av digital data.

I tidigare forskning har digitala teknologier för brottspreventions-, trygghets- och säkerhetsarbete ofta diskuterats under rubriker som övervakningsteknologier eller som olika former av digitaliserad *policing*, med engelskans benämning (exempelvis platformiserad, prediktiv eller smart övervakning eller polisbevakning, se Brayne 2017; Ferguson 2017; Kutnowski 2017; Egbert 2019; Fyfe, Gundhus & Rønn 2018; Kaufmann, Egbert & Leese 2019; Hälterlein 2021; Fest m.fl. 2023; Egbert & Leese 2021; Leese 2023; Egbert m.fl. 2024; Galis, Gundhus & Vradis 2025). Stora delar av denna forskning har också fokuserat på teknologier som är direkt kopplade till polisens arbete. Dessa begrepp fångar därför inte fullt ut det snabbt växande fältet av digitala teknologier som används av aktörer utanför polisväsendet med syftet att skapa, mäta och upprätthålla trygghet och säkerhet i offentliga och halvoffentliga miljöer. Till skillnad från digitala polisiära verktyg har dessa teknologier ofta en ”mjuk” inramning och karaktär, med låg synlighet och vardagligt inbäddad användning. Det vardagliga användandet innebär att teknologierna sällan präglas av samma juridiska eller etiska diskussioner som digital

övervakning eller digitalt polisiärt arbete. Sammantaget gör detta att de hamnar utanför många etablerade forskningsfält om övervakning och polisiär praktik. För att tydliggöra skillnaden föreslår vi begreppet ”digitala trygghetsteknologier” för att fånga detta mångfasetterade empiriska fenomen och dess samhälleliga roll. Med digitala trygghetsteknologier avser vi ett brett spektrum av digitala lösningar som har det gemensamt att de syftar till satt skapa, mäta eller upprätthålla trygghet i samhället. Hit räknas exempelvis mobilapplikationer för larm, kommunikation eller delning av plats, digitala övervakningssystem såsom kameror eller sensorer för ljud och rörelser, samt mjukvaruverktyg för analys och samkörning av data. Även teknologier som algoritmiska analysplattformar och digitala tvillingar, det vill säga datormodeller av fysiska miljöer för simulering och planering av trygghetsinsatser ingår i detta fält.

Vi menar att dessa teknologier inte är neutrala eller enbart tekniska, utan aktivt deltar i att forma vad trygghet är, vem eller vad som uppfattas som ett hot mot denna trygghet, och vilka implikationer detta får, exempelvis gällande vilka grupper och platser som blir föremål för särskild kontroll eller intervention. Begreppet svarar också mot en bredare samhällelig förändring som benämns som ”säkerhetisering” (*securitization*). Med detta avses den process där samhälleliga problem genom retorisk och politisk inramning omdefinieras till säkerhetsfrågor, vilket möjliggör och legitimerar införandet av undantagsliknande åtgärder för styrning och politik (Buzan, Wæver & Wilde 1998; Balzacq & Guzzini 2015; Larsson & Rhinard 2021). Det finns anledning att särskilt studera vad som sker när denna process möter digitalisering. Nya teknologier accelererar och förändrar villkoren för säkerhetisering genom att möjliggöra nya former av datadrivna verktyg, övervakning och ökad involvering av aktörer inom och utanför staten. Detta innebär inte bara en förstärkning av säkerhetiseringsprocesser, utan introducerar också kvalitativa förändringar gällande aktörskap, ansvarsfördelning och vad som faktiskt räknas som ”säkerhet” och ”trygghet” i praktiken. Att analysera digitala trygghetsteknologier blir därför ett sätt att förstå säkerhetiseringens fortsatta omformulering när samhälleliga problem, tekniska innovationer och politiska prioriteringar kopplas samman i nya så kallade sociotekniska system.

Med avstamp i säkerhetiseringsfältet och forskningsfältet Science and Technology Studies (STS) vill vi visa att även till synes ”mjuka” teknologier, som ofta presenteras som mindre ingripande och mer legitima, riskerar att normalisera och förstärka en logik där trygghet görs till en fråga om övervakning, kartläggning och kontroll med hjälp av digitalisering och nya teknologier. Genom att introducera och problematisera begreppet digitala trygghetsteknologier vill vi möjliggöra analyser av teknologiers diskursiva, materiella och politiska implikationer för hur trygghet produceras, vilka subjekt som skapas som hot eller skyddsvärda, samt hur ansvar förskjuts mellan offentliga och privata aktörer.

Digitala trygghetsteknologier som empiriskt och teoretiskt fenomen

Vår ingång i denna fråga kan förstås utifrån flera samhällsförändringar. Den accelererande digitaliseringen i stort är förstås grundläggande, där digitala teknologier på bred front omformar såväl välfärd och styrning som vardagsliv (Winter 2025; Winter & Hermansson 2025; Kaun 2025; Kaun & Männiste 2025). Parallellt med denna utveckling har de senaste decennierna inneburit ett allt större fokus på frågor om trygghet och otrygghet inom politik och media, både i världen och i lokalsamhället. Trygghet har blivit en central samhällsfråga, inte minst i kriminalpolitiska diskurser (Brandén 2022; Hermansson 2019; 2022; Sahlin Lilja 2021). Forskning visar att denna utveckling innebär en förskjutning från traditionella välfärdsfrågor till frågor om brott, risk och individens känsla av otrygghet, där begreppet trygghet används för att beskriva såväl materiella som emotionella dimensioner (Hermansson 2019; 2022). Vi befinner oss i mötet mellan tilltron till digitaliseringens möjligheter och detta ökade fokus på trygghet och säkerhet som prioriterad samhällsfråga.

Forskare har sedan tidigare beskrivit hur ansvaret för brottsförebyggande och trygghetsfrämjande arbete har individualiserats, decentraliserats och privatiserats, där såväl offentliga som privata aktörer säger sig besitta lösningar på trygghetsproblem. Som en effekt har nya samarbeten mellan dessa båda sfärer uppstått (Garland 2001; Boels & Verhage 2016; Hansen Löfstrand 2021). Nya lagar på området påverkar också sådana

konstellationer, exempelvis har trycket på kommunerna ökat med en ny lag som ålägger dem ett tydligare ansvar för brottsförebyggande arbete (SFS 2023:196). I centrum för den här utvecklingen står därför kommuner, regioner och fastighetsbolag samt de privata aktörer som tillhandahåller kunskap och digitala verktyg, och anpassar dem efter rådande policy och lagformulering. Sist men inte minst riktas fokus alltmer mot vanliga medborgare, både som målgrupp för vissa teknologier och medaktörer i trygghetsarbete. Mot denna bakgrund är det därmed ingen överraskning att marknaden för digitala trygghetsteknologier växer.

Digitala trygghetsteknologier befinner sig alltså på ett fält bestående av olika strukturella faktorer, såsom lagstiftning och marknader, och därmed också olika typer av aktörer. Detta kan förstås som en form av ”trippel helix”, där offentliga aktörer (till exempel polis, regioner och kommuner), forsknings- och utvecklingsaktörer (universitet och högskolor) samt den privata sektorn (teknikföretag, inkubatorer och matchningsplattformar) samverkar och konkurrerar om en gemensam men samtidigt diffus uppgift, nämligen att skapa trygghet. Utöver dessa aktörer har vi också de tänkta respektive de faktiska användarna, från kommuntjänstemän och bostadsbolagsrepresentanter till lärare, föräldrar och hyresgäster. De olika aktörerna, med sina olika positioner och intressen, förväntningar och behov, har det gemensamt att deras praktiska relation till och användning av trygghetsteknologier är avgörande för teknologiernas etablering och legitimitet.

Som vi nämnde inledningsvis rymmer begreppet digitala trygghetsteknologier en bred flora av digitala system. För att förstå hur de etableras och får betydelse i samhället krävs en förståelse som fångar de visioner och förhoppningar som omgärdar teknologierna, deras tekniska och materiella förutsättningar, samt de vardagliga praktiker som möjliggör användningen av dem. Det är samspelet snarare än en hierarki mellan dessa nivåer som bäst förklarar hur teknologier etableras och legitimeras, eller hur de inte gör det. Teoretiskt förstår vi därför dessa teknologier som sociotekniska system, vilket innebär ett samspel där *materialitet*, *praktiker* och *föreställningar* hela tiden påverkar och omformar varandra. Förståelsen bygger på antagandet om en ömsesidig tillblivelse där anpassningar och förändringar sker i flera led samtidigt snarare än i enkla

orsakskedjor (Suchman 2020). Dimensionerna är tätt sammanflätade: visioner om framtida trygghet materialiseras i tekniska lösningar som i sin tur formar och formas av användarnas handlingar och rutiner.

Att analysera digitala trygghetsteknologier utifrån dessa tre dimensioner gör det möjligt att förstå hur teknologier formas, används och får mening och konsekvenser långt utöver sin tekniska funktion eller avsedda syfte. I stället för att endast betrakta teknologierna som neutrala verktyg belyser vår tredelade analysram hur de samhälleliga förväntningarna och visionerna kring trygghet (föreställningar), de materiella egenskaperna (materialitet) samt de vardagliga användningssätten (praktiker) tillsammans samproducerar vad trygghet blir i praktiken och hur olika aktörer involveras i dess upprätthållande. Genom att analytiskt särskilja dessa tre dimensioner kan vi synliggöra hur digitala trygghetsteknologier inte bara är tekniska objekt, utan också sociotekniska system där olika aktörer, såsom utvecklare, beslutsfattare, användare och även icke-användare, samverkar med, och ibland motverkar, varandra i skapandet av vad kollektiv trygghet är och hur den ska uppnås. Ansatsen möjliggör också en fördjupad förståelse av varför vissa teknologier får genomslag medan andra möter motstånd, liksom hur frågor om ansvar, makt och ojämlikhet vävs in i teknologiernas vardagliga användning. För att fånga den komplexitet som präglar digitala trygghetsteknologier krävs således en analys som både särskiljer och förenar de föreställningar som omgärdar teknologierna, deras materiella och tekniska förutsättningar samt de praktiker som växer fram kring dem. Genom att använda denna tredelade analysram kan vi synliggöra hur trygghetsteknologier formas och omformas i mötet mellan visioner, teknik och vardagsliv. Vi ska därför kort utveckla vad vi menar med dessa tre dimensioner och hur de tillsammans utgör sociotekniska system.

Föreställningar

Föreställningar om digitala trygghetsteknologier utgör en central del av deras sociotekniska kontext. Dessa föreställningar handlar både om individuella såväl som kollektiva uppfattningar gällande hur användare tolkar och skapar mening kring teknologier i sin vardag (Bucher 2018; Winter & Hermansson 2025) och om policy- eller marknadsdrivna visioner om

vilken framtid teknologin möjliggör (Jasanoff 2015; Winter 2025). Inom ramen för så kallade sociotekniska föreställningar (Jasanoff 2015) blir teknologier bärare av bredare samhälleliga förhoppningar om en bättre framtid. Exempelvis kan teknologier förstås som nationsbyggande projekt där föreställningar om nationens bästa underbygger, motiverar och legitimerar storskaliga investeringar i teknisk infrastruktur. Föreställningar är performativa, de bidrar inte bara till diskursiva förändringar utan formar och förändrar också praktikerna. Hur teknologi förstås påverkar hur den implementeras och används och därmed också hur den är utformad materiellt (Williamson 2018).

Materialitet

Materialiteten i digitala trygghetsteknologier handlar om de tekniska och fysiska förutsättningarna – funktioner, gränssnitt och handlingsmöjligheter – som teknologierna erbjuder olika användare (Norman 1988; Hutchby 2001). Handlingsmöjligheter som begrepp kommer från engelskans *affordances* och används för att analysera just vilka möjligheter men också vilka begränsningar som är inbyggda i teknologin. Därmed blir också ojämlikhet och exkludering relevant i relation till materialitet och begränsningar, eftersom vi utgår från att teknologier inte är neutrala. Vi inspireras här av Sasha Costanza-Chocks (2020) kritiska frågor om hur handlingsmöjligheter uppstår, för vem och i vilken kontext. Materialiteten bär på antaganden om användare, platser och behov och kan därigenom reproducera eller förstärka befintliga ojämlikheter. Exempelvis kan teknologier vara otillgängliga för vissa användare, något som snarare vittnar om handlingsomöjligheter (jämför engelskans *dis-* och *dys-affordances*, Costanza-Chock 2020).

Praktiker

Med praktiker avses de vardagliga handlingar, rutiner och känslomässiga erfarenheter som växer fram kring digitala trygghetsteknologier som sociotekniska system. Det handlar om hur teknologierna faktiskt används, justeras och anpassas för att integreras i eller förändra arbetsprocesser såväl som rutiner i privatliv eller offentlig verksamhet. Praktiker rör frågor om vad vi gör med och i relation till teknologier. Vilka

rutiner uppstår, förändras eller avbryts och vilka känslor och kroppsliga erfarenheter uppstår i relation till detta? Här handlar det också om vilka praktiker som är nödvändiga för att implementera och underhålla den infrastruktur som digitala trygghetsteknologier behöver. Här bygger vi på tidigare sätt att konceptualisera teknologier som sociologiska företeelser i och med att de utgörs av och har betydelse för sociala relationer, social interaktion och kulturella uttryck (Suchman m.fl. 2017).

Material och metod

Vi närmar oss föreställningar, materialitet och praktiker kring digitala trygghetsteknologier genom en analys av tre fallstudier, valda för att spegla bredden och variationen av sådana trygghetsteknologier i samtida svenska kontexter. Fallstudierna bygger på empiriska data insamlade inom ramen för tre olika forskningsprojekt.[1] Datainsamlingen har bestått av kvalitativa, semistrukturerade djupintervjuer med totalt 31 individer: applikationsutvecklare, företagsägare, forskare, tjänstemän samt medarbeterare i organisationer direkt involverade i implementering och användning. Utöver intervjuerna har vi analyserat skriftligt material såsom reklam, hemsidor, rapporter och företagsutvärderingar. I Collactivatefallet ingår även deltagande observation vid fältbesök i kommunala bostadshus där smarta sensorer har installerats. I fallet Cosafe genomfördes fyra av intervjuerna av en medforskare som deltog i projektet.

Materialet har sedan analyserats genom tematisk kodning för att identifiera centrala aspekter kopplade till föreställningar, materialitet och praktiker. Initialt genomfördes kodningen med en lyhördhet och öppenhet för empirins variation där de teoretiska begreppen funnits med i bakhuvudet snarare än som en strikt styrning av den analytiska processen. Fallbeskrivningarna fungerar i vår artikel som konkreta illustrationer av några av de mest framträdande egenskaperna hos fenomenet digitala trygghetsteknologier.

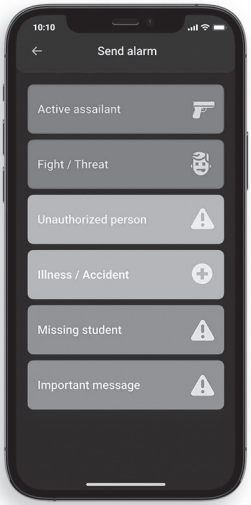
1. ”Prioriteringar och kunskap i digital brottsprevention” 2022–2023, finansierat av Anna Ahlström och Ellen Terserus stiftelse; ”Automating Welfare” 2020–2025, finansierat av Östersjöstiftelsen; ”Trygghetsteknologiers löften och konsekvenser” 2023–2025, finansierat av Länsförsäkringars forskningsfond.

Tre exempel på digitala trygghetsteknologier

Med utgångspunkt i vår analysram – föreställningar, materialitet och praktiker – presenterar vi i det följande tre empiriska exempel som illustrerar bredden och komplexiteten i samtida digitala trygghetsteknologier. I varje fallstudie analyseras hur dessa tre dimensioner samspelar och vad det innebär för teknologiernas roll i såväl specifika arbetsprocesser som mer övergripande antaganden om trygghet. Detta möjliggör en fördjupad förståelse för både teknologiernas samhälleliga förankring och deras praktiska konsekvenser för olika aktörer och användargrupper. Våra tre fallstudier representerar tre olika sätt att inhämta, producera och använda digital data i trygghetsskapande syfte, eller vad vi kallar för datafiering av trygghetsarbete. Våra exempel representerar tre huvudsakliga former av datafiering: kommunikation och larmhantering (Cosafe), övervakande sensorsystem (Collactivate) och plattform för trygghetsarbete (Embrace).

Cosafe: tekniskt alibi och ansvarsförskjutning i praktiken

Cosafe utgör ett tydligt fall av när digital trygghetsteknologi implementeras som svar på samhällelig oro men där teknologins löften har svårt att infrias i mötet med organisatoriska praktiker och användarnas faktiska vardag. Cosafe grundades 2014 och är ett företag som riktar sig till användare inom offentlig sektor, skolor och företag med syftet att möjliggöra mer effektiv incidenthantering: förebyggande, larmande och uppföljande. Enligt företaget använder omkring en tredjedel av Sveriges kommuner Cosafe i någon form, och de finns även i andra delar av Europa och Latinamerika. Utöver Cosafeapplikationen erbjuder företaget appar för grannsamverkan (Coyards) och båtägare (Coboats).



Användargränssnitt i Cosafeappen. Bildkälla: Cosafes hemsida.

Föreställningar: normalisering av oro och beredskapsretorik

Cosafe lanseras som ett svar på ökande samhällelig oro för våld och otrygghet i exempelvis skolan. Produkten framhålls av både leverantören och användarna (skolledare, lärare) som ett verktyg för att stärka beredskapen och förebygga det oväntade. Både företaget och användarna delar en gemensam föreställning om att Cosafe adresserar ett trygghetsproblem som tidigare saknat struktur men som nu får sin lösning i ny teknologi. Införandet av appen följer en säkerhetiseringslogik där ny teknik legitimeras genom diskurser om risk, men också via administrativa och politiska krav på trygghet. En skolledare uttrycker det så här:

> Det har tagits emot väldigt väl som ett sätt att öka tryggheten … Sen behöver vi som skolledning också säkerställa att man installerar appen, att man kontinuerligt får utbildning.

Appen beskrivs som en självklar del i skolans krisplan, och flera användare lyfter en miljö där det ”händer saker” och behovet att snabbt kunna ”signalera” om stöd vid kris eller hotfull händelse. Samtidigt menar några av lärarna att Cosafe installeras och legitimeras som ett sätt att ”checka av” trygghet och signalera beredskap, att ”ha något på plats ifall det värsta händer”, men med svag koppling till verkliga behov eller genomgripande organisatoriska rutiner. Beslut om implementering grundas enligt de användare vi pratat med på diskussioner om potentiella händelser och ett allmänt samhällsklimat snarare än på faktiska incidenter som behövt åtgärdas eller förebyggas:

> Det har inte varit några incidenter, men jag tror bara i någon form av samhällsklimat att man börjar tänka: Vad skulle kunna hända och hur skulle vi kunna arbeta med det? […] det är något som folk uppskattar, att det finns en diskussion och dialog kring mer säkerhet, men det finns ingen infrastruktur för själva systemet. (En lärare.)

Användarna beskriver ofta en dubbelhet: appen är självklar i krisplanen ”ifall något händer”, men i praktiken är det sällan någon har behövt använda den i skarpt läge. Samtidigt uttrycks både ett ointresse och en osäkerhet gällande hur den är tänkt att användas i praktiken. Föreställningen om beredskap blir ett symboliskt värde i sig. Känslan av trygghet

handlar alltså inte så mycket om appens faktiska funktion, utan om föreställningen av att ha ”checkat av” att något görs. Användarna uttrycker att införandet sker för ”säkerhets skull” – ”en alibifunktion” som en lärare säger och att behovet egentligen är svårgripbart:

> Jag tror att det ändå finns, ger någon form av trygghetskänsla […] Sen i praktiken har jag svårt att se att den skulle användas, så att många ser det nog säkert som någon form av ytterligare marknadsmässig sak som vi investerar i och som försvinner för att man vill ha det som lite en alibifunktion. Men annars tror jag att det finns en trygghetsaspekt i det som kan vara viktig och att det finns något som jag kan använda mig av om det händer något.

Cosafe legitimeras i stor utsträckning av den övergripande samhällsdiskursen kring ökad oro för brott, terrorhot och allmänt stigande känslor av osäkerhet, något som känns igen från tidigare studier (Winter & Hermansson 2025). Flera användare uttrycker att appen svarar mot ett slags allmänt behov av beredskap även om de konkreta riskerna som diskuteras av intervjupersonerna ofta kan gälla andra former av hot än fysiskt våld, exempelvis hot mot demokratin eller cybersäkerhet. Det betyder att föreställningen om trygg teknik blir bredare än appens faktiska användningsområde. Samtidigt rymmer användarnas beskrivningar både kritik och accepterande. Å ena sidan uppfattas appen som något som ”checkar av” åtgärder för trygghet, å andra sidan ifrågasätts om den motsvarar de verkliga behoven eller riskerna i verksamheten. På detta sätt fungerar tekniken som ett ”tekniskt alibi”; man har gjort något för tryggheten oavsett om man möter ett behov eller om de faktiska riskerna ligger inom appens domän. Detta speglar ett vidare samhällsmönster där tekniska lösningar får legitimera åtgärder mot en förutsatt och alltid närvarande risk, och där svaren på olika typer av hot reduceras till teknologi, även när problemen kan vara av annan karaktär än vad tekniken är gjord för. Appen legitimerar därmed inte bara sig själv, utan också en politik och praktik där tekniklösningar blir normala svar på breda, ibland diffust definierade, hotbilder.

Materialitet: kommunikationsplattformens begränsningar i krissituationer

Cosafe är utformad för att möjliggöra larmande, kommunikation och snabb respons vid hotfulla situationer eller pågående dödligt våld, med olika funktioner som riktar sig till olika målgrupper (till exempel skolledning eller hela personalen). Appen ska erbjuda möjligheter till snabb informationsspridning och larm, men kräver att mottagare, processer och ansvar är definierade och förankrade i verksamheten i förväg. På så vis är dess funktionalitet beroende av organisatorisk infrastruktur och tydliga rutiner. I våra intervjuer betonar skolledare vikten av pågående utbildning, rutinintegrering och rollfördelning men beskriver samtidigt att ansvaret för rutiner och faktisk larmhantering ofta blir otydligt, och att det för många användare är oklart vad som gäller i en verklig krissituation. I intervjuerna framhålls återkommande att larmen ibland ”dränks” i informationsflödet och att det blir svårt att ”veta vad som är riktlinjer och vad som gäller” när många kommunicerar samtidigt i appen. Flera lärare berättar också att de i vissa situationer litar mer på egna, informella kanaler eller direktkontakt än på appen. Stress och osäkerhet om när larmet gäller, och för vem, riskerar att göra det svårare att agera rätt:

> Om det är som du tänkt då, att du undervisar och det går ut ett larm, då har du kollat på din telefon typ, du inrymmer, blockerar dörrar … men skulle jag också kunna missa det larmet eller ha stängt av telefonen? Jag vet inte hur det där funkar … generellt är det dåligt för undervisningen att vara uppkopplad på det sättet tycker jag. (En lärare.)

Trots visionen om ökad trygghet innebär materialiteten alltså att vissa risker och oklarheter flyttas från fysiska processer till den digitala teknologin. I vissa fall skapas då nya former av otrygghet, exempelvis när ansvaret för informationsspridning är diffust. Som så många ”mjuka” trygghetssystem bär appen på löften om tillgänglighet och kontroll, men blir samtidigt ett exempel på hur teknisk infrastruktur har inneboende begränsningar: förmedlingskedjan är lång och risken ökar att instruktioner, rollfördelningar och ansvar förloras i digitala flöden, särskilt under pressade situationer. Teknologin erbjuder en uppsättning möjligheter men reproducerar samtidigt organisatoriska och praktiska problem.

Teknologin fångar heller inte, och upplevs inte kunna kompensera för de sociala och relationella dimensioner som vissa lärare menar är skolans verkliga trygghetsutmaningar, såsom att se och bekräfta elever. Flera lärare menar att trygghet i praktiken ofta bottnar i sådana mellanmänskliga relationer.

När vi frågar användare och utvecklare om risker med själva appanvändningen menar de flesta att det inte finns några sådana. Men verkliga krissituationer som vid Risbergska visar att riskerna inte är hypotetiska och att användningen kan få mycket allvarliga konsekvenser.

Praktiker: diskrepans mellan krisretorik och vardagsanvädning

Det finns en upplevd diskrepans mellan vad appen lovar – handlingskraft och trygghet – och vad den innebär i praktiken. För vissa användare innebär appen rent av en källa till ökad oro, ifrågasättande eller en slags digital övervakning i vardagen där man har ”jobbet i fickan” (som en lärare säger). Appen blir liggandes oanvänd eller till och med ifrågasatt. I de fall där den används framkommer att införandet av Cosafe ofta inte åtföljs av tillräcklig utbildning, förankring eller rutiner för faktisk användning. Användare beskriver att informationen om hur appen ska användas ofta är instrumentell och frånkopplad de specifika diskussioner som förts om verkliga hot och behov. Avsaknaden av etablerade rutiner och tydliga riktlinjer riskerar att skapa osäkerhet om vad som faktiskt ska göras vid en incident, vilket en lärare utrrycker så här:

> Vi informerades om det, vi vet vad vi ska göra men hur informerar man studenter […] Alltså den här typen av infrastruktur, för att få ett sånt system att funka, tycker jag det har vi inte genomfört, utan det är snarare att man har tagit in applikationen då.

Även teknologier som uppfattas som potentiellt onödiga men ändå harmlösa kan få avgörande och förödande konsekvenser på liv och död när instruktioner och ansvarsfördelning är otydliga. Efter Risbergskaskjutningen uttrycker Cosafes vd att de tillhandahåller ett verktyg där ansvaret ligger hos varje enskild verksamhet:

> Cosafe tillhandahåller ett tekniskt verktyg för kommunikation i kritiska situationer. Ansvaret för implementering, träning och uppföljning ligger hos varje

enskild verksamhet och det är i samverkan mellan organisation och teknik som trygghet byggs över tid.

Ansvar för trygghet är gärna något som tas av privata aktörer när det gäller att erbjuda tekniska lösningar och att formulera visioner om ökad säkerhet i skolmiljöer. Leverantörer som Cosafe betonar att deras system kan bidra till att skapa trygghet, effektiv incidenthantering och stärkt krisberedskap – något som också lyfts i kommunikationen vid upphandling och utbildning av skolpersonal. Samtidigt visar våra intervjuer och Cosafes egna uttalanden att det operativa och långsiktiga ansvaret för att tekniken ska fungera i praktiken, samt för de faktiska konsekvenserna i en krissituation, läggs på skolans ledning och enskilda användare. Detta riskerar att skapa en situation där teknikleverantören erbjuder ett verktyg och en trygghetsvision men där det är skolpersonal och huvudmän som förväntas omvandla den visionen till fungerande vardagsrutiner och som står ensamma med att hantera otydligheter när de uppstår i skarpt läge. Därigenom förskjuts både det vardagliga och det etiska ansvaret för elevernas trygghet från systemleverantören till skolans organisation och till enskilda medarbetare, något som blir särskilt tydligt och brutalt när systemet sätts på prov vid allvarliga incidenter.

Collactivate: digital övervakning som tjänst

Under våren 2022 installerade flera kommunala bostadsbolag, däribland Uppsalahem, smarta sensorer från företaget Collactivate i gemensamma utrymmen såsom korridorer och trapphus i sina fastigheter. Det handlade bland annat om ett bostadshus och ett garage där boende passerar dagligen. Sensorerna registrerar data om rörelsemönster, ljud och lukter i dessa gemensamma utrymmen. Via en wifi-router kan sensorerna också registrera antalet mobiltelefoner som används i närheten. En sensor är utformad som en enkel låda. Den påminner i utseendet om en brandvarnare och väcker inte mycket uppmärksamhet bland de boende och förbipasserande. Utifrån så kallade tröskelvärden för avvikelser har en åtgärdstrappa satts upp. Till exempel kan lådan aktivera blinkande lampor eller ett larmljud för att störa människor som uppehåller sig för länge i korridoren

och källaren. I ett nästa steg kan väktare, eller den så kallade trygghetsgruppen inom bostadsbolaget, kallas till området. Om Uppsalahem upptäcker avvikelser från vad som har definierats som normala rörelsemönster upprepade gånger för samma område, ökar bolaget åtgärderna och dokumenterar systematiskt det identifierade problemet genom till exempel ytterligare övervakning från säkerhetsbolaget. De åtgärder som sätts in börjar alltid med den minst kostsamma, till exempel blinkande ljus eller störande ljud, för att sedan, vid behov, avancera till mer kostsamma interventioner som fysiskt bevakande personal. All insamlad data samlas och visas i en panel som visualiserar rörelsemönster och data som överskrider tröskelvärden för avvikande rörelser i området, vilka sedan sammanställs och presenteras för kunden, i det här fallet Uppsalahem.

De insamlade uppgifterna gör de trygghetsskapande åtgärderna mätbara och spårbara i realtid. Siffrorna ger evidensbaserade motiv för ytterligare övervakning och kontroll, till exempel med hjälp av övervakningskameror. Vid tillfället för våra intervjuer fanns planer på att även inkludera boende och invånare mer så att de skulle kunna rapportera misstänkta individer eller incidenter, vilka då skulle matas in i den allmänna instrumentpanelen. Lokala grannsamverkansgrupper skulle då i sin tur kunna meddelas automatiskt vid misstänkta rörelser i området genom att exempelvis länka WhatsApp-grupper för grannsamverkan till systemet.

Föreställningar: värdet med datafiering av trygghetsarbete

Collactivate beskrivs som en digital övervakningstjänst som förenar effektivitet med trygghet. På företagets hemsida kan potentiella kunder läsa:

> Med tjänsten Trygghet medverkar vi till att skapa ett tryggare lokalsamhälle. Genom att styra trygghetsresurser till de platser de behövs som mest sänker vi kostnader och ökar tryggheten. Det gör vi genom att detektera och samla in otrygga händelser och automatiskt dygnet runt förmedla dessa till trygghetsaktörer i realtid och skapa insikter VART och NÄR händelser sker. På så sätt kan vi skapa rätt åtgärd på rätt plats i rätt tid.

Utgångspunkten är alltså att sensorgenererad data ger ett förbättrat kunskapsunderlag och därmed ökad trygghet. Genom att dokumentera så kallade otrygga händelser i realtid ska tryggheten ökas. Här beskrivs

dock inte vad otrygga händelser är eller hur den insamlade datan leder till ökad trygghet. En av våra intervjupersoner vid Uppsalahem, en projektledare som har jobbat med Collactivate sedan några år tillbaka, beskriver processen så här:

> Jag tror att ju bättre underlag du har desto mer kan du göra och förändra … Om du kan visa siffror, om du kan visa att ”vi har haft fyrtio olika avvikelser inom det här området och det beror på det här” då börjar folk förstå ”okej, vi måste göra något”. Det blir en annan sak … Ja, men jag känner att vi kommer att kunna använda det här för att … Det blir en mycket bättre grund för att göra en förändring. Och bara att ”det är rörigt”. Det är en så vag sak att säga. ”Hyresgästerna tycker att det är osäkert. Det är stökigt.” Ja, men vad är det? ”När var det? Vad hände?” Vi kan inte riktigt svara på det. Så att det nu blir ganska knivskarpt, fyrtio anomalier, det är på natten. ”Jaha, vad är det?” ”Jo, men det är folk som stannar uppe i trapphuset.” ”Okej.” Ja, men då kan vi rama in problemet lite mer så där och sedan göra något.

Utöver en ökad konkretisering hävdas det att trygghetsarbete även kan bli snabbare med hjälp av digital teknik. Trygghetsarbetet kan till och med automatiseras med hjälp av fördefinierade tröskelvärden och en automatisk upptrappning av åtgärden. När och hur tillsynspersonal sätts in styrs exempelvis genom sensordata. Innovationschefen på Uppsalahem beskriver pilotprojektet med Collactivate som en möjlighet: ”Ny teknik kan accelerera vårt innovationsarbete och ger oss bättre förutsättningar att skapa trygga bostadsområden” (Uppsalahem 2021). Den dominerande föreställningen är alltså att trygghetsarbetet blir snabbare, effektivare och samtidigt säkrare. Föreställningarna ger uttryck för en datafiering av trygghetsarbetet, att omvandla avvikande händelser till siffror som möjliggör att mäta och jämföra incidenterna över tid. Dock stannar föreställningarna där.

Materialitet: smarta sensorer leverar objektivitet

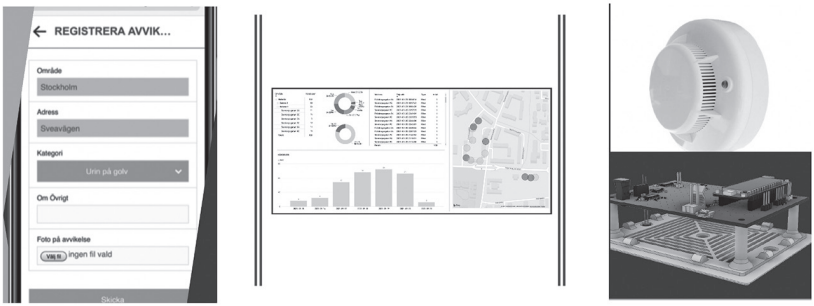
Själva tekniken är förhållandevis enkel. Den vita brandlarmslika lådan sitter på väggen i gemensamma utrymmen som trapphus och källarutrymmen. Sensorer registrerar rörelser, lukt, fukt och påslagna mobiltelefoner. Datan sparas i Amazons molntjänst (Amazon Web Services) och levereras sedan till kunden i form av en panel som presenterar den aggregerade datan i stapeldiagram och *hot spot*-kartor.

Vår intervjuperson på Collactivate, en programutvecklare, beskriver teknologin på följande sätt:

> Och det gör vi på två sätt, både för ”ologiska” sensorer och ”logiska” sensorer. De ”ologiska” sensorerna är de boende och personalen som rapporterar när något är onormalt. Det kan till exempel vara att man hittar droger, eller om man ser att städaren går och hittar cannabisfimpar eller hittar massor av läskburkar, godispapper eller någonting. Ja, då kan man ju få en indikation på vad är det som pågår där. Eller att någon har kissat i hissen eller något liknande. Sedan har vi de boende som kan rapportera när en osäker incident upptäcks. Och så har vi de ”logiska” sensorerna. Ni har varit på Uppsala och sett de här enheterna. De såg lite annorlunda ut i Uppsala. Men det här är vår sensor, som vi kallar den. Den använder ett, vad vi kallar, tröskelvärde, när en händelse överskrider dessa parametrar, då ska något hända och åtgärdstrappan sätts igång.

Citatet ger uttryck för förväntningen att högre objektivitet uppnås med hjälp av sensorgenererade data. Genom att sätta diskreta värden på otrygga händelser hoppas man kunna överkomma ”ologiska” rapporter från boende. Detta kan betraktas som ett utslag för vad José van Dijck (2014) har kallat dataism – övertygelsen att data levererar objektivare kunskap än mänskliga observatörer: människor är ologiska medan sensorer är logiska och systematiska och erbjuder tillförlitlig och objektiv kunskap.

Enligt företagets informationsmaterial levererar den fysiska sensorn smart data i realtid och erbjuder ”trygghet som en service”. Det är inte



Collactivates användargränssnitt, panelgränssnitt och sensorlåda. Bildkälla: Collactivates hemsida.

bara själva trygghetssensorerna som säljs utan även en app och panelgränssnitt som synliggör avvikande incidenter. Digitalt trygghetsarbete med smarta sensorer ter sig alltså inte som en engångsinvestering i hårdvara utan som en långsiktig lösning i en prenumerationstjänst, vad som kan kallas för en sorts infrastrukturell inlåsning. Sensorn fungerar inte utan mjukvaran och tvärtom.

Praktiker: utökat samarbete och infrastrukturell inlåsning

Sensorsystemet möjliggör och kräver nya praktiker i trygghetsarbetet hos kommunala bostadsbolag. Både mjukvaran och den fysiska sensorn kräver underhållsarbete över tid. Därmed uppstår nya uppgifter för boendevärdar och bostadsbolaget med att kontrollera själva sensorerna samt att övervaka datan som kontinuerligt samlas i panelgränssnittet.

Utöver det ständigt pågående underhållsarbetet används panelinformationen i samarbete med kommunen vad gäller tilldelning av resurser och konkreta åtgärder som ombyggnation, vaktpersonal och liknande. En av Uppsalahems medarbetare beskriver dessa nya sätt att arbeta med trygghet på följande sätt:

> Jag kan tänka mig att uppgifterna kan användas för många ändamål. Ett är att få veta ”vad som är normalt?” och ”vad som händer?” Det är jättebra. Sedan kan vi använda i det här stora säkerhetsarbetet tillsammans med kommunen, det här EST-arbetet där vi rapporterar incidenter till kommunen och sedan arbetar vi tillsammans med det. Så jag tror att det kan vara av stort värde där. Sedan måste man paketera data. Man kan inte bara säga ”det har varit ett skrik”. Det är inte på det sättet. Men man måste säga ”här har vi haft den här typen av anomali”. Jag tror att det definitivt kommer att vara användbart i EST-arbetet.

EST – effektiv samordning för ökad trygghet – ska möjliggöra systematisk samverkan mellan kommun, polis och fastighetsbolag med målet att öka tryggheten. Enligt Socialstyrelsen står EST huvudsakligen för systematisk och domänöverskridande informationsinhämtning för brottsförebyggande arbete. Information eller data kan här vara uppgifter om skadegörelse eller om samlingsplatser för ungdomar i både offentliga och halvoffentliga miljöer, såsom trapphus och källarutrymmen. Sensordatan blir följaktligen en del av den informationsinhämtning som ska möjliggöra snabba åtgärder, som förebyggande insatser från polisens sida, och

bostadsbolagens trygghetsarbete kopplas därmed närmare det polisiära arbetet. För bostadsbolaget blir sensordatan också underlag för att argumentera för utökat stöd och resurser från kommunen. Sammanfattningsvis ger Collactivate uttryck för en datafiering, en dataism och en infrastrukturell inlåsning som är kännetecknande för trygghetsteknologier i allmänhet.

Embrace: digitalisering genom manuellt arbete?

Embrace är Sveriges ledande företag när det gäller tillhandahållandet av digitala system för rapportering och analys av aktiviteter kopplade till otrygghet och brottslighet. Företaget grundades 2016 av en professor i kriminologi och psykologi i samarbete med ett universitets innovationsavdelning. Företaget menar att systemet utvecklades som ett svar på den efterfrågan som kommuner formulerat gällande ett mer effektivt, strukturerat och kunskapsbaserat digitalt stöd för brottsförebyggande och trygghetsfrämjande arbete. Det används av flera hundra organisationer, främst kommuner, men även av fastighetsägare och andra aktörer.

Föreställningar: systematikens och rapporteringens ideal

I både marknadsföring och användarnas egna beskrivningar framställs Embrace som den självklara lösningen för förbättrad brottsprevention. Embrace vilar på föreställningen om att deras system möjliggör ett kunskapsbaserat, systematiskt och samverkande brottsförebyggande arbete som kan öka tryggheten och minska brottsligheten. I vissa sammanhang talar representanter för Embrace till och med om en nollvision för brott, och att företagets system är den rätta vägen för att komma dit (Lorentzon 2021). De centrala ledorden återkommer ständigt: systematik, struktur, kunskapsbaserat, samverkan.

Fokus har dock skiftat över tid. Från att ha lanserats som ett verktyg för EST-samordnande trygghetsarbete (som nämndes i relation till Collactivate ovan) betonas sedan 2023 i stället hur systemet möjliggör för kommuner att leva upp till den nya lagen om kommuners ansvar för brottsförebyggande arbete (SFS 2023:196). Företaget har därefter kommit att betona att det inte enbart är systemet som erbjuds utan även kunskapsstöd

och partnerskap med relevanta organisationer. Genom att koppla sin produkt direkt till ny lagstiftning framstår Embrace inte bara som ett tekniskt verktyg utan som en självklar del av efterlevnaden av juridiska och politiska krav. Trovärdigheten förstärks ytterligare av grundarens och de anställdas akademiska meriter, vilket bäddar in systemet i en vetenskaplig legitimitet. I föreställningarna om systemet ingår därmed också ett reproducerande av den generella samhällstendensen att trygghet och brottsprevention inte enbart ses som polisens ansvar utan även kommunernas, att samverkan mellan kommuner, polis, fastighetsägare och andra aktörer är nödvändig samt att företaget kan möjliggöra detta.

Systemets legitimitet vilar i hög grad på att användarna själva bekräftar och reproducerar de föreställningar som företaget förmedlar. Nästan samtliga intervjuer och det material vi analyserat innehåller samma berättelse: dåtidens arbete beskrivs som fragmenterat och osystematiskt (med spontana mejl och slumpmässiga möten), medan framtiden, genom Embrace, förväntas präglas av ordning, analys och kunskap:

> Med hjälp av Embrace har vi blivit mer effektiva i vårt brottsförebyggande och trygghetsskapande arbete i kommunen. Embrace gör det lättare för våra rapportörer att rapportera in händelser och platser som är otrygghetsskapande eller upplevs otrygga. För oss har Embrace varit avgörande för att omhänderta de rapporter som inkommer. Vi kan nu visualisera händelser och platser och identifiera mönster såsom hot spots, hot times och trender. Embrace underlättar även det brottsförebyggande och trygghetsskapande arbetet i samverkan – helt plötsligt är det lätt för oss att presentera en lägesbild som vi alla är överens om. (En kommunal tjänsteman citerad på Embraces hemsida.)

Både produktbeskrivningar och användarintervjuer vittnar om ett nästan unisont tal om ”systematik”, framtida resultat och styrkan i att flera aktörer kan rapportera och samverka inom samma system. Det är särskilt slående hur ofta ord som ”rapporter”, ”rapportörer” och ”rapportering” återkommer i såväl företagsmaterial som användarintervjuer. Själva rapporterandet är en kärnpraktik som laddas med löfte om systematik och evidens. Rapportören framställs som en självklar roll i det framtida kommunala trygghetsarbetet och bär i sig på en legitimitet. Handlingen ”att rapportera” blir en indikator på framgång och ansvarstagande snarare än att faktiska resultat visar på systemets effektivitet. På så vis blir systemet

mer än en neutral infrastruktur – det är kollektiva, institutionellt förankrade och offentligt framförda visioner om en önskvärd framtid. Det blir ett system som sätter villkoren för vad som räknas som relevant att rapportera och vilka som anses vara relevanta att göra det. Systematik betyder därmed inte nödvändigtvis att kunskapen om trygghet blir djupare, utan att den formas efter vad systemet kan innehålla och kategorisera. Embrace fungerar performativt inte bara genom att sprida en vision om framtida effektivitet – som motiverar investeringar, förändrar arbetssätt och formar vad som räknas som kunskap och framgång i det brottsförebyggande arbetet, även innan faktiska resultat går att påvisa – utan också genom en slags administrativ förskjutning där rapportering blir ett trygghetsarbete i sig. Den framtid som målas upp har dock lite med den vardagliga praktiken att göra, vilken vi snart ska återkomma till.

Materialitet: plattformen som kunskapsstruktur

Embrace tillhandahåller ett system som utgörs av en digital plattform som är tekniskt utformad för rapportering och analys av händelser som brott, otrygghetsrelaterade incidenter och aktiviteter. I systemet kan användare rapportera allt från olika former av brott, ordningsstörningar, otrygga platser eller miljöer, ansamlingar av personer, klotter, vandalism eller annan skadegörelse, belysningsproblem och liknande. Dessa observationer kodas in i fördefinierade kategorier i systemet och blir sedan till visualiseringar, statistik samt geografiska och tidsmässiga lägesbilder. Plattformen erbjuder även moduler för integration med andra datakällor (från polisen, Statistiska centralbyrån och annan demografisk data). Dessa handlingsmöjligheter styr vilken kunskap som blir möjlig att inhämta: systemet kräver standardiserad rapportering och tydliga kategorier och tenderar därför att prioritera sådant som lätt kan kodas, visualiseras och mätas. Det ”systematiska” realiseras dock först när volym och kvalitet på inmatad data når en viss nivå – något många användare brottas med i vardagen eftersom det återkommande problemet handlar om att ett tillräckligt antal rapporter för att kunna göra efterfrågade analyser saknas. Det handlar alltså inte bara om vad systemet kan rapportera utan vad det kräver att användaren rapporterar på rätt sätt och tillräckligt mycket av.

Systemet bygger på att användarna, oftast kommunanställda, löpande rapporterar in observationer och incidenter i det geografiska område de verkar i. Här betonas ofta att även rapporter som inte kommer till polisens kännedom, exempelvis om aktiviteter eller platser förknippade med otrygghet, ska rapporteras in. Utifrån det underlag som kommer in i systemet kan man sedan skapa lägesbilder och analyser som ger beslutsfattare och verksamheter ett underlag för att planera, rikta och följa upp insatser, samt utvärdera dessa.

Plattformen är utformad för att underlätta och förenkla arbetet men kräver också utbildning och support som tillhandahålls av företaget. Systemet kompletteras därför av utbildningar, seminarier och kundtjänst, vilket förstärker dess roll som kunskapsnav snarare än enbart teknisk lösning och mjukvara. Materialiteten är också performativ genom att den möjliggör rapportering av ett visst antal händelser, det vill säga vad som ska räknas som relevant data, samt vilka aktörer som ska rapportera och hur kunskap därefter ska produceras och kommuniceras. Tekniskt sett representerar Embrace ett typiskt exempel på vad vi skulle kalla en mjuk, distribuerad och till synes icke-integritetskränkande digital trygghetsteknologi. Det kräver inga spektakulära övervakningsverktyg utan snarare löpande datarapportering, visualisering och systematisering av vardagliga observationer och händelser bundna till specifika kategorier för vad otrygghet kan vara inom systemet. Systemets materialitet styr, selekterar och begränsar vad som blir möjligt att rapportera och analysera. Det påverkar sedan direkt vilka företeelser som räknas och vilka platser eller grupper som hamnar i fokus, och därmed vad som kan mobilisera och motivera resurstilldelning.

Praktiker: rapporteringens byråkrati och manuella logik

De praktiker som ryms i vardagens arbete med implementeringen och användningen av Embraces system karaktäriseras inte av den automatiserade kunskap och systematik som präglar föreställningarna om systemet, utan av omfattande organiseringsarbete. Kommunala tjänstemän måste lägga mycket tid på att identifiera, rekrytera, motivera, instruera och följa upp de aktörer som är tänkta att kontinuerligt rapportera in aktiviteter i systemet. Dessa rapportörer är ofta personer i andra yrkesgrupper inom

kommunen, exempelvis personal inom skola, hemtjänst och socialtjänst. Att upprätthålla rapporteringen kan ofta vara utmanande eftersom den inte ingår i dessa aktörers ordinarie arbetsuppgifter och kompetensområde. För att få systemet att fungera krävs också löpande stöd och utbildning till användarna. En betydande del av arbetet består därför inte i att analysera data, utan att hålla rapporteringen vid liv genom utbildning, påminnelser och relationsarbete. Det språkliga mönstret av att tala om ”rapporter” och ”rapportörer” får här också en praktisk dimension. I visionen om rapporterandet konstrueras handlingen att rapportera som det centrala beviset på att trygghetsarbetet bedrivs på ett systematiskt sätt. I den vardagliga praktiken innebär det att ”det systematiska” inte skapas av teknologin i sig, utan av ett tidskrävande manuellt arbete som sprids ut på ofta redan belastade personalgrupper. I praktiken förutsätter därmed alltså den nya teknologin en pågående mobilisering av mänskliga resurser: att någon rapporterar, att andra tolkar och att ytterligare aktörer utvärderar. Tjänstemännen beskriver ofta att det är svårt att uppnå både volym och systematik (Winter 2025).

När rapporterna sedan kommer till användning, exempelvis i samverkansmöten och liknande, menar de kommunala tjänstemännen att mötena förvisso är centrala men ofta bygger på redan etablerade rutiner och relationer för hur lägesbilder skapas. Samtidigt kvarstår också många andra praktiker från tiden före Embrace. Många aktörer fortsätter att använda parallella kanaler som mejl, telefonsamtal eller spontant utbyte av information, vilket både underminerar systemets exklusivitet och visar på dess begränsningar. Den vardagliga användningen av systemet medför därmed ett manuellt och relationellt arbete som ligger långt bort från den förenklade och digitaliserade bild som förmedlas i föreställningarna. Detta kastar nytt ljus över retoriken om ett ”kunskapsbaserat och systematiskt brottsförebyggande arbete”. I praktiken handlar det snarare om en byråkratisering av trygghetsarbetet, där rapporteringsrutinen blir ett mål i sig, frikopplad från den otrygghetsproblematik som rapporteringen skulle adressera.

Avslutning

Våra fallstudier visar att digitala trygghetsteknologier inte bara är neutrala tekniska verktyg utan också sociotekniska system där trygghet formas och omformas i skärningspunkten mellan föreställningar, materialitet och praktiker i samspel mellan många olika aktörer. Föreställningar om trygghet och trygghetsteknologier är performativa: de motiverar och legitimerar investeringar och förändrade arbetssätt och formar hur teknologier faktiskt används och förstås i den vardagliga praktiken (se också Williamson 2018; Winter 2025). Samtidigt riskerar samma föreställningar skapa en normalisering av hotbilder och förstärka diskurser om trygghet och otrygghet, vilket i sin tur kan skapa eller förstärka känslor av oro och därmed också behovet av nya digitala lösningar (Winter & Hermansson 2025). Vad som presenteras som ett ökat behov av ny teknologi riskerar i ett vidare led att skapa nya osäkerheter genom organisatoriska utmaningar, i själva ansvarsfördelningen samt genom hur teknologierna faktiskt ska användas.

Medan det finns breda samhälleliga förhoppningar om att digital teknik ska skapa effektivitet och kollektiv trygghet, visar våra analyser hur löften om systematik och kunskapsbaserat trygghetsarbete ofta krockar med praktiska och organisatoriska begränsningar. Resultatet blir ibland nya former av organisatorisk osäkerhet och nya risker, vilket händelserna vid Risbergska brutalt illustrerar. Att information skickas till fel mottagare, eller att felaktiga rekommendationer ges om förhållningssätt är bara två exempel på nya former av otrygghet, tvärtemot ursprungliga intentioner.

Användningen av dessa teknologier medför också nya former av ansvarsfördelning snarare än att avlasta exempelvis polisens arbete. Fler aktörer – kommuner, bostadsbolag, företag och olika slags personal – förväntas både ta och ges ett större ansvar för upprätthållande av trygghet. Samarbetet inom så kallade trippelhelix-formationer bestående av akademin, offentlig sektor och privata företag leder dessutom inte sällan till infrastrukturell inlåsning av offentliga institutioner. När trygghet levereras som en prenumerationstjänst som inkluderar mjuk- och hårdvaror ökar också risken för sådan inlåsning och ett förskjutet ansvar.

Digitala trygghetsteknologier visar också på att trygghet blir alltmer en del av säkerhetiseringsprocessen. Digitalt trygghetsarbete som knyter an till mjukare värden och subjektiva upplevelser blir en brygga till hårdare säkerhetsåtgärder, till exempel genom att dra in bostadsbolag och skolor i polisiärt arbete. Dessutom öppnas halvoffentliga platser som trappuppgångar och källare för systematisk kontroll och övervakning genom arbetet med smarta sensorer och appar. Ett centralt tema för att förstå trygghetsteknologier är således också den individualisering och privatisering av trygghetsarbete som pågår. I den växande trygghetsmarknaden blir otrygghet en förutsättning för att motivera fortsatta investeringar i digitala lösningar. Därmed riskerar löftet om trygghet att bli ett rörligt mål, där teknologins legitimitet vilar mer på dess administrativa och känslomässiga effekter än på faktiska utfall.

Vidare visar vår analys av digitala trygghetsteknologier på en större samhällsförändring, där trygghet och säkerhet flyter ihop samtidigt som de ska göras distinkt, avgränsade och objektiva genom att mätas med hjälp av digitala teknologier. Sammanflätningen av trygghet och säkerhet bör förstås som metoder för styrning, ökad kontroll och minskad frihet, oavsett om de är kopplade till individers upplevelser (trygghet) eller till lösningar på problem (säkerhet). Ytterligare argument för att använda sig av en definition av digitala trygghetsteknologier som inkluderar både trygghet och säkerhet möter vi när det kommer till den utveckling vi sett i Sverige de senaste decennierna med den faktiska användningen av digitala trygghetsteknologier och den i stort sett ofrånkomliga marknad som vi numera befinner oss i. Digitala trygghetsteknologier befäster sammanflätningen av trygghet och säkerhet samtidigt som de integrerar den kollektiva nivån med individuella erfarenheter och upplevelser i relation till otrygghet. Genom att samla och producera systematisk information och kunskap kring otrygghet reproducerar de samtidigt själva den känslomässiga utgångspunkten att våra samhällen har blivit mer osäkra. Genom att introducera och möjliggöra mätningen av fenomen som tidigare inte har inkluderats systematiskt i trygghetsarbetet och som rör sig på en vardaglig nivå tar sig säkerhetsdiskursen in i nya områden med potential för kommersialisering.

Det alltmer ökade fokus på trygghet och brottsprevention som materialiseras i nya lagar, policyer och teknologier har också medfört ett ökat ansvar för både offentliga och privata aktörer. Kommuner, skolor och andra aktörer inom offentlig sektor införskaffar i allt större grad produkter för att uppfylla juridiska krav på brottsförebyggande arbete. Dessa nya digitala trygghetsteknologier verkar under radarn på traditionell brottsförebyggande polisiär verksamhet. Snarare är de inramade som en sorts mjuk teknologi som lovar ekonomisk såväl som administrativ effektivitet samtidigt som de sägs undvika att inkräkta på människors privatliv eller vardag (till skillnad från övervakningskameror eller kroppsvisitering). Men även dessa teknologier bidrar, menar vi, till produktion av såväl risk som kontroll då de inte bara observerar utan även formar rumsliga och sociala föreställningar om hot, och konstruerar vissa grupper, beteenden och platser som riskfyllda. Våra fall visar hur digitala trygghetsteknologier skapar nya former av styrning där ansvar först förskjuts till privata företag som erbjuder tekniska lösningar för att sedan ytterligare förskjutas till slutanvändarna. Detta innebär risk för en avpolitisering av trygghetsfrågan, där teknologiska lösningar framstår som självskrivna och utan politiskt ansvar, samtidigt som de kan förstärka eller skapa nya ojämlikheter beroende på hur de används och vilka aktörer och områden som omfattas.

Sammanfattningsvis visar Cosafe, Collactivate och Embrace att ”digital trygghet” inte är något neutralt fenomen, utan resultatet av ständiga omförhandlingar om ansvar, risk, plats och kunskap. Risbergska-exemplet synliggör särskilt hur digitala system kan skapa nya gränser för ansvar och ibland även förstärka hotbilder snarare än förebygga dem. Det understryker behovet av fortsatt kritisk granskning av teknikens sociala och politiska konsekvenser, av samtal om kollektiv trygghet och de krav och förväntningar vi placerar på våra digitala lösningar.

Referenser

Balzacq, Thierry & Guzzini, Stefano (2015). ”Introduction: ’What Kind of Theory – if any – is Securitization?’”, *International Relations*, 29:1, s. 97–102, https://doi.org/10.1177/0047117814526606a.

Boels, Dominique & Verhage, Antoinette (2016). ”Plural Policing: A State-of-the-Art Review”, *Policing: An International Journal*, 39:1, s. 2–18, https://doi.org/10.1108/PIJPSM-05-2015-0069.

Brandén, Jennie (2022). *In the Name of Safety. Power, Politics and the Constitutive Effects of Local Governing Practices in Sweden*. Avhandling, Umeå universitet.

Brayne, Sarah (2017). ”Big Data Surveillance: The Case of Policing”, *American Sociological Review*, 82:5, s. 977–1008, https://doi.org/10.1177/0003122417725865.

Bucher, Taina (2018). *If…Then. Algorithmic Power and Politics*. Oxford : Oxford University Press.

Buzan, Barry, Wæver, Ole & Wilde, Jaap de (1998). *Security. A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Costanza-Chock, Sasha (2020). *Design Justice: Community-Led Practices to Build the Worlds We Need*. London: The MIT Press, https://doi.org/10.7551/mitpress/12255.001.0001.

Dagens Nyheter (2025a). ”Två döda efter utrymning – Örebro utreder ifrågasatt säkerhetsapp”, 9 april.

Dagens Nyheter (2025b). ”Säkerhetsapp gav olika besked – sju larm på fem minuter”, 29 juni.

Dijck, José van (2014). ”Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology, *Surveillance & Society*, 12:2, s. 197–208, https://doi.org/10.24908/ss.v12i2.4776.

Egbert, Simon (2019). ”Predictive Policing and the Platformization of Police Work”, *Surveillance & Society*, 17:1–2, s. 83–88, https://doi.org/10.24908/ss.v17i1/2.12920.

Egbert, Simon & Leese, Matthias (2021). *Criminal Futures. Predictive Policing and Everyday Police Work*. Abingdon: Taylor & Francis.

Egbert, Simon, Galis, Vasilis, Gundhus, Helene O.I. & Wathne, Christin Thea (2024). ”The Platformization of Policing: A Cross-National Analysis”, i Kuldova, Tereza Østbø, Gundhus, Helene O.I. & Wathne, Christin Thea (red.), *Policing and Intelligence in the Global Big Data Era, Volume I: New Global Perspectives on Algorithmic Governance*, s. 349–392. Cham: Palgrave Macmillan.

Ferguson, Andrew Guthrie (2017). *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Fest, Isabelle, Schäfer, Mirko, Dijck, José van & Meijer, Albert (2023). ”Understanding Data Professionals in the Police: A Qualitative Study of System-Level Bureaucrats”, *Public Management Review*, 25:9, s. 1664–1684, https://doi.org/10.1080/14719037.2023.2222734.

Fyfe, Nick, Gundhus, Helene Oppen & Rønn, Kira Vrist (2018). ”Introduction”, i idem (red.), *Moral Issues in Intelligence-Led Policing*, s. 1–22. Abingdon: Routledge.

Galis, Vasilis, Gundhus, Helene O.I. & Vradis, Antonis (red.) (2025). *Critical Perspectives on Predictive Policing. Anticipating Proof?* Cheltenham: Edward Elgar Publishing.

Garland, David (2001). *The Culture of Control. Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

Hansen Löfstrand, Cecilia (2021). "Marketization in a State-Centred Policing Context: The Case of Sweden", *European Journal of Criminology*, 18:6, s. 899–917, https://doi.org/10.1177/1477370819882905.

Hermansson, Klara (2019). *Symbols and Emotions in Swedish Crime Policy Discourse*. Avhandling, Stockholms universitet.

Hermansson, Klara (2022). "The Symbolic Potential of Security: On Collective Emotions in Swedish Criminal Policy Discourse", *Emotions and Society*, 4:3, s. 395–410, https://doi.org/10.1332/263169021X16517125618359.

Hutchby, Ian (2001). "Technologies, Texts and Affordances", *Sociology*, 35:2, s. 441–456, https://doi.org/10.1177/S0038038501000219.

Hälterlein, Jens (2021). "Epistemologies of Predictive Policing: Mathematical Social Science, Social Physics and Machine Learning", *Big Data & Society*, 8:1, https://doi.org/10.1177/2053951721003118.

Jasanoff, Sheila (2015). "Future Imperfect: Science, Technology, and the Imaginations of Modernity", i Jasanoff, Sheila & Kim, Sang-Hyun (red.), *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*, s. 1–33. Chicago: University of Chicago Press.

Kaufmann, Mareile, Egbert, Simon, & Leese, Matthias (2019). "Predictive Policing and the Politics of Patterns", *The British Journal of Criminology*, 59:3, s. 674–692, https://doi.org/10.1093/bjc/azy060.

Kaun, Anne (2025). "Temporalities of Welfare Automation: On Timing, Belatedness, and Perpetual Emergence", *Time & Society*, 34:3, s. 418–434, https://doi.org/10.1177/0961463X251313572.

Kaun, Anne & Männiste, Maris (2025). "Public Sector Chatbots: AI Frictions and Data Infrastructures at the Interface of the Digital Welfare State", *New Media & Society*, 27:4, s. 1962–1985, https://doi.org/10.1177/14614448251314394.

Kutnowski, Moish (2017). "The Ethical Dangers and Merits of Predictive Policing", *Journal of Community Safety and Well-Being*, 2:1, s. 13–17, https://doi.org/10.35502/jcswb.36.

Larsson, Sebastian & Rhinard, Mark (2021). *Nordic Societal Security. Convergence and Divergence*. New York: Routledge.

Leese, Matthias (2023). "Enacting Criminal Futures: Data Practices and Crime Prevention", *Policing and Society*, 33:3, s. 333–347, https://doi.org/10.1080/10439463.2022.2112192.

Lorentzon, Anna (2021). "Hans innovation bidrar till minskad brottslighet och ett tryggare samhälle", intervju med Embraces grundare på Mötesplats Social Innovations hemsida, 27 april, https://socialinnovation.se/si/forskning-i-samverkan/forskning-i-samverkan-som-forandrar-sverige/hans-innovation-bidrar-till-minskad-brottslighet-och-ett-tryggare-samhalle/ (hämtad 29 september 2025).

Norman, Donald A. (1988). *The Psychology of Everyday Things*. New York: Basic Books.
Sahlin Lilja, Hanna (2021). *The Emergence, Establishment, and Expansion of Fear of Crime Research in Sweden*. Avhandling, Lunds universitet.
SFS 2023:196. *Lag om kommuners ansvar för brottsförebyggande arbete.*
Suchman, Lucy (2020). ”Agencies in Technology Design: Feminist Reconfigurations”, i Wallach, Wendell & Asaro, Peter (red.), *Machine Ethics and Robot Ethics*, s. 361–375. London: Routledge.
Suchman, Lucy, Blomberg, Jeanette, Orr, Julian E. & Trigg, Randall (2017). ”Reconstructing Technologies as Social Practice”, i Jimenez, Alberto Corsin (red.), *The Anthropology of Organisations*, s. 431–447. London: Routledge.
Uppsalahem (2021). ”Nytt pilotprojekt hos Uppsalahem utforskar möjligheterna med smarta sensorer i fastigheten”, 16 december, https://www.uppsalahem.se/om-oss/nyheter-och-pressmeddelanden/nytt-pilotprojekt-hos-uppsalahem-utforskar-mojligheterna-med-smarta-sensorer-i-fastigheten/ (hämtad 23 juni 2025).
Williamson, Ben (2018). ”Silicon Startup Schools: Technocracy, Algorithmic Imaginaries and Venture Philanthropy in Corporate Education Reform”, *Critical Studies in Education*, 59:2, s. 218–236, https://doi.org/10.1080/17508487.2016.1186710.
Winter, Katarina (2025). ”Longing and Lacking: Pasts, Presents, and Futures in Municipal Crime Prevention Technology”, *Nordic Journal of Science and Technology Studies*, 13:1, s. 81–92, https://doi.org/10.5324/njsts.v13i1.5857.
Winter, Katarina & Hermansson, Klara (2025). ”(Dis)affordances and Abandonment: Understanding Everyday user Engagement with Security Apps”, *Sociologisk Forskning*, 62:1–2, s. 59–84, https://doi.org/10.37062/sf.62.27825.
Örebro kommun (2025). ”Örebro kommun har utrett säkerhetsappen Cosafe”, 26 maj, uppdaterad 27 maj, https://www.orebro.se/nyheter/nyheter/2025-05-26-orebro-kommun-har-utrett-sakerhetsappen-cosafe.html (hämtad 10 september 2025).