



JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Hanna Olofsson

När får algoritmer övervaka i arbetslivet?

En rättslig analys av när algoritmisk övervakning
och arbetsledning inskränker på arbetstagares integritet

JURM02 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Jenny Julén Votinius

Termin: VT26

Innehåll

Summary	4
Sammanfattning	5
Förord.....	6
Förkortningar.....	7
1 Inledning	9
1.1 Bakgrund	9
1.2 Syfte och frågeställningar.....	11
1.3 Metod och material.....	11
1.3.1 Metod	11
1.3.2 Material	13
1.4 Avgränsningar	14
1.5 Forskningsläge.....	15
1.6 Disposition.....	16
2 Integritet som grundläggande rättighet.....	18
2.1 Europakonventionen om rätten till privatliv.....	18
2.1.1 Tillämpningsområde	18
2.1.2 Gränsdragningen mellan tillåten och otillåten övervakning i Europadomstolens praxis	20
2.1.2.1 Otillåtna övervakningsåtgärder	20
2.1.2.2 Tillåtna övervakningsåtgärder	22
2.2 Den Europeiska sociala stadgan	24
2.2.1 Funktion och tillämpningsområde.....	24
2.2.2 Centrala rättigheter kopplade till arbetslivet.....	25
2.3 EU-stadgan	26
2.3.1 Allmänt om stadgan	26
2.3.2 Materiellt innehåll och begränsningar.....	26
2.4 Regeringsformen	28
2.5 Diskussion	29
3 EU:s rättsakter	32
3.1 Rätten till integritet enligt GDPR.....	32
3.1.1 Syfte och tillämpningsområde.....	32
3.1.2 Definitioner och känsliga personuppgifter.....	33
3.1.3 De grundläggande principerna	34
3.1.4 Rättslig grund	35
3.1.5 Den registrerades rättigheter	37
3.1.6 Särskilt om automatiserat beslutsfattande och profilering.....	39

3.2	AI förordningen	40
3.2.1	Syfte och tillämpningsområde.....	40
3.2.2	En riskbaserad modell	41
3.2.3	Särskilda krav vid högrisk-AI	43
3.3	Plattformsdirektivet	45
3.3.1	Syfte och tillämpningsområde.....	45
3.3.2	Reglering av algoritmisk verksamhetsledning	46
3.3.2.1	Förbjudna system.....	46
3.3.2.2	Transparens, tillsyn och mänsklig granskning	47
3.3.2.3	Övriga krav	48
3.4	Diskussion	48
4	Svensk rätt	52
4.1	Arbetsgivarens arbetsledningsrätt och kontrollbefogenheter.....	52
4.2	Lagstadgade begränsningar av arbetsledningsrätten	54
4.2.1	Ett fragmenterat regelverk.....	54
4.2.2	Konstitutionella begränsningar	54
4.2.3	Begränsningar enligt EU:s rättsakter	55
4.2.4	Straffrättsliga begränsningar	59
4.3	God sed på arbetsmarknaden som begränsning av arbetsledningsrätten	60
4.4	Diskussion	62
5	Analys och slutsats	65
	Källförteckning	73

Summary

This thesis examines when the use of algorithmic surveillance and management in the workplace becomes an unlawful intrusion into employees' privacy. Due to rapid technological development, where digital tools and artificial intelligence are increasingly used to monitor, direct and evaluate work, the thesis aims to analyse this legal boundary under current law. The focus is on the requirements under EU law and Swedish law when using such systems and whether the current legal framework is sufficient to meet these developments. To answer these questions, the thesis uses a legal dogmatic method together with an EU law method.

The analysis shows that there is no unified legal framework governing algorithmic surveillance and management. Instead, the legal position is shaped through an interaction between different legal systems and regulations. As a general rule, a surveillance measure must have a legal basis, pursue a legitimate aim and be proportionate in relation to that aim in order to be considered lawful. The assessment particularly takes into account factors such as transparency, the scope of the surveillance and the possibility of mapping or profiling the employee. At the same time, Swedish law shows that employers, through the managerial prerogative, have far-reaching authority to direct and distribute work. However, employees' privacy interests must be given significant weight in the balancing of interests, meaning that a particularly strong employer interest is required for the measure to be considered lawful.

Furthermore, the thesis shows that the current fragmented legal framework is in several ways inadequate in relation to rapid technological development. In particular, the increasing use of algorithmic surveillance and management creates legal boundary issues that existing rules are not fully adapted to handle. Although new EU initiatives, such as the AI Act and the Platform Work Directive, strengthen the protection of workers, uncertainties still remain regarding how these rules should be applied in practice. This is especially the case in traditional employment relationships outside the platform work sector.

Overall, it can be concluded that the point at which algorithmic surveillance and management become unlawful intrusions into employees' personal privacy is largely determined through a concrete and nuanced proportionality assessment. This means that similar measures can be allowed in one situation but not in another, making it difficult to set a clear general limit. However, it is clear that there are strong requirements for transparency, that continuous and extensive surveillance is generally not allowed and that certain forms of algorithmic surveillance and management may be accepted, provided that the employer's interest carries sufficient weight in the balancing of interests.

Sammanfattning

Denna redogörelse behandlar när algoritmisk övervakning och arbetsledning övergår från att vara tillåten i arbetslivet till att utgöra ett otillåtet intrång i arbetstagares personliga integritet. Mot bakgrund av den snabba tekniska utvecklingen, där digitala verktyg och artificiell intelligens i allt större utsträckning används för att övervaka, styra och utvärdera arbete, syftar uppsatsen till att analysera denna gränsdragning enligt gällande rätt. Fokus ligger på vilka krav som följer av EU-rätt och svensk rätt vid användningen av sådana system samt om det nuvarande regelverket är tillräckligt för att möta utvecklingen. För att besvara dessa frågor har uppsatsen utgått från en rättsdogmatisk metod i kombination med en EU-rättslig metod.

Genomgången visar att det inte finns ett enhetligt regelverk för algoritmisk övervakning och arbetsledning, utan att rättsläget i stället formas genom ett samspel mellan olika normsystem. För att en övervakningsåtgärd ska vara tillåten krävs som utgångspunkt att den har stöd i lag, tillgodoser ett legitimt syfte och är proportionerlig i förhållande till detta syfte. Bedömningen tar särskilt hänsyn till faktorer såsom transparens, övervakningens omfattning och möjligheten att kartlägga arbetstagaren. Vidare framgår det i svensk rätt att arbetsgivaren genom arbetsledningsrätten har ett långtgående handlingsutrymme att styra och fördela arbetet. Arbetstagarens integritetsintresse ska dock tillmätas stor vikt vid en intresseavvägning, vilket innebär att det krävs ett särskilt tungt vägande arbetsgivarintresse för att åtgärden ska anses tillåten.

Därutöver visar uppsatsen att det nuvarande fragmenterade regelverket i flera avseenden framstår som otillräckligt i förhållande till den snabba tekniska utvecklingen. Särskilt den ökade användningen av algoritmisk arbetsledning och övervakning aktualiserar rättsliga gränsdragningsproblem som befintliga regler inte fullt ut är anpassade för att hantera. Även om nya EU-rättsliga initiativ, såsom AI-förordningen och plattformsdirektivet, stärker skyddet, kvarstår osäkerheter i hur reglerna ska tillämpas i praktiken. Särskilt gäller detta i traditionella anställningsförhållanden utanför plattformarbete.

Sammantaget kan det konstateras att gränsen för när algoritmisk övervakning och arbetsledning övergår till att utgöra ett otillåtet intrång i arbetstagares personliga integritet i stor utsträckning avgörs genom en konkret och nyanseerad proportionalitetsbedömning. Bedömningen är situationsberoende, vilket innebär att liknande kontrollåtgärder kan vara tillåtna i ett sammanhang men otillåtna i ett annat. Därför är en generell gräns svår att fastställa. Det kan dock fastslås att informationskravet är långtgående, att kontinuerlig och omfattande övervakning som huvudregel är otillåten samt att vissa former av algoritmisk övervakning och arbetsledning kan accepteras, förutsatt att arbetsgivarens intresse väger tillräckligt tungt vid intresseavvägningen.

Förord

Till att börja med vill jag rikta ett stort tack till min handledare Jenny Julén Votinius för värdefull vägledning, konstruktiva synpunkter och stöd under arbetets gång. Din uppmuntran och våra diskussioner har varit väldigt betydelsefulla och underlättat processen.

Jag vill även tacka familj och vänner för deras stöd, inte bara under denna process utan under hela utbildningen.

Hanna Olofsson

Förkortningar

AD	Arbetsdomstolen
AI	Artificiell intelligens
AI-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008
Artikel 29-gruppen	Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter
BrB	Brottsbalk (1962:700)
Dataskyddslagen	lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Dir.	Kommittédirektiv
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EPRS	European Parliamentary Research Service
EU-domstolen	Europeiska unionens domstol
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europeiska sociala stadgan	Europarådets sociala stadga (reviderad)
EUT	Europeiska unionens officiella tidning

FEUF	Fördraget om Europeiska unionens funktionssätt
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
GPS	Global Positioning System
IMY	Integritetsskyddsmyndigheten
JO	Justitieombudsmannen
Kamerabevakningslagen	Lag (2018:1200) om kamerabevakning
LAS	Lagen (1982:80) om anställningsskydd
MBL	Lagen (1976:580) om medbestämmande i arbetslivet
Plattformsdirektivet	Europaparlamentets och rådets förordning (EU) 2024/2831 av den 23 oktober 2024 om förbättrade arbetsvillkor för plattformsarbete
Prop.	Proposition
RF	Regeringsformen (1974:152)
SFS	Svensk författningssamling
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Övervakning på arbetsplatsen är inget nytt fenomen utan har förekommit under lång tid. Historiskt har arbetsgivare använt olika former av kontroll för att följa upp arbetstagares prestationer, exempelvis genom att registrera arbetstid, mäta produktion eller använda ackordsbaserad ersättning. Den tekniska utvecklingen har skapat nya möjligheter till omfattande övervakning av anställda. Samtidigt har en förändrad ledningskultur, där fokus i högre grad ligger på individuell snarare än kollektiv prestationsmätning, vuxit fram. Detta har bidragit till en utvidgning och intensifiering av övervakningen av anställda.¹

Under de senaste åren har denna utveckling i synnerhet tagit sig uttryck i en ökad digital övervakning i arbetslivet. En viktig förklaring är de förändrade arbetsformer som följde av covid-19-pandemin, då distans- och hybridarbete blev vanligt förekommande. Dessa arbetsformer medförde ett ökat behov av uppföljning och kontroll av arbetet, eftersom den traditionella fysiska övervakningen i stor utsträckning begränsades. Detta behov bidrog till att digitala övervakningsverktyg utvecklades, främst genom att tekniken blev enklare och billigare att använda. Även efter pandemins slut finns det inget som tyder på att nivån av övervakning har minskat. Tvärtom har övervakningsfunktioner i många fall blivit en integrerad del av ordinarie digitala arbetsverktyg.²

Denna utveckling har gett upphov till en diskussion om arbetstagares rätt till privatliv. Fackliga organisationer har pekat på övervakning i arbetslivet som ett allvarligt problem och efterfrågat ett starkare rättsligt skydd.³ Även media har uppmärksammat att övervakning är vanligt förekommande och att många arbetstagare upplever sig vara kontinuerligt övervakade.⁴ Under senare år har dessutom flera konkreta fall behandlats, där övervakning i arbetslivet bedömts strida mot gällande regler om integritetsskydd. I ett beslut från Justitieombudsmannen (JO) kritiserades Södertälje kommun för att ha infört en rutin där kommunen, genom ett upphandlat externt företag, löpande lät genomföra manuella sökningar i en databas med offentliga handlingar från domstolar och myndigheter. Syftet med sökningarna var att kontrollera om

¹ Kirstie Ball, "Workplace Surveillance: An Overview", *Labor History*, vol. 51, nr 1 (februari 2019), s. 88 f.

² Integritetsskyddsmyndigheten, *Integritet och ny teknik 2020–2024: Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen*, Rapport (2025), s. 30, <https://www.imy.se/publikationer/integritet-och-ny-teknik-20202024/>.

³ "Massövervakningen av anställda på jobbet måste regleras", TCO, 27 maj 2025, <https://tco.se/fakta-och-politik/arbetsratt/massovervakningen-av-anstallda-pa-jobbet-maste-regleras>; "Allt fler övervakas på jobbet", Handels, 9 oktober 2025, <https://www.handels.se/aktuellt/2025/allt-fler-overvakas-pa-jobbet/>.

⁴ "Digital övervakning på kontoret är vanligare än många tror", Ingenjören, 20 maj 2025, <https://ingenjoren.se/2025/05/20/digital-overvakning-pa-kontor-ar-vanligare-an-de-flesta-inser/>.

kommunanställda hade dömts för vissa brott. JO konstaterade att kontrollerna genomfördes utan lagligt stöd eller samtycke från de anställda, vilket utgjorde ett betydande intrång i de anställdas personliga integritet.⁵ Därutöver har Integritetsskyddsmyndigheten beslutat om sanktionsavgift mot H&M för otillåten kameraövervakning i ett arbetsutrymme utan tillräcklig rättslig grund och informationsgivning.⁶ Även i den rättsvetenskapliga litteraturen har frågan uppmärksamats. Selberg har redan under covid-19-pandemin framhållit att det ofta är svårt att avgöra vilka former av övervakning som är tillåtna och efterlyste en tydligare och mer sammanhållen reglering av arbetstagares integritetsskydd.⁷

Parallellt med att övervakningsfrågor och skyddet för arbetstagares privatliv blivit alltmer centrala har en ny teknisk dimension tillkommit genom utvecklingen av artificiell intelligens. Genom AI kan datorer analysera data, ge rekommendationer och utföra uppgifter som tidigare krävde mänsklig bedömning.⁸ I arbetslivet har detta bidragit till framväxten av algoritmisk arbetsledning, där tekniska system används för att stödja eller automatisera beslut om hur arbetet leds, fördelas och bedöms.⁹ I praktiken kan sådana system användas för att anställa arbetstagare, organisera det dagliga arbetet samt avsluta anställningar. Systemen används även för att kontrollera arbetet och kan i vissa fall gå längre än traditionell arbetsplatsövervakning, genom möjligheten att bearbeta arbetsplatsdata.¹⁰ I de flesta fall används dessa system som ett stöd för mänskliga chefer, snarare än för att helt automatisera beslutsfattandet.¹¹

Algoritmisk arbetsledning är särskilt utbredd inom plattformsarbete, men förekommer i allt större utsträckning även inom andra delar av arbetsmarknaden, såsom industri, kontorsarbete och professionella tjänsteföretag.¹² Inom plattformsarbete utgör algoritmisk arbetsledning en central del av hur

⁵ JO:s beslut 19 oktober 2023, dnr 7143–2022.

⁶ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021–771.

⁷ Niklas Selberg, "En agenda för framtidens arbetsrätt", *Dagens Arena*, 1 oktober 2020, avs. Arenaessä, <https://www.dagensarena.se/essa/en-agenda-framtidens-arbetsratt/>.

⁸ European Parliamentary Research Service (EPRS), *Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the future of work*, EPRS Study, PE 774.670 (2025), s. 1 f., https://www.europarl.europa.eu/RegData/etudes/STUD/2025/774670/EPRS_STU%282025%29774670_EN.pdf.

⁹ "Algoritmisk arbetsledning", Arbetsmiljöverket, 13 februari 2026, <https://www.av.se/halsa-och-sakerhet/digitalisering/algoritmisk-arbetsledning/>.

¹⁰ Jeremias Adams-Prassl, "Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'", *European Labour Law Journal*, vol. 13, nr 1 (2 februari 2022), s. 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4024374.

¹¹ EPRS, *Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the future of work*, s. 6.

¹² Adams-Prassl, "Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'", s. 5; Carin Håkansta, *Vad händer med arbetsmiljön när AI blir chef? Sammanställning av forskningsbaserad kunskap och slutsatser från en tvärvetenskaplig policykonferens* (Karolinska Institutet, rapport 2025), s. 9–10 och den refererade statistiken, <https://ki.se/media/271339/download>.

arbetet organiseras, eftersom funktioner såsom fördelning av arbetsuppgifter och matchning av uppdrag med arbetstagare inte hade varit möjliga i utan algoritmerna. För att sådana system ska fungera krävs kontinuerlig insamling och analys av data om arbetstagarnas aktiviteter, vilket innebär att också övervakning blir en integrerad del av arbetsledningen.¹³

Dessa parallella utvecklingar, å ena sidan den ökade användningen av digitala övervakningssystem i arbetslivet och å andra sidan framväxten av algoritmisk arbetsledning, ger upphov till fördjupade frågor och nya gränsdragningar om arbetstagares rätt till integritet och privatliv. Ger dagens rättsliga ramar ett tillräckligt och effektivt skydd för arbetstagares integritet?

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att analysera när algoritmisk övervakning och arbetsledning övergår till att utgöra ett otillåtet intrång i den personliga integriteten enligt gällande rättslig reglering. Genom att undersöka hur automatiserade system används för övervakning, kontroll och arbetsledning samt hur dessa bedöms enligt relevanta rättsliga normer, avser uppsatsen att klarlägga vilka gränser som gäller för tillåten övervakning och arbetsledning i ett digitaliserat arbetsliv.

För att uppnå syftet ställs följande frågeställning: *Vilka gränser uppställer gällande reglering i EU och Sverige mellan tillåten algoritmisk övervakning och arbetsledning å ena sidan och otillåtet intrång i den personliga integriteten å andra sidan?*

Därutöver diskuteras även frågan om det befintliga regelverket är tillräckligt, eller om den tekniska utvecklingen ger upphov till ett behov av ytterligare reglering för att säkerställa ett effektivt skydd för arbetstagares personliga integritet.

1.3 Metod och material

1.3.1 Metod

I uppsatsen används en rättsdogmatisk metod i kombination med en EU-rättslig metod, med särskilt fokus på skyddet för enskildas rättigheter. Valet av metod grundas i uppsatsens syfte och frågeställning, vilka förutsätter en systematisk genomgång och tolkning av de rättsregler som reglerar algoritmisk övervakning och arbetsledning i arbetslivet. Den rättsdogmatiska metoden används för att identifiera och analysera relevant rättsligt material samt för att klarlägga gällande rätt genom en genomgång av erkända rättskällor, såsom

¹³ “Platform work: Algorithmic management”, Eurofound, 30 maj 2025, <https://www.eurofound.europa.eu/en/publications/all/platform-work-algorithmic-management>.

lagstiftning, rättspraxis och förarbeten.¹⁴ Argumentationen förs de lege lata, vilket innebär att den inriktas på att beskriva och tolka gällande rätt. De rättsliga bedömningarna grundas i hur rättsreglerna är utformade och tillämpas enligt nuvarande lagstiftning. Den rättsliga analysen mynnar ut i en diskussion om hurvida det finns ett behov av ytterligare reglering, utan att innefatta överväganden om hur rätten bör förändras.¹⁵

Eftersom centrala delar av regleringen av algoritmisk övervakning och arbetsledning har sitt ursprung i EU-rätten utgör den EU-rättsliga metoden en naturlig och nödvändig del av redogörelsen. Metoden innefattar en tolkning av de rättsliga regelverk som gäller inom EU-rätten och tar sin utgångspunkt i Sveriges medlemskap i Europeiska unionen. Medlemskapet medför att principen om direktivkonform tolkning ska beaktas, vilket innebär att nationella bestämmelser ska tolkas i ljuset av EU-rättsliga regler och deras ändamål.¹⁶ Mot denna bakgrund beaktas EU-rättens rättskällehära, enligt vilken primär-rätten, såsom EU-fördragen och EU-stadgan, är överordnad sekundär-rätten, däribland förordningar och direktiv.¹⁷

Vidare utgår uppsatsen från ett rättighetsperspektiv, med utgångspunkt i de mänskliga rättigheterna och särskilt rätten till privatliv. Detta perspektiv möjliggör en bedömning av algoritmisk övervakning och arbetsledning där individens rättigheter står i centrum och bidrar till en fördjupad förståelse av hur det rättsliga ramverket är utformat för att skydda personlig integritet i arbetslivet.

Som ett komplement till de traditionella rättskällorna används rättsvetenskaplig litteratur i form av doktrin. Doktrin anses i regel inte utgöra en självständig rättskälla, utan har sin betydelse genom dem övertygande kraften i de argument som framförs. Samtidigt har doktrinen en viktig funktion genom att erbjuda en mer sammanhållen och lättillgänglig framställning av rättsläget än vad som ofta följer av lagtext, praxis och förarbeten var för sig.¹⁸ Detta framstår som särskilt värdefullt på ett område som befinner sig i ett tidigt skede av rättsutvecklingen, där regleringen fortfarande är under framväxt och praxis är begränsad. Därav finns det skäl att i större utsträckning beakta även icke bindande rättskällor, såsom doktrin och olika vägledande dokument, för att fylla ut och konkretisera rättsläget. I denna uppsats används därför doktrinen för att komplettera analysen av rättskällorna och för att synliggöra de olika

¹⁴ Jan Kleineman, "Rättsdogmatisk metod", i: Maria Nääv och Mauro Zamboni (red.) *Juridisk metodlära*, 3 uppl., (Studentlitteratur AB, 2025), s. 25.

¹⁵ Kleineman, "Rättsdogmatisk metod", s. 44.

¹⁶ Jörgen Hettne och Ida Otken Eriksson, *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*, 2 uppl. (Nordstedts Juridik, 2011), s. 188 f.

¹⁷ Hettne och Otken Eriksson, *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*, s. 40 ff.

¹⁸ Kleineman, "Rättsdogmatisk metod", s. 34 och s. 40 f.

uppfattningar och den pågående debatt som finns kring algoritmisk övervakning och arbetsledning i arbetslivet.

Vid framställningen har artificiell intelligens använts som ett stöd för språklig bearbetning och för att bolla idéer kring struktur och formuleringar. Användningen har uteslutande haft ett redaktionellt och stödjande syfte och samtliga rättsliga analyser, urval av material och slutsatser har gjorts självständigt av författaren.

1.3.2 Material

Det material som används i uppsatsen består huvudsakligen av EU-rättsliga rättskällor, europeiskt rättighetsskydd, svensk rätt samt rättsvetenskaplig litteratur. Urvalet av källor motiveras av att regleringen av algoritmisk övervakning och arbetsledning inte återfinns i ett enhetligt regelverk, utan är spridd över flera rättsliga nivåer som tillsammans formar det rättsliga ramverket.

På EU-rättslig nivå analyseras dataskyddsregleringen GDPR¹⁹, AI-förordningen²⁰ och plattformsdirektivet²¹, vilka utgör centrala rättsliga ramverk för regleringen av algoritmisk övervakning och arbetsledning i arbetslivet. Dessa regelverk studeras i syfte att klarlägga de rättsliga krav som ställs på behandling av personuppgifter, användning av artificiell intelligens och algoritmbaserad arbetsledning. Därutöver syftar redogörelsen även till att belysa hur dessa regelverk samspelar och i vilken mån de kompletterar eller överlappar varandra.

Vidare används rättighetsreglering, i form av EU-stadgan²², Europakonventionen (EKMR)²³ och Europeiska sociala stadgan²⁴. Dessa analyseras i syfte att fastställa innebörden av rätten till privatliv och personlig integritet samt att identifiera under vilka förutsättningar denna rätt kan begränsas genom arbetsgivarens kontroll- och övervakningsåtgärder. I detta sammanhang ges särskild vikt åt proportionalitetsprincipen och de krav som följer av

¹⁹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

²⁰ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

²¹ Europaparlamentets och rådets förordning (EU) 2024/2831 av den 23 oktober 2024 om förbättrade arbetsvillkor för plattformarbete.

²² Europeiska unionens stadga om de grundläggande rättigheterna, antagen i Nice den 7 december 2000 och rättsligt bindande sedan Lissabonfördragets ikraftträdande den 1 december 2009.

²³ Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, antagen i Rom den 4 november 1950, ETS nr 5.

²⁴ Europarådets sociala stadga (reviderad), antagen i Strasbourg den 3 maj 1996, ETS nr 163.

rättighetsskyddet. Relevant praxis från Europadomstolen och EU-domstolen används för att konkretisera och tolka dessa rättigheter, i den mån sådan praxis bidrar till att klargöra integritetsskyddets räckvidd i arbetslivet.

Avseende den svenska rätten beaktas i första hand arbetsledningsrätten i syfte att klargöra arbetsgivarens kontroll- och ledningsbefogenheter i anställningsförhållanden. I anslutning till detta behandlas även EU-rättens ställning i svensk rätt samt hur unionsrätten påverkar och begränsar det nationella utrymmet för arbetsledning. Därutöver beaktas kompletterande reglering, såsom dataskyddslagen och kamerabevakningslagen, i den mån dessa är relevanta för övervakningsåtgärder i arbetslivet. När det gäller nyare regelverk som ännu inte har implementerats i svensk rätt, används förarbeten och andra vägledande dokument för att belysa lagstiftarens intentioner och hur reglerna är avsedda att tolkas i en framtida rättstillämpning.²⁵

Som komplement till de ovan redovisade traditionella rättskällorna har även rättsvetenskaplig litteratur beaktats och redovisats. De verk som återkommande används i framställningen och som haft särskild betydelse för tolkningen av såväl nationell som EU-rättslig reglering är bland annat Erik Grahns och Susanna Kjällströms arbete, David Frydinger m.fl.s framställning av GDPR samt Sören Ömans kommentarer. Dessa ger en samlad och systematiserad överblick av det svenska rättsläget, särskilt i fråga om arbetsgivarens kontrollåtgärder och arbetstagares integritetsskydd, och har därför utgjort en central utgångspunkt i analysen ur ett svenskt arbetsrättsligt perspektiv.

Därutöver har internationell forskning, främst av Jeremias Adams-Prassl samt en studie från European Parliamentary Research Service (EPRS), beaktats. Dessa källor belyser algoritmisk arbetsledning, plattformsarbete och digital kontroll ur ett EU-rättsligt och komparativt perspektiv, vilket bidrar till en fördjupad förståelse av det europeiska rättsläget och möjliggör en placering av den nationella regleringen i ett bredare sammanhang.

Slutligen används material från Integritetsskyddsmyndigheten samt uttalanden och rapporter från fackliga organisationer för att belysa hur övervakning och kontroll i arbetslivet uppmärksammas i svensk rättstillämpning och samhällsdebatt. Detta material används främst illustrativt för att sätta den rättsliga analysen i ett praktiskt sammanhang.

1.4 Avgränsningar

Uppsatsen fokuserar på algoritmisk övervakning och arbetsledning i arbetslivet, det vill säga övervakning som sker genom automatiserade system och

²⁵ Se SOU 2026:3 *Genomförande av plattformsdirektivet*, Arbetsmarknadsdepartementet; SOU 2025:101 *Anpassningar till AI-förordningen: Säker användning, effektiv kontroll och stöd för innovation*, Finansdepartementet.

algoritmisk analys av arbetstagares beteenden, prestationer eller arbetsutförande. Uppsatsen tar sikte på arbetsledning som styrs av AI och avgränsas därmed till AI-baserad arbetsledning, vilket innebär att former av arbetsledning som inte bygger på AI faller utanför framställningen. Även andra former av övervakning, såsom rent manuell kontroll eller traditionella kontrollåtgärder utan algoritmiska inslag, behandlas endast i den mån det är nödvändigt för att sätta den algoritmiska övervakningen i sitt sammanhang. Uppsatsen behandlar inte i någon större utsträckning frågor om sanktioner, skadestånd eller rättsmedel, utan fokuserar på gränsdragningen för tillåten övervakning. Mot denna bakgrund behandlas exempelvis inte artikel 13 EKMR i anslutning till artikel 8 EKMR, och inte heller de nationella bestämmelserna om påföljder.

Vidare avgränsas uppsatsen från en närmare analys av arbetsmiljörättsliga och diskrimineringsrättsliga frågor. Även om algoritmisk övervakning och arbetsledning kan ge upphov till arbetsmiljöproblem eller risker för diskriminering, ligger sådana frågor utanför uppsatsens huvudsakliga fokus. Uppsatsen behandlar i stället algoritmisk övervakning och arbetsledning utifrån ett integritetsrättsligt perspektiv, med syfte att analysera när övervakning övergår till att utgöra ett otillåtet intrång i arbetstagares personliga integritet enligt gällande rätt.

1.5 Forskningsläge

Övervakning i arbetslivet har länge behandlats i rättsvetenskaplig litteratur, med fokus på arbetsgivarens kontrollbefogenheter och arbetstagares rätt till personlig integritet. Den tidigare forskningen har främst analyserat traditionella kontrollåtgärder, såsom kroppsvisioneringar, TV-övervakning, kontroll av e-post, hälsoundersökningar, drogtestar och personlighetstester, samt de intresseavvägningar som dessa ger upphov till. Ett exempel är Annamaria Westergårds avhandling *Integritetsfrågor i arbetslivet* från början av 2000-talet, där dessa frågor analyseras utifrån de tekniska förutsättningar och kontrollformer som var aktuella vid den tidpunkten. Det bör samtidigt framhållas att analysen redan då tog sin utgångspunkt i en utveckling där de tekniska möjligheterna att övervaka arbetstagare successivt ökade.

Digitaliseringens genomslag i arbetslivet har under senare år medfört ett ökat fokus på digital övervakning och behandling av personuppgifter. Här kan särskilt nämnas Erik Grahn och Susanna Kjällström, som i *Anställdas integritetsskydd och dataskyddsförordningen* behandlar integritetsskyddet i ljuset av GDPR. Samtidigt har utvecklingen fortsatt i snabb takt sedan denna framställning publicerades 2017, genom såväl tekniska framsteg som tillkomsten av nya EU-rättsliga regelverk. Den tekniska utvecklingen har möjliggjort nya och mer avancerade former av övervakning i arbetslivet, vilket aktualiserar ytterligare frågor om integritet och kontroll som inte behandlats i denna framställning, Regelverk såsom AI-förordningen och plattformsdirektivet, som i

dag har betydelse för bedömningen av sådana övervakningsåtgärder, har därför inte analyserats i detta sammanhang.

Med detta i beaktning kan två parallella utvecklingslinjer identifieras. Dels finns ett etablerat forskningsfält rörande övervakning och integritet i arbetslivet, dels en snabbt framväxande reglering kopplad till artificiell intelligens och algoritmisk arbetsledning. Den senare utvecklingen har i huvudsak behandlats i internationell litteratur, exempelvis av Jeremias Adams-Prassl samt i en studie från EPRS, där frågor om algoritmisk styrning och digital kontroll analyseras ur ett EU-rättsligt perspektiv. I dessa framställningar behandlas bland annat hur algoritmer används för att organisera, övervaka och utvärdera arbete, samt vilka rättsliga och strukturella utmaningar detta medför i förhållande till befintliga regelverk. Dessa redogörelser ger värdefull vägledning, men är i stor utsträckning begränsade till EU-nivån.

För att uppnå en mer fullständig förståelse av rättsläget krävs även en analys av hur dessa EU-rättsliga regelverk samspelar med nationell rätt, särskilt arbetsledningsrätten och dess begränsningar. Detta innebär att även om det finns en omfattande forskning om integritet i arbetslivet, aktualiserar den tekniska utvecklingen fortlöpande nya frågor och förändrade förutsättningar som påverkar den rättsliga bedömningen. Detta innebär att tidigare analyser inte fullt ut fångar de utmaningar som dagens mer avancerade former av övervakning ger upphov till. Samtidigt innebär detta att det finns ett tydligt utrymme för fortsatt forskning på området.

Mot denna bakgrund syftar uppsatsen till att bidra till forskningen genom att analysera algoritmisk övervakning och arbetsledning som ett självständigt rättsligt problem, där både etablerade integritetsperspektiv och nyare EU-rättsliga regelverk beaktas i ett sammanhang. Genom att föra samman dessa parallella utvecklingar och perspektiv erbjuder uppsatsen en mer heltäckande analys av rättsläget och adresserar därmed en befintlig lucka i forskningen.

1.6 Disposition

Uppsatsen är uppdelad i fem kapitel och inleds med en introduktion till ämnet i kapitel 1. Här redogörs för bakgrunden till uppsatsen, problemområdet och dess relevans. Vidare presenteras uppsatsens syfte och frågeställning samt de avgränsningar och metodval som ligger till grund för uppsatsen.

I kapitel 2 redogörs vidare för det grundläggande rättighetsskyddet. Där analyseras skyddet för privatliv och personuppgifter enligt Europakonventionen, med särskilt fokus på artikel 8 EKMR, samt den Europeiska sociala stadgan. Därefter behandlas motsvarande skydd enligt EU-stadgan och rättighetsskyddet i regeringsformen.

I kapitel 3 behandlas den EU-rättsliga lagstiftning som är relevant för algoritmisk övervakning och arbetsledning i arbetslivet. Fokus ligger på

dataskyddsregleringen GDPR och dess regler om behandling av personuppgifter samt på AI-förordningen och dess betydelse för användningen av artificiell intelligens i arbetslivet. Plattformdirektivet berörs därefter med avseende på dess bestämmelser om algoritmiska system och automatiserad arbetsledning.

I kapitel 4 behandlas den svenska rättsliga reglering som är av betydelse för algoritmisk övervakning och arbetsledning i arbetslivet. Kapitlet innehåller en genomgång av arbetsledningsrätten och dess begränsningar. I detta sammanhang behandlas även den svenska implementeringen av EU:s rättsakter samt deras betydelse för den nationella regleringen av algoritmiska system och automatiserad arbetsledning.

Avslutningsvis, i kapitel 5, förs en sammanfattande diskussion där de rättsliga ramar som behandlats i uppsatsen analyseras. Kapitlet avslutas med uppsatsens slutsatser, där frågeställningen besvaras och centrala iakttagelser sammanfattas.

2 Integritet som grundläggande rättighet

2.1 Europakonventionen om rätten till privatliv

2.1.1 Tillämpningsområde

Rätten till skydd för privatlivet betraktas som en grundläggande rättighet och skyddas i flera internationella rättsakter, däribland FN:s allmänna förklaring om mänskliga rättigheter, EKMR och EU-stadgan. Av dessa intar artikel 8 EKMR en särskilt central och viktig ställning, vilken fastslår rätten till respekt för privat- och familjeliv, hem och korrespondens.²⁶ Vad som närmare ingår i dessa begrepp är dock svårt att avgränsa generellt och har i stor utsträckning utvecklats genom rättspraxis.²⁷ Där har det klargjorts att skyddet omfattar flera aspekter av en persons identitet, både fysiska och sociala, såsom könsidentitet, namn, sexuell läggning och hälsa. Det inbegriper även relationer till familj samt olika former av kommunikation, exempelvis telefonsamtal och e-post.²⁸ Som utgångspunkt åligger det de fördragsslutande staterna att garantera de fri- och rättigheter som anges i konventionen för alla som befinner sig under deras jurisdiktion.²⁹

Vid prövning av rättigheten är ett första steg att bedöma om ett ingrepp har skett, det vill säga om den aktuella åtgärden omfattas av rättighetsskyddet.³⁰ I anslutning till detta är det av särskilt intresse att se hur Europadomstolen har bedömt frågan om i vilken utsträckning artikel 8 kan åberopas i arbetslivet. Frågan prövades första gången 1992 i ett mål om husrannsakan på ett advokatkontor, där domstolen uttalade att begreppet privatliv inte enbart avser den strikt privata sfären utan även kan omfatta delar av en individs yrkesliv. Domstolen framhöll att det inte alltid går att dra en tydlig gräns mellan aktiviteter i arbetslivet och andra delar av en persons liv. Det betonades även att rätten till privatliv omfattar möjligheten att etablera och utveckla relationer med andra människor, något som ofta sker på arbetsplatsen. I domskälen framhölls även att tidigare praxis visar att telefonavlyssning kan utgöra ett intrång i privatlivet, även när den omfattar både privata och affärsmässiga samtal. Vidare slog Europadomstolen fast att även en persons kontor kan omfattas av

²⁶ Kent Källström, Jonas Malmberg och Caroline Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten* (Iustus, 2025), s. 299.

²⁷ Hans Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna* (Nordstedts juridik, 2023), s. 441.

²⁸ Se *Klass and Others v. Germany*, (5029/71) dom 6 september 1978, p. 41; *Weber and Saravia v. Germany* (54934/00) dom 29 juli 2006, p. 77; *S. and Marper v. the United Kingdom* (30562/04 och 30566/04) dom 5 december 2008, p. 66.

²⁹ Artikel 1 EKMR.

³⁰ Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, s. 442.

begreppet hem, vilket innebär att rekvisiten privatliv och hem i vissa fall även inkluderar yrkesmässiga verksamheter och lokaler.³¹

Detta synsätt har senare bekräftats i Europadomstolens praxis.³² Domstolen har även slagit fast att artikel 8 EKMR skyddar rätten att etablera och utveckla yrkesmässiga och affärsmässiga relationer. Mot denna bakgrund kan även ett avsked prövas i förhållande till bestämmelsen.³³ Det har i senare praxis klargjorts att artikel 8 EKMR även innebär en positiv förpliktelse för konventionsstaterna. Detta innebär att staten ska säkerställa att bestämmelsen respekteras även i relationer mellan enskilda. Inom arbetsrätten medför detta att även privata arbetsgivares agerande kan omfattas av skyddet.³⁴

Skyddet enligt artikel 8 EKMR är emellertid inte absolut. Om ett ingrepp konstateras enligt första stycket ska det prövas mot artikelns andra stycke, där tre krav uppställs: att åtgärden har stöd i lag, tillgodoser ett legitimt syfte och är nödvändig i ett demokratiskt samhälle. Om dessa krav inte är uppfyllda är ingreppet konventionsstridigt.³⁵

Det första kravet, laglighet, innebär att intrånget måste ha stöd i nationell rätt och att den aktuella bestämmelsen uppfyller vissa kvalitetskrav. Den ska vara tillgänglig, förutsebar och tillräckligt preciserad.³⁶ I fråga om övervakning i arbetslivet innebär detta att varje åtgärd måste ha ett tydligt rättsligt stöd och ske i enlighet med fastställda lagstadgade villkor och förfaranden.³⁷ Det andra kravet innebär att intrånget måste ske för något av de ändamål som anges i artikel 8.2 EKMR, såsom statens säkerhet, allmän säkerhet, ekonomiskt välstånd, förebyggande av oordning eller brott samt skydd för hälsa, moral eller andra personers fri- och rättigheter. Av praxis framgår att Europadomstolen sällan ifrågasätter de ändamål som staten åberopar.³⁸

Det tredje och sista kravet för att ett ingrepp ska vara tillåtet är att det måste vara nödvändigt i ett demokratiskt samhälle. Det är ofta i förhållande till detta krav som de flesta osäkerheterna finns.³⁹ För att kravet ska vara uppfyllt har Europadomstolen uttalat att åtgärden måste svara mot ett trängande samhällsligt behov och vara proportionerlig i förhållande till det legitima syfte som

³¹ Niemietz v. Germany (13710/88) dom 16 december 1992, p. 27–33.

³² Se t. ex. Lindstrand Partners Advokatbyrå AB v. Sweden (18700/09) dom 20 december 2016.

³³ Oleksandr Volkov v. Ukraine (21722/11) dom 27 maj 2013, p. 165–167.

³⁴ Se Bărbulescu v. Romania (61496/08) dom 5 september 2017, p. 111.

³⁵ Artikel 8 EKMR; Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, s. 442 f.

³⁶ Se exempelvis Sunday Times v. the United Kingdom (6538/74) dom 26 april 1979, p. 49; Foxley v. the United Kingdom (33274/96) dom 20 juni 2000.

³⁷ Klass and Others v. Germany, p. 43.

³⁸ Klass and Others v. Germany, p. 46; Leander v. Sweden (9248/81) dom 26 mars 1987, p. 49.

³⁹ Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, s. 443.

eftersträvas. Domstolen har i detta sammanhang framhållit att undantag från konventionens rättigheter ska tolkas och tillämpas restriktivt.⁴⁰

2.1.2 Gränsdragningen mellan tillåten och otillåten övervakning i Europadomstolens praxis

Nedan uppmärksammas ett antal rättsfall från Europadomstolen för att belysa hur bedömningen i praktiken görs när det gäller övervakningsåtgärder. Genom dessa avgöranden illustreras när en sådan åtgärd anses vara tillåten och när den bedöms vara så ingripande att rätten till privatliv enligt artikel 8 EKMR anses ha kränkts.

2.1.2.1 Otillåtna övervakningsåtgärder

Ett av de tidigaste fallen om övervakning i arbetslivet rörde avlyssning av kommunikation på arbetsplatsen. I *Halford v. the United Kingdom* gällde målet en kvinnlig polis som, efter att ha nekats befordran under flera år, gjorde gällande att hennes telefonsamtal i tjänsten och i hemmet hade avlyssnats i syfte att användas mot henne i en diskrimineringsprocess.⁴¹ Europadomstolen fann att avlyssningen av tjänstetelefonerna, som ansågs omfattas av hennes privatliv, utgjorde ett ingrepp enligt artikel 8 EKMR och avfärdade därav argumentet att arbetsgivaren fritt kunde kontrollera kommunikation på arbetsplatsen. Domstolen fäste särskild vikt vid att någon information om avlyssningen inte hade lämnats, vilket påverkade hennes berättigade förväntan på integritet.⁴² Vidare ansågs det sannolikt att åtgärden syftade till att samla bevis som kunde användas mot henne. Eftersom avlyssningen saknade tillräckligt stöd i nationell lag ansågs den inte vara i enlighet med lag och innebar därmed en kränkning av artikel 8.⁴³ Någon kränkning avseende telefonsamtal från hemmet konstaterades däremot inte, då det inte kunde styrkas att dessa faktiskt hade avlyssnats.⁴⁴

Ett liknande mål med samma utgång är *Copland v. the United Kingdom*. Även här rörde det en statligt anställd, denna gång vid ett universitet, vars telefon-, e-post- och internetanvändning övervakades på initiativ av den biträdande rektorn. Staten medgav att kontrollerna hade genomförts och anförde att syftet var att utreda i vilken utsträckning arbetstagaren använde arbetsgivarens resurser för privata ändamål.⁴⁵ Europadomstolen konstaterade att övervakning av telefonsamtal från arbetsplatsen omfattas av skyddet för privatliv och korrespondens enligt artikel 8 EKMR och att det som en logisk följd även gäller e-post och internetanvändning i arbetet. Vidare framhölls att uppgifter om telefonsamtal, såsom datum, längd och uppringda nummer, samt lagring

⁴⁰ *Silver and Others v. the United Kingdom* (5947/72, 6205/73, 7052/75, 7061/74, 71077/75, 7113/75, 7136/75) dom 25 mars 1983, p. 97.

⁴¹ *Halford v. the United Kingdom* (20605/92) dom 25 juni 1997, p. 9–11 och p. 16–17.

⁴² *Halford v. the United Kingdom*, p. 44–45.

⁴³ *Halford v. the United Kingdom*, p. 48 och p. 51.

⁴⁴ *Halford v. the United Kingdom*, p. 50–60.

⁴⁵ *Copland v. the United Kingdom* (62617/00) dom 3 april 2007, p. 7–16 och p. 34–35.

av personuppgifter faller inom bestämmelsens tillämpningsområde och kan utgöra ett intrång oberoende av hur de samlats in eller använts. Eftersom arbetstagaren inte hade informerats om övervakningen ansågs hon dessutom ha en berättigad förväntan på integritet, varför insamlingen av uppgifter utan hennes vetskap utgjorde ett ingrepp.⁴⁶ Domstolen lämnade frågan öppen om sådan övervakning i vissa fall kan vara nödvändig i ett demokratiskt samhälle för att uppnå ett legitimt syfte, men konstaterade att ingreppet i detta fall inte var i enlighet med lag på grund av avsaknad av nationell reglering.⁴⁷

Ett annat vägledande rättsfall i hur bedömningen görs avseende övervakning i förhållande till integritet är *Bărbulescu v. Romania*. Fallet gällde en arbetstagare som använt ett av arbetsgivaren tillhandahållet Yahoo Messenger-konto i tjänsten, vilket senare övervakades i realtid av den privata arbetsgivaren. Övervakningen resulterade i att privata meddelanden med bland annat hans partner och bror samlades in och användes som grund för uppsägning. Detta skedde trots att de interna reglerna visserligen förbjöd privat användning, men inte uttryckligen angav att kommunikationen kunde komma att övervakas eller granskas i innehåll.⁴⁸ Europadomstolen konstaterade, med hänvisning till sin tidigare praxis, att kommunikation på arbetsplatsen omfattas av tillämpningsområdet för artikel 8 EKMR.⁴⁹ Vidare framhölls att de nationella domstolarna inte hade säkerställt ett tillräckligt skydd för hans rätt till privatliv och korrespondens, eftersom de bland annat inte hade prövat om han informerats om övervakningen, dess omfattning eller om mindre ingripande åtgärder hade kunnat användas. Därför förelåg en kränkning av konventionens artikel 8.⁵⁰

Genom det ovan redovisade rättsfallet har Europadomstolen utvecklat sex kriterier som särskilt ska beaktas vid avvägningen mellan arbetsgivarens och arbetstagarens intressen. För det första om arbetstagaren har informerats om möjlig övervakning. För det andra hur omfattande övervakningen varit och graden av intrång i privatlivet, särskilt om innehållet i kommunikationen har granskats, under hur lång tid samt vilka som haft tillgång till uppgifterna. För det tredje om arbetsgivaren har anfört legitima skäl för åtgärden. För det fjärde om mindre ingripande alternativ har varit möjliga. För det femte vilka konsekvenser övervakningen fått för arbetstagaren och hur resultaten använts. Slutligen om arbetstagaren haft tillgång till tillräckliga skyddsåtgärder, särskilt mot att arbetsgivaren får tillgång till innehållet i kommunikationen utan föregående information.⁵¹

⁴⁶ *Copland v. the United Kingdom*, p. 41–44.

⁴⁷ *Copland v. the United Kingdom*, p. 48.

⁴⁸ *Bărbulescu v. Romania*, p. 11–23.

⁴⁹ *Bărbulescu v. Romania*, p. 81.

⁵⁰ *Bărbulescu v. Romania*, p. 140–141.

⁵¹ *Bărbulescu v. Romania*, p. 121.

I litteraturen har det framhållits att *Bărbulescu v. Romania* kan innebära att högre krav framöver ställs på Arbetsdomstolens intresseavvägningar i mål om integritetskänsliga åtgärder. Det har även påpekats att det svenska rättsskyddet i vissa fall kan framstå som otillräckligt, eftersom arbetstagare i praktiken kan behöva riskera sin anställning för att få sådana åtgärder prövade.⁵²

2.1.2.2 *Tillåtna övervakningsåtgärder*

Utöver de ovan redovisade fallen, där Europadomstolen har funnit överträdelser av artikel 8, finns det i senare praxis även avgöranden där domstolen har kommit fram till att någon överträdelse inte föreligger.

Ett första exempel är *Libert v. France*, där en anställd vid det franska järnvägsbolaget avskedades efter att innehållet på hans arbetsdator granskats och visat att han lagrat pornografiskt material samt förfalskade intyg. Sökanden gjorde gällande att arbetsgivaren hade öppnat personliga filer på datorn i hans frånvaro.⁵³ Inledningsvis konstaterade domstolen att artikel 8 var tillämplig, eftersom även icke-yrkesmässiga uppgifter som lagras på en arbetsdator kan omfattas av skyddet för privatliv.⁵⁴ Domstolen fann vidare att det förelåg ett ingrepp i artikel 8 EKMR, eftersom arbetsgivaren hade öppnat filer på arbetstagarens dator utan hans vetskap och att arbetsgivaren i detta fall skulle betraktas som en offentlig aktör.⁵⁵

Därefter prövade Europadomstolen om ingreppet var i enlighet med lag och fann att nationell rätt innehöll tillräckliga regler och garantier, bland annat genom att filer som inte tydligt markerats som privata presumeras vara arbetsrelaterade och därmed kunde öppnas utan arbetstagarens närvaro.⁵⁶ Vid bedömningen av legitimt syfte godtog domstolen att åtgärden syftade till att skydda arbetsgivarens intressen och säkerställa att arbetsredskap användes i enlighet med gällande regler. Domstolen framhöll även att arbetsgivaren har ett legitimt intresse av att upprätthålla en väl fungerande verksamhet genom att kontrollera att arbetstagare fullgör sina arbetsuppgifter korrekt och med tillräcklig noggrannhet.⁵⁷ I proportionalitetsbedömningen framhölls att nationell rätt innehöll skydd för privatlivet och att de nationella domstolarna gjort en noggrann avvägning, där det särskilt beaktades att filerna inte var tydligt markerade som privata samt att arbetstagaren i stor omfattning använt arbetsdatorn för privata ändamål. Mot denna bakgrund ansågs åtgärden proportionerlig och staten inte ha överskridit sitt bedömningsutrymme, varför någon överträdelse av artikel 8 inte förelåg.⁵⁸

⁵² Erik Grahn och Susanna Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen* (Wolters Kluwer, 2017), s. 23.

⁵³ *Libert v. France* (588/13) dom 22 februari 2018, p. 7–12.

⁵⁴ *Libert v. France*, p. 23–25.

⁵⁵ *Libert v. France*, p. 37–42.

⁵⁶ *Libert v. France*, p. 44.

⁵⁷ *Libert v. France*, p. 45–46; se även *Bărbulescu v. Romania*, p. 127.

⁵⁸ *Libert v. France*, p. 48–53.

Ett andra exempel är *López Ribalda and Others v. Spain*, som rörde dold kameraövervakning av anställda som senare sades upp. Sökandena gjorde gällande att övervakningen och domstolarnas användning av materialet var felaktig samt att vissa förlikningar hade ingåtts under påtryckning.⁵⁹ Europadomstolen konstaterade inledningsvis att artikel 8 EKMR var tillämplig och att målet rörde statens positiva förpliktelser.⁶⁰ Vid den efterföljande intresseavvägningen utgick domstolen från de sex kriterier som utvecklats i *Bărbulescu v. Romania*. Domstolen betonade i detta sammanhang att dessa kriterier ska tillämpas med hänsyn till arbetslivets särskilda förhållanden och den tekniska utvecklingen, som möjliggör allt mer ingripande former av övervakning.⁶¹

Inledningsvis framhöll domstolen att det fanns en tydlig rättslig ram som syftade till att skydda arbetstagares privatliv i den aktuella situationen.⁶² Vidare bedömdes intrånget i privatlivet som begränsat, samtidigt som arbetsgivaren ansågs ha starka skäl att införa övervakningen mot bakgrund av konkreta misstankar om allvarliga oegentligheter. Domstolen beaktade att spansk rätt innehöll tillräckliga skyddsmekanismer och att de klagande inte utnyttjat tillgängliga rättsmedel, varför staten inte ansågs ha överskridit sitt bedömningsutrymme. Till skillnad från det rumänska fallet bedömdes därför den dolda kameraövervakningen vara proportionerlig och berättigad, trots att arbetstagarna inte informerats i förväg, och någon överträdelse av artikel 8 EKMR förelåg således inte.⁶³

Ett avslutande exempel rör ett mer nyligen avgjort fall om GPS-spårning, vilket illustrerar hur domstolen bedömer användningen av ny teknik i arbetslivet. Fallet rörde en medicinsk representant som i sitt arbete använde en tjänstebil utrustad med GPS, där arbetsgivaren tydligt hade informerat om systemet och dess syfte. Systemet användes bland annat för att skilja mellan tjänsteresor och privata resor samt för att kontrollera rapporterade körsträckor.⁶⁴ Efter att tekniska avvikelser uppmärksammats installerades en andra GPS-enhet i klagandes fordon, vilket möjliggjorde en jämförelse som visade på brister i den tidigare rapporteringen och misstänkt manipulation av systemet.⁶⁵ Mot denna bakgrund inleddes ett disciplinärt förfarande som ledde till hans uppsägning. Klaganden gjorde gällande att behandlingen av GPS-uppgifter och användningen av dessa som grund för uppsägningen utgjorde ett

⁵⁹ *López Ribalda and Others v. Spain* (1874/13; 8567/13) dom 17 oktober 2019, p. 10–18.

⁶⁰ *López Ribalda and Others v. Spain*, p. 92–95 och p. 109–110.

⁶¹ *López Ribalda and Others v. Spain*, p. 115–116.

⁶² *López Ribalda and Others v. Spain*, p. 119–120.

⁶³ *López Ribalda and Others v. Spain*, p. 126 och p. 137.

⁶⁴ *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, (26968/16) dom 13 december 2022, p. 6–8 och p. 11–13.

⁶⁵ *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, p. 17–21 och p. 26.

intrång i hans rätt till privatliv enligt artikel 8 EKMR, särskilt eftersom bevisningen enligt honom hade inhämtats i strid med gällande rätt.⁶⁶

Europadomstolen fann att någon överträdelse av artikel 8 EKMR inte förelåg, då de nationella myndigheterna ansågs ha uppfyllt sin positiva förpliktelse att skydda klagandens privatliv.⁶⁷ Domstolen konstaterade att artikel 8 var tillämplig eftersom geolokaliseringsdata utgjorde personuppgifter och möjliggjorde en kontinuerlig kartläggning av arbetstagarens rörelser, vilket innebar ett ingrepp i privatlivet.⁶⁸ I likhet med tidigare praxis tog domstolen sin utgångspunkt i de sex kriterier som utvecklats för att bedöma intresseavvägningen.⁶⁹ Domstolen fäste särskild vikt vid att klaganden hade informerats om GPS-systemet och dess syfte, vilket han också bekräftat genom att underteckna ett dokument där det framgick att körsträckor kunde kontrolleras och ligga till grund för disciplinära åtgärder. Det beaktades även att klaganden inte hade överklagat dataskyddsmyndighetens beslut om systemets laglighet.⁷⁰ Slutligen framhöll Europadomstolen att de nationella domstolarna gjort en noggrann avvägning mellan klagandens rätt till privatliv och arbetsgivarens intresse av att säkerställa verksamhetens funktion och kontrollera sina kostnader, och att intrånget därmed hölls inom vad som var nödvändigt.⁷¹

2.2 Den Europeiska sociala stadgan

2.2.1 Funktion och tillämpningsområde

Den Europeiska sociala stadgan, som antogs 1961 och reviderades 1996, är ett instrument inom Europarådet som syftar till att skydda ekonomiska och sociala rättigheter. Till skillnad från Europakonventionen, som främst omfattar medborgerliga och politiska rättigheter, fokuserar den sociala stadgan på frågor kopplade till arbetsliv, social trygghet och hälsa. Den Europeiska stadgan anses innehålla de mest långtgående internationella åtagandena när det gäller arbetsrättsliga skyldigheter för stater.⁷²

Samtidigt har medlemsstaterna en viss flexibilitet i sina åtaganden, eftersom de kan välja att binda sig till vissa delar av stadgan. Det krävs dock att ett minimikrav av artiklar och kärnrättigheter accepteras. Sverige har ratificerat den reviderade stadgan och åtagit sig en stor del av dess bestämmelser, även

⁶⁶ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 90.

⁶⁷ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 124–125.

⁶⁸ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 95–97.

⁶⁹ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 109.

⁷⁰ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 113 och p. 116.

⁷¹ Florindo de Almeida Vasconcelos Gramaxo v. Portugal, p. 120 och p. 124.

⁷² Birgitta Nyström, *Introduktion till den europeiska arbetsrätten* (Nordstedts Juridik, 2024), s. 18 och s. 32.

om vissa delar inte har accepterats. Dessa omfattar exempelvis lön för helgdagar och ökad ersättning för övertid.⁷³

För att säkerställa efterlevnaden av dessa åtaganden övervakas regelverket av Europeiska kommittén för sociala rättigheter, som består av 15 oberoende experter. Kontrollen sker dels genom regelbunden rapportering från medlemsstaterna, dels genom ett kollektivt klagomålsförfarande. Kommittén granskar i detta arbete hur staterna uppfyller sina åtaganden och avger bedömningar samt, vid behov, kritik. Det kollektiva klagomålsförfarandet innebär att vissa organisationer, såsom fackförbund och arbetsgivarorganisationer, kan rikta klagomål mot en stat för bristande efterlevnad av stadgan. Enskilda individer har däremot inte någon egen klagorätt, vilket innebär att förfarandet fungerar som ett övervakningsinstrument på kollektiv nivå.⁷⁴

2.2.2 Centrala rättigheter kopplade till arbetslivet

I den reviderade Europeiska sociala stadgan finns flera bestämmelser av särskild betydelse för arbetslivet, såsom rätten till arbete, skälig lön, föreningsrätt, rätt till förhandlingar och stridsåtgärder, skydd för barn och ungdomar samt skydd vid uppsägning.⁷⁵ Flera av dessa bestämmelser saknar dock direkt relevans för frågan om algoritmisk övervakning och arbetsledning i arbetslivet och behandlas därför inte närmare i denna framställning. I stället är det framför allt artikel 2 och 26 som kan vara av särskilt intresse och kommer därför att analyseras närmare.

Artikel 2 reglerar rätten till rättvisa arbetsvillkor och innehåller flera konkreta krav på hur arbete ska organiseras. Den omfattar bland annat en skyldighet för staterna att verka för en rimlig begränsning av arbetstiden, att säkerställa rätt till betald semester samt att tillförsäkra arbetstagare vila genom exempelvis veckovila och helgdagar. Vidare framhålls att särskilda risker i arbetet, såsom arbete i farliga eller hälsovådliga miljöer, i första hand ska förebyggas. Om sådana risker inte helt kan undanröjas ska arbetstagare i stället kompenseras, exempelvis genom kortare arbetstid eller längre ledighet.⁷⁶

Artikel 26 i den Europeiska sociala stadgan behandlar rätten till värdighet i arbetet och ålägger staterna att vidta åtgärder för att skydda arbetstagare mot kränkande beteenden. Bestämmelsen omfattar bland annat sexuella trakasserier och andra former av ovärdigt bemötande, såsom klandervärt, skadligt eller aggressivt beteende som kan kränka arbetstagarens värdighet. Staterna ska genom lämpliga åtgärder, såsom information, förebyggande insatser och skyddsmekanismer, säkerställa att sådana beteenden motverkas och att arbetstagare får stöd om de utsätts. Det krävs dock inte att särskild lagstiftning

⁷³ Nyström, *Introduktion till den europeiska arbetsrätten* (Nordstedts Juridik, 2024), s. 32 f.

⁷⁴ Nyström, *Introduktion till den europeiska arbetsrätten*, s. 18 och s. 33 f.

⁷⁵ Se artiklarna 1, 4–7 och 24 i Europeiska sociala stadgan.

⁷⁶ Se artikel 2 i Europeiska sociala stadgan.

införs. Bestämmelsen tar därmed sikte på mellanmännsliga beteenden i arbetslivet, där sexuella trakasserier och mobbning utgör centrala exempel.⁷⁷

Mot bakgrund av det ovan anförda kan det konstateras att ingen av de aktuella bestämmelserna direkt tar sikte på arbetsgivares övervakning eller arbetstagares personliga integritet.

2.3 EU-stadgan

2.3.1 Allmänt om stadgan

EU-stadgan är en central rättskälla vid bedömningen av om åtgärder, såsom algoritmisk övervakning och arbetsledning, utgör ett otillåtet intrång i den personliga integriteten. EU-stadgan antogs år 2000 men blev rättsligt bindande först 2009 i och med Lissabonfördragets ikraftträdande. Som en del av EU:s primärrätt kan dess bestämmelser, under vissa förutsättningar som utvecklats i EU-domstolens praxis, ges både direkt och horisontell effekt. Stadgan innehåller ett brett spektrum av rättigheter, varav flera har tydlig koppling till arbetslivet.⁷⁸

EU-stadgan är bindande för medlemsstaterna när de tillämpar unionsrätten och riktar sig, med beaktande av subsidiaritetsprincipen, såväl till unionens institutioner, organ och byråer som till medlemsstaterna i dessa situationer. Detta innebär att medlemsstaterna är skyldiga att respektera de rättigheter som stadgan garanterar, iakttä dess principer och främja deras tillämpning inom ramen för sina befogenheter.⁷⁹

2.3.2 Materiellt innehåll och begränsningar

I detta sammanhang är särskilt artiklarna 7 och 8 i EU-stadgan av betydelse. Artikel 7 skyddar rätten till respekt för privat- och familjeliv, vilket även omfattar den enskildes bostad och kommunikationer. Bestämmelsen omfattar även rätten till respekt för den enskildes bostad och kommunikationer. Enligt de officiella förklaringarna till EU-stadgan ska artikeln tolkas i överensstämmelse med artikel 8 EKMR och ges samma innebörd och räckvidd som denna. Att begreppet ”korrespondens” ersatts med ”kommunikation” återspeglar den tekniska utvecklingen och innebär att skyddet även omfattar moderna kommunikationsformer.⁸⁰

⁷⁷ Artikel 26.1-2 i Europeiska sociala stadgan; Prop. 1997/98:82 *Europarådets sociala stadga*, s. 32 f.

⁷⁸ Nyström, *Introduktion till den europeiska arbetsrätten*, s. 66.

⁷⁹ Artikel 51 EU-stadgan; Europeiska unionens officiella tidning, *Förklaringar avseende stadgan om de grundläggande rättigheterna*, EUT C 303/02, ISSN 1725-2504, 14 december 2007, kommentar till artikel 51.

⁸⁰ EUT, *Förklaringar avseende stadgan om de grundläggande rättigheterna*, kommentar till artikel 7.

Därutöver etablerar artikel 8 i EU-stadgan en självständig rätt till skydd för personuppgifter. Bestämmelsen uppställer krav på att personuppgifter ska behandlas lagligt, för specificerade ändamål och med stöd i samtycke eller annan legitim grund. Den innehåller även rätt till tillgång och rättelse samt krav på oberoende tillsyn. Av de officiella förklaringarna framgår att bestämmelsen bland annat har sin grund i Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter samt i artikel 8 EKMR.⁸¹ Det aktuella direktivet har ersatts av GDPR, vilket gör att hänvisningen från artikel 8 i stadgan nu kan göras direkt till denna förordning.⁸² Det framgår även av GDPR att förordningen respekterar de grundläggande rättigheter och principer som erkänns i stadgan.⁸³

Begränsningar av dessa rättigheter regleras i artikel 52.1, enligt vilken inskränkningar endast får ske om de är föreskrivna i lag, förenliga med rättigheternas väsentliga innehåll samt uppfyller kraven på nödvändighet och proportionalitet. De ska dessutom tillgodose ett mål av allmänt samhällsintresse eller skydda andra personers rättigheter och friheter. Följaktligen är de begränsningar som får göras i dessa rättigheter desamma som enligt artikel 8 EKMR.⁸⁴

Artikel 52.3 innehåller därutöver en uttrycklig koppling till Europakonventionen. I den mån EU-stadgan omfattar rättigheter som motsvarar de som garanteras enligt konventionen, ska dessa ges samma innebörd och räckvidd. Detta innebär att den praxis som utvecklats inom ramen för Europakonventionen är vägledande även vid tolkningen av stadgans bestämmelser. Bestämmelsen hindrar dock inte unionsrätten från att tillhandahålla ett mer omfattande skydd än vad som ställs upp i Europakonventionen.⁸⁵

Mot denna bakgrund har EU-domstolen i sin praxis ytterligare konkretiserat innebörden av skyddet enligt artiklarna 7 och 8, särskilt i mål som rör omfattande datalagring. Domstolen har därvid konsekvent betonat att åtgärder som innebär generell och odifferentierad insamling eller lagring av uppgifter utgör allvarliga intrång i de grundläggande rättigheterna och är otillåtna.⁸⁶ I senare

⁸¹ EUT, *Förklaringar avseende stadgan om de grundläggande rättigheterna*, kommentar till artikel 8.

⁸² Artikel 94 GDPR.

⁸³ Se skäl 4 i GDPR.

⁸⁴ Artikel 52.1 EU-stadgan; EUT, *Förklaringar avseende stadgan om de grundläggande rättigheterna*, kommentar till artikel 7.

⁸⁵ Mark Klamberg, "Skydd enligt Europeiska unionens stadga om de grundläggande rättigheterna", i: Cecilia Magnusson Sjöberg, Karatina Fast Lappalainen och Daniel Westman (red.), *Rättsinformatik: juridiken i det digitala informationssamhället*, 5 uppl., (Studentlitteratur AB, 2024) s. 164.

⁸⁶ Mål C-293/12 och C-594/12 *Digital Rights Ireland m.fl.*, dom 8 april 2014, EU:C:2014:238; Mål C-203/15 och C-698/15 *Tele2 Sverige m.fl.*, dom 21 december 2016, EU:C:2016:970.

praxis har domstolen dock öppnat för undantag i särskilt utpekade situationer som rör nationell säkerhet, såsom vid allvarliga hot om terrorism.⁸⁷

2.4 Regeringsformen

Skyddet för grundläggande fri- och rättigheter i svensk rätt kommer till uttryck i 2 kap. regeringsformen (1974:152), RF. I kapitlet skyddas flertalet rättigheter, däribland politiska friheter, enskildas integritet och rättssäkerhetsgarantier.⁸⁸ En central begränsning är att regeringsformens fri- och rättighetskydd i första hand riktar sig mot det allmänna. Det innebär att skyddet aktualiseras i relationen mellan individ och stat, men som utgångspunkt inte i förhållandet mellan privata aktörer. Detta får betydelse i arbetslivet, där skyddet enligt RF typiskt sett endast är direkt tillämpligt för offentligt anställda.⁸⁹

Genom en senare ändring har lagstiftaren däremot stärkt skyddet mot intrång från det allmännas sida genom att införa en bestämmelse om betydande integritetsintrång.⁹⁰ Denna nya bestämmelse, som även är den mest relevanta i förevarande sammanhang, är 2 kap. 6 § RF. Bestämmelsens andra stycke ger skydd mot betydande intrång i den personliga integriteten och tar särskilt sikte på övervakning eller kartläggning av den enskildes personliga förhållanden från det allmännas sida utan uttryckligt samtycke. Den är generellt utformad och omfattar såväl databehandling av personuppgifter som manuell övervakning, varvid frågan om en åtgärd utgör övervakning eller kartläggning ska avgöras utifrån dess faktiska effekter.⁹¹

Skyddet i 2 kap. 6 § andra stycket RF är emellertid begränsat till vissa typer av åtgärder och aktualiseras endast vid intrång av viss betydande grad. Vid bedömningen av om ett intrång är att anse som betydande ska bland annat uppgifternas karaktär och omfattning, ändamålet med behandlingen samt hur uppgifterna används och sprids beaktas. Bedömningen är dessutom föränderlig och påverkas bland annat av den tekniska utvecklingen.⁹² Rättigheten är vidare inte absolut utan begränsningar får göras, förutsatt att de är godtagbara i ett demokratiskt samhälle och inte går utöver vad som är nödvändigt eller utgör ett hot mot den fria åsiktsbildningen. Vidare krävs att en sådan åtgärd har stöd i lag.⁹³

⁸⁷ Mål C-511/18, C-512/18 och C-520 *La Quadrature du net m.fl.*, dom 6 oktober 2020, EU:C:2020:791, p. 135 och p. 179.

⁸⁸ Henrik Jermsten, *Regeringsformen* (1974:152) 2 kap., Karnov (JUNO).

⁸⁹ AD 1984 nr 94; AD 1991 nr 45.

⁹⁰ Prop 2009/10:80 *En reformerad grundlag*, s. 1.

⁹¹ Prop 2009/10:80 s. 181; Sören Öman, ”Grundlagsskydd”, i: Cecilia Magnusson Sjöberg, Karatina Fast Lappalainen och Daniel Westman (red.), *Rättsinformatik: juridiken i det digitala informationssamhället*, 5 uppl., (Studentlitteratur AB, 2024) s. 154 f.

⁹² Prop 2009/10:80 s. 184 f.; Öman, ”Grundlagsskydd”, s. 154 f.

⁹³ 2 kap. 12 § RF; Prop. 1993/94:24 *med förslag till ändrade regler om kroppsvisitation och kroppsbesiktning, m.m.*, s. 23.

Det har i doktrinen framhållits att regeringsformen saknar ett direkt motsvarande skydd för privat- och familjeliv i den mening som följer av artikel 8 EKMR. Bestämmelsen i 2 kap. 6 § RF är avsiktligt mer begränsad och omfattar endast vissa kvalificerade integritetsintrång. I stället kommer mer övergripande skyddsaspekter till uttryck genom målsättningsstadgandet i 1 kap. 2 § RF. Detta innebär dock inte nödvändigtvis att skyddsnivån i svensk rätt är lägre, men det medför att rättighetsskyddet i praktiken ofta måste tolkas och tillämpas i ljuset av Europakonventionens bestämmelser.⁹⁴

I detta sammanhang är kopplingen till Europakonventionen av särskild betydelse. Sverige ratificerade konventionen år 1952 och inkorporerade den i svensk rätt genom lag (1994:1219), vilken trädde i kraft 1995. Skyddet har därefter förstärkts ytterligare genom 2 kap. 19 § RF, som stadgar att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden enligt konventionen. Bestämmelsen innebär inte att Europakonventionen ges grundlagsstatus, men den medför att en föreskrift som strider mot konventionen samtidigt står i strid med grundlagen.⁹⁵ Detta innebär att Europakonventionen har en stark ställning i svensk rätt och utgör ett viktigt komplement till regeringsformens skydd, särskilt i den privata sektorn där RF inte är direkt tillämplig.

2.5 Diskussion

Det mest centrala rättighetsskyddet återfinns i artikel 8 EKMR, som etablerar ett brett och dynamiskt skydd för privatlivet. Genom Europadomstolens praxis har detta skydd även kommit att omfatta stora delar av arbetslivet. Vidare aktualiseras skyddet redan vid konstaterandet av ett ingrepp och begränsas genom de krav som uppställs i artikel 8.2, där proportionalitetsbedömningen är central. Bedömningen skiljer sig beroende på om det rör statens negativa förpliktelser vid egna ingrepp eller dess positiva förpliktelser att säkerställa ett effektivt skydd i relationer mellan enskilda.

Genom avgöranden som *Halford v. the United Kingdom* och *Copland v. the United Kingdom*, vilka rör statens negativa förpliktelser, har domstolen klargjort att även kommunikation på arbetsplatsen omfattas av skyddet och att bristande information i sig kan vara avgörande för att ett ingrepp ska anses otillåtet. Informationskravet framstår därmed som en central komponent i bedömningen och utgör ett viktigt skydd mot dold och godtycklig övervakning. Genom *Bărbulescu v. Romania* har skyddet ytterligare förstärkts, inte minst genom att domstolen tydliggjort statens positiva förpliktelser och därmed öppnat för att även privata arbetsgivares åtgärder omfattas. De sex kriterier som utvecklades i domen utgör idag en tydlig struktur för

⁹⁴ Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, s. 442.

⁹⁵ Prop. 1993/94:117 *Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor*, s. 11; Danelius m.fl., *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, s. 48.

intresseavvägningen och bidrar till en mer förutsebar rättstillämpning. Samtidigt visar senare praxis, såsom *Libert v. France* och *López Ribalda and Others v. Spain*, att domstolen också erkänner arbetsgivarens legitima intresse av att kontrollera verksamheten och säkerställa att arbetsuppgifter utförs korrekt. Bedömningen blir därmed i hög grad beroende av proportionalitet, där faktorer som syfte, omfattning och tillgängliga skyddsåtgärder vägs mot varandra.

En tydlig tendens i praxis är att domstolen anpassar sin bedömning till den tekniska utvecklingen. I *López Ribalda and Others v. Spain* framhålls uttryckligen att kriterierna måste tillämpas med hänsyn till nya tekniska möjligheter, vilket bekräftas i senare fall som *Libert v. France*. Detta tyder på att artikel 8 ges ett dynamiskt innehåll, där nya former av övervakning successivt inkluderas inom skyddets räckvidd. Utvecklingen från telefonsamtal till e-post, internetanvändning och geolokaliseringsdata illustrerar att domstolen konsekvent utgår från samma grundprincip: att åtgärder som möjliggör insyn i individens beteende och kommunikation typiskt sett faller inom privatlivets sfär. Mot denna bakgrund, och trots att algoritmisk övervakning och arbetsledning ännu inte uttryckligen har prövats, finns det starka skäl att anta att även sådana åtgärder omfattas av skyddet enligt artikel 8 EKMR.

I relation till detta finns en motsvarande bestämmelse om personlig integritet i nationell rätt genom 2 kap. 6 § andra stycket RF. Detta skydd är emellertid mer begränsat, då det endast omfattar vissa kvalificerade intrång från det allmännas sida och inte aktualiseras i förhållandet mellan privata aktörer. Regeringsformen ger därmed inte ett mer långtgående skydd än artikel 8 EKMR, utan framstår snarare som ett mer avgränsat komplement.

Trots den starka rättighetsnivån som artikel 8 EKMR fastställer finns det även utmaningar. Som har framhållits i litteraturen kan det i praktiken vara svårt för arbetstagare att få integritetskänsliga åtgärder prövade, inte minst eftersom det ofta kräver att de ifrågasätter arbetsgivarens agerande på ett sätt som kan få konsekvenser för anställningen. Detta pekar på en viss diskrepans mellan det principiella skyddet i konventionen och den faktiska möjligheten att göra det gällande.

Vid sidan av Europakonventionen innehåller Europarådets andra regelverk, den Europeiska sociala stadgan, ett omfattande system av arbetsrättsliga skyldigheter för medlemsstaterna. Den Europeiska sociala stadgan reglerar en rad centrala aspekter av arbetslivet och syftar till att säkerställa skäliga arbetsvillkor, god arbetsmiljö och skydd för arbetstagares värdighet.

Det kan dock konstateras att den Europeiska sociala stadgan saknar bestämmelser som direkt tar sikte på arbetsgivares övervakning eller arbetstagares personliga integritet i den mening som aktualiseras vid algoritmisk övervakning och arbetsledning. Artikel 2 behandlar i huvudsak frågor om arbetstid,

vila och fysiska arbetsförhållanden, medan artikel 26 tar sikte på mellanmänskliga beteenden i arbetslivet, såsom trakasserier och mobbning. Stadgan ger därmed inte något tydligt rättsligt stöd för att bedöma denna typ av åtgärder, utan får i stället ses som ett mer övergripande ramverk vars betydelse i detta sammanhang främst är indirekt.

Parallellt med Europarådets system innehåller EU:s rättighetsstadga, i artiklarna 7 och 8, ett skydd för rätten till privatliv respektive skyddet av personuppgifter. Sammantaget innebär dessa bestämmelser att gränsen mellan tillåten arbetsledning och otillåten övervakning avgörs genom en avvägning mellan arbetsgivarens intressen och arbetstagarens grundläggande rättigheter, där åtgärden måste ha en tydlig rättslig grund samt vara nödvändig och proportionerlig. Bestämmelserna motsvarar i stor utsträckning artikel 8 EKMR och rättighetsskydden överlappar därmed i hög grad. Det anges uttryckligen i stadgan att rättigheterna ska ha samma innebörd och räckvidd, vilket innebär att Europadomstolens praxis, som redogjorts för ovan, utgör en viktig tolkningsgrund. Detta illustrerar det nära samspelet mellan regelverken.

Samtidigt ger EU-stadgan ett mer utvecklat och självständigt skydd för personuppgifter genom artikel 8. EU-domstolen har i sin praxis intagit en restriktiv hållning till omfattande datainsamling och särskilt markerat att generell och odifferentierad lagring av uppgifter är otillåten. Även om algoritmisk övervakning och arbetsledning i arbetslivet inte har prövats specifikt, ger denna praxis vägledning för bedömningen och talar för att sådana system kan vara otillåtna om de bygger på motsvarande former av generell och omfattande datalagring.

Sammanfattningsvis framstår Europakonventionen som det mest centrala rättsliga ramverket i fråga om övervakning i arbetslivet, då Europadomstolens praxis i större utsträckning erbjuder konkret vägledning genom avgöranden som direkt rör arbetsgivares kontrollåtgärder. EU-domstolens praxis avseende artiklarna 7 och 8 i EU:s rättighetsstadga är däremot mer generell och tar i huvudsak sikte på databehandling och övervakning i ett bredare perspektiv. Detta innebär att Europakonventionen tillhandahåller ett mer kontextnära bedömningsunderlag, medan EU-rätten snarare uppställer mer långtgående krav i frågor om generell och odifferentierad datalagring. Regeringsformen och den Europeiska sociala stadgan ingår visserligen i rättighetsramen, men tillför i detta sammanhang inte något ytterligare självständigt skydd för arbetstagare.

3 EU:s rättsakter

3.1 Rätten till integritet enligt GDPR

3.1.1 Syfte och tillämpningsområde

Den 27 april 2016 antogs dataskyddsregleringen GDPR efter flera års förhandlingar mellan EU:s medlemsstater, vilket markerade en ny fas i den europeiska och svenska dataskyddsrättens utveckling.⁹⁶ Förordningen antogs med stöd av artikel 16 fördraget om Europeiska unionens funktionssätt (FEUF), vilken ger EU befogenhet att fastställa regler om skydd för personuppgifter.⁹⁷

Förordningen avser att skapa en mer enhetlig och likvärdig tillämpning av dataskyddsbestämmelserna inom EU samt att stärka skyddet för enskildas personuppgifter. Till skillnad från tidigare reglering i form av direktiv är GDPR en förordning och därmed direkt tillämplig i medlemsstaterna.⁹⁸ Samtidigt innehåller GDPR bestämmelser som ger medlemsstaterna utrymme att komplettera regleringen nationellt. En sådan är artikel 88, som möjliggör mer specifika nationella regler om behandling av anställdas personuppgifter inom anställningsförhållanden. Bestämmelsen utgör en öppningsklausul som tillåter avvikelser eller mer långtgående regler än vad som följer av förordningen.⁹⁹

Dataskyddsförordningen har enligt artikel 1 ett dubbelt syfte. Den ska dels säkerställa ett fritt flöde av personuppgifter inom EU utan nationella begränsningar, dels skydda fysiska personers grundläggande rättigheter och friheter. Detta kommer till uttryck i förordningens bestämmelser, där skyddet för den enskilde kombineras med harmoniserade regler för att möjliggöra en fungerande inre marknad.¹⁰⁰

Regelverkets tillämplighet framgår av artikel 2. Enligt artikel 2.1 omfattar förordningen behandling av personuppgifter som är helt eller delvis automatiserad samt, i vissa fall, manuell behandling. Med helt automatiserad behandling avses behandling som sker elektroniskt, exempelvis vid ärendehandläggning, löneutbetalningar eller hantering av kundregister. Delvis automatiserad behandling kan avse uppgifter som samlas in manuellt men därefter sammanställs eller behandlas digitalt. Även rent manuell behandling, det vill säga

⁹⁶ David Frydlinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskydds-förordningen* (Nordstedts Juridik, 2018), s. 28.

⁹⁷ Skäl 1 och 12 i GDPR.

⁹⁸ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 16.

⁹⁹ Sören Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar* (11 september 2025, version 3A, JUNO), kommentaren till artikel 88 under rubriken Inledning.

¹⁰⁰ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 1 under rubriken Inledning.

uppgifter som enbart hanteras på papper, omfattas under förutsättning att de ingår i eller är avsedda att ingå i ett register.¹⁰¹

3.1.2 Definitioner och känsliga personuppgifter

I artikel 4 GDPR finns ett flertal relevanta begrepp definierade. Av artikel 4.1 framgår vad som utgör en personuppgift, vilket är det viktigaste begreppet i förordningen. Begreppet personuppgift har vid innebörd och omfattar alla typer av uppgifter som kan kopplas till en fysisk person, oavsett personens roll eller ställning. Det kan exempelvis röra sig om namn, kontaktuppgifter eller tekniska uppgifter som IP-adresser och GPS-information, även när identifiering sker genom att flera uppgifter kombineras.¹⁰²

Förordningen skiljer mellan två huvudsakliga kategorier av personuppgifter. Den första omfattar generella personuppgifter, vilket innefattar alla uppgifter som kan kopplas till en fysisk person. Den andra kategorin utgör en delmängd av dessa och benämns i förordningen som särskilda kategorier av personuppgifter, vanligtvis kallade känsliga personuppgifter. Enligt artikel 9.1 är behandling av sådana uppgifter som huvudregel förbjuden och omfattar bland annat uppgifter om etniskt ursprung, politiska åsikter, religiösa övertygelser, fackligt medlemskap samt genetiska och biometriska uppgifter. Behandling kan endast ske om något av undantagen i artikel 9.2 är uppfyllt, exempelvis uttryckligt samtycke, arbetsrättsliga skyldigheter eller viktiga allmänna intressen.¹⁰³

Utöver dessa kategorier innehåller förordningen även särskilda regler om behandling av personuppgifter som rör lagöverträdelse, brottsmisstankar och liknande uppgifter enligt artikel 10. Sådan behandling får som utgångspunkt endast utföras under kontroll av myndighet eller när den är tillåten enligt unionsrätten eller nationell rätt med lämpliga skyddsåtgärder. Bestämmelsen kan aktualiseras vid vissa former av arbetsplatsövervakning, exempelvis kameraövervakning. Enbart registrering av händelseförlopp utgör normalt inte brottsuppgifter förrän materialet används för att dokumentera eller följa upp ett brott.¹⁰⁴ Algoritmisk övervakning och arbetsledning som på motsvarande sätt identifierar och avskiljer sådant material för dessa ändamål är inte tillåten utan stöd i artikel 10, liksom när känsliga personuppgifter behandlas utan tillämpligt undantag enligt artikel 9.

¹⁰¹ "Syfte och tillämpningsområde", Integritetsskyddsmyndigheten, 11 juni 2025, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/syfte-och-tillampningar/>.

¹⁰² Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 44 f.

¹⁰³ Artikel 9 GDPR; Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 45 f.

¹⁰⁴ Integritetsskyddsmyndigheten, *Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet "personuppgifter som rör lagöverträdelse som innefattar brott" i artikel 10 i dataskyddsförordningen*, (2021), s. 2.

Vidare i artikel 4.1 definieras begreppet registrerad, vilket avser den fysiska person som personuppgifterna rör. En registrerad är enligt bestämmelsen en identifierad eller identifierbar fysisk person. I artikel 4.7 definieras därutöver begreppet personuppgiftsansvarig, vilket avser den som ensam eller tillsammans med andra fastställer ändamålen med och medlen för behandlingen av personuppgifter. Det är normalt organisationen, exempelvis ett aktiebolag, en förening eller en myndighet, som är personuppgiftsansvarig och inte enskilda chefer eller anställda. Dock kan även fysiska personer i vissa fall kan vara ansvariga, exempelvis inom enskild näringsverksamhet.¹⁰⁵ Slutligen definieras dessutom begreppet behandling i artikel 4.2 och omfattar bland annat insamling, registrering, organisering, strukturering och lagring av information.

Mot denna bakgrund faller användningen av algoritmisk övervakning och arbetsledning tydligt inom förordningens tillämpningsområde. Det innebär att införandet och användningen av sådana system endast är tillåten om arbetsgivaren kan visa att det finns en rättslig grund för behandlingen.¹⁰⁶

3.1.3 De grundläggande principerna

De grundläggande principerna i artikel 5 GDPR utgör kärnan i dataskyddsförordningen och fastställer ramarna för vad som anses utgöra en tillåten personuppgiftsbehandling. Det åligger den personuppgiftsansvarige att säkerställa att principerna iakttas samt att kunna visa hur dessa efterlevs, i enlighet med artikel 5.2.¹⁰⁷ Nedan följer en genomgång av de olika principerna.

Enligt artikel 5.1 (a) ska behandlingen vara laglig, korrekt och öppen. Principen om laglighet innebär att personuppgifter endast får behandlas om det finns rättsligt stöd för behandlingen, exempelvis i dataskyddsförordningen eller annan särskild lagstiftning. Till skillnad från den allmänna utgångspunkten att allt som inte är förbjudet är tillåtet, gäller inom personuppgiftsrätten i stället att behandling är otillåten om det saknas lagstöd.¹⁰⁸ Principen om laglighet kan därmed förstås som en hänvisning till de rättsliga grunderna i artikel 6.1.¹⁰⁹ Begreppet korrekthet innebär att behandlingen ska vara rättvis, skälig och proportionerlig i förhållande till den registrerade. Detta förutsätter en avvägning mellan den personuppgiftsansvariges intressen och den registrerades integritetsintresse. Behandlingen ska vidare vara begriplig och ske på ett öppet sätt, med beaktande av vad den registrerade rimligen kan förvänta sig.

¹⁰⁵ "Personuppgiftsansvariga och personuppgiftsbiträden", Integritetsskyddsmyndigheten, 11 juni 2025, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/>.

¹⁰⁶ Adams-Prassl, "Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'", s. 10.

¹⁰⁷ "Grundläggande principer", Integritetsskyddsmyndigheten, 11 juni 2025, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/>.

¹⁰⁸ Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 35.

¹⁰⁹ Prop. 2017/18:105 *Ny dataskyddslag*, s. 47.

Slutligen innebär öppenhet att den registrerade ska få information om varför och hur uppgifterna används samt om sina rättigheter, exempelvis möjligheten att få uppgifter rättade eller raderade.¹¹⁰

Artikel 5.1 (b) uttrycker principen om ändamålsbegränsning, vilket innebär att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och på förhand fastställda ändamål. Ändamålen ska därmed vara tydliga och klart definierade.¹¹¹ Den så kallade finalitetsprincipen innebär vidare att personuppgifter får behandlas för ett nytt ändamål, under förutsättning att detta är förenligt med det ursprungliga ändamålet. Den registrerade ska i sådana fall informeras innan den nya behandlingen påbörjas, i enlighet med artiklarna 13.3 och 14.4.¹¹²

Artikeln innehåller därutöver ytterligare krav för behandling av personuppgifter. Dessa innebär bland annat att endast relevanta och nödvändiga uppgifter får behandlas, att uppgifterna ska vara korrekta och aktuella, att de inte får lagras längre än vad som krävs samt att de ska skyddas genom lämpliga tekniska och organisatoriska åtgärder.¹¹³

Flera av principerna i artikel 5 kan aktualiseras vid algoritmisk övervakning och arbetsledning i arbetslivet, särskilt principen om öppenhet i artikel 5.1. Arbetsplatskontexten kräver en hög grad av transparens och förutsebarhet och det innebär bland annat att arbetstagare ska få tydlig information om hur övervakningssystem fungerar samt vilka kriterier som används. Vid automatiserad e-postövervakning bör exempelvis reglerna bakom systemets bedömningar vara fullt transparenta och användaren informeras innan åtgärder vidtas.¹¹⁴

3.1.4 Rättslig grund

För att en behandling ska vara laglig enligt GDPR krävs, utöver att de grundläggande principerna i artikel 5 iakttas, att minst en av de sex rättsliga grunderna i artikel 6 är uppfylld.¹¹⁵ I förordningen görs en åtskillnad mellan två situationer där en laglig grund kan föreligga, dels när den registrerade har lämnat sitt samtycke enligt 6.1 (a), dels när behandlingen är nödvändig av andra skäl enligt 6.1 (b-f). Dessa rättsliga grunder speglar den avvägning

¹¹⁰ ”Grundläggande principer”, Integritetsskyddsmyndigheten.

¹¹¹ Mål C-175/20 *SS mot Valsts ie mumu dienests*, dom 24 februari 2022, EU:C:2022:124, punkterna 65 och 68.

¹¹² Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 5 under rubriken Återanvändning för andra ändamål – Finalitetsprincipen.

¹¹³ Se artikel 5.1 (c-f) GDPR.

¹¹⁴ Adams-Prassl, ”Regulating Algorithms at Work: Lessons for a ‘European Approach to Artificial Intelligence’”, s. 11; Artikel 29-gruppen för uppgiftsskydd, *Yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen*, WP 249, antaget den 8 juni 2017, s. 15.

¹¹⁵ ”Rättslig grund”, Integritetsskyddsmyndigheten, 11 juni 2025, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/>.

mellan integritetsskydd och legitima samhällsintressen som präglar dataskyddsförordningen.¹¹⁶

Enligt artikel 4.11 innebär samtycke att den registrerade genom en frivillig, specifik, informerad och otvetydig viljeyttring godtar behandlingen av personuppgifter. Det är den personuppgiftsansvarige som ska kunna visa att samtycke har lämnats, i enlighet med artikel 7.1. Högsta domstolen har understrukit att samtycket måste föreligga innan behandlingen påbörjas och inte kan lämnas i efterhand med rättslig verkan.¹¹⁷ I arbetsrättsliga sammanhang kan frivilligheten dock ifrågasättas mot bakgrund av den maktobalans som präglar anställningsförhållandet. Europeiska dataskyddsstyrelsen (EDPB) har framhållit att samtycke sällan är en lämplig rättslig grund i förhållandet mellan arbetsgivare och arbetstagare, men att det undantagsvis kan vara giltigt om den registrerade inte riskerar negativa konsekvenser oavsett om samtycke lämnas eller inte.¹¹⁸

Avtal enligt artikel 6.1 (b) kan utgöra laglig grund när behandlingen av personuppgifter är nödvändig för att fullgöra ett avtal eller för att vidta åtgärder på den registrerades begäran inför att ett avtal ingås. Denna artikel är ofta tillämplig inom arbetsrätten, där arbetsgivare typiskt sett behöver behandla arbetstagares personuppgifter för att exempelvis betala ut lön och andra förmåner samt tillhandahålla arbetsrelaterad utrustning och tjänster.¹¹⁹

Artikel 6.1 (c) avser behandling som är nödvändig för att uppfylla en rättslig förpliktelse, vilket enligt artikel 6.3 ska ha stöd i nationell rätt eller EU-rätt. Sådan skyldighet kan följa av lag, kollektivavtal eller internationella överenskommelser som innebär att personuppgifter ska lämnas till exempelvis en myndighet, domstol eller annan.¹²⁰ Det kan även avse behandling av personuppgifter i syfte att uppfylla skyldigheter att rapportera till Skatteverket eller andra myndigheter, liksom att bevara uppgifter i enlighet med bokföringslagens bestämmelser.¹²¹

Slutligen finns ytterligare tre rättsliga grunder som kan aktualiseras i olika situationer. Artikel 6.1 (d) avser behandling som är nödvändig för att skydda den registrerades eller en annan fysisk persons grundläggande intressen, exempelvis i situationer där behandlingen är avgörande för liv eller hälsa och

¹¹⁶ Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 139.

¹¹⁷ Jfr NJA 2005 s. 361.

¹¹⁸ European Data Protection Board, *Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679*, version 1.1, antagna 4 maj 2020, p. 21-22, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_sv.pdf.

¹¹⁹ Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 140.

¹²⁰ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 6 under rubriken Led c – Rättslig förpliktelse; AD 2021 nr 23.

¹²¹ Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 141.

samtycke inte kan lämnas. Artikel 6.1 (e) avser behandling som är nödvändig för myndighetsutövning eller för att utföra uppgifter av allmänt intresse och aktualiseras främst för myndigheter och andra offentliga organ. Denna rättsliga grund möjliggör att statliga och kommunala verksamheter kan fullgöra sina uppdrag. Artikel 6.1 (f) utgör en generalklausul som reglerar intresseavvägningen, vilken möjliggör behandling av personuppgifter efter en avvägning mellan berättigade intressen och den registrerades integritetsskydd. Offentliga myndigheter får dock inte stödja sin behandling på denna grund när de utför sina uppgifter, i enlighet med artikel 6.1 st. 2.¹²²

I arbetsrättsliga sammanhang kan särskilt artikel 6.1 (f) aktualiseras vid användning av algoritmisk arbetsledning. En sådan behandling kan i vissa fall stödjas på arbetsgivarens berättigade intresse, men förutsätter en noggrann proportionalitetsbedömning där nödvändighet, rättvisa, transparens och integritetsskydd vägs in. Ju mer ingripande övervakningen är, desto svårare är den att motivera. Exempelvis anses tangentbordsloggning och musspåring ofta som oproportionerliga åtgärder, samtidigt som ansiktsigenkänning på arbetsplatsen i regel är otillåten.¹²³

3.1.5 Den registrerades rättigheter

Utöver de bestämmelser som riktar sig till personuppgiftsansvariga och anger under vilka förutsättningar personuppgifter får behandlas innehåller GDPR i kapitel III ett antal rättigheter för den registrerade, vilka måste iakttas för att behandlingen ska anses laglig.

Inledningsvis innehåller artikel 12 allmänna bestämmelser om hur information och kommunikation med registrerade ska lämnas. Informationen ska vara koncis, tydlig och lättillgänglig, ges på ett klart och begripligt språk samt som huvudregel tillhandahållas skriftligt och utan kostnad.¹²⁴ Vidare regleras i artiklarna 13 och 14 vilken information som den personuppgiftsansvarige ska lämna på eget initiativ. Den registrerade har bland annat rätt att få information om ändamålen med behandlingen, den rättsliga grunden, hur länge personuppgifter lagras samt vilka rättigheter som följer av dataskyddsförordningen. Informationen ska även omfatta vem som är personuppgiftsansvarig och

¹²² Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 141ff; "Rättslig grund", Integritetsskyddsmyndigheten.

¹²³ Artikel 29-gruppen, *Yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen*, s. 16 och 19; Adams-Prassl, "Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'", s. 10 f.

¹²⁴ Artikel 29-gruppen för uppgiftsskydd, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679, WP260 rev.01*, antagna den 29 november 2017 och senast granskade den 11 april 2018, s. 6 f.

möjligheten att inge klagomål till Integritetsskyddsmyndigheten och syftar till att säkerställa en rättvis och öppen behandling.¹²⁵

EU-domstolen har, i ett mål mellan Integritetsmyndigheten och AB Storstockholms Lokaltrafik, lämnat ett förhandsavgörande för att klargöra hur artiklarna 13 och 14 ska tolkas i situationer där personuppgifter samlas in genom övervakning.¹²⁶ Domstolen uttalade att personuppgifter som registreras genom kroppsburna kameror ska anses vara direkt insamlade från den registrerade, vilket innebär att informationsskyldigheten enligt artikel 13 ska tillämpas och att information i regel ska lämnas vid insamlingen. Artikel 14, som gäller uppgifter som samlas in från andra källor, är därför inte tillämplig i sådana situationer.¹²⁷

Den registrerade har vidare rätt till tillgång till sina personuppgifter och att få bekräftelse på om uppgifter behandlas, enligt artikel 15. Den personuppgiftsansvarige ska på begäran tillhandahålla en kopia av uppgifterna, ett så kallat registerutdrag.¹²⁸ Därutöver följer av artikel 16 en rätt att få felaktiga personuppgifter rättade och ofullständiga uppgifter kompletterade, under förutsättning att uppgifterna rör den registrerade själv.¹²⁹ Enligt artikel 17 finns även en rätt till radering. Rätten gäller när behandlingen strider mot förordningen eller inte längre är nödvändig för det ändamål för vilket uppgifterna samlats in, exempelvis efter återkallat samtycke eller invändning mot behandlingen.¹³⁰

Vidare ger artikel 18 den registrerade rätt att begära begränsning av behandlingen, vilket innebär att uppgifterna, med vissa undantag, endast får lagras och i övrigt inte behandlas.¹³¹ Slutligen följer av artikel 21 en rätt att invända mot behandling som grundas på uppgift av allmänt intresse, myndighetsutövning eller intresseavvägning. Om en invändning görs ska behandlingen som utgångspunkt upphöra, om inte avgörande berättigade skäl kan visas av den personuppgiftsansvariga.¹³²

¹²⁵ Skäl 60–61 i GDPR; ”De registrerades rättigheter”, Integritetsskyddsmyndigheten, 11 juni 2025, <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/>.

¹²⁶ Mål C-422/24 *Integritetsskyddsmyndigheten mot AB Storstockholms Lokaltrafik*, dom 18 december 2025, EU:C:2025:980, p. 15-16.

¹²⁷ Mål C-422/24, punkterna 41-42 och 45.

¹²⁸ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 15 under rubriken Inledning.

¹²⁹ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 16 under rubriken Begäran om rättelse eller komplettering.

¹³⁰ Skäl 65 i GDPR.

¹³¹ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 18 under rubriken Inledning.

¹³² Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 21 under rubriken Första punkten – Generell rätt till invändningar.

Gällande algoritmisk arbetsledning och kontroll är transparens och förutsägbarhet särskilt viktigt. Arbetstagare ska få tydlig information om vilken övervakning som sker, vilka syften behandlingen har och under vilka förutsättningar den används. Det bör även finnas möjligheter för den registrerade att begränsa eller påverka hur uppgifter samlas in. Policys och riktlinjer om övervakning ska vara klara, lättillgängliga och utformas med hänsyn till arbetstagarnas rättigheter, eftersom sådan behandling kan få betydande konsekvenser för den personliga integriteten.¹³³

3.1.6 Särskilt om automatiserat beslutsfattande och profilering

Som framgått ovan kan övervakning och insamling av digitala uppgifter vara tillåten. Algoritmisk övervakning och arbetsledning är därmed inte i sig förbjuden, förutsatt att de relevanta kraven iakttas. GDPR innehåller dock en särskild reglering av automatiserat beslutsfattande, vilken kan få betydelse för bedömningen av sådana system. I det följande avsnittet redogörs därför särskilt för denna reglering och dess innehåll.

Artikel 22 reglerar automatiserade individuella beslut. Bestämmelsen innebär som huvudregel att den registrerade har rätt att inte bli föremål för beslut som enbart grundas på automatiserad behandling, inklusive profilering, om beslutet medför rättsliga följder eller annars påverkar personen på ett betydande sätt. Profilering definieras i artikel 4.4 och innebär varje form av automatiserad behandling av personuppgifter som används för att bedöma personliga egenskaper, såsom arbetsprestationer, ekonomisk situation, hälsa, preferenser, beteende eller förflyttningar. För att bestämmelsen ska aktualiseras krävs att beslutet fattas utan faktisk mänsklig inblandning.¹³⁴ Om ett beslut däremot fattas av en eller flera personer anses det inte vara automatiserat, även om automatiserad behandling eller profilering har använts som stöd i beslutsprocessen.¹³⁵

Undantag från denna huvudregel finns dock i vissa situationer. Det gäller exempelvis när behandlingen är nödvändig för att ingå eller fullgöra ett avtal, är tillåten enligt särskild lagstiftning eller grundar sig på den registrerades uttryckliga samtycke. Därutöver ska den personuppgiftsansvarige vidta lämpliga åtgärder för att säkerställa den registrerades friheter, rättigheter och berättigade intressen.¹³⁶

¹³³ Artikel 29-gruppen, *Yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen*, s. 23.

¹³⁴ Frydlinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 220 f.

¹³⁵ Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 22 under rubriken Första punkten – Rätt att slippa automatiserat beslutsfattande.

¹³⁶ Artikel 22.2–3 GDPR; skäl 71 i GDPR.

I samband med automatiserat beslutsfattande uppställs även ett utökat krav på information. Artikel 13.2 (f) respektive 14.2 (g) reglerar särskild information i förhållande till automatiserade beslut i artikel 22. Regleringen innebär att den personuppgiftsansvarige ska informera den registrerade om att metoden används, lämna meningsfull information om den bakomliggande logiken samt förklara behandlingens betydelse och de förutsedda konsekvenserna. Komplexiteten i automatiserat beslutsfattande minskar inte kravet på transparens, utan förstärker snarare behovet av tydlig och begriplig information för att den registrerade ska kunna förstå grunderna för beslutet.¹³⁷ Vidare följer av artikel 15.1 (h) motsvarande rätt till information som enligt bestämmelserna ovan, där den registrerade ska få upplysningar om behandlingens förutsedda följder snarare än en förklaring av ett enskilt beslut.¹³⁸

Som ett led i automatiserat beslutsfattande och profilering kan dessutom en konsekvensbedömning krävas enligt artikel 35. Sådana bedömningar aktualiseras särskilt i samband med denna typ av behandling, men krävas i alla situationer där en viss personuppgiftsbehandling, särskilt vid användning av ny teknik, sannolikt medför en hög risk för enskildas rättigheter och friheter.¹³⁹ Det är därmed typen av behandling som aktualiserar skyldigheten att genomföra en konsekvensbedömning, snarare än den konkreta risknivån efter planerade skyddsåtgärder. En konsekvensbedömning innebär att den planerade personuppgiftsbehandlingen kartläggs och analyseras, med särskilt fokus på riskens ursprung, art, särdrag och allvar.¹⁴⁰

3.2 AI-förordningen

3.2.1 Syfte och tillämpningsområde

AI-förordningen utgör det första rättsliga ramverket för artificiell intelligens som på ett samlat sätt behandlar de risker och rättsliga frågor som tekniken aktualiserar. Regelverket markerar samtidigt ett tidigt europeiskt initiativ att inta en framträdande roll i den globala utvecklingen av AI-reglering.¹⁴¹ Regelverket har antagits med rättsligt stöd i artiklarna 16 och 114 FEUF och har som övergripande syfte att säkerställa att artificiell intelligens utvecklas och används på ett sätt som respekterar grundläggande rättigheter, demokratiska värden och rättsstatens principer inom unionen. Samtidigt ska innovation och den inre marknadens funktion främjas.¹⁴²

¹³⁷ Artikel 29-gruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/67*, s. 26

¹³⁸ Artikel 29-gruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/67*, s. 28.

¹³⁹ Artikel 35.1 och 35.3 (a) GDPR.

¹⁴⁰ Skäl 84 i GDPR; Öman, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, kommentaren till artikel 35 under rubriken Första punkten – I vilka fall en konsekvensbedömning ska göras.

¹⁴¹ ”AI Act”, Europeiska kommissionen, 7 maj 2026, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

¹⁴² Artikel 1 AI-förordningen; Skäl 3 i AI-förordningen.

Förordningen ska tillämpas parallellt med befintlig EU-rätt och inte påverka unionsrätten om socialpolitik eller nationell arbetsrätt, inklusive regler om anställningsvillkor och relationen mellan arbetsgivare och arbetstagare. Regleringen inskränker inte heller befintliga bestämmelser om dataskydd eller skyddet för grundläggande rättigheter.¹⁴³

Av artikel 2 i AI-förordningen framgår att regelverket är tillämpligt på aktörer som levererar, tillhandahåller, importerar eller distribuerar AI-system inom unionen.¹⁴⁴ Ur ett arbetsrättsligt perspektiv, särskilt vid algoritmisk övervakning och arbetsledning, är det relativt ovanligt att arbetsgivare klassificeras som leverantörer. I stället är det främst tillhandahållandet av AI-system som blir relevant, det vill säga när en juridisk person använder ett sådant system i sin verksamhet.¹⁴⁵ Under vissa särskilda omständigheter kan dock arbetsgivare, särskilt större teknikföretag, ha en dubbel roll. De kan vara leverantör när de utvecklar och släpper ut AI-system på marknaden och samtidigt tillhandahållare när systemen utvecklas och används internt.¹⁴⁶ Förordningen innehåller därutöver flertalet undantag från sitt tillämpningsområde, däribland AI-system som används för rent privat bruk samt system som enbart används för forskning och utveckling.¹⁴⁷

Vidare är det centrala begreppet AI-system definierat i artikel 3.1. Här avses ett maskinbaserat system som, med viss grad av autonomi, utifrån indata genererar förutsägelser, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer. Det anges att det är av vikt att definiera begreppet tydligt och i linje med internationella standarder för att främja rättssäkerhet, internationell samordning och flexibilitet i takt med den tekniska utvecklingen.¹⁴⁸

3.2.2 En riskbaserad modell

Förordningen bygger på en riskbaserad modell där AI-system bedöms och regleras utifrån vilka konsekvenser de kan få för individer och samhällsintressen. Utifrån denna bedömning placeras systemen i olika nivåer, vilket avgör vilka rättsliga krav och begränsningar som blir tillämpliga.¹⁴⁹

¹⁴³ Skäl 9 i AI-förordningen.

¹⁴⁴ Se artikel 2.1 och artiklarna 3.3–7 i AI-förordningen.

¹⁴⁵ Artikel 3.4 AI-förordningen; Aída Ponce Del Castillo och Simon Taes, "Artificial Intelligence and Labour Law", i Nathalie A. Smuha (red.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press (2025), s. 356.

¹⁴⁶ Zahra Yusifli, *Labour Rights and the EU Artificial Intelligence Act: How to Get Away with High-Risk AI*, University of Luxembourg Law Research Paper No. 2025-01 (15 jan 2025), s. 7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5098359.

¹⁴⁷ Artikel 2.8 & 2.10 AI-förordningen.

¹⁴⁸ Skäl 12 i AI-förordningen.

¹⁴⁹ "AI-förordningen", Integritetsskyddsmyndigheten, 18 februari 2026, <https://www.imy.se/verksamhet/ai/ai-forordningen/>.

Den första kategorin omfattar AI-system som anses medföra en oacceptabel risk. Enligt artikel 5.1 i AI-förordningen får vissa typer av AI-system varken släppas ut på marknaden, tas i bruk eller användas. Det gäller bland annat system som möjliggör manipulation, exploatering, social kontroll eller övervakning. Dessa användningsområden anses särskilt ingripande och omfattas därför av ett uttryckligt förbud, eftersom de kan stå i strid med flera av unionens grundläggande värden, däribland rätten till privatliv enligt EU-stadgan.¹⁵⁰

Särskilt relevant i arbetslivet är förbudet mot AI-system som tolkar eller analyserar arbetstagares känslouttryck på arbetsplatsen, med undantag för medicinska eller säkerhetsrelaterade ändamål. Det innebär att system som drar slutsatser om exempelvis en anställds sinnesstämning i möte med kunder utgör otillåten känslougenkänning. Däremot omfattas inte AI-system som identifierar fysiska tillstånd, såsom att identifiera trötthet hos yrkeschaufförer och föreslår pauser, eftersom sådana funktioner inte anses utgöra känslougenkänning i förordningens mening.¹⁵¹ Även AI-system som genom biometriska uppgifter kategoriserar individer utifrån exempelvis politiska åsikter, religiös övertygelse eller facklig tillhörighet, liksom vissa former av biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser, är otillåtna.¹⁵²

Den andra kategorin avser AI-system som klassificeras som högrisk. Av artikel 6 i AI-förordningen och bilaga III till förordningen framgår när sådan klassificering ska ske, däribland system som används inom anställning och arbetsledning. Det omfattar exempelvis AI vid rekrytering och urval, system som fattar eller stödjer beslut om arbetsvillkor samt system som används för att övervaka och utvärdera arbetstagares prestationer och beteenden.¹⁵³ Klassificeringen motiveras av att sådana system kan få betydande konsekvenser för individers karriärmöjligheter, försörjning och rättigheter i arbetslivet.¹⁵⁴ Om ett system klassificeras som högrisk följer särskilda rättsliga krav, vilka behandlas närmare i kapitel 2.2.3.

Ett AI-system som omfattas av bilaga III behöver dock inte alltid klassificeras som högrisk enligt undantaget i artikel 6.3. Detta förutsätter att systemet inte medför en betydande risk för enskildas rättigheter, fysiska hälsa eller säkerhet. Vid denna bedömning ska särskild hänsyn tas till i vilken utsträckning systemet kan medföra negativa effekter på grundläggande rättigheter enligt EU-stadgan, däribland rätten till privatliv och arbetstagares rättigheter.¹⁵⁵ Undantaget gäller därutöver endast i vissa särskilt angivna situationer,

¹⁵⁰ Skäl 28 i AI-förordningen.

¹⁵¹ Skäl 18 i AI-förordningen; Kommissionens riktlinjer om de förbjudna användningsområdena för artificiell intelligens enligt förordning (EU) 2024/1689 (AI-förordningen), C(2025) 5052 final, s. 88 f.

¹⁵² Artikel 5.1 (g-h) AI-förordningen; Kommissionens riktlinjer C(2025) 5052 final, s. 2 f.

¹⁵³ Se bilaga III punkt 4 i AI-förordningen.

¹⁵⁴ Skäl 57 i AI-förordningen.

¹⁵⁵ Skäl 48 i AI-förordningen.

exempelvis när AI-systemet enbart identifierar beslutsmonster utan att ersätta mänsklig bedömning.¹⁵⁶ Det har framhållits i litteraturen att möjligheten till undantag enligt artikel 6.3 inte nödvändigtvis försvagar regelverket i praktiken. Särskilt i fråga om AI-system för arbetsledning är utrymmet för att tillämpa undantaget begränsat, eftersom förutsättningarna är restriktivt utformade och svåra att uppfylla i större skala.¹⁵⁷

Den tredje kategorin avser AI-system med begränsad transparensrisk. Dessa omfattas av särskilda informationskrav enligt artikel 50, vilka träder i kraft under augusti 2026. Kravet innebär bland annat att användare ska informeras när de interagerar med AI samt att AI-genererat innehåll, såsom deepfakes eller generativt material av allmänt intresse, ska kunna identifieras som artificiellt framställt.¹⁵⁸

Den fjärde kategorin, liten eller ingen risk, omfattas inte av några särskilda krav i förordningen. Det finns stadgade uppförandekoder i artikel 95, vilka är frivilliga för leverantörer eller tillhandahållare att följa. De flesta AI-systemen som används i dag faller inom denna kategori, exempelvis datorspel eller spamfilter.¹⁵⁹

3.2.3 Särskilda krav vid högrisk-AI

AI-system som klassificeras som högrisk omfattas av särskilda rättsliga krav enligt AI-förordningen.¹⁶⁰ Kraven kan delas in i två kategorier: dels de som gäller generellt för alla högrisk-system, dels de som riktar sig särskilt till vissa aktörer.

Avseende den första kategorin, de generella skyldigheterna, uppställs bland annat krav på ett systematiskt riskhanteringssystem samt på att den data som används håller hög kvalitet och är relevant. Även teknisk dokumentation ska säkerställas så att systemets funktion och beslutsfattande kan granskas.¹⁶¹ Därutöver finns bestämmelser om transparens och mänsklig kontroll. Systemen ska vara utformade så att deras utdata kan tolkas och användas på ett ändamålsenligt sätt samt stå under effektiv mänsklig kontroll.¹⁶² Vidare krävs att systemen uppfyller krav på noggrannhet, robusthet och cybersäkerhet.¹⁶³ Syftet med dessa krav är att begränsa risker och säkerställa hög tillförlitlighet, med hänsyn till systemets avsedda användning och sammanhang. För

¹⁵⁶ Se artikel 6.3 (c) AI-förordningen; skäl 53 i AI-förordningen.

¹⁵⁷ Yusifli, *Labour Rights and the EU Artificial Intelligence Act*, s. 18.

¹⁵⁸ Kommissionens riktlinjer C(2025) 5052 final, s. 1; ”AI-Act”, Europeiska kommissionen.

¹⁵⁹ Kommissionens riktlinjer C(2025) 5052 final, s. 1; ”AI-Act”, Europeiska kommissionen.

¹⁶⁰ Se avsnitt 2 ”Krav på AI-system med hög risk” i AI-förordningen.

¹⁶¹ Se artikel 9–12 AI-förordningen.

¹⁶² Se artikel 13–14 AI-förordningen.

¹⁶³ Se artikel 15 AI-förordningen.

samtliga obligatoriska krav gäller att de ska tillämpas på ett proportionerligt sätt med hänsyn till den tekniska utvecklingen.¹⁶⁴

Den andra kategorin varierar beroende på vilken funktion aktören har inom regelverkets struktur. Dessa särskilda skyldigheter riktats främst mot leverantörer och innebär bland annat krav på kvalitetsstyrningssystem, bevarande av dokumentation och samarbete med behöriga myndigheter.¹⁶⁵ Skyldigheterna fokuserar främst på teknisk funktion och tillförlitlighet, snarare än på ett direkt skydd mot risker för hälsa, säkerhet och grundläggande rättigheter.¹⁶⁶

För tillhandahållare, vilka är mer relevanta i denna kontext enligt tidigare resonemang¹⁶⁷, finns dock två bestämmelser inom denna kategori som anses särskilt centrala. Artikel 26 i AI-förordningen reglerar tillhandahållarens skyldigheter. Bestämmelsen innebär bland annat att lämpliga tekniska och organisatoriska åtgärder ska vidtas samt att personer med ansvar för mänsklig kontroll ska ha tillräcklig kompetens och AI-kunnighet.¹⁶⁸ I anslutning till detta innehåller bestämmelsen även särskilda regler om användning av högrisk-AI på arbetsplatsen, vilket kräver att arbetsgivaren ska informera arbetstagarrepresentanter och berörda arbetstagare om att systemet används.¹⁶⁹ Detta informationskrav kompletterar befintliga regler och påverkar inte arbetsgivares skyldigheter att informera eller samråda med arbetstagare enligt annan unionsrätt eller nationell rätt.¹⁷⁰

Därutöver ska tillhandahållaren genomföra en konsekvensbedömning innan systemet tar i bruk, enligt artikel 27. Syftet med bedömningen är att identifiera och analysera vilka risker användningen kan medföra för enskildas grundläggande rättigheter samt vilka åtgärder som behöver vidtas för att begränsa dessa risker.¹⁷¹ Det framhålls även att det är tillhandahållaren, det vill säga arbetsgivaren, som bär det avgörande ansvaret för att säkerställa att de grundläggande rättigheterna iakttas.¹⁷²

I litteraturen har det ifrågasatts hur effektiv den ovan redovisade regleringen kommer att vara i praktiken. Även om nya skyldigheter införs, överläts riskidentifiering och bedömningen av vad som är en acceptabel risk i stor utsträckning till leverantörerna själva. Detta kan leda till en annan riskvärdering än den hos dem som faktiskt berörs och bär konsekvenserna. Möjligheten till

¹⁶⁴ Skäl 64 i AI-förordningen.

¹⁶⁵ Artikel 16–22 AI-förordningen.

¹⁶⁶ Nathalie A. Smuha och Karen Yeung, ”The European Union’s AI Act: Beyond Motherhood and Apple Pie?”, i: Nathalie A. Smuha (red.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press (2025), s. 241.

¹⁶⁷ Se avsnitt 2.2.1.

¹⁶⁸ Skäl 91 i AI-förordningen.

¹⁶⁹ Artikel 26.7 AI-förordningen.

¹⁷⁰ Skäl 92 i AI-förordningen.

¹⁷¹ Skäl 96 i AI-förordningen.

¹⁷² Skäl 93 i AI-förordningen.

självbedömning anses därmed kunna försvaga den rättssäkerhet som modellen är avsedd att skapa. Därutöver anses det finnas en risk att konsekvensbedömningar i praktiken reduceras till formella dokumentationsåtgärder snarare än ett effektivt skydd för grundläggande rättigheter.¹⁷³

3.3 Plattformdirektivet

3.3.1 Syfte och tillämpningsområde

Plattformdirektivet syftar till att förbättra arbetsvillkoren och stärka skyddet för personuppgifter vid plattformarbete. Målen är nära sammanlänkade och ömsesidigt förstärkande, vilket innebär att dataskydd och arbetsrättsligt skydd ska tillmätas likvärdig betydelse.¹⁷⁴ Detta återspeglas även i direktivets rättsliga grund, då det har antagits med stöd av artiklarna 153.2 b och 153.1 b FEUF om arbetsvillkor samt artikel 16.2 FEUF om skydd för personuppgifter.¹⁷⁵ Direktivet har sin grund i den snabba digitaliseringen av arbetslivet och den ökade användningen av algoritmbaserade system för att organisera, övervaka och styra arbete genom digitala plattformar. Plattformdirektivet är ett svar på dessa utmaningar och syftar till att säkerställa ett grundläggande skydd när plattformarbete leds och kontrolleras genom automatiserade system.¹⁷⁶

Plattformdirektivet kompletterar dataskyddsförordningen genom att införa mer specifika regler för behandling av personuppgifter i samband med plattformarbete. Medan dataskyddsförordningen anger den allmänna ramen för dataskydd, innehåller direktivet särskilda bestämmelser om användningen av automatiserade övervaknings- och beslutssystem i arbetsrelaterade sammanhang.¹⁷⁷

Enligt artikel 1.1 i plattformsdirektivet ska syftet uppnås genom tre typer av åtgärder: att underlätta fastställandet av korrekt sysselsättningsstatus, att främja transparens, rättvisa och mänsklig kontroll vid algoritmisk verksamhetsledning samt att öka transparensen kring plattformarbete.¹⁷⁸ I denna framställning ligger fokus på den andra delen, det vill säga regleringen av algoritmisk verksamhetsledning. Det framhålls att det inom detta område finns behov av ytterligare rättigheter för personer som utför plattformarbete, för att motverka obalanser i en algoritmiskt styrd arbetsmiljö, stärka rättssäkerheten och förbättra arbetsvillkoren.¹⁷⁹

¹⁷³ Smuha och Yeung, ”The European Union’s AI Act: Beyond Motherhood and Apple Pie?”, s. 241 f.

¹⁷⁴ Artikel 1.1 plattformsdirektivet; Skäl 16 i plattformsdirektivet.

¹⁷⁵ Skäl 16 i plattformsdirektivet.

¹⁷⁶ Artikel 1.1 plattformsdirektivet; Skäl 4 i plattformsdirektivet.

¹⁷⁷ Skäl 38 i plattformsdirektivet.

¹⁷⁸ Se artikel 1.1 (a-c) plattformsdirektivet.

¹⁷⁹ Skäl 14 i plattformsdirektivet.

Vidare framgår av plattformsdirektivets artikel 1.2 och 1.3 att regelverket är tillämpligt på personer som utför plattformsarbete inom unionen och som har, eller kan anses ha, ett anställningsförhållande enligt nationell rätt. Direktivet gäller för digitala arbetsplattformar som organiserar arbete som utförs inom EU, oavsett var plattformen är etablerad eller vilken lag som annars skulle vara tillämplig.¹⁸⁰

Tillämpningsområdet konkretiseras genom definitionerna i artikel 2. En digital arbetsplattform är en aktör som tillhandahåller en tjänst på distans där organiseringen av arbete mot ersättning utgör en central del av verksamheten. Plattformen använder automatiserade övervaknings- eller beslutssystem i denna organisering. Det som särskiljer sådana plattformar från andra on-lineaktörer är att arbetet organiseras och kontrolleras genom system som behandlar personuppgifter och fattar eller stödjer beslut som påverkar arbetsvillkor.¹⁸¹ Med plattformsarbete avses arbete som organiseras genom en sådan digital plattform och som utförs av en enskild person på grundval av ett avtalsförhållande med plattformen eller en intermediär.¹⁸² Direktivet träffar således situationer där arbete inom unionen organiseras och styrs genom digitala och algoritmiska system.

3.3.2 Reglering av algoritmisk verksamhetsledning

Kapitel III reglerar algoritmisk verksamhetsledning och utgör en av dess mest centrala delarna i direktivet. Bestämmelserna tar sikte på användningen av automatiserade övervaknings- och beslutssystem som, genom algoritmer, övertar funktioner som tidigare utförts av en mänsklig företrädare för arbetsgivaren. Enligt skälen till direktivet är denna form av teknikanvändning särskilt utbredd inom digitala arbetsplattformar.¹⁸³ Denna reglering av algoritmisk verksamhetsledning anses i flera avseenden rättsutvecklande. Den omfattar inte bara arbetstagare utan även uppdragstagare samt kännetecknas av en förhållandevis långtgående materiell reglering.¹⁸⁴

3.3.2.1 *Förbjudna system*

Inledningsvis i kapitel III uppställs särskilda förbud mot viss behandling av personuppgifter utan några uttryckliga undantag. Artikel 7 i plattformsdirektivet innebär att uppgifter om en persons emotionella eller psykologiska tillstånd, privata samtal och biometriska uppgifter för identifiering inte får behandlas. Förbudet avser även behandling av känsliga personuppgifter, såsom uppgifter om ras eller etniskt ursprung, hälsotillstånd och fackligt medlemskap. Vidare får personuppgifter inte samlas in när en person inte erbjuder eller utför plattformsarbete och inte heller behandlas i syfte att förutse utövandet av grundläggande rättigheter, såsom föreningsfrihet eller rätt till

¹⁸⁰ Skäl 17–18 i plattformsdirektivet.

¹⁸¹ Artikel 2 (a) plattformsdirektivet; skäl 19 i plattformsdirektivet.

¹⁸² Artikel 2 (b) plattformsdirektivet.

¹⁸³ Skäl 8 i plattformsdirektivet.

¹⁸⁴ SOU 2026:3 s. 177.

kollektiva åtgärder.¹⁸⁵ Förbuden gäller för alla som utför plattformsarbete och är tillämpliga redan från rekryterings- eller urvalsskedet.¹⁸⁶

3.3.2.2 *Transparens, tillsyn och mänsklig granskning*

Utöver detta är bestämmelserna om algoritmisk arbetsledning i plattformsdirektivet uppbyggda i tre steg som tillsammans bildar en sammanhållen struktur för hur algoritmisk arbetsledning och övervakning av plattformsarbete får ske.¹⁸⁷

För det första uppställs i artikel 9 krav på transparens kring användningen av automatiserade övervaknings- och beslutssystem. Informationen ska bland annat omfatta om sådana system används, vilka uppgifter och aktiviteter som övervakas eller utvärderas, syftet med övervakningen samt hur personuppgifterna behandlas och till vilka mottagare de kan överföras. Dessa upplysningar ska lämnas till personer som utför plattformsarbete, representanter för plattformsarbetstagare samt, på begäran, nationella behöriga myndigheter.¹⁸⁸ Informationen ska lämnas i ett tydligt och lättillgängligt format och ska vara koncis, enkel och begriplig i den mån systemen och deras funktioner direkt påverkar personen eller dennes arbetsvillkor.¹⁸⁹

För det andra uppställs i artikel 10 krav på tillsyn och regelbunden utvärdering av automatiserade övervaknings- och beslutssystem. Digitala arbetsplattformar ska, med deltagande av arbetstagarrepresentanter, granska hur beslut som fattas eller stöds av sådana system påverkar personer som utför plattformsarbete, särskilt i fråga om arbetsvillkor och likabehandling. Om utvärderingen visar risk för diskriminering eller andra rättighetsintrång ska plattformen vidta nödvändiga åtgärder, exempelvis ändra eller upphöra med systemets användning.¹⁹⁰ Utvärderingen syftar dock främst till ett proaktivt arbete för att förebygga diskriminerande eller rättighetskränkande beslut.¹⁹¹

För det tredje uppställs i artikel 11 krav på mänsklig granskning av beslut. Till skillnad från de två föregående stegen avser denna bestämmelse endast beslut som fattas eller stöds av automatiserade beslutssystem och inte automatiserade övervakningssystem. Personer som utför plattformsarbete har rätt att utan oskäligt dröjsmål få en förklaring till sådana beslut samt möjlighet att diskutera beslutet med en utsedd kontaktperson hos plattformen.¹⁹² Särskilt ingripande beslut, exempelvis om avstängning av konto eller vägran att betala för utfört arbete, ska motiveras skriftligt.¹⁹³ Den som berörs har också rätt att

¹⁸⁵ Artikel 7.1 (a-f) plattformsdirektivet.

¹⁸⁶ Artikel 7.2 plattformsdirektivet.

¹⁸⁷ Se uppdelningen i SOU 2026:3 s. 178.

¹⁸⁸ Artikel 9.1 plattformsdirektivet.

¹⁸⁹ Artikel 9.2 plattformsdirektivet; Skäl 44 i plattformsdirektivet.

¹⁹⁰ Artikel 10.1–4 plattformsdirektivet.

¹⁹¹ SOU 2026:3 s. 222.

¹⁹² Artikel 11.1 plattformsdirektivet.

¹⁹³ Artikel 11.2 plattformsdirektivet.

begära omprövning av beslutet. Kränker beslutet dennes rättigheter ska plattformen rätta beslutet eller vidta andra åtgärder, exempelvis ändra eller upphöra med användningen av det automatiserade systemet.¹⁹⁴ I de inledande skälen till förordningen förtydligas att de rättigheter som avses i detta sammanhang bland annat omfattar arbetstagarrättigheter, rätten till icke-diskriminering samt rätten till skydd för den enskildes personuppgifter.¹⁹⁵

3.3.2.3 Övriga krav

Utöver de förbjudna systemen och den trestegsreglering som beskrivits ovan uppställer kapitel III även vissa ytterligare krav.

Av artikel 10.5 i plattformsdirektivet framgår att vissa särskilt ingripande beslut ska fattas av en människa. Detta gäller bland annat beslut om att begränsa, tillfälligt avbryta eller avsluta en persons konto eller avtalsförhållande, liksom andra beslut med motsvarande negativa konsekvenser för den som utför plattformarbete.¹⁹⁶ Vidare uppställs i artikel 8 krav på en dataskyddsrelaterad konsekvensbedömning. Eftersom behandling av personuppgifter genom automatiserade övervaknings- och beslutssystem typiskt sett innebär en hög risk för enskildas rättigheter ska digitala arbetsplattformar genomföra en sådan bedömning enligt artikel 35 GDPR. Vid genomförandet ska synpunkter inhämtas från personer som utför plattformarbete och deras representanter.¹⁹⁷

Därutöver återfinns, i kapitel VI, bestämmelser som syftar till att främja kollektivförhandlingar inom plattformarbete. Plattformdirektivets artikel 25 innebär att medlemsstaterna ska vidta åtgärder för att stärka arbetsmarknadens parter och underlätta utövandet av rätten till kollektivförhandlingar, särskilt i frågor som rör plattformarbetares rättigheter vid algoritmisk arbetsledning.¹⁹⁸

3.4 Diskussion

Dataskyddsförordningen utgör den centrala rättsliga ramen för behandling av personuppgifter inom EU och är därmed en viktig utgångspunkt i bedömningen av algoritmisk övervakning och arbetsledning i arbetslivet.

Bedömningen av om en personuppgiftsbehandling är tillåten enligt GDPR sker genom en samlad prövning av flera bestämmelser. Först måste de grundläggande principerna i artikel 5 GDPR vara uppfyllda, såsom laglighet, ändamålsbegränsning, dataminimering och transparens. Därefter krävs att behandlingen har stöd i någon av de rättsliga grunderna i artikel 6 GDPR. Slutligen ska behandlingen utformas så att den registrerades rättigheter enligt artiklarna

¹⁹⁴ Artikel 11.3 plattformsdirektivet.

¹⁹⁵ Skäl 49 i plattformsdirektivet.

¹⁹⁶ Artikel 10.5 plattformsdirektivet.

¹⁹⁷ Artikel 8 plattformsdirektivet.

¹⁹⁸ Artikel 35 plattformsdirektivet.

12–21 GDPR respekteras, exempelvis rätten till information, tillgång, rättelse, radering och invändning. Tillsammans anger dessa bestämmelser ramar för hur och när personuppgifter får behandlas.

GDPR innehåller även särskilda bestämmelser som tar sikte på den tekniska utvecklingen och användningen av algoritmiska system. I riktlinjer från Artikel 29-gruppen framhålls att artikel 22 GDPR har tillkommit mot bakgrund av tekniska framsteg inom analys av stora datamängder, artificiell intelligens och maskininlärning, vilka kan få betydande konsekvenser för enskildas rättigheter och friheter.¹⁹⁹ När artikel 22 GDPR är tillämplig är utgångspunkten restriktiv, eftersom den registrerade har som huvudregel rätt att inte bli föremål för helt automatiserade beslut. Undantagen är dessutom snävt utformade samt förenade med förstärkta skyddsåtgärder.

Samtidigt är tillämpningsområdet begränsat. Artikel 22 GDPR omfattar endast beslut som fattas helt automatiserat, vilket innebär att beslut med mänsklig medverkan faller utanför, även om automatiserad behandling eller profilering har använts som stöd. En betydande del av den algoritmiska arbetsledning och övervakning som förekommer i arbetslivet träffas därför inte av bestämmelsen.

GDPR fångar därmed endast delvis den utveckling som sker inom algoritmisk arbetsledning. I praktiken avgörs därför tillåtligheten i stor utsträckning genom tillämpningen av de allmänna principerna och rättsliga grunderna i artiklarna 5 och 6 GDPR. Krav på laglighet, transparens och proportionalitet blir då centrala. Inom arbetsrätten anses samtycke normalt inte vara en lämplig rättslig grund, eftersom anställningsförhållandet präglas av en maktobalans. Arbetsgivaren måste därför i regel stödja behandlingen på annan grund och visa att övervakningen är nödvändig och proportionerlig i förhållande till sitt syfte. Krav på konsekvensbedömning kan även bli aktuellt även när artikel 22 inte är tillämplig, eftersom behandlingen i många fall kan antas innebära en hög risk för enskildas rättigheter och friheter.

Parallellt med GDPR-regleringen, etablerar AI-förordningen ett unionsgemensamt och riskbaserat regelverk för utveckling och användning av artificiell intelligens. Genom en kategorisering av AI-system i förbjudna, högrisk-, begränsad risk- och lågrisksystem knys olika rättsliga krav till den potentiella påverkan tekniken kan ha på hälsa, säkerhet och grundläggande rättigheter. Särskilt i arbetslivet aktualiseras regleringen genom att system för rekrytering, arbetsledning och övervakning i många fall klassificeras som högrisk och därmed omfattas av krav på riskhantering, transparens, mänsklig kontroll och konsekvensbedömning. Regelverket riktar sig i första hand mot leverantörer men ålägger även tillhandahållare, såsom arbetsgivare, självständiga

¹⁹⁹ Artikel 29-gruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/67*, s. 5.

skyldigheter, samtidigt som det ska tillämpas parallellt med befintlig EU-rätt och nationell arbetsrätt.

Det kan konstateras att endast ett begränsat antal övervakningsåtgärder är uttryckligen förbjudna enligt AI-förordningen. Förbuden tar sikte på särskilt ingripande användningsområden, såsom vissa former av känsligenkänning eller biometrisk kategorisering. Merparten av system för övervakning och arbetsledning regleras därför i stället inom ramen för högriskkategorin. Detta innebär att stora delar av algoritmisk övervakning och arbetsledning i grunden är tillåtna, förutsatt att de uppställda kraven uppfylls. Regleringen begränsar således vissa extrema användningar, men etablerar inte något generellt förbud mot AI-baserad kontroll i arbetslivet.

Mot denna bakgrund kan det även noteras att en betydande del av det praktiska ansvaret enligt AI-förordningen i arbetslivet i realiteten faller på arbetsgivaren i rollen som tillhandahållare. Det gäller särskilt skyldigheten att genomföra konsekvensbedömningar och säkerställa att användningen av systemet inte leder till kränkningar av grundläggande rättigheter. Samtidigt är arbetsgivaren den strukturellt starkare parten i anställningsförhållandet, vilket gör det problematiskt att denne ges en avgörande roll i bedömningen av rättighetsintrång. Regleringen beaktar därav endast i begränsad utsträckning den maktasymmetri som präglar relationen. Denna svaghet har även uppmärksamats i doktrin. Det har i detta sammanhang framhållits att regleringen i begränsad utsträckning beaktar den grundläggande maktobalansen i anställningsförhållandet och att den kollektiva dimensionen, i form av sektorsspecifik reglering och stärkt facklig medverkan, i stort sett saknas.²⁰⁰

Vidare etablerar plattformsdirektivet en tydlig och konkret reglering av algoritmisk verksamhetsledning. Regleringen bygger på en kombination av förbud mot vissa typer av databehandling, krav på transparens kring automatiserade system samt mekanismer för tillsyn och mänsklig kontroll. Därutöver innehåller direktivet kompletterande bestämmelser, exempelvis krav på konsekvensbedömning av dataskyddsrisker och regler som syftar till att stärka kollektivförhandlingar.

Regleringen innebär i flera avseenden ett mer arbetslivsinriktat skydd än vad som följer av GDPR och AI-förordningen. Direktivet uppmärksammar exempelvis den maktobalans som kan finnas mellan plattform och arbetstagare genom att uttryckligen främja kollektivförhandlingar. Därutöver ges automatiserad övervakning och kontroll en framträdande plats i regleringen, genom särskilda bestämmelser om transparens, tillsyn och begränsningar i hur sådana system får användas och hur plattformsarbetarna ska skyddas.

²⁰⁰ Se exempelvis Yusifli, *Labour Rights and the EU Artificial Intelligence Act*, s. 18–19; Adams-Prassl, *Regulating Algorithms at Work: Lessons for a ‘European Approach to Artificial Intelligence’*, s. 20; EPRS, *Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the future of work*, s. III.

Regleringen omfattar dessutom inte enbart helt automatiserade beslut, utan även situationer där automatiserade system används som stöd i arbetsledningen, vilket skiljer sig från regleringen i GDPR.

Det framhålls i plattformsdirektivets ingress att ytterligare reglering behövs för att skydda arbetstagare och förbättra arbetsvillkoren vid algoritmisk verksamhetsledning.²⁰¹ Detta tyder på att den befintliga EU-rättsliga regleringen inte anses tillräcklig för att hantera de risker som sådana system kan medföra. Samtidigt är direktivets tillämpningsområde begränsat till plattformsarbete, vilket innebär att det förstärkta skyddet endast gäller en begränsad arbetstargrups. Majoriteten av EU:s arbetskraft omfattas därmed inte av motsvarande arbetsrättsliga skydd mot algoritmisk övervakning och styrning, trots att sådana system även förekommer i mer traditionella anställningsförhållanden.²⁰² Direktivet adresserar därmed endast en del av den bredare utvecklingen mot digital och algoritmisk arbetsledning i arbetslivet.

Sammantaget ger EU-rätten genom GDPR, AI-förordningen och plattformsdirektivet en grundläggande skyddsnivå vid användning av algoritmiska system i arbetslivet. Regelverken behandlar dock olika aspekter av problematiken och har skilda tillämpningsområden, vilket innebär att de tillsammans inte bildar en helt sammanhängande och arbetsplatsspecifik regleringsram. Skyddet mot algoritmisk övervakning och arbetsledning framstår därför i viss mån som fragmenterat, där vissa arbetstargrupper, särskilt plattformsarbetare, omfattas av mer detaljerade regler än övriga arbetstagare.

²⁰¹ Se skäl 14 i plattformsdirektivet.

²⁰² EPRS, *Digitalisation, Artificial Intelligence and Algorithmic Management in the Workplace: Shaping the future of work*, s. III.

4 Svensk rätt

4.1 Arbetsgivarens arbetsledningsrätt och kontrollbefogenheter

En central utgångspunkt för arbetsgivarens möjligheter att kontrollera, övervaka och leda arbetet är den så kallade arbetsledningsrätten, vilken ger ett vidsträckt utrymme att organisera och styra verksamheten. Denna rätt har vuxit fram ur ett historiskt sammanhang där relationen mellan arbetsgivare och arbetstagare länge präglats av en tydlig maktobalans. I äldre rättsliga och ekonomiska strukturer hade arbetsgivaren en långtgående frihet att disponera över arbetstagarens arbetskraft, som successivt blev en del av den moderna arbetsrätten. Genom decemberkompromissen 1906, där det i kollektivavtalen på LO/SAF-området fastslogs att arbetsgivaren äger rätt att leda och fördela arbetet, kom arbetsledningsrätten att etableras som en grundläggande princip.²⁰³ Detta utvecklades och bekräftades i tidig praxis från Arbetsdomstolen, där arbetsgivaren inom ramen för arbetsledningsrätten ansågs kunna inhämta uppgifter om arbetsprestationer i den mån det krävdes för att fastställa lön. Någon generell rätt till sådan kontroll erkändes dock inte, utan en avvägning skulle göras mellan arbetsgivarens intresse av korrekt lönesättning och arbetstagarens rätt till integritet.²⁰⁴

Principen har dock på senare tid utvecklats och är inte längre lika långtgående som under början av 1900-talet. Utvecklingen har successivt gått mot att begränsa arbetsgivarens arbetsledningsrätt genom lagstiftning och kollektivavtal, exempelvis genom lagen (1976:580) om medbestämmande i arbetslivet (MBL) och lagen (1982:80) om anställningsskydd (LAS).²⁰⁵

Även ur ett internationellt perspektiv förstås arbetsledningsrätten som ett uttryck för den asymmetri som präglar anställningsförhållandet. Arbetsgivaren tillerkänns denna rätt för att möjliggöra anpassning av arbetets utförande utan att varje förändring kräver arbetstagarens samtycke. Detta särskiljer anställningsavtalet från andra avtalstyper och bidrar till en mer flexibel och effektiv organisering av verksamheten.²⁰⁶

²⁰³ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 201 f.; Mia Rönnmar, *Arbetsledningsrätt och arbetsskyldighet: en kooperativ studie av kvalitativ flexibilitet i svensk, engelsk och tysk kontext* (Juristförlaget i Lund, 2004) s. 45.

²⁰⁴ AD 1934 nr 38; Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 303.

²⁰⁵ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 201 f.; Rönnmar, *Arbetsledningsrätt och arbetsskyldighet: en kooperativ studie av kvalitativ flexibilitet i svensk, engelsk och tysk kontext*, s. 45.

²⁰⁶ Simon Deakin och Frank Wilkinson, "Labour law and economic theory: a reappraisal", i: Hugh Collins, Paul Davies och Roger Rideout (red.), *Legal Regulation of the Employment Relation*, Kluwer Law International (2000), s. 47.

I dag utgör arbetsledningsrätten gällande rätt i Sverige, trots att den inte är uttryckligen lagreglerad.²⁰⁷ Principen har ställningen av en allmän rättsgrund-sats, anses gälla generellt i alla anställningsförhållanden och har i doktrin be-skrivits som en dold klausul i kollektivavtalet.²⁰⁸ Arbetsdomstolen har genom sin praxis utvidgat kollektivavtalets kompetensområde till att även omfatta åtgärder som rör den enskilda arbetstagarens integritet, utan krav på särskilt medgivande från arbetstagaren. Arbetstagaren blir därmed bunden av sådana åtgärder, förutsatt att en intresseavvägning utfaller till förmån för de intressen som talar för åtgärdens genomförande.²⁰⁹ Därtill är arbetsgivaren enligt MBL skyldig att förhandla med berörd arbetstagarorganisation innan beslut fattas i frågor som rör verksamheten eller arbetsledningen. Hur denna förhandlings-skyldighet ska fullgöras beror på om arbetsgivaren är bunden av kollektivav-tal eller inte.²¹⁰

Inom ramen för arbetsledningsrätten kan arbetsgivaren ensidigt fatta beslut om hur arbetet ska organiseras och utföras, vilket även innefattar olika former av kontrollåtgärder.²¹¹ Dessa tar sig särskilt uttryck i arbetsgivarens möjlighet att följa upp arbetstagarens prestationer, vilket i praktiken kan ske genom olika former av övervakning. Arbetsgivaren kan därigenom kräva att arbets-tagaren underkastar sig åtgärder som innebär ett intrång i den personliga in-tegритeten, särskilt när åtgärderna förutsätter arbetstagarens medverkan. En sådan skyldighet kan utöver arbetsledningsrätten även följa av anställnings-avtal eller kollektivavtal. I praktiken innebär detta att arbetsgivaren ges ett betydande utrymme att införa olika former av integritetskänsliga åtgärder, såsom kontroll- och övervakningsåtgärder, i verksamheten.²¹²

Även om arbetsledningsrätten ger arbetsgivaren ett vidsträckt utrymme att leda och organisera arbetet, är den inte obegränsad. Den utgör en utfyllande rättsgrund som endast kan utövas inom de ramar som följer av lag, kollektiv-avtal och individuella anställningsavtal. Även åtgärder som har stöd i dessa rättsgrunder får inte strida mot gällande rätt eller god sed på arbetsmark-naden.²¹³ Detta innebär att arbetsgivarens handlingsutrymme är föremål för flera rättsliga begränsningar, vilka behandlas i det följande.

²⁰⁷ AD 2023 nr 75; AD 2013 nr 19.

²⁰⁸ Se AD 1932 nr 100; AD 1934 nr 179; Källström, Malmberg och Johansson, *Anställ-ningsförhållandet: en inledning till den individuella arbetsrätten*, s. 73; Rönmar, *Arbetsled-ningsrätt och arbetskyldighet: en kooperativ studie av kvalitativ flexibilitet i svensk, engelsk och tysk kontext*, s. 45.

²⁰⁹ AD 1997 nr. 29; Annamaria Westregård, *Integritetsfrågor i arbetslivet* (Juristförlaget i Lund, 2002), s. 31-32.

²¹⁰ Se 10-13 §§ MBL.

²¹¹ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 210.

²¹² Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 18.

²¹³ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 212; Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 18.

4.2 Lagstadgade begränsningar av arbetsledningsrätten

4.2.1 Ett fragmenterat regelverk

Inom svensk rätt finns ett flertal lagregler som begränsar möjligheten att vidta integritetskänsliga åtgärder i arbetslivet. Dessa regler är emellertid inte samlade i en enhetlig lagstiftning, utan återfinns utspridda i olika delar av rättssystemet, vilket försvårar överskådligheten.²¹⁴ Frågan om ett stärkt och mer sammanhållet integritetsskydd i arbetslivet har utretts vid upprepade tillfällen, där behovet av en särskild lagstiftning har framhållits. Någon sådan lag har dock inte införts.²¹⁵ Trots omfattande utredningsarbete saknas således alltså en sammanhållen lagstiftning till skydd för arbetstagares personliga integritet. Bedömningen av om en integritetskänslig åtgärd är tillåten får i stället göras med utgångspunkt i ett flertal nationella och internationella rättskällor.²¹⁶

De lagbestämmelser som en integritetskänslig åtgärd i arbetslivet främst kan aktualisera återfinns i dataskyddsregleringen, Europakonventionen, kamera-bevakningslagen (2018:1200) samt i 4 kap. brottsbalken (1962:700). För of-fentligt anställda tillkommer därutöver det grundlagsskydd som gäller mot integritetskänsliga åtgärder från det allmänna även åberopas när staten upp-träder som arbetsgivare.²¹⁷ Dessa regelverk behandlas därför närmare i det följande.

4.2.2 Konstitutionella begränsningar

Beträffande rättighetsskyddet enligt Europakonventionen och regeringsfor-men hänvisas till kapitel 2 i denna framställning.²¹⁸ Som där konstaterats har Europakonventionen en stark ställning i svensk rätt och lag får inte meddelas i strid med konventionen enligt 2 kap. 19 § RF. Därutöver gäller konventionen som svensk lag genom lag (1994:1219) om den europeiska konventionen an-gående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Genom denna konventionslag tydliggörs konventionens ställning som rätts-källa i svensk rätt.²¹⁹ Europakonventionen och regeringsformen utgör därmed

²¹⁴ Westregård, *Integritetsfrågor i arbetslivet*, s. 35.

²¹⁵ SOU 2002:18 *Personlig integritet i arbetslivet*, Klimat- och näringslivsdepartementet; SOU 2009:44 *Integritetsskydd i arbetslivet*, Arbetsmarknadsdepartementet; SOU 2017:52 *Så stärker vi den personliga integriteten*, Justitiedepartementet.

²¹⁶ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 15 f.

²¹⁷ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 18.

²¹⁸ Se särskilt kapitel 2.1 och 2.4 i denna redogörelse.

²¹⁹ Carl Henrik Ehrenkrona, lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, inledande kommentar till lagen, Karnov (JUNO).

centrala nationella begränsningar av arbetsgivarens arbetsledningsrätt och ska beaktas vid bedömningen av integritetskänsliga åtgärder i arbetslivet.

I svensk praxis har det konstaterats att artikel 8 EKMR, i vissa fall, tillåter kontrollåtgärder såsom drogtestning i arbetslivet. Arbetsdomstolen har i flera avgöranden uttalat att sådan testning som utgångspunkt är förenlig med konventionen, men att den under vissa särskilda omständigheter kan stå i strid med artikel 8 EKMR och såldes även strida mot svensk rätt.²²⁰

Vidare har även JO uttalat sig i ett praktiskt ärende förhållande till rättighetsregleringen i svensk rätt, vilket tidigare kortfattat berörts.²²¹ I huvudsak avsåg ärendet Södertälje kommuns rutin att, genom ett externt företag, genomföra manuella sökningar i databaser med offentliga uppgifter från domstolar och myndigheter. Syftet med kontrollerna var att klarlägga om anställda hade dömts för vissa brott. Kontrollerna skedde löpande under anställningstiden och omfattade flera brottstyper. De anställda informerades om att kontrollerna skedde, men saknade möjlighet att påverka vilka uppgifter som lämnades ut eller att kontrollera deras aktualitet och riktighet.²²²

JO fann att såväl kontroller av anställda som av slutkandidater i rekryteringsprocesser var olagliga och stred mot både 2 kap. 6 § RF och artikel 8 EKMR. Kontrollerna bedömdes utgöra ett betydande intrång i den personliga integriteten, då de innebar en systematisk övervakning och kartläggning av enskildas personliga förhållanden. De genomfördes utan samtycke och saknade nödvändigt lagstöd. Vid bedömningen fäste JO särskild vikt vid att kontrollerna skedde kontinuerligt och i stor omfattning, vilket ansågs avgörande för att de skulle utgöra ett integritetsintrång. Detta oavsett vilken information som framkom av kontrollerna eller att de anställda hade informerats.²²³

4.2.3 Begränsningar enligt EU:s rättsakter

Utöver de konstitutionella begränsningarna av arbetsledningsrätten sätter även de EU-rättsakter som tidigare redogjorts för ramarna för arbetsgivarens handlingsutrymme.²²⁴ EU-rätten har företräde framför nationell rätt, vilket innebär att medlemsstaterna är skyldiga att följa de rättsakter som beslutas inom unionen. Dessa utgörs av förordningar, direktiv och beslut.²²⁵ Regelverk såsom GDPR, AI-förordningen och plattformsdirektivet utgör därmed en del av den svenska rättsordningen, vilket innebär att de bedömningar och

²²⁰ Se exempelvis AD 2001 nr 3; AD 2009 nr 36.

²²¹ Se kapitel 1.1 i denna framställning.

²²² JO:s beslut 19 oktober 2023, dnr 7143–2022, s. 1 ff.

²²³ JO:s beslut 19 oktober 2023, dnr 7143–2022, s. 10 ff.

²²⁴ Se redogörelsen i kap. 3.

²²⁵ Artikel 288 i fördraget om Europeiska unionens funktionssätt; ”EU:s lagar och regler”, Sveriges riksdag, 3 maj 2023, <https://www.riksdagen.se/sv/sa-fungerar-riksdagen/sa-fungerar-en-eu-lag-blir-till/eus-lagar-och-regler/>.

avvägningar som redogjorts för i kapitel 3 får direkt betydelse även på nationell nivå

GDPR kompletteras dessutom av nationella regler om behandling av personuppgifter. Den mest centrala lagen i detta sammanhang är lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, även kallad dataskyddslagen. Detta regelverk medför att GDPR:s tillämpningsområde, med vissa i lagen angivna undantag, utsträcks till att omfatta även sådana områden där EU saknar lagstiftningskompetens. Därutöver innehåller dataskyddslagen även vissa kompletterande bestämmelser i de delar där förordningen medger utrymme för nationell reglering.²²⁶ Exempelvis regleras tillsynsmyndighetens befogenheter och handläggning i 6 kap. och i 5 kap. återfinns bestämmelser som begränsar den registrerades rättigheter. Bland annat föreskrivs här att rätten till information enligt GDPR inte gäller i den utsträckning den personuppgiftsansvarige enligt lag eller annan författning är förhindrad att lämna ut uppgifterna.²²⁷

En annan nationell lag som kompletterar GDPR och som är särskilt relevant i frågor om övervakning i arbetslivet är kamerabevakningslagen (2018:1200).²²⁸ Kameraövervakning är tillåtet enligt lagen under förutsättning att den sker för att utföra en uppgift av allmänt intresse som följer av lag, annan författning, kollektivavtal eller beslut. Bevakningen måste vara nödvändig för att uppnå sitt syfte och får endast bedrivas om intresset av bevakningen väger tyngre än den enskildes intresse av att inte bli bevakad. Detta innebär att en proportionalitetsbedömning ska göras, där särskild hänsyn tas till bland annat bevakningens ändamål, hur den utförs och vilket område som omfattas. Därutöver ska den personuppgiftsansvarige dokumentera bedömningen och säkerställa att förutsättningarna för bevakningen är uppfyllda.²²⁹

Från och med den 1 april 2025 har tillståndsregleringen för kamerabevakning förändrats. Till skillnad från tidigare krävs inte längre tillstånd, utan i stället gäller ett regelverk som anger under vilka förutsättningar kamerabevakning får bedrivas.²³⁰ Denna förändring innebär att det formella förhandsgodkännandet har avskaffats, vilket i praktiken ger arbetsgivare ett vidare handlingsutrymme. Det ankommer numera på den enskilde arbetsgivaren att själv säkerställa att bevakningen är förenlig med gällande rätt, vilket innebär att handlingsutrymmet i detta avseende är mindre begränsat än tidigare.

²²⁶ Se 1 kap. 2–4 §§ dataskyddslagen; Frydinger m.fl., *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, s. 68 ff.

²²⁷ Se 5 kap. 1 § dataskyddslagen; Prop. 2017/18:105, s. 103.

²²⁸ Se 1 § kamerabevakningslagen.

²²⁹ Se 7–9 §§ kamerabevakningslagen.

²³⁰ SFS 2025:220; ”Regler för verksamheters kamerabevakning”, Integritetsskyddsmyndigheten, 27 april 2026, <https://www.imy.se/verksamhet/kamerabevakning/Regler-for-verksamheters-kamerabevakning/>.

För såväl kamerabevakningslagen, GDPR och dataskyddslagen är det Integritetsskyddsmyndigheten som är ansvarig tillsynsmyndighet.²³¹ Avseende kamerabevakning har Integritetsskyddsmyndigheten uttryckt att sådan bevakning i arbetslivet i vissa fall kan vara tillåten, exempelvis vid övervakning av riskfyllda arbetsmoment, i butiksmiljöer för att förebygga brott eller i särskilt utsatta utrymmen, under förutsättning att åtgärder vidtas för att begränsa personuppgiftsbehandlingen. Däremot har IMY betonat att kamerabevakning som används för att löpande kontrollera arbetstagares prestationer, liksom bevakning av privata utrymmen eller med ljudupptagning, som utgångspunkt inte tillåten.²³²

I ett beslut från Integritetsskyddsmyndigheten rörande H&M:s kamerabevakning framgår att tillåtligheten av kamerabevakning i arbetslivet avgörs genom en konkret intresseavvägning, med bakgrund i såväl GDPR som kamerabevakningslagen.²³³ Fallet rörde både yttre och inre säkerhetskameror samt processkameror. De yttre säkerhetskamerorna användes för att bevaka lastområden och parkeringsplatser, medan de inre säkerhetskamerorna övervakade accessvägar inne i fastigheten. Processkamerorna användes för att kontrollera den maskinella utrustningen och arbetsflödet. Därutöver kamerabevakades en gruppledares arbetsplats under fem nätter efter misstankar om stölder, brister i arbetet och obehörig åtkomst till information.²³⁴

I bedömningen av om rättslig grund förelåg framhöll IMY särskilt att integritetsintresset på en arbetsplats som utgångspunkt väger tungt, eftersom kamerabevakning kan göra det möjligt att följa och analysera anställdas arbetsmönster och beteenden. Beträffande säkerhetskamerorna betonades dock att bevakningen var begränsad till särskilda riskområden och inte omfattade fasta arbetsplatser. De inre säkerhetskamerorna ansågs nödvändiga för att förebygga brott och arbetsplatsolyckor, medan processkamerorna bedömdes nödvändiga för att motverka driftstörningar och hantera olyckor. IMY fäste även vikt vid att processkamerorna riktades mot maskinell utrustning och kompletterades med digital maskering för att begränsa exponeringen av personal. Mot denna bakgrund ansågs bevakningsintresset väga tyngre än integritetsintresset beträffande säkerhets- och processkamerorna.²³⁵ Därav kan det konstateras att bevakning som syftar till att förebygga brott eller olyckor kan godtas, förutsatt att den är proportionerlig och begränsad till vad som är nödvändigt.

²³¹ Se 2 § och 2 a § förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten; 3 § förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

²³² "Kamerabevakning av anställda", Integritetsskyddsmyndigheten, 28 mars 2025, <https://www.imy.se/verksamhet/kamerabevakning/personuppgiftsansvar-och-kamerabevakades-rattigheter/kamerabevakning-av-anstallda/>.

²³³ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021-771, s. 7 ff.

²³⁴ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021-771, s. 3.

²³⁵ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021-771, s. 9 ff.

Däremot ansåg IMY att det inte förelåg rättslig grund för den tillfälliga övervakningen i arbetsrummet. Även om H&M hade ett berättigat intresse av att utreda misstänkta oegentligheter och säkerhetsrisker på arbetsplatsen bedömde IMY att mindre integritetsingripande åtgärder inte hade prövats i tillräcklig utsträckning innan kamerabevakningen inleddes. Det framhölls särskilt att kamerabevakning som riktas mot anställda vid misstanke om missförhållanden är en särskilt integritetskänslig åtgärd och att höga krav därför ställs på nödvändighet och proportionalitet. Mot denna bakgrund ansågs bevakningen varken uppfylla nödvändighetskravet eller väga tyngre än arbetstagarnas integritetsintresse.²³⁶ Därav kan det konstateras att en integritetskänslig bevakning, såsom dold övervakning i kontrollsyfte, i regel anses otillåten och saknar rättslig grund.

Avseende informationsskyldigheten framgick att IMY ställde krav på tydlig och lättillgänglig information om kamerabevakningen i flera led. Kraven ansågs i huvudsak uppfylla beträffande säkerhets- och processkamerorna genom skyltning och kompletterande information. Dock förelåg vissa brister, såsom avsaknad av kontaktuppgifter till dataskyddsombudet, vilket innebar att skyldigheten inte var fullt uppfylld. Vidare konstaterades att den helt utblivna informationen om bevakningen i arbetsrummet innebar att behandlingen, utöver bristen på rättslig grund, även ansågs strida mot informationskraven enligt kamerabevakningslagen och GDPR.²³⁷

Till skillnad från vad som gäller i förhållande till GDPR saknas det i nuläget motsvarande kompletterande lagstiftning i svensk rätt för AI-förordningen och plattformsdirektivet. Dessa rättsakter är relativt nya och befinner sig fortfarande i genomförandefas i nationell rätt. Beträffande AI-förordningen har det i den statliga utredningen om nationella anpassningar föreslagits att kompletterande nationell reglering införs genom en ny lag och en ny förordning samt att ett system med flera marknadskontrollmyndigheter inrättas. Post- och telestyrelsen föreslår ha ett övergripande ansvar, medan ansvaret för högrisk-AI delas med Integritetsskyddsmyndigheten och Finansinspektionen. Utredningen föreslår att begreppen i den nationella kompletteringsregleringen ska ha samma innebörd och tolkas på samma sätt som i AI-förordningen, i syfte att säkerställa en enhetlig tillämpning mellan EU-rätt och svensk rätt. Hänvisningar till AI-förordningen i sanktionsbestämmelser ska vara statiska, medan övriga hänvisningar ska vara dynamiska och avse förordningens vid var tid gällande lydelse. Därutöver bedöms behov finnas av kompletterande bestämmelser, bland annat avseende sekretess och uppgiftsskyldighet.²³⁸

Avseende plattformsdirektivet krävs det, enligt den statliga utredningen om genomförandet av direktivet, att en ny lag om plattformsarbete införs för att möjliggöra implementeringen i svensk rätt. Detta motiveras av att

²³⁶ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021-771, s. 12 f.

²³⁷ Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021-771, s. 14 ff.

²³⁸ SOU 2025:101 s. 28 f. och s. 142 f.

motsvarande bestämmelser i stor utsträckning saknas i svensk rätt, vilket försvårar ett genomförande inom ramen för befintlig lagstiftning. Vidare föreslås att lagen ska vara tvingande, samtidigt som den i vissa delar ges en semidispositiv utformning.²³⁹ När det gäller algoritmisk arbetsledning föreslås en uppdelning mellan dataskyddsrelaterade regler och regler avseende arbetstagares inflytande. Härtill kommer att tillsynsansvaret delas upp, där Integritetsskyddsmyndigheten ansvarar för dataskyddsrelaterade frågor och Arbetsmiljöverket för övrig tillsyn.²⁴⁰ Utredningen belyser att definitionen av automatiserade övervakningssystem är bred och teknikneutral vilket innebär att den kan komma att omfatta såväl åtgärder som GPS-spårning, registrering av tangenttryckningar samt felfrekvenser.²⁴¹

Särskilt gällande användningen av GPS-spårning har Integritetsskyddsmyndigheten framhållit att sådan teknik innebär en närgången form av övervakning som kan medföra betydande integritetsrisker. Användningen måste därför vila på en rättslig grund, där privata arbetsgivare typiskt sett stödjer sig på en intresseavvägning, medan offentliga arbetsgivare ska kunna visa att behandlingen är nödvändig för en uppgift av allmänt intresse. För att vara tillåten krävs vidare att behandlingen har ett berättigat och sakligt motiverat ändamål, exempelvis kopplat till säkerhet, statistik eller resursfördelning och att den inte är mer ingripande än nödvändigt. IMY har samtidigt betonat att positioneringssystem som utgångspunkt inte får användas för att kontrollera arbetstagares arbetstid eller raster, annat än vid konkreta misstankar om missbruk. Särskild hänsyn ska även tas till arbetstagares privatliv, vilket innebär att övervakning utanför arbetstid som huvudregel inte är tillåten och att det i vissa fall bör finnas möjlighet att tillfälligt stänga av spårningen.²⁴²

Sammantaget kan det konstateras att implementeringen och anpassningen till EU-rätten i flera avseenden inte innebär några större förändringar av de begränsningar i arbetsledningsrätten som redan följer av tidigare gällande unionsrättsliga principer. Genomförandet medför varken ett mer långtgående skydd eller några andra bedömningar än de som redan följer av EU:s rättsakter. Regleringen innebär således inte något väsentligt utökat integritetsskydd i svensk rätt.

4.2.4 Straffrättsliga begränsningar

Utöver de begränsningar av arbetsledningsrätten som tidigare redogjorts för finns även nationella straffrättsliga regler som syftar till att skydda den personliga integriteten i arbetslivet. Dessa rättsregler kan begränsa arbetsgivarens handlingsutrymme genom att ange när vissa övervaknings- och

²³⁹ SOU 2026:3 s. 22.

²⁴⁰ SOU 2026:3 s. 25 ff.

²⁴¹ SOU 2026:3 s. 117 f.

²⁴² ”Kontroll och övervakning av anställda”, Integritetsskyddsmyndigheten, 6 maj 2025, <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/kontroll-och-overvakning-av-anstallda/>.

kontrollåtgärder är otillåtna. Dessa bestämmelser återfinns i 4 kap. brottsbalken (1962:700), BrB. De som främst kan aktualiseras i ett arbetsrättsligt sammanhang vid algoritmisk övervakning och arbetsledning avser brytande av post- och telehemlighet, olovlig avlyssning samt dataintrång.²⁴³ Brottet brytande av post- eller telehemlighet innebär att någon obehörigen tar del av ett meddelande som förmedlas via post eller elektronisk kommunikation, såsom telefoni eller datakommunikation.²⁴⁴ Skyddet gäller enligt 4 kap. 8 § BrB under själva överföringen och enligt 4 kap. 9 § BrB även efter att meddelandet nått mottagaren. I arbetslivet anses det normalt inte otillåtet att arbetsgivaren tar del av arbetsrelaterat material, exempelvis post som är adresserad till verksamheten. Däremot kan det vara otillåtet att ta del av material som är märkt som privat eller framstår som personligt riktat till arbetstagaren.²⁴⁵

Vidare är det enligt 4 kap. 9 a § BrB är det förbjudet att i hemlighet avlyssna eller spela in samtal som man själv inte deltar i. Bestämmelsen omfattar endast hemlig avlyssning, vilket innebär att inspelning eller avlyssning som sker öppet, exempelvis efter information eller med samtycke, i regel inte omfattas av förbudet.²⁴⁶ Avslutningsvis är det enligt bestämmelsen om dataintrång straffbart att obehörigen bereda sig tillgång till uppgifter i ett datasystem som är avsedda för automatiserad behandling, liksom att utan tillstånd ändra, utplåna, blockera eller registrera sådana uppgifter.²⁴⁷ Ur ett arbetsrättsligt perspektiv innebär straffbestämmelsen att arbetsgivaren i regel inte agerar otillåtet när denne tar del av arbetsrelaterad information i arbetsgivarens egna system. Däremot kan åtkomst till uppgifter av tydligt privat karaktär, exempelvis filer eller mappar märkta som privata, utgöra ett otillåtet förfarande. Rättsläget i denna del är dock inte fullt ut klarlagt genom praxis.²⁴⁸

4.3 God sed på arbetsmarknaden som begränsning av arbetsledningsrätten

Parallellt med kravet att en åtgärd ska vara förenlig med gällande rätt ska integritetskänsliga åtgärder i arbetslivet även vara förenliga med god sed på arbetsmarknaden. Arbetsdomstolen har vid flera tillfällen prövat innebörden av begreppet. I praxis utgår bedömningen vanligen från att en åtgärd måste strida mot allmän moral eller framstå som rättsstridig för att anses oförenlig med god sed.²⁴⁹ Möjligheterna att ifrågasätta arbetsledningsbeslut med

²⁴³ Se 4 kap. 8 §, 4 kap. 9 §, 4 kap. 9 a § och 4 kap. 9 c § BrB.

²⁴⁴ Se definitionen av begreppet ”elektroniskt kommunikationsnät” i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation.

²⁴⁵ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 25 f.

²⁴⁶ Prop. 1975/19 *Regeringens proposition om lagstiftning om skydd mot avlyssning*, s. 102 ff.; Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 26.

²⁴⁷ 4 kap. 9 c § BrB.

²⁴⁸ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen*, s. 26 f.

²⁴⁹ AD 1967 nr 26 och där gjorda uttryckliga hänvisningar.

hänvisning till god sed har därför traditionellt varit begränsade.²⁵⁰ Samtidigt innebär en utövning av arbetsledningsrätten i strid med god sed att åtgärden kan anses utgöra ett avtalsbrott i det enskilda anställningsförhållandet, vilket i sin tur kan medföra skadeståndsansvar för arbetsgivaren.²⁵¹

Av Arbetsdomstolens praxis kan det konstateras att innebörden av begreppet god sed varierar beroende på sammanhang och typen av arbetsledningsbeslut.²⁵² I denna framställning är dess tillämpning i relation till kontrollåtgärder särskilt relevant, varför dessa bedömningar står i fokus. Arbetsdomstolen har i detta sammanhang prövat tillåtligheten av exempelvis alkohol- och drogtest-er samt utpasseringskontroller. I dessa fall har bedömningen tagit sin utgångspunkt i en proportionalitetsprincip, där en intresseavvägning görs mellan arbetsgivarens behov av åtgärden och arbetstagarens intresse av skydd för den personliga integriteten.²⁵³ Arbetsdomstolen har därvid hänvisat till artikel 8 EKMR och uttalat att kravet på proportionalitet ligger i linje med konventionens bestämmelser.²⁵⁴ Detta synsätt får även stöd i doktrin, där det framhålls att arbetsledningsåtgärder som kränker rättigheter enligt EKMR kan anses strida mot god sed på arbetsmarknaden. Vidare betonas att sådana värde-öppna principer i anställningsförhållanden möjliggör en konventionskonform tolkning, vilket ger utrymme att låta Europakonventionens rättighetsskydd få genomslag i bedömningen.²⁵⁵

Kortfattat har följande utgångspunkter fastställts i praxis. Avseende utpasseringskontroller kan man utläsa att sådana åtgärder i princip anses tillåtna som ett medel för att motverka stölder, särskilt när de är begränsade till exempelvis kontroll av väskor eller fordon. Arbetsgivaren bör dock informera om konsekvenserna av en vägran och en enstaka vägran utgör som utgångspunkt inte saklig grund för uppsägning.²⁵⁶ Avseende alkohol- och drogtest-er framgår att sådana kontrollåtgärder i regel kan tillåtas efter en intresseavvägning, särskilt i verksamheter där kraven på säkerhet är höga eller där verksamheten är riskfylld.²⁵⁷ I dessa fall krävs inte heller någon konkret misstanke för att genomföra generella tester, och även riktade tester kan motiveras vid en låg misstankegrad.²⁵⁸ Samtidigt ställs krav på att arbetstagaren informeras om dess syfte och genomförande samt att det bör informeras om konsekvenserna av en vägran. Vidare tar bedömningen tar sin utgångspunkt i objektiva kriterier,

²⁵⁰ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 255.

²⁵¹ Se AD 1983 nr 46.

²⁵² Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 255 f.

²⁵³ Se exempelvis 1997 nr 29; AD 2001 nr 3; AD 2009 nr 36.

²⁵⁴ Se AD 2013 s. 19 under rubriken ”Sammanfattande bedömning av kollektivavtalets innebörd och frågan om kollektivavtalsbrott”.

²⁵⁵ Källström, Malmberg och Johansson, *Anställningsförhållandet: en inledning till den individuella arbetsrätten*, s. 65 f.

²⁵⁶ AD 1997 nr 29.

²⁵⁷ AD 1991 nr 45; AD 1998 nr 97; AD 2009 nr 36; AD 2013 nr 19.

²⁵⁸ AD 1998 nr 97; AD 2001 nr 3; AD 2009 nr 36.

således prövas frågan om det utgör en integritetskränkande åtgärd inte utifrån hur det upplevs av den enskilda arbetstagaren.²⁵⁹

Arbetsdomstolen i sin praxis har intagit en återhållsam hållning i frågor om arbetsgivarens rätt att vidta kontrollåtgärder. I stället för att formulera generella riktlinjer har domstolen betonat att sådana frågor i första hand bör regleras genom lagstiftning. Någon sådan lagreglering har emellertid inte tillkommit och därför får bedömningen som gjorts i praxis anses vägledande.²⁶⁰

Sören Öman har i sin analys behandlat den intresseavvägning som Arbetsdomstolen gjort i fråga om arbetsgivarens möjlighet att kontrollera och övervaka i förhållande till arbetstagares e-post. Det framhålls att kontinuerlig och generell övervakning av privat mejl typiskt sett är svår att förena med proportionalitetskravet, medan mer begränsade och riktade kontroller i större utsträckning kan motiveras. Vidare betonas betydelsen av att skilja mellan arbetsrelaterad och privat information, liksom vikten av transparens i kontrollåtgärder.²⁶¹

4.4 Diskussion

Genomgången i detta kapitel visar att arbetsgivaren i svensk rätt har ett långtgående utrymme att kontrollera och övervaka arbetstagare, med arbetsledningsrätten som central utgångspunkt. Denna rätt gäller generellt i alla anställningsförhållanden och innebär att det i grunden är arbetsgivaren som bestämmer över arbetets organisering och utförande. Detta innefattar även möjligheten att vidta olika former av kontroll- och övervakningsåtgärder, vilka i praktiken kan innebära intrång i arbetstagarens personliga integritet.

Samtidigt är detta utrymme inte obegränsat. Arbetsledningsrätten inskränks genom lag, kollektivavtal och god sed på arbetsmarknaden. Av särskild betydelse i detta sammanhang är de lagstadgade begränsningarna, där EU-rätten intar en framträdande roll. EU-rätten gäller som lag i svensk rätt, har företräde framför nationell rätt och är i stor utsträckning harmoniserad. Även om nationell reglering i vissa fall kan gå längre än EU-rätten, framgår det inte av genomgången att svensk rätt har gjort detta i de aktuella delarna. De lagar som införts, eller är under införande, speglar i väsentliga delar EU-rätten. Kamerabevakningslagen utgör visserligen ett nationellt komplement. Utvecklingen, särskilt genom avskaffandet av tillståndskravet, kan dock snarare tolkas som en förskjutning mot ett ökat handlingsutrymme för arbetsgivaren än ett förstärkt integritetsskydd. Gränsdragningen för algoritmisk övervakning

²⁵⁹ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen* s. 42 f.

²⁶⁰ Grahn och Kjällström, *Anställdas integritetsskydd: och dataskyddsförordningen* s. 41 f.

²⁶¹ Sören Öman, "Privat e-post på arbetet", i: Birgitta Nyström, Annamaria Westergård och Hans-Heinrich Vigel (red.), *Liber amicorum Reinhold Fahlbeck* (Juristförlaget i Lund, 2005), s. 690 ff.

och arbetsledning får därför i stor utsträckning bedömas utifrån de avvägningar som följer av GDPR, AI-förordningen och plattformsdirektivet.

Hur dessa regelverk, såväl EU-rättsliga som nationella, har tillämpats i praktiken av JO och IMY ger vägledning för hur bedömningar i svensk rätt görs i fråga om kontrollåtgärder i arbetslivet. JO:s beslut visar att kontinuerlig och omfattande övervakning utgör ett avgörande kriterium vid bedömningen av förenligheten med 2 kap. 6 § RF och artikel 8 EKMR, vilket är särskilt relevant vid algoritmisk övervakning och arbetsledning som typiskt sett är just löpande och omfattande. IMY:s beslut tydliggör att arbetsplatsen är en särskilt skyddsvärd miljö och att åtgärder som möjliggör kartläggning av arbetstagare väger tungt i proportionalitetsbedömningen. Även fastställs att informationsskyldigheten är långtgående. Samtidigt framgår att vissa kontrollåtgärder kan vara tillåtna för exempelvis brottsförebyggande syften, men inte om de används för löpande kontroll av arbetstagares prestationer. Motsvarande avvägning återkommer även i IMY:s vägledning om GPS-övervakning, där berättigade ändamål kan föreligga, men där användningen måste vara begränsad och inte mer ingripande än nödvändigt.

Vid sidan av detta sätter även straffrätten en yttersta gräns för arbetsgivarens kontrollmöjligheter. Bestämmelserna i 4 kap. brottsbalken tydliggör att det finns en gräns för hur långt arbetsgivaren får gå när det gäller intrång i arbetstagarens privata sfär. Även i en arbetssituation är det som utgångspunkt inte tillåtet att ta del av privat kommunikation, såsom privata mejl, eller att obehörigen bereda sig tillgång till uppgifter i datasystem. Samtidigt visar genomgången att gränsdragningen mellan vad som är arbetsrelaterat och privat inte alltid är tydlig, och att rättsläget i vissa delar är oklart.

Utöver de lagstadgade begränsningarna kan även god sed på arbetsmarknaden fungera som en yttersta gräns för vilka integritetskänsliga åtgärder som kan accepteras. Även om utrymmet att angripa arbetsledningsbeslut med hänvisning till god sed traditionellt har varit begränsat, visar Arbetsdomstolens praxis att kontrollåtgärder prövas genom en proportionalitetsbedömning, där arbetsgivarens intresse vägs mot arbetstagarens integritet. Denna bedömning ligger i linje med artikel 8 EKMR, vilket även Arbetsdomstolen har hänvisat till.

Det bör samtidigt noteras att den praxis avseende god sed som utvecklats främst avser mer traditionella och fysiska kontrollåtgärder, såsom alkohol- och drogtestning. Därmed kan det konstateras att motsvarande prövning av nya kontrollmöjligheter, såsom algoritmisk övervakning och arbetsledning, saknas. Det får dock antas att samma bedömningsramar skulle tillämpas även i en digital kontext. Dessa bedömningar från Arbetsdomstolen visar att arbetsgivaren har ett relativt långtgående utrymme att vidta sådana kontrollåtgärder, särskilt när de är motiverade av säkerhetsskäl eller bedrivs i riskfyllda verksamheter. Mot denna bakgrund framstår särskilt resonemanget om att

kontinuerlig och generell övervakning av uppgifter med privat karaktär är svår att förena med proportionalitetskravet som relevant, då algoritmisk övervakning och arbetsledning typiskt sett innebär omfattande och löpande datainsamling som kan omfatta även sådana privata uppgifter.

Det har i doktrin framhållits att den nationella regleringen av integritet i arbetslivet framstår som fragmentarisk. Regleringen är utspridd mellan EU-rätt, nationella lagbestämmelser, kollektivavtal och individuella anställningsavtal, och kompletteras därutöver av öppna normer såsom god sed på arbetsmarknaden. Vid en samlad bedömning leder detta till att olika rättskällor i stor utsträckning överlappar varandra snarare än bildar ett enhetligt system, vilket exempelvis kan ses i likheterna mellan bedömningen enligt god sed och proportionalitetskravet enligt artikel 8 EKMR. Trots upprepade lagstiftningsförsök saknas alltså en samlad reglering av integritet i arbetslivet, vilket får betraktas som en brist i rättsordningen.

Sammanfattningsvis framträder en rättsordning där arbetsgivaren har en långtgående kontrollmöjlighet, men där gränserna för tillåtna integritetsintrång i stor utsträckning bestäms genom EU-rättsliga regelverk och kompletteras av spridda nationella bestämmelser. Praxis från JO och IMY tydliggör att kontinuerlig, generell och kartläggande övervakning är svår att förena med gällande rätt, särskilt i en arbetsmiljö där integritetsintresset väger tungt och informationsskyldigheten är långtgående. Även straffrätten och principen om god sed sätter yttersta ramar, även om dessa främst prövats i mer traditionella sammanhang. Sammantaget framstår rättsläget som fragmentariskt, där flera regelverk samverkar men samtidigt överlappar.

5 Analys och slutsats

Efter en genomgång av relevanta rättsregler, praxis och doktrin kan det konstateras att det saknas ett entydigt svar på var gränsen går mellan tillåten algoritmisk övervakning och arbetsledning respektive otillåtet intrång i den personliga integriteten. Framställningen visar att regleringen av algoritmisk övervakning och arbetsledning inte återfinns i ett enhetligt och sammanhållet regelverk, utan i ett flertal rättskällor med skilda funktioner och räckvidd. Rätten till privatliv enligt artikel 8 EKMR, tillsammans med motsvarande skydd i EU-stadgan och regeringsformen, utgör en övergripande rättslig ram. Parallellt reglerar GDPR, AI-förordningen och plattformsdirektivet mer specifika aspekter av personuppgiftsbehandling, AI-system och till viss del arbetsledning. Den svenska rättsordningen präglas samtidigt av arbetsledningsrättens centrala ställning, vilken ger arbetsgivaren ett långtgående utrymme att organisera och kontrollera arbetet.

I detta fragmenterade rättsläge aktualiseras därför frågan hur dessa regelverk samverkar i praktiken och vilka konkreta gränser som kan urskiljas. Redogörelsen visar att gränsdragningen i stor utsträckning sker genom en intresseavvägning mellan arbetsgivarens intresse av att leda och kontrollera verksamheten och arbetstagarens rätt till privatliv. Denna avvägning är emellertid komplex, särskilt i en kontext där övervakningen sker genom avancerade algoritmiska system.

Den intresseavvägning som aktualiseras tar sin utgångspunkt i att arbetsgivaren, inom ramen för arbetsledningsrätten, har ett långtgående utrymme att vidta kontroll- och övervakningsåtgärder. Denna rättsgrundsats gäller generellt i anställningsförhållanden och speglar den inneboende asymmetrin mellan arbetsgivare och arbetstagare. Den framstår som nödvändig för att möjliggöra en effektiv organisering och styrning av verksamheten utan krav på löpande samtycke. Samtidigt innebär detta att arbetsledningsrätten också rymmer omfattande kontrollmöjligheter, vilket i praktiken öppnar för integritetskänsliga åtgärder. I fråga om algoritmisk övervakning och arbetsledning kan det med detta i beaktande konstateras att användningen av digitala och algoritmiska system för att följa upp prestationer, organisera arbetet och fatta beslut som rör anställningen i sig inte är otillåten, utan kan utgöra ett legitimt inslag i arbetsledningen. Snarare kan det tolkas som att sådana system utgör en naturlig vidareutveckling av redan accepterade kontrollformer.

Denna utgångspunkt, som följer av arbetsledningsrätten, kommer även till uttryck i Europadomstolens praxis. Domstolen har där erkänt att arbetsgivaren har ett legitimt intresse av att kontrollera verksamheten och säkerställa att arbetsuppgifter utförs korrekt. Det har exempelvis accepterats att kontrollåtgärder som syftar till att skydda arbetsgivarens intressen och säkerställa att arbetsredskap används i enlighet med interna regler är tillåtet. Detta innebär att även algoritmisk övervakning och arbetsledning kan omfattas av likande

legitima intresse, exempelvis för att effektivisera verksamheten eller säkerställa korrekt arbetsutförande.

Av redogörelsen kan det dock konstateras att arbetsledningsrätten inte obegränsad. Den kan endast utövas inom de ramar som följer av lag, kollektivavtal och individuella anställningsavtal. Vidare får inte kontrollåtgärderna strida mot gällande rätt eller god sed på arbetsmarknaden. Inom svensk rätt har EU:s rättsakter och rättighetsskydd stark ställning och kompletteras nationellt av främst kamerabevakningslagen och straffrättsliga regler. Dessa rättskällor får därmed en central betydelse vid bedömningen om en övervakningsåtgärd strider mot lag.

Därför krävs, för att övervakningen ska vara tillåten enligt lagstiftning, att vissa rättsliga krav är uppfyllda. Det krävs att behandlingen av personuppgifter har en rättslig grund och i allmänt är förenlig med GDPR, dataskyddslagen och kamerabevakningslagen. Eftersom GDPR är teknikneutral och avser behandling av personuppgifter i allmänhet, omfattar den även algoritmisk övervakning och arbetsledning, trots att denna inte uttryckligen regleras. Avseende rättslig grund aktualiseras samtycke sällan i arbetslivet, utan behandlingen grundas i praktiken oftast på ett berättigat intresse. Detta förutsätter att arbetsgivarens intresse av övervakningen väger tyngre än arbetstagarens intresse av skydd för sin personliga integritet. Om den algoritmiska övervakningen och arbetsledningen kan motiveras genom en sådan intresseavvägning, och övriga krav i GDPR såsom informationsskyldigheten iakttas, kan behandlingen som utgångspunkt anses laglig.

Vidare kan konstateras att algoritmisk övervakning och arbetsledning i många fall inte träffas av de mer restriktiva reglerna om automatiserat beslutsfattande eller behandling av känsliga personuppgifter i GDPR. Detta beror på att systemen ofta innefattar ett visst mått av mänsklig inblandning och i regel baseras på uppgifter som prestationsdata, arbetstider, positioner och loggar. Samtidigt kan algoritmiska analyser indirekt ge upphov till känsliga uppgifter, exempelvis genom att identifiera mönster som antyder på exempelvis hälsa eller religiösa och politiska preferenser. Hur sådana indirekta slutsatser ska bedömas rättsligt är emellertid oklart, eftersom uppgifterna i sig inte nödvändigtvis utgör känsliga personuppgifter i lagens mening.

I fråga om kamerabevakning kan sådan vara tillåten i vissa situationer, exempelvis vid övervakning av riskfyllda arbetsmoment, i butiksmiljöer i brottsförebyggande syfte eller i särskilt utsatta utrymmen. Detta förutsätter dock att åtgärder vidtas för att begränsa personuppgiftsbehandlingen och att övervakningen inte går längre än vad som är nödvändigt. I denna intresseavvägning beaktas särskilt om övervakningen är begränsad eller om den möjliggör kartläggning av arbetstagares beteenden och rörelsemönster, varvid det senare ska väga tungt i integritetsbedömningen. Även om dessa bedömningar avser en annan typ av kontrollåtgärder, ger de uttryck för generella principer om

nödvändighet och proportionalitet som kan få betydelse, om än indirekt, vid bedömningen av algoritmisk övervakning och arbetsledning.

Parallellt med dessa regelverk finns de nyare rättsakterna AI-förordningen och plattformsdirektivet, vilka, även om de ännu inte fullt ut trätt i kraft, är rättsligt bindande för medlemsstaterna. AI-förordningen bygger på en riskbaserad modell där AI-system inom anställning och arbetsledning, såsom system för övervakning och utvärdering av arbetstagare, i regel klassificeras som högrisk. Detta medför krav på bland annat riskhantering, datakvalitet, transparens, teknisk dokumentation och mänsklig kontroll, samt att arbetstagare informeras och att konsekvensbedömningar genomförs. Samtidigt är endast ett begränsat antal användningar uttryckligen förbjudna, såsom vissa former av känsligenkänning eller biometrisk kategorisering. Detta resulterar i att algoritmisk övervakning och arbetsledning i stor utsträckning är tillåten under förutsättning att regelverkets krav uppfylls.

Vidare utgör plattformsdirektivet det enda regelverk som uttryckligen reglerar algoritmisk arbetsledning. Det etablerar en mer arbetslivsinriktad reglering genom krav på transparens, mänsklig kontroll och regelbunden utvärdering av algoritmiska system. Enligt direktivet är det exempelvis förbjudet att behandla uppgifter om en arbetstagares emotionella eller psykologiska tillstånd samt privata samtal. Regleringen omfattar inte enbart helt automatiserade beslut, utan även situationer där automatiserade system används som stöd i arbetsledningen. Vidare uppmärksammar direktivet maktbalansen mellan arbetsgivare och arbetstagare genom att stärka den kollektiva dimensionen. Regelverket innebär således att algoritmisk övervakning och arbetsledning kan vara tillåten, men att tydligare gränser samtidigt uppställs för denna typ av övervakning och arbetsledning. Samtidigt är direktivets tillämpningsområde begränsat till plattformarbete, vilket innebär att det förstärkta skyddet endast omfattar en begränsad del av arbetsmarknaden. En betydande del av de arbetstagare som exponeras för algoritmisk övervakning och arbetsledning faller därmed utanför dess tillämpningsområde och omfattas inte av dessa mer långtgående skyddsregler.

Utöver detta krävs även att övervakningen är förenlig med det grundläggande rättighetsskyddet. Särskilt centralt är kravet på proportionalitet enligt artikel 8 EKMR och motsvarande bestämmelser i EU-stadgan. I praxis syns en tydlig trend att anpassa sina bedömningar efter den tekniska utvecklingen, varför algoritmisk övervakning och arbetsledning därför kan antas bli föremål för samma bedömningar. Enligt dessa måste en integritetskänslig åtgärd vara nödvändig i förhållande till sitt syfte och inte gå längre än vad som är motiverat. Särskilt vid bedömningen har det av Europadomstolen beaktas bland annat övervakningsåtgärdens syfte, omfattning och tillgängliga skyddsåtgärder vägs mot varandra. Övervakning har ansetts tillåten i situationer som exempelvis vid kontroll av arbetsredskap, utredning av misstänkta

oegentligheter eller uppföljning av arbetsprestationer, särskilt när arbetstagaren informerats i förväg.

I senare praxis rörande GPS-spårning har Europadomstolen godtagit övervakning trots att geolokaliseringsdata möjliggör en kontinuerlig kartläggning av arbetstagarens rörelser. Domstolen betonade att arbetstagaren hade informerats om systemet och dess syfte, samt att uppgifterna kunde användas för kontroll och disciplinära åtgärder. Vid den samlade bedömningen ansågs övervakningen nödvändig och proportionerlig, efter en avvägning mellan arbetstagarens rätt till privatliv och arbetsgivarens intresse av att säkerställa verksamhetens funktion och kontrollera kostnader. Detta fall är av särskild relevans för algoritmisk övervakning och arbetsledning. Liksom vid GPS-spårning möjliggör sådana system en kontinuerlig och detaljerad insamling av uppgifter om arbetstagarens beteende och prestation. Avgörandet visar att även långtgående övervakning kan godtas, förutsatt att den är transparent, har ett legitimt syfte och inte går utöver vad som är nödvändigt

Utöver att vara förenlig med gällande rättsregler måste en kontrollåtgärd alltid uppfylla kraven på god sed på arbetsmarknaden. Arbetsdomstolens praxis visar att kontrollåtgärder prövas genom en proportionalitetsbedömning, där arbetsgivarens intresse vägs mot arbetstagarens integritet, i linje med artikel 8 EKMR. I praxis rörande exempelvis alkohol- och drogtestning samt utpasseringskontroller har även integritetskänsliga åtgärder i stor utsträckning godtagits, särskilt när de motiverats av säkerhetsskäl eller förekommit i riskfyllda verksamheter.

Mot denna bakgrund kan algoritmisk övervakning och arbetsledning i många fall vara tillåten, förslagsvis vid användning av system som sammanställer produktivitetsdata på en övergripande nivå, såsom antal hanterade ärenden eller leveranser per arbetspass. Om systemet används som ett stöd för arbetsledningen och är transparent för arbetstagarna talar mycket för att åtgärden är proportionerlig och därmed tillåten. Även schemaläggning och arbetsfördelning med hjälp av algoritmer kan, mot denna bakgrund, i många fall anses ligga inom arbetsgivarens rätt att leda arbetet. Detta dock förutsatt att systemen inte innebär automatiserade beslut utan möjlighet till mänsklig kontroll. Samtidigt måste en individuell bedömning göras i varje enskilt fall, vilket innebär att det är svårt att dra några generella iakttagelser av vägledande karaktär.

Gränsen passeras däremot när övervakningen blir så ingripande att den inte längre kan anses proportionerlig eller saknar tillräcklig rättslig grund. Detta kan ske på flera sätt. En första situation där gränsen kan anses överskriden är när övervakningen är alltför omfattande eller detaljerad. System som möjliggör en kontinuerlig registrering av arbetstagares beteende, exempelvis genom övervakning av tangentbordsaktivitet eller musrörelser, innebär ett betydande intrång i den personliga integriteten och har ansetts svåra att förena med

kraven i 6 kap. GDPR. Sådana åtgärder har i doktrin framhållits som typiska exempel på övervakning som bör bedömas som oproportionerlig.

Även avgörande från JO och IMY visar att sådan kontinuerlig, generell och kartläggande övervakning i regel är svår att förena med gällande rätt och därmed med proportionalitetskravet. IMY har särskilt framhållit att arbetsplatsen utgör en skyddsvärd miljö, vilket innebär att arbetsgivarens intresse måste väga tungt för att övervakningen ska kunna motiveras. Mot denna bakgrund har dold övervakning i kontrollsyrte samt registerkontroller utan lagligt stöd ansetts otillåtna. Även EU-domstolen har betonat att åtgärder som innebär generell och odifferentierad insamling eller lagring av uppgifter utgör allvarliga intrång i EU-stadgans bestämmelser och är därför otillåtna. Därav framstår det som att motsvarande former av algoritmisk övervakning och arbetsledning, särskilt vid kontinuerlig och detaljerad datainsamling, i många fall riskerar att bedömas som oproportionerliga och därmed otillåtna enligt gällande rätt.

En ytterligare situation som framträder i praxis är när övervakning anses otillåten på grund av otillräcklig transparens. Om arbetstagaren inte informeras om vilka uppgifter som samlas in, hur de används och i vilket syfte, undermineras möjligheten att utöva de rättigheter som följer av GDPR. Av IMY:s praxis framgår tydligt att informationsskyldigheten är långtgående.

Även enligt artikel 8 EKMR intar informationskravet en central roll. I praxis, såsom *Halford v. the United Kingdom* och *Copland v. the United Kingdom*, har bristande information varit avgörande för bedömningen. I dessa fall har avlyssning av tjänstetelefoner samt övervakning av telefon-, e-post- och internetanvändning ansetts strida mot artikel 8, eftersom arbetstagarna inte haft anledning att förvänta sig övervakningen. I senare praxis har informations-skyldigheten även aktualiserats inom ramen för statens positiva förpliktelser. Bristar i de nationella domstolarnas prövning av om arbetstagaren informerats ledde i detta fall till att artikel 8 EKMR ansågs överträdd, eftersom frågan inte hade utretts tillräckligt.

En tredje situation där övervakning kan anses otillåten uppkommer när åtgärden når en sådan nivå att den omfattas av straffrättsliga förbud. Bestämmelserna i 4 kap. brottsbalken innebär att vissa former av kontroll inte enbart är otillåtna, utan även straffbara, exempelvis vid brytande av post- och telehemlighet, olovlig avlyssning eller dataintrång. Dessa regler sätter därmed en yttersta gräns för arbetsgivarens kontrollmöjligheter och tydliggör att intrång i arbetstagarens privata sfär, såsom att ta del av privat kommunikation eller obehörigen bereda sig tillgång till uppgifter i datasystem, som utgångspunkt inte är tillåtna. Samtidigt visar genomgången att gränsdragningen mellan vad som är arbetsrelaterat och privat inte alltid är tydlig, vilket bidrar till osäkerhet i rättstillämpningen.

Med detta i beaktande kan det i många fall antas att algoritmisk övervakning och arbetsledning riskerar att bedömas som otillåten, eftersom den typiskt sett är kontinuerlig, omfattande och närgången. Därigenom framstår den som särskilt integritetskänslig. Till skillnad från mer traditionella kontrollåtgärder, vilka ofta är tidsmässigt eller funktionellt avgränsade, kännetecknas algoritmisk övervakning och arbetsledning i regel av en fortlöpande och systematisk insamling av uppgifter om arbetstagarens beteende, prestation och i vissa fall även rörelsemönster. Detta möjliggör inte endast enstaka kontrollåtgärder, utan även en mer omfattande och långvarig kartläggning av den enskildes arbetsutövning. Avgörandena från IMY, JO och EU-domstolen tyder därför på att kontrollåtgärder som möjliggör en sådan omfattande och varaktig insyn i arbetstagarens arbetsliv ofta riskerar att bedömas som oproportionerliga, särskilt när det möjliggör kartläggning av arbetstagares beteenden och rörelsemönster.

Samtidigt framgår av rättspraxis att integritetskänsliga kontrollåtgärder inte i sig är otillåtna och motsvarande former av övervakning i närliggande situationer har godtagits. Detta kan indikera på att rättstillämpningen inte fullt ut fångar alla de särskilda integritetsrisker som följer av algoritmisk övervakning och arbetsledning. Exempelvis har drog- och alkoholtester samt utpasseringskontroller i stor utsträckning godtagits, trots att de är fysiskt ingripande och i hög grad integritetskänsliga. I dessa fall har arbetsgivarens intressen, såsom säkerhet, arbetsmiljö och förebyggande av olyckor eller oegentligheter, i många intresseavvägningar ansetts väga tyngre än det intrång i den personliga integriteten som åtgärderna innebär.

Även kontinuerlig GPS-övervakning har i vissa fall accepterats, särskilt när arbetstagaren har informerats om systemets existens och syfte samt när användningen varit kopplad till legitima ändamål, såsom att skilja mellan privata och arbetsrelaterade resor och att kontrollera rapporterade körsträckor. Trots att GPS-övervakningen även omfattade tid utanför arbetstid, ansågs arbetsgivarens intresse av att säkerställa verksamhetens funktion och kontrollera sina kostnader väga tyngre än arbetstagarens intresse av skydd för den personliga integriteten. Integritetsmyndigheten har dock samtidigt betonat att positioneringssystem utgör en särskilt närgången form av övervakning, vilket förutsätter återhållsamhet vid användningen samt tekniska och organisatoriska åtgärder, såsom möjligheten att stänga av spårning utanför arbetstid. Därav finns de olikheter i bedömningarna.

Sammantaget illustrerar detta att bedömningarna är kontextberoende och att likartade åtgärder kan utfalla olika beroende på hur proportionalitetsavvägningen görs i det enskilda fallet. Detta skapar en osäkerhet i hur motsvarande avvägning skulle utfalla vid algoritmisk övervakning och arbetsledning samt i vilken utsträckning arbetsgivarens intresse av att organisera och kontrollera arbetet skulle tillmätas avgörande betydelse. Trots att viss vägledning kan hämtas från närliggande åtgärder har denna typ av övervakning ännu inte

prövats, vilket innebär att det saknas tydliga svar i rättstillämpningen. Det saknas därmed vägledning om hur reglerna ska tolkas och tillämpas praktiskt rörande algoritmisk övervakning och arbetsledning.

Det anförda visar därför på att det i praktiken är svårt att fastställa en tydlig gräns mellan tillåten och otillåten algoritmisk övervakning och arbetsledning. En central förklaring är att regleringen i stor utsträckning bygger på öppna och flexibla normer. Osäkerheten förstärks ytterligare av AI-förordningen och plattformsdirektivet, vilka är relativt nya och innehåller begrepp, såsom högrisk-AI och algoritmisk arbetsledning, som ännu inte har fått en närmare innebörd genom praxis. Gränsdragningen överlämnas därmed i stor utsträckning till rättstillämpningen, vilket innebär att avgörande frågor får lösas genom efterhandsbedömningar i det enskilda fallet. Detta minskar förutsebarheten och skapar osäkerhet för såväl arbetsgivare som arbetstagare, med konsekvenser för rättssäkerheten i ett område som präglas av snabb teknisk utveckling. Mot denna bakgrund framstår det som att det finns ett behov av ytterligare klargöranden, antingen genom lagstiftning eller genom en utveckling i praxis.

Samtidigt visar denna redogörelse på den betydande komplexitet som präglar såväl regelverket som de frågeställningar som är föremål för reglering. Även om det finns ett behov av ytterligare klargöranden illustrerar de flertalet statliga utredningar som ännu inte lett till lagstiftning, tillsammans med avskaffandet av tillståndskravet för kamerabevakning, de svåra avvägningar och praktiska utmaningar som området medför. Detta framträder även i IMY:s tillsynsärende rörande H&M, där myndigheten framhöll att integritetsintresset väger tungt på arbetsplatsen, men där merparten av kamerabevakningen ändå ansågs tillåten och främst brast i förhållande till informationskraven snarare än avsaknaden av rättslig grund. Fallet illustrerar därmed den komplexa intresseavvägning som måste göras utifrån de konkreta sakomständigheterna, men också de lagstiftningstekniska svårigheter som området präglas av. Områdets komplexa karaktär tycks således även ha påverkat lagstiftningsarbetet, vilket återspeglas i en fragmentarisk reglering och en splittrad snarare än sammanhållen rättsutveckling.

Sammanfattningsvis visar denna redogörelse att följande slutsatser kan dras. Gränsen för när algoritmisk övervakning och arbetsledning övergår till att utgöra ett otillåtet intrång i arbetstagares personliga integritet avgörs genom en samlad bedömning av flera rättsliga faktorer. Avgörande är om övervakningen har en rättslig grund, uppfyller kraven på proportionalitet och sker med tillräcklig transparens. Samtidigt är denna gräns inte tydligt definierad i lagstiftningen, utan framträder genom en kombination av rättighetsbaserade principer, dataskyddsregler och arbetsrättsliga normer. Detta innebär att gränsdragningen i praktiken är svår att fastställa och i stor utsträckning beroende av omständigheterna i det enskilda fallet. Därtill innebär det fragmenterade rättsläget att arbetstagare omfattas av olika skyddsnivåer.

Plattformsarbetare åtnjuter exempelvis ett starkare skydd mot algoritmisk övervakning och arbetsledning än andra arbetstagare, bland annat genom förbud mot behandling av vissa särskilt integritetskänsliga uppgifter.

Den tekniska utvecklingen, särskilt framväxten av algoritmisk arbetsledning, har ytterligare försvårat den rättsliga bedömningen. Även om regelverk såsom GDPR och EKMR är teknikneutrala och avsedda att kunna anpassas till ny teknisk utveckling, innebär detta i praktiken att de måste tolkas i ljuset av tekniska förhållanden som lagstiftaren inte fullt ut kunnat förutse. Detta ger upphov till nya och komplexa avvägningar, där etablerade rättsliga principer ska tillämpas på situationer som saknar tydlig vägledning i praxis. De nyare EU-rättsliga regelverken, såsom AI-förordningen och plattformsdirektivet, utgör viktiga steg mot en mer ändamålsenlig reglering av algoritmisk övervakning och arbetsledning. Samtidigt befinner de sig fortfarande i ett tidigt skede och präglas av oklara begrepp, begränsad praxis och ett ännu outvecklat tolkningsunderlag. Detta innebär att deras praktiska betydelse och genomslag i rättstillämpningen i stor utsträckning återstår att klarlägga.

I dagsläget saknas därför en tydlig och förutsebar gräns för när algoritmisk övervakning och arbetsledning övergår till att utgöra ett otillåtet intrång i arbetstagares personliga integritet. Detta innebär att det rättsliga skyddet, trots sin omfattning, i praktiken kan vara svårt att tillämpa och därmed inte fullt ut tillgodoser behovet av rättssäkerhet i ett allt mer digitaliserat arbetsliv. Detta talar för ett behov av både reformer och förtydliganden, liksom ett mer sammanhållet regelverk som bättre speglar den tekniska utvecklingen och säkerställer ett effektivt skydd för arbetstagare som den svagare parten i anställningsförhållandet.

En central fråga i den fortsatta rättsutvecklingen är om gränsen för vad som utgör otillåten algoritmisk övervakning och arbetsledning håller på att förskjutas. Att plattformsarbetare tillerkänns ett mer långtgående skydd kan förklaras av att deras arbete i hög grad bygger på kontinuerlig utlämning till algoritmiska övervaknings- och styrsystem, vilket innebär att deras personliga integritet är särskilt utsatt. Samtidigt bör detta förstås som en fråga om genomförande och upprätthållande av skyddet, snarare än som ett uttryck för att mer ingripande integritetsintrång generellt ska accepteras inom andra delar av arbetslivet. Plattformsarbetare framstår snarare som den arbetsgrupp där problematiken blivit mest tydlig och akut, samtidigt som liknande integritetsrisker förekommer även för andra arbetstagare i ett allt mer digitaliserat arbetsliv. Det finns därför skäl att anta att den utveckling som nu sker på plattformsområdet på sikt kan komma att påverka skyddsnivån även för andra arbetstagare. Utvecklingen tyder därmed på att arbetstagares personliga integritet successivt ges en starkare ställning i rättsutvecklingen, vilket i förlängningen kan innebära att fler former av algoritmisk övervakning och arbetsledning kommer att bedömas som otillåtna integritetsintrång.

Källförteckning

KÄLLOR

Offentligt tryck

Sverige

Propositioner

Prop. 1975/19 *Regeringens proposition om lagstiftning om skydd mot avlyssning.*

Prop. 1993/94:24 *med förslag till ändrade regler om kroppsvisitation och kroppsbesiktning, m.m.*

Prop. 1993/94:117 *Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor.*

Prop. 1997/98:82 *Europarådets sociala stadga.*

Prop 2009/10:80 *En reformerad grundlag.*

Prop. 2017/18:105 *Ny dataskyddslag.*

Utredningsbetänkande

SOU 2002:18 *Personlig integritet i arbetslivet.* Klimat- och näringslivsdepartementet.

SOU 2009:44 *Integritetsskydd i arbetslivet.* Arbetsmarknadsdepartementet.

SOU 2017:52 *Så stärker vi den personliga integriteten.* Justitiedepartementet.

SOU 2025:101 *Anpassningar till AI-förordningen: Säker användning, effektiv kontroll och stöd för innovation.* Finansdepartementet.

SOU 2026:3 *Genomförande av plattformsdirektivet.* Arbetsmarknadsdepartementet.

Europeiska unionen

Artikel 29-gruppen för uppgiftsskydd. *Riktlinjer om öppenhet enligt förordning (EU) 2016/679, WP260 rev.01, antagna den 29 november 2017 och senast granskade den 11 april 2018. Tillgänglig på:*

<https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf> (besökt 11 maj 2026).

Artikel 29-arbetsgruppen för uppgiftsskydd. *Yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen*, WP 249, antaget den 8 juni 2017. Tillgänglig på: <https://ec.europa.eu/newsroom/article29/items/610169/en> (besökt 11 maj 2026).

European Data Protection Board. *Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679*, version 1.1, antagna 4 maj 2020. Tillgänglig på: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_sv.pdf (besökt 11 maj 2026).

European Parliamentary Research Service (EPRS). *Digitalisation, Artificial Intelligence and Algorithmic Management in the Workplace: Shaping the Future of Work*, EPRS Study, PE 774.670 (2025). Tillgänglig på: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/774670/EPRS_STU%282025%29774670_EN.pdf (besökt 11 maj 2026).

Europeiska unionens officiella tidning (EUT). *Förklaringar avseende stadgan om de grundläggande rättigheterna*, EUT C 303/02, ISSN 1725–2504, 14 december 2007.

Kommissionens riktlinjer om de förbjudna användningsområden för artificiell intelligens som fastställs i förordning (EU) 2024/1689 (AI-förordningen), C(2025) 5052 final.

Rättsfall

Arbetsdomstolen

AD 1932 nr 100.

AD 1934 nr 38.

AD 1934 nr 179.

AD 1967 nr 26.

AD 1997 nr. 29.

AD 1983 nr 46.

AD 1984 nr 94.

AD 1991 nr 45.

AD 1998 nr 97.

AD 2001 nr 3.

AD 2009 nr 36

AD 2013 nr 19.

AD 2021 nr 23.

AD 2023 nr 75.

Högsta domstolen

NJA 2005 s. 361.

JO-beslut och Datainspektionens tillsynsbeslut

JO:s beslut 19 oktober 2023, dnr 7143–2022.

Datainspektionens tillsynsbeslut 2024-04-18, dnr 2021–771.

Europeiska unionens domstol (EU-domstolen)

Mål C-293/12 och C-594/12 *Digital Rights Ireland m.fl.*, dom 8 april 2014, EU:C:2014:238.

Mål C-203/15 och C-698/15 *Tele2 Sverige m.fl.*, dom 21 december 2016, EU:C:2016:970.

Mål C-511/18, C-512/18 och C-520 *La Quadrature du net m.fl.*, dom 6 oktober 2020, EU:C:2020:791.

Mål C-175/20 *SS mot Valsts ieņēmumu dienests*, dom 24 februari 2022, EU:C:2022:124.

Mål C-422/24 *Integritetsskyddsmyndigheten mot AB Storstockholms Lokaltrafik*, dom 18 december 2025, EU:C:2025:980.

Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen)

Klass and Others v. Germany, (5029/71) dom 6 september 1978.

Sunday Times v. the United Kingdom (6538/74) dom 26 april 1979.

Silver and Others v. the United Kingdom (5947/72, 6205/73, 7052/75, 7061/74, 71077/75, 7113/75, 7136/75) dom 25 mars 1983.

Leander v. Sweden (9248/81) dom 26 mars 1987.

Niemietz v. Germany (13710/88) dom 16 december 1992.

Halford v. the United Kingdom (20605/92) dom 25 juni 1997.

Foxley v. the United Kingdom (33274/96) dom 20 juni 2000.

Weber and Saravia v. Germany (54934/00) dom 29 juli 2006.

Copland v. the United Kingdom (62617/00) dom 3 april 2007.

S. and Marper v. the United Kingdom (30562/04 och 30566/04) dom 5 december 2008.

Oleksandr Volkov v. Ukraine (21722/11) dom 27 maj 2013.

Lindstrand Partners Advokatbyrå AB v. Sweden (18700/09) dom 20 december 2016.

Bărbulescu v. Romania (61496/08) dom 5 september 2017.

Libert v. France (588/13) dom 22 februari 2018.

López Ribalda and Others v. Spain (1874/13; 8567/13) dom 17 oktober 2019.

Florindo de Almeida Vasconcelos Gramaxo v. Portugal, (26968/16) dom 13 december 2022.

Integritetsskyddsmyndigheten – IMY

Integritetsskyddsmyndigheten. ”AI-förordningen”, 18 februari 2026.
<https://www.imy.se/verksamhet/ai/ai-forordningen/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. ”De registrerades rättigheter”, 11 juni 2025.
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. ”Grundläggande principer”, 11 juni 2025.
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. *Integritet och ny teknik 2020-2024: Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen*. Rapport. Diarienummer IMY-2024-2570. 2025. Tillgänglig på: <https://www.imy.se/publikationer/integritet-och-ny-teknik-20202024/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Kamerabevakning av anställda", 28 mars 2025. <https://www.imy.se/verksamhet/kamerabevakning/personuppgiftsansvar-och-kamerabevakades-rattigheter/kamerabevakning-av-anstallda/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Kontroll och övervakning av anställda", 6 maj 2025. <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/kontroll-och-overvakning-av-anstallda/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Regler för verksamheters kamerabevakning", 27 april 2026. <https://www.imy.se/verksamhet/kamerabevakning/Regler-for-verksamheters-kamerabevakning/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Personuppgiftsansvariga och personuppgiftsbiträden", 11 juni 2025. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Rättslig grund", 11 juni 2025. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet "personuppgifter som rör lagöverträdelse som innefattar brott" i artikel 10 i dataskyddsförordningen. Diarienummer IMYRS 2021:1. 2021. Tillgänglig på: <https://www.imy.se/globalassets/dokument/rattsligt-stallningstagande/imyrs-2021-1-lagovertradelser.pdf> (besökt 11 maj 2026).

Integritetsskyddsmyndigheten. "Syfte och tillämpningsområde", 11 juni 2025. <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/syfte-och-tillampningar/> (besökt 11 maj 2026).

Övrigt

Arbetsmiljöverket. "Algoritmisk arbetsledning", 13 februari 2026. <https://www.av.se/halsa-och-sakerhet/digitalisering/algoritmisk-arbetsledning/> (besökt 11 maj 2026).

Eurofound. "Platform work: Algorithmic management", 30 maj 2025. <https://www.eurofound.europa.eu/en/publications/all/platform-work-algorithmic-management> (besökt 11 maj 2026).

Europeiska kommissionen. "AI Act", 7 maj 2026. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (besökt 11 maj 2026).

Handels. "Allt fler övervakas på jobbet", 9 oktober 2025. <https://www.handels.se/aktuellt/2025/allt-fler-overvakas-pa-jobbet/> (besökt 11 maj 2026).

Ingenjören. "Digital övervakning på kontoret är vanligare än många tror", 20 maj 2025. <https://ingenjoren.se/2025/05/20/digital-overvakning-pa-kontor-ar-vanligare-an-de-flesta-inser/> (besökt 11 maj 2026).

Sveriges riksdag. "EU:s lagar och regler", 3 maj 2023. <https://www.riksdagen.se/sv/sa-fungerar-riksdagen/sa-fungerar-eu/en-eu-lag-blir-till/eus-lagar-och-regler/> (besökt 11 maj 2026).

TCO. "Massövervakningen av anställda på jobbet måste regleras", 27 maj 2025. <https://tco.se/fakta-och-politik/arbetsratt/massovervakningen-av-anstallda-pa-jobbet-maste-regleras> (besökt 11 maj 2026).

LITTERATUR

Adams-Prassl, Jeremias. "Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'". *European Labour Law Journal*, vol. 13, nr. 1 (2 februari 2022). Tillgänglig via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4024374 (besökt 11 maj 2026).

Ball, Kirstie. "Workplace Surveillance: An Overview". *Labor History*, vol. 51, nr 1 (februari 2010): s. 87–106. Tillgänglig på: https://www.researchgate.net/publication/45229880_Workplace_Surveillance_An_Overview (besökt 11 maj 2026).

Danelius, Hans, Danelus, Johan, Bull, Thomas och Cameron, Iain. *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*. 6 uppl., Nordstedts juridik, 2023.

Deakin, Simon och Wilkinson, Frank. "Labour law and economic theory: a reappraisal", i: Hugh Collins, Paul Davies och Roger Rideout (red.), *Legal Regulation of the Employment Relation*, Kluwer Law International, 2000.

Del Castillo, Aída Ponce och Taes, Simon. "Artificial Intelligence and Labour Law", i: Smuha, Nathalie A. (red.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2025.

Ehrenkrona, Carl Henrik. Kommentar till lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, Karnov (JUNO) (besökt 11 maj 2026).

Frydinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline och Beyer, Sandra. *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*. 1 uppl., Nordstedts Juridik, 2018.

Grahn, Erik och Kjällström, Susanna. *Anställdas integritetsskydd: och dataskyddsförordningen*. 1 uppl., Wolters Kluwer, 2017.

Hettne, Jörgen, och Otken Eriksson, Ida. *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*. 2 uppl., Norstedts Juridik, 2011.

Håkansta, Carin. *Vad händer med arbetsmiljön när AI blir chef? Sammanställning av forskningsbaserad kunskap och slutsatser från en tvärvetenskaplig policykonferens*. Rapport. Karolinska Institutet, 2025. Tillgänglig på: <https://ki.se/media/271339/download> (besökt 11 maj 2026).

Jermsten, Henrik. Kommentar till Regeringsformen (1974:152), Karnov (JUNO) (besökt 11 maj 2026).

Klamberg, Mark. "Skydd enligt Europeiska unionens stadga om de grundläggande rättigheterna", i: Cecilia Magnusson Sjöberg, Karatina Fast Lappalainen och Daniel Westman (red.), *Rättsinformatik: juridiken i det digitala informationssamhället*. 5 uppl., Studentlitteratur AB, Lund 2024.

Kleineman, Jan. 'Rättsdogmatisk metod', i: Maria Nääv och Mauro Zamboni (red), *Juridisk metodlära*. 3 uppl., Studentlitteratur AB, Lund 2025.

Källström, Kent, Malmberg, Jonas och Johansson, Caroline. *Anställningsförhållandet: en inledning till den individuella arbetsrätten*. 7 uppl., Iustus, 2025.

Nyström, Birgitta. *Introduktion till den europeiska arbetsrätten*. 1 uppl., Nordstedts Juridik, 2024.

Rönmar, Mia. *Arbetsledningsrätt och arbetsskyldighet: en kooperativ studie av kvalitativ flexibilitet i svensk, engelsk och tysk kontext*. Juristförlaget i Lund, 2004.

Selberg, Nicklas. "En agenda för framtidens arbetsrätt". *Dagens Arena*, 1 oktober 2020, avs. Arenaessä. Tillgänglig på: <https://www.dagensarena.se/essa/en-agenda-framtidens-arbetsratt/> (besökt 11 maj 2026).

Smuha, Nathalie A. och Yeung, Karen. "The European Union's AI Act: Beyond Motherhood and Apple Pie?", i: Smuha, Nathalie A. (red.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2025.

Westregård, Annamaria. *Integritetsfrågor i arbetslivet*. Juristförlaget i Lund, 2002.

Yusifli, Zahra. *Labour Rights and the EU Artificial Intelligence Act: How to Get Away with High-Risk AI*, University of Luxembourg Law Research Paper No. 2025-01, 15 januari 2025. Tillgänglig via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5098359 (besökt 11 maj 2026).

Öman, Sören. *Dataskyddsförordningen (GDPR) m.m.: en kommentar* (11 september 2025, version 3A, JUNO).

Öman, Sören. "Grundlagsskydd", i: Cecilia Magnusson Sjöberg, Karatina Fast Lappalainen och Daniel Westman (red.), *Rättsinformatik: juridiken i det digitala informationssamhället*. 5 uppl., Studentlitteratur AB, Lund 2024.

Öman, Sören. "Privat e-post på arbetet", i: Birgitta Nyström, Annamaria Westergård och Hans-Heinrich Vigel (red.), *Liber amicorum Reinhold Fahlbeck*, Juristförlaget i Lund, 2005.