

HANDBOK



Förebyggande av olaglig profilering idag och i framtiden: en vägledning

Manuskriptet till denna handbok färdigställdes 2018.

Bilder (omslag och insida): © stock.adobe.com-Savvapanf Photo

Mer information om Europeiska unionen finns på internet (<http://europa.eu>).

Luxemburg: Europeiska unionens publikationsbyrå, 2022

Print	ISBN 978-92-9461-451-3	doi:10.2811/413254	TK-06-18-031-SV-C
PDF	ISBN 978-92-9461-430-8	doi:10.2811/551066	TK-06-18-031-SV-N

© Europeiska unionens byrå för grundläggande rättigheter, 2022

Återgivning är tillåten med angivande av källan. För all användning eller återgivning av foton eller annat material som inte omfattas av FRA:s upphovsrätt måste tillstånd inhämtas direkt från upphovsrättsinnehavarna.

Printed by the Publications Office in Luxembourg

Förebyggande av olaglig profilering idag och i framtiden: en vägledning

Innehåll

FIGURER OCH TABELLER.....	5
FÖRKORTNINGAR.....	6
INLEDNING.....	7
SAMMANFATTNING AV DE VIKTIGASTE PUNKTERNA.....	11
1 BAKGRUND: VAD ÄR PROFILERING?.....	17
1.1. Hur definieras profilering?.....	17
1.1.1. Profilering inom ramen för brottsbekämpning och gränsförvaltning.....	19
1.1.2. Hur definieras algoritmisk profilering?.....	21
1.2. När är profilering olaglig?.....	25
1.2.1. Förbudet mot diskriminering.....	26
1.2.2. Rätten till respekt för privatlivet och skydd av personuppgifter.....	34
1.3. Vilka effekter kan olaglig profilering få för brottsbekämpning och gränsförvaltning?.....	42
1.3.1. Inverkan på förtroendet för polisen och gränsförvaltningen och relationerna till samhället.....	43
1.3.2. Profileringens effektivitet.....	54
2 LAGLIG PROFILERING: PRINCIP OCH PRAKTIK.....	57
2.1. Visa respekt för den personliga värdigheten.....	59
2.2. Rimliga och objektiva grunder.....	63
2.2.1. Undvika fördomar.....	63
2.2.2. Tydlig vägledning för tjänstemän.....	64
2.2.3. Målinriktad utbildning.....	66
2.2.4. Rimliga skäl till misstanke: användning av underrättelser och information.....	72
2.2.5. Formulär för kontroll och visitering vid profilering inom brottsbekämpning.....	81
2.3. Ansvarighet.....	85
2.3.1. Intern övervakning.....	87
2.3.2. Kroppsburna kameror.....	93
2.3.3. Klagomålsmekanismer.....	97
3 ALGORITMISK PROFILERING.....	105
3.1. Ramen för dataskydd som styr algoritmisk profilering.....	108
3.1.1. Uppgifterna måste behandlas för ett särskilt syfte.....	110
3.1.2. Enskilda personer måste informeras.....	113
3.1.3. Säker förvaring av uppgifter: register, loggar och lagringsregler.....	115
3.1.4. Olaglig behandling måste upptäckas och förebyggas.....	116
3.2. Stora databaser för gränsförvaltning och säkerhetsinsatser.....	121
3.2.1. Minimering av riskerna för de grundläggande rättigheterna vid behandling av uppgifter i stora databaser.....	125

SLUTSATS.....	130
BILAGA.....	131
HÄNVISNINGAR.....	134

Figurer och tabeller

Figur 1:	Processen för algoritmisk profilering inom ramen för brottsbekämpning och gränsförvaltning	23
Figur 2:	Överträdelse av rätten till integritet och skydd av personuppgifter – bedömningsprocessen	40
Figur 3:	De senaste poliskontrollerna som uppfattades som etnisk profilering av dem som stoppades under de fem åren före EU-Midis II-undersökningen, per EU-medlemsstat och målgrupp (%)	48
Figur 4:	Den självuppfyllande profetians cykel	53
Figur 5:	Tre förutsättningar för ett respektfullt möte	61
Figur 6:	Processen och målen för utarbetandet av målinriktad utbildning	67
Figur 7:	Indikatorer som betraktas som användbara eller mycket användbara för att känna igen personer som försöker resa in i landet på ett olagligt sätt innan tjänstemännen pratar med dem (%)	74
Figur 8:	Kombination av faktorer	79
Figur 9:	Faktorer för icke-diskriminerande profilering	80
Figur 10:	Åtgärder i samband med intern övervakning	89
Figur 11:	Onlineverktyg som visar uppgifter om kontroller och visiteringar i London	92
Figur 12:	Översikt över klagomålsmekanismer i EU:s medlemsstater	99
Figur 13:	Minimikrav för konsekvensbedömningar	119
Tabell 1:	Egenskaper för specifikt underrättelsebaserat och prognostiserat polisarbete	20
Tabell 2:	Dataskyddskrav – skillnader mellan polisdirektivet och den allmänna dataskyddsförordningen	36
Tabell 3:	Typer av vägledning, deras egenskaper och berörda parter medverkan	65
Tabell 4:	Identifiering av den korrekta rättsliga ramen beroende på syftet med behandlingen av personuppgifter	111
Tabell 5:	Skyldighet att ge enskilda personer information om profilering: typ av uppgifter, kommunikationssätt och undantag ...	113
Tabell 6:	Utvalda EU-instrument för behandlingen av stora mängder personuppgifter för gränsförvaltning och brottsbekämpning	122
Tabell 7:	Befintliga och planerade stora it-system inom EU	131

Förkortningar

EDPS	Europeiska datatillsynsmannen
EES	In- och utresesystemet
Etias	EU-system för reseuppgifter och resetillstånd
EU	Europeiska unionen
EU-Midis	Europeiska unionens undersökning av minoriteter och diskriminering
Europa-konventionen	Europeiska konventionen om de mänskliga rättigheterna
FN	Förenta nationerna
FRA	Europeiska unionens byrå för grundläggande rättigheter
Frontex	Europeiska gräns- och kustbevakningsbyrån
It	Informationsteknik
OHCHR	Kontoret för FN:s högkommissarie för mänskliga rättigheter
OSSE	Organisationen för säkerhet och samarbete i Europa
SIS II	Schengens informationssystem
TCN	Tredjelandetsmedborgare
UNHCR	FN:s råd för mänskliga rättigheter
VIS	Informationssystemet för viseringar

Inledning

Den tekniska utvecklingen har medfört en ökad användning av profilering inom en rad olika områden, däribland marknadsföring, sysselsättning, hälso- och sjukvård, finansverksamhet, brottsbekämpning, gränskontroll och säkerhet. Användningen av profileringsverktyg för att underlätta arbetet inom brottsbekämpning och gränsförvaltning har under senare år rönt allt större uppmärksamhet bland EU:s medlemsstater. Profilering används regelbundet, och lagligt, av tjänstemän inom brottsbekämpning och gränsbevakning för att förebygga, utreda och lagföra brott samt för att förebygga och upptäcka irreguljär invandring. Olaglig profilering kan emellertid undergräva förtroendet för myndigheterna, i synnerhet polisen, och stigmatisera enskilda samhällsgrupper. Detta kan i sin tur öka spänningarna mellan samhällsgrupperna och de brottsbekämpande myndigheterna om användningen av profilering uppfattas som diskriminerande.

I denna vägledning förklaras vad profilering innebär, vilken rättslig ram som utgör dess grund och varför en laglig profilering inte bara är nödvändig för att uppfylla de grundläggande rättigheterna, utan även helt avgörande för att effektivisera polisverksamheten och gränsförvaltningen. Vägledningen innehåller även praktiska riktlinjer om hur olaglig profilering kan undvikas vid insatser inom polisverksamheten och gränsförvaltningen. Principerna och riktlinjerna i vägledningen förklaras med hjälp av exempel, fallstudier och rättspraxis både inom och utanför EU.

Varför behöver vi denna vägledning?

Profilering väcker ett antal frågor om de grundläggande rättigheterna (1). Profileringen kan bryta mot väletablerade rättsliga principer, däribland om jämlikhet och icke-diskriminering samt rätten till skydd av privatliv och personuppgifter. Frågor har även väckts när det gäller profileringens effektivitet vid bekämpning av olaglig verksamhet och de möjliga negativa konsekvenserna för relationen mellan myndigheterna (däribland polis och gränsförvaltning) och de samhällsgrupper de tjänar.

Som ett svar på dessa frågor offentliggjorde Europeiska unionens byrå för grundläggande rättigheter (FRA) vägledningen *Mot ett effektivare polisarbete. Förstå och förhindra diskriminerande etnisk profilering* år 2010. Vägledningen var inriktad på polisens användning av profilering, i synnerhet i samband med utövan av kontroll- och visiteringsbefogenheter. Dess syfte var att ge tjänstemän på mellannivå ett verktyg för att undvika diskriminerande profilering grundad på etnicitet.

Sedan dess har den tekniska utvecklingen förändrat förutsättningarna för profilering i grunden. En stor del av profileringen bygger numera på resultaten av datoranalyser av omfattande dataset. Ur ett rättsligt perspektiv innebär de omarbetade – striktare – regler för uppgiftsskydd som började tillämpas i EU från maj 2018 att nya standarder infördes för insamling, analys och användning av personuppgifter.

Denna uppdaterade vägledning utgår från dessa betydande förändringar för att bygga vidare på och utöka 2010 års vägledning så att den speglar de nya rättsliga och praktiska förutsättningarna. I vägledningen beskrivs en mer övergripande strategi mot olaglig profilering som även omfattar

- profilering inom ramen för gränsförvaltning,
- diskriminerande profilering på alla grunder, däribland nationalitet, ålder och kön, utöver etniskt ursprung, samt
- algoritmisk, eller datorbaserad, profilering.

Denna version från 2018 innehåller även nya exempel och fallstudier som speglar utvecklingen och innovationerna inom profilering.

(1) Se FRA (2018e), s. 85-87; FRA (2017c), s. 88-89 och FRA (2016), s. 83-85.

Vem bör använda denna vägledning?

Vägledningen är i första hand utformad för dem som är ansvariga för utbildning av tjänstemän inom brottsbekämpning och gränsförvaltning. Den kan även hjälpa tjänstemän på mellannivå att genomföra profilerings tekniker på ett lagligt sätt. Syftet med vägledningen är att öka förståelsen för teori och praktik inom profilering och att i konkreta ordalag beskriva hur profilering kan användas i enlighet med de grundläggande rättigheterna.

Vägledningen omfattar profilering som utförs av poliser i yttre tjänst – till exempel vid kontroll och visitering – och kontroller som utförs av gränsvakter vid gränspassager när ett beslut har fattats om att en person ska genomgå en fördjupad kontroll. När det gäller gränsförvaltning kan vägledningen fungera som ett hjälpmedel för dem som är ansvariga för utbildningen av gränsbevakningspersonal enligt artikel 36.5 i förordningen om den europeiska gräns- och kustbevakningen (förordning (EU) nr 2016/1624).

I vägledningen behandlas även profilering på grundval av analyser av storskaliga dataset, inbegripet sådana som regleras av EU-lagstiftningen. Profilering i andra situationer, exempelvis profilering som utförs inom den privata sektorn för kommersiella ändamål, ligger utanför tillämpningsområdet för denna vägledning. FRA bedriver ytterligare forskning inom detta ämne ⁽²⁾.

Hur bör denna vägledning användas?

Vägledningen innehåller en översikt över de viktigaste principerna och riktlinjerna för profilering inom ramen för brottsbekämpning och gränsförvaltning. Den kan läsas i sin helhet eller användas som referens i samband med utbildning.

Vägledningen innehåller tre kapitel. Kapitel 1 innehåller en förklaring av begreppet profilering och de fall då profileringen kan vara olaglig. Här finns även en beskrivning av profileringens möjliga negativa inverkan på individer, samhällsgrupper och utövandet av polis- och gränsförvaltningens befogenheter. I kapitel 2 beskrivs de principer och riktlinjer som tjänstemän inom brottsbekämpning och gränsbevakning bör följa för att genomföra lagliga profileringar. Slutligen ägnas kapitel 3 åt algoritmisk profilering. Eftersom praxis inom detta område inte är särskilt utvecklad innehåller detta kapitel inte så många konkreta exempel. I stället redovisas de

(2) Se FRA:s projekt om [artificiell intelligens, stordata och grundläggande rättigheter](#).

huvudsakliga riskerna för de grundläggande rättigheterna i samband med datorbaserad profilering och de viktigaste rättsliga krav som fastställts genom den allmänna dataskyddsförordningen och polisdirektivet.

Ett antal visuella element framhäver de olika aspekterna av vägledningen. De viktigaste budskapen sammanfattas som punktuppställningar i de gula rutorna. De viktigaste aspekterna av den rättsliga ramen presenteras i de ljusblå rutorna, och de gröna rutorna innehåller praktiska exempel. Andra rutor innehåller information om viktiga fokuspunkter, fallstudier och exempel på rättspraxis. Trots att ansträngningar har gjorts för att variera fallstudierna kommer många av exemplen från Förenade kungariket. Detta beror på att Förenade kungariket har bekämpat olaglig profilering sedan 1980-talet, medan de andra medlemsstaterna har börjat arbeta med problemet först under senare år. Förenade kungariket har således kunnat utveckla mer omfattande och långvariga regler och riktlinjer inom de områden där exemplen kommer ifrån.

Hur har vägledningen utarbetats?

FRA anordnade ett möte med sakkunniga inom olika områden för att diskutera ett första utkast av vägledningen och inhämta synpunkter på utformningen av den slutliga produkten.

I detta avseende vill FRA tacka alla sakkunniga från kontoret för FN:s högkommissarie för mänskliga rättigheter (OHCHR), Europeiska gräns- och kustbevakningsbyrån (Frontex), kontoret för demokratiska institutioner och mänskliga rättigheter (ODIHR) vid organisationen för säkerhet och samarbete i Europa (OSSE), Amnesty International, Europeiska nätverket mot rasism (ENAR), det internationella centrumet för migrationspolitikutveckling (ICMPD), FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, European Digital Rights, Open Society Initiative for Europe samt företrädare för Frankrikes ombudsman, den nederländska, danska och österrikiska polisen samt den polska gränsbevakningen för deras värdefulla synpunkter under utarbetandet av vägledningen.

Sammanfattning av de viktigaste punkterna

1. Skyddade egenskaper får aldrig vara den enda grunden för profilering

- Profilering inbegriper en **kategorisering av individer** utifrån deras egenskaper.
- Innan myndigheterna inom brottsbekämpning och gränsförvaltning samlar in och behandlar **personuppgifter** måste de säkerställa att insamlingen och behandlingen av personuppgifter har en rättslig grund, har ett giltigt och berättigat syfte och är nödvändig och proportionerlig.
- **Skyddade egenskaper** som ras, etniskt ursprung, kön eller religion kan ingå bland de faktorer som de brottsbekämpande myndigheterna och gränsbevakningspersonalen tar hänsyn till när de utövar sina befogenheter, men de **får inte vara det enda eller huvudsakliga skälet till att en individ väljs ut.** (Mer information om skyddade egenskaper finns i [avsnitt 1.2.1](#)).
- Profilering som endast eller huvudsakligen bygger på en eller flera skyddade egenskaper betraktas som direkt diskriminering. Den **kränker individens rättigheter och friheter** och är därmed **olaglig**.

2. Varje möte med en enskild person bör ske på ett respektfullt, yrkesmässigt och informativt sätt

- Ett **möte med god kvalitet** innebär inte i sig att en orättvis profilering undviks, men gör sannolikt att mötet blir mer framgångsrikt och minskar de möjliga negativa effekterna av polisens eller gränsbevakningspersonalens kontroller. Inom gränsförvaltningen anses ett yrkesmässigt och respektfullt uppträdande i sig vara en rättslig skyldighet.
- Ett **yrkesmässigt och respektfullt uppträdande** ökar i allmänhet personens nöjdhet under mötet.
- Om personen som kontrolleras **får en förklaring av skälen** ökar allmänhetens förtroende för polisen och gränsbevakningen, samtidigt som misstankarna om orättvis profilering minskar.
- Respekt och artighet kan emellertid **aldrig motivera olagliga gränskontroller eller visiteringar**.

3. Profilering bör bygga på objektiva och rimliga grunder

- För att vara lagliga måste kontroller och hänvisningar till fördjupad kontroll **baseras på rimliga och objektiva skäl** till misstanke.
- Personliga egenskaper får användas som berättigade faktorer för profilering. För att undvika diskriminering **måste det emellertid även finnas rimliga skäl till misstanke** som bygger på annan information än de skyddade egenskaperna.
- Brottsbekämpning och gränsförvaltning som baseras på **specifika och uppdaterade underrättelser** är sannolikt mer **objektiva**.
- Det grundläggande är att ett beslut att kontrollera en person eller hänvisa honom/henne till en fördjupad kontroll **inte enbart får baseras på en tjänstemans uppfattning** om personen, eftersom den kan baseras på stereotyper och/eller fördomar.

4. Olaglig profilering har en negativ inverkan på polisarbetet och gränsförvaltningen

- **Olaglig profilering undergräver förtroendet för polisen och gränsbevakarna.** Den kan försämra relationerna mellan polisen/gränsbevakarna och de minoriteter eller andra samhällsgrupper som känner sig utpekade. Denna känsla av orättvisa kan leda till att vissa individer och grupper förlorar förtroendet för polisen och andra myndigheter, vilket i sin tur kan leda till minskad rapportering av brott och ett sämre samarbete med myndigheterna. Myndigheterna kan i sin tur bli miss-tänksamma mot vissa grupper, vilket kan leda till fler olagliga profileringar.
- **Olaglig profilering minskar profileringens ändamålsenlighet**, eftersom den takt i vilken individer stoppas, antingen av polisen eller vid gränsen, inte nödvändigtvis motsvarar andelen överträdelse bland olika grupper.
- Det finns risk för en **självuppfyllande profetia** om en minoritetsgrupp utsätts för oproportionerliga kontroller av polis eller gränsbevakningspersonal, vilket kan leda till ett högre antal arresteringar eller kontroller vid gränsen.

5. Olaglig profilering har rättsliga och ekonomiska konsekvenser, och det är tjänstemännen som är ansvariga

- Tjänstemän inom brottsbekämpning och gränsförvaltning är **ansvariga** för att hålla profileringen inom lagens gränser.
- **Insamling av tillförlitliga, korrekta och aktuella uppgifter** är avgörande för att säkerställa ansvarigheten.
- **Effektiva klagomålsmekanismer** kan både avskräcka från maktmissbruk och bidra till att säkerställa och återupprätta allmänhetens förtroende för polisen och gränsmyndigheterna.
- **Återkopplingsmöten med företrädare för allmänheten** (för att ta del av åsikter, diskutera profilering och samla in feedback om verksamheten) gör det möjligt att dra viktiga lärdomar och förbättra profileringarna.

6. Algoritmisk profilering måste omfatta särskilda skyddsåtgärder för dataskydd

- Vid utveckling och användning av algoritmisk profilering kan **snedvridning** förekomma i varje steg av processen. För att undvika detta och andra möjliga överträdelser av de grundläggande rättigheterna bör **både it-experterna och de tjänstemän som tolkar uppgifterna ha en ingående förståelse för de grundläggande rättigheterna**.
- Användning av **tillförlitliga uppgifter** är av avgörande betydelse. Om data som återspeglar en befintlig snedvridning eller kommer från otillförlitliga källor matas in i en algoritm uppstår snedvridna och otillförlitliga resultat.
- Algoritmisk profilering måste vara **berättigad, nödvändig och proportionerlig**.
- Behandlingen av uppgifter måste ha **ett specifikt syfte**.
- Enskilda personer har **rätt till insyn i personregister** genom information om vilka personuppgifter som samlats in och lagrats, om behandlingen av personuppgifterna och om sina personliga rättigheter.
- Uppgifterna bör **samlas in, behandlas och lagras på ett säkert sätt**. Myndigheterna ska föra register över behandlingen av personuppgifter (inbegripet vad som görs med uppgifterna) och de tillhörande loggarna (med information om den eller de personer som har tillgång till uppgifterna).
- Olaglig databehandling måste **förebyggas och upptäckas** 1) genom konsekvensbedömning i förväg och 2) genom användning av integritetsverktyg som är "inbyggda" i algoritmen.

Relevanta webbplatser

Europeiska unionen

Europeiska unionens domstol (EU-domstolen): <https://www.curia.eu>

Unionslagstiftning: <http://eur-lex.europa.eu/>

Europeiska unionens byrå för grundläggande rättigheter (FRA): <http://fra.europa.eu>

Europaparlamentet: <https://www.europarl.europa.eu/portal/sv>

Europarådet

Europarådets ministerkommitté: <http://www.coe.int/cm>

Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen):
<http://www.echr.coe.int>

Förenta nationerna

Kontoret för FN:s högkommissarie för mänskliga rättigheter (OHCHR):

<http://www.ohchr.org>

Bekämpning av diskriminering

Europeiska kommissionen mot rasism och intolerans (ECRI): <http://www.coe.int/ecri>

Europeiska nätverket för likabehandlingsorgan (Equinet):

<http://www.equineteurope.org/>

Nationella likabehandlingsorgan: <https://equineteurope.org/members-map/>

Dataskydd

Europeiska datatillsynsmannen (EDPS): <https://edps.europa.eu/>

Europeiska dataskyddsstyrelsen (EDPB): https://edpb.europa.eu/edpb_sv

Nationella dataskyddsmyndigheter: https://edpb.europa.eu/about-edpb/about-edpb/members_sv

Brottsbekämpning

Independent Police Complaints Authorities' Network (IPCAN): <https://ipcan.org/>

Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol): <https://www.cepol.europa.eu/sv>

Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol):

<https://www.europol.europa.eu/sv/about-europol>

Gränsförvaltning

Europeiska gräns- och kustbevakningsbyrån (Frontex): <https://frontex.europa.eu/sv/>

Europeiska stödkontoret för asylfrågor (Easo): <https://www.easo.europa.eu/>

Stora databaser

Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa): <https://www.eulisa.europa.eu/>

1

Bakgrund: Vad är profilering?

I detta avsnitt förklaras vad som avses med profilering och vilka grundläggande rättigheter som kan påverkas. Profilering beskrivs inom ramen för brottsbekämpning och gränsförvaltning med särskilt fokus på tre viktiga delar:

- Begreppet profilering och de olika metoder som används av myndigheter inom brottsbekämpning och gränsförvaltning. I detta avsnitt beskrivs även några av de olika typerna av profilering.
- De viktigaste principer och grundläggande rättigheter som måste respekteras om profilering ska kunna utföras på ett lagligt sätt, i synnerhet icke-diskriminering och rätten till skydd av privatliv och personuppgifter.
- De potentiella negativa följderna av profilering, däribland de möjliga konsekvenserna för enskilda personer, relationen med olika samhällsgrupper och förtroendet för myndigheterna inom brottsbekämpning och gränsförvaltning.

1.1. Hur definieras profilering?

Profilering innebär en **kategorisering av enskilda personer** utifrån deras personliga egenskaper. Dessa egenskaper kan vara "oföränderliga" (t.ex. ålder eller längd) eller "föränderliga" (t.ex. kläder, vanor, intressen och andra inslag i beteendet). Profilering innefattar datautvinning, varigenom enskilda personer kategoriseras **på grundval**

av några av deras observerbara egenskaper för att dra slutsatser, med en viss felmarginal, om andra egenskaper som inte är observerbara (3).

Huvudpunkter

- Profilering innebär en **kategorisering av enskilda personer** utifrån ett antagande om deras egenskaper.
- Det finns två huvudsakliga syften med profilering inom ramen för brottsbekämpning och gränsförvaltning: att **identifiera kända individer baserat på underrättelser om specifika personer** och att genom en **prediktionsmetod** identifiera "okända" individer som kan vara intressanta för myndigheter inom brottsbekämpning och gränsförvaltning. Båda dessa syften kan medföra medvetna eller omedvetna partiska handlingar som kan uppfattas som diskriminerande av enskilda personer.
- Profilering som utförs av gränsvakter och poliser kan påverkas av fördomar som härrör från individuella eller institutionella erfarenheter. Dessa fördomar kan bidra till och förändra bedömningen av profileringen och därmed påverka polisarbetets laglighet och effektivitet.
- Stereotyper kan återspegla en viss statistisk sanning. Även i dessa fall kan de emellertid **skapar problem** om de leder till att en enskild person behandlas som en medlem av en grupp och inte på grundval av sin individuella situation.
- Vid utveckling och användning av algoritmisk profilering **kan snedvridning förekomma i varje steg av processen**. För att undvika detta och andra möjliga överträdelser av de grundläggande rättigheterna bör både de it-expert som utformar algoritmerna och de tjänstemän som samlar in och tolkar uppgifterna ha en ingående förståelse för de grundläggande rättigheterna och hur de ska tillämpas i detta sammanhang.

Profilering används i följande syften:

- Att generera kunskap genom att analysera befintliga uppgifter för att göra antaganden om en viss person. Detta bygger på tidigare erfarenheter och statistiska analyser för att fastställa samband mellan vissa egenskaper och särskilda resultat eller beteenden.
- Att ge stöd åt beslutsprocesser, genom att använda dessa samband för att fatta beslut om vilka åtgärder som bör vidtas.

(3) Dinant J.-M., Lazaro C., Pouillet Y., Lefever N. och Rouvroy A. (2008), s. 3.

Detta innebär att profilering är ett kraftfullt verktyg för tjänstemän inom brottsbekämpning och gränsförvaltning. Metoden medför emellertid vissa betydande risker:

- Profileringen fastställer allmänna samband som inte alltid gäller för varje enskild person. En viss individ kan vara "undantaget från regeln".
- Profiler kan generera felaktiga samband, både för enskilda individer och för grupper.
- Profiler kan skapa skadliga stereotyper och leda till diskriminering.
- Vissa stereotyper kan återspegla en statistisk sanning. Även i dessa fall kan stereotyper emellertid skapa problem om de leder till att en enskild person behandlas som en medlem av en grupp och inte som en individ.

Exempel

Risk för felaktig profilering

Antagandet att kvinnor lever längre än män har stöd i forskningen, men det finns trots allt män som kan leva längre än vissa kvinnor. Beslut mot kvinnor som bygger på detta antagande riskerar därför att vara felaktiga i varje enskilt fall och kan endast vara giltiga ur ett generellt perspektiv.

En bilägare kan låta en släkting eller vän använda bilen, och därför kan ägandet av bilen inte ligga till grund för en profilering om riskfyllt körbeteende.

1.1.1. Profilering inom ramen för brottsbekämpning och gränsförvaltning

Profilering används regelbundet, och lagligt, av tjänstemän inom brottsbekämpning och gränsbevakning för att förebygga, utreda och lagföra brott samt för att förebygga och upptäcka irreguljär invandring.

Med **profilering** avses "varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna

fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar” (4). Resultaten av denna databehandling används som vägledning vid insatser inom gränsförvaltning och brottsbekämpning, däribland kontroll och visitering, arrestering, nekande av åtkomst till vissa områden eller hänvisning till fördjupad kontroll vid gränsen. Det finns två huvudsakliga användningsområden för profilering:

- För att identifiera enskilda personer på grundval av specifika underrättelser. För detta ändamål används en profil med en förteckning över specifika misstänkta personers egenskaper, på grundval av bevis som samlats in vid en särskild händelse.
- Som en prediktionsmetod för att identifiera ”okända” individer som kan vara av intresse för brottsbekämpning och gränsförvaltning. Denna metod bygger på dataanalyser och välgrundade antaganden utifrån tidigare erfarenheter. I idealiska fall är prediktionsmetoderna inriktade på beteenden. I praktiken ligger fokus emellertid ofta inte (eller inte enbart) på beteenden, utan på synliga fysiska egenskaper som ålder, kön eller etniskt ursprung.

I tabell 1 finns en jämförelse mellan de viktigaste egenskaperna hos dessa två typer av profilering i samband med polisarbete.

Tabell 1: Egenskaper för specifikt underrättelsebaserat och prognostiserat polisarbete

	Specifikt underrättelsebaserat polisarbete	Prognostiserat polisarbete
Sammanhang	Ett brott har begåtts, eller en varning har utfärdats om en specifik person	Inget brott har begåtts, eller ingen varning har utfärdats om en specifik person
Metod	Reaktiv	Proaktiv
Mål	Att gripa den/de misstänkta	Att förutse var och när brott kan äga rum eller vem som kan försöka komma in i landet på ett olagligt sätt

(4) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (polisdirektivet) (EUT L 119, 4.5.2016, s. 89).

Använda uppgifter	Specifika underrättelser med anknytning till fallet (den "individuella profilen")	Allmänna underrättelser med anknytning till flera olika fall
Typ av process	En kombination av databaserade och mänskliga processer	Huvudsakligen databaserade ("riskanalys")

Källa: FRA, 2018.

Båda typerna av profilering kan vara olagliga om de inte utförs enligt särskilda skyddsåtgärder, däribland en objektiv och rimlig motivering av profileringen. I [kapitel 2](#) och [kapitel 3](#) finns praktisk information om hur man kan säkerställa att profileringen är laglig och uppfyller de mänskliga rättigheterna.

1.1.2. Hur definieras algoritmisk profilering?

Den snabba tekniska utvecklingen innebär att profileringen allt oftare bygger på användningen av uppgifter som lagras i databaser och system för informationsteknik (it-system). Vid algoritmisk profilering används olika tekniker för att skapa profiler baserade på samband och mönster i uppgifterna. Algoritmisk profilering gör att tjänstemän inom brottsbekämpning och gränsförvaltning kan rikta in sig på enskilda personer eller särskilda grupper som utgör en viss risk på grundval av dataanalysen.

Algoritmisk profilering väcker viktiga frågor kring de grundläggande rättigheterna, bland annat möjlig diskriminering och kränkning av rätten till skydd av privatliv och personuppgifter. I detta avsnitt av vägledningen beskrivs hur tjänstemän inom brottsbekämpning och gränsförvaltning i sitt dagliga arbete kan använda och behandla uppgifter i linje med de grundläggande rättigheterna.

Behandling av personuppgifter: vad säger lagen?

De rättsliga normerna för behandling av personuppgifter i syfte att skapa profiler fastställs i EU:s rättsliga ram för dataskydd. Enligt både artikel 4.4 i den allmänna dataskyddsförordningen och artikel 3.4 i polisdirektivet avses med profilering "varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar".

I artikel 22.1 i dataskyddsförordningen fastslås att profilering endast kan godtas om beslutet inte enbart grundas på automatiserad behandling och inte har rättsliga följder som kan påverka enskilda personer i betydande grad.

Profilering som omfattas av polisdirektivet (se [avsnitt 3.1](#) om algoritmisk profilering och dataskydd) bör uppfylla kraven i artikel 11.3 i polisdirektivet. Där fastslås att "[p]rofilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 (*) ska förbjudas i enlighet med unionsrätten".

(*) Med "särskilda kategorier av personuppgifter" avses "personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning". Se polisdirektivet, artikel 10.1.

Den metod som används för att generera profiler för algoritmisk profilering liknar en teknik som kallas "**beteendeanalys**", vilken innebär att kopplingar görs mellan vissa egenskaper och beteendemönster. I [figur 1](#) visas hur algoritmer kan användas för att göra förutsägelser.

Fokus på hur algoritmer används som stöd vid beslutsfattande

Den ökade tillgången till och användningen av data gör att beslutsfattandet allt oftare underlättas eller ersätts av prediktiva modelleringsmetoder, dvs. användning av algoritmer. En algoritm är en sekvens av kommandon som gör att en dator kan omvandla ett ingångsvärde till ett utgångsvärde. Många algoritmer bygger på statistiska metoder och tekniker som beräknar förhållandena mellan olika variabler. Till exempel kan data om hur mycket alkohol en grupp av personer dricker och den förväntade livslängden inom samma grupp användas tillsammans för att beräkna alkoholdrickandets genomsnittliga inverkan på den förväntade livslängden.

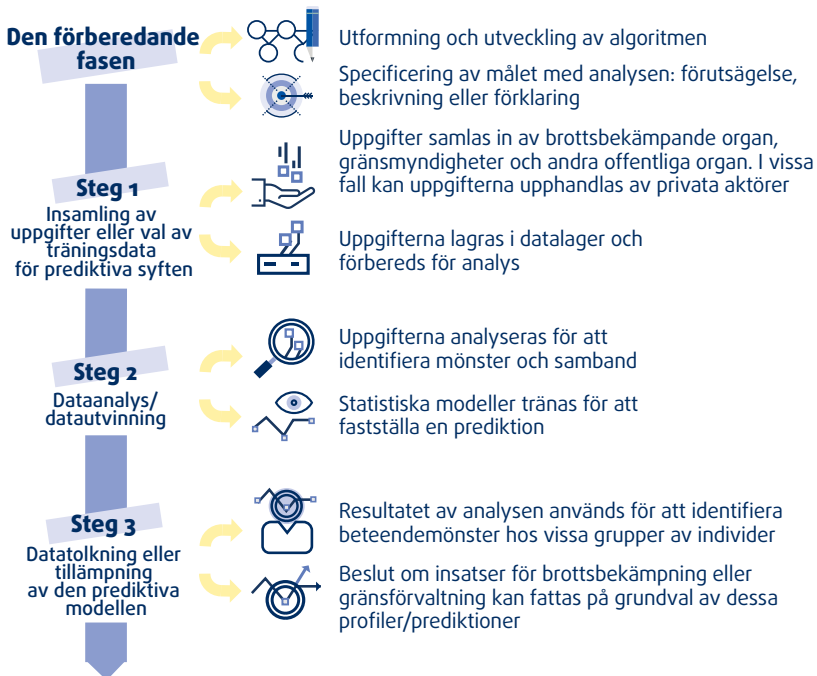
Algoritmernas utgångsvärden har alltid en viss sannolikhet, vilket innebär att det finns en osäkerhet kring de förhållanden eller klassificeringar som beräknas. E-postleverantörer använder till exempel algoritmer för att identifiera vilka meddelanden som är skräppost och skickar dessa till skräppostmappen.

Algoritmerna fungerar bra, men de är inte perfekta. Det händer att skräppost inte upptäcks, utan skickas direkt till inkorgen. Detta kallas ett falskt negativt resultat (dvs. meddelandet identifieras felaktigt som skräppost). Det kan även hända att godkända e-postmeddelanden fångas upp av spamfiltret och skickas till skräppostmappen. Detta kallas ett falskt positivt resultat.

En grundläggande förståelse för hur algoritmer kan bidra till beslutsfattandet gör att tjänstemännen kan identifiera och ställa rätt frågor om möjliga problem med användningen av algoritmer, däribland risken för diskriminering och kränkning av rätten till skydd av privatliv och personuppgifter.

För mer information, se FRA (2018b).

Figur 1: Processen för algoritmisk profilering inom ramen för brottsbekämpning och gränsförvaltning



Källa: FRA, 2018 (anpassat från/baserat på Perry, W.L. et al. [2013], s. 11–15, och Zarsky, T.Z. [2002–2003], s. 6–18).

Skapandet av algoritmer för att utarbeta prognoser är en komplicerad process som kräver många beslut av flera personer som deltar i processen. Processen bygger inte enbart på de regler som följs av en dator, utan även på insamling, bearbetning och analys av uppgifter. Detta är en mänsklig process som omfattar flera olika steg och som kräver beslut av utvecklare och chefer. Den statistiska metoden är endast en del av processen för utarbetandet av de slutgiltiga regler som används för prognoser, klassificering eller beslut (5). I varje enskilt fall kan det sätt på vilket uppgifterna samlas in och används vara diskriminerande.

Exempel

För att vara effektiv och exakt måste programvara för ansiktsgenkänning matas med stora mängder bilder och data. Ju mer data som finns tillgängliga, desto exaktare blir resultatet. Trots detta har de bilder som används för att träna algoritmerna hittills främst visat ljushyade män och förhållandevis få kvinnor och/eller personer med annat etniskt ursprung. Programvaran har därför gett mindre exakta resultat, vilket har ökat sannolikheten för felaktigheter för personer som tillhör dessa grupper. Om metoden används av tjänstemän inom brottsbekämpning eller gränsbevakning för att skapa profiler och, till exempel, besluta om en arrestering, kan detta leda till misstag med allvarliga följder för den enskildes rättigheter och friheter.

För mer information, se Center on Privacy and Technology at Georgetown Law (2016) och Buolamwini J., Gebru T. (2018).

Partiskhet kan förekomma i varje steg av processen för algoritmisk profilering. För att undvika diskriminerande snedvridning och kränkningar av rätten till dataskydd och integritet bör både de som utformar algoritmerna och de tjänstemän inom brottsbekämpning och gränsförvaltning som samlar in och tolkar uppgifterna ha en god förståelse för de grundläggande rättigheterna och deras tillämpning i detta sammanhang.

Användning av tillförlitliga uppgifter är av avgörande betydelse. Vid algoritmisk profilering måste uppgifternas kvalitet bedömas för att säkerställa att de är tillförlitliga: ju lägre variabilitet, desto högre tillförlitlighet. Användning av uppgifter som återspeglar en befintlig snedvridning eller kommer från otillförlitliga källor för att bygga

(5) FRA (2018b), s. 4.

upp en algoritm leder till partiska och otillförlitliga resultat. Fel kan även uppstå i samband med de prediktioner som utläses av uppgifterna:

- Falsa positiva resultat avser fall där enskilda personer har valts ut och utsatts för fördjupad granskning på grund av en felaktig förutsägelse om att de utgör en risk.
- Falsa negativa resultat avser personer som utgör en verklig risk inom ramen för insatser för brottsbekämpning och gränsförvaltning men som inte har identifierats som en risk av systemet.

1.2. När är profilering olaglig?

Huvudpunkter

- Personliga egenskaper får användas som berättigade faktorer för profilering. För att säkerställa att profileringen inte är diskriminerande, och därmed olaglig, måste det emellertid även finnas rimliga skäl till misstanke som bygger på annan information än de **skyddade grunderna**.
 - De skyddade grunderna omfattar kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder och sexuell läggning.
 - Skyddade grunder kan avslöjas, utläsas eller förutses utifrån andra personuppgifter.
- Innan myndigheterna inom brottsbekämpning och gränsförvaltning samlar in och behandlar **personuppgifter** måste de säkerställa att insamlingen och behandlingen av personuppgifter har en rättslig grund, har ett giltigt och berättigat syfte och är nödvändig och proportionerlig.
 - Personuppgifter är alla typer av information som kan användas för att identifiera en person direkt eller indirekt, t.ex. ett namn, ett identifikationsnummer, lokaliseringuppgifter eller någon annan fysisk, fysiologisk, genetisk, psykologisk, ekonomisk, kulturell eller social identitet som är specifik för en person.

Profilering som används på ett lagligt sätt är en **laglig utredningsteknik**. För att vara laglig måste den baseras på **objektiva och rimliga motiveringar** och uppfylla de grundläggande rättigheterna, däribland rätten till icke-diskriminering och skydd av personuppgifter. Profilering anses sakna en objektiv och rimlig motivering "om den

inte eftersträvar ett berättigat mål eller om det inte finns något rimligt förhållande mellan de använda medlen och det mål som eftersträvas” (6).

Profilering kan beröra många olika grundläggande rättigheter. Detta avsnitt är inriktat på de grundläggande rättigheter som främst påverkas av olaglig profilering: rätten till icke-diskriminering och rätten till skydd av privatliv och personuppgifter. Profilering betraktas som olaglig om den

- innebär en omotiverad särskiljande behandling av enskilda personer på grundval av skyddade grunder (se [avsnitt 1.2.1](#)), eller
- på ett omotiverat sätt inkräktar på enskilda personers privatliv och/eller inte uppfyller reglerna för behandling av personuppgifter (se [avsnitt 1.2.2](#)).

1.2.1. Förbudet mot diskriminering

Förbud mot diskriminering: vad säger lagen?

”All diskriminering på grund av bland annat kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning **ska vara förbjuden.”** (*)

Artikel 21 i EU-stadgan om de grundläggande rättigheterna

”Åtnjutandet av varje rättighet som anges i lag skall säkerställas utan diskriminering på någon grund såsom kön, ras, hudfärg, språk, religion, politisk eller annan åsikt, nationellt eller socialt ursprung, tillhörighet till nationell minoritet, förmögenhet, börd eller ställning i övrigt. Ingen skall bli diskriminerad av en offentlig myndighet på någon grund såsom dem som nämnts under punkt 1.”

Artikel 1 i protokoll nr 12 till Europeiska konventionen om de mänskliga rättigheterna

(*) Det bör noteras att många av medlemsstaterna i praktiken har utökat skyddet mot diskriminering utöver de grunder som förtecknas i EU-stadgan och i Europeiska konventionen om de mänskliga rättigheterna (Europakonventionen).

(6) Europeiska kommissionen mot rasism och intolerans (Ecri) (2007), punkt 28.

Diskriminering är "när en person på grund av ras eller etniskt ursprung behandlas mindre förmånligt än en annan person behandlas, har behandlats eller skulle ha behandlats i en jämförbar situation" på grund av förmodade eller verkliga personliga egenskaper (7). Dessa egenskaper kallas "skyddade grunder" eller "skyddade egenskaper" i lagstiftningen om icke-diskriminering. Mer information om den europeiska lagstiftningen och rättsläran inom området för icke-diskriminering finns i 2018 års upplaga av handboken i europeisk diskrimineringsrätt, som publiceras gemensamt av FRA och Europarådet (8).

Det finns flera olika typer av diskriminering:

Direkt diskriminering är när en person behandlas mindre förmånligt *enbart eller huvudsakligen* baserat på en skyddad grund, t.ex. ras, kön, ålder, funktionshinder eller etniskt ursprung (9).

Exempel

Efter ett terroristhot får polisen befogenhet att stoppa och visitera alla som misstänks vara inblandade i terrorism. Hotet tros komma från en terroristorganisation som är aktiv i en viss del av världen, men det finns inte några ytterligare specifika underrättelser. Om en polis stoppar en man enbart eller huvudsakligen mot bakgrund av att hans utseende antyder att han kan ha sitt ursprung i den berörda regionen utgör detta en direkt diskriminering som är olaglig.

Indirekt diskriminering anses förekomma när en *skenbart neutral* bestämmelse eller ett skenbart neutralt kriterium eller förfaringsätt särskilt missgynnar personer med särskilda skyddade egenskaper jämfört med andra personer, om inte bestämmelsen, kriteriet eller förfaringsättet objektivt motiveras av ett berättigat mål och om medlen för att uppnå detta mål är lämpliga och proportionerliga (10).

(7) Rådets direktiv 2000/43/EG av den 29 juni 2000 om genomförandet av principen om likabehandling av personer oavsett ras eller etniskt ursprung (EGT L 180, 19.7.2000, s. 22), samt rådets direktiv 2000/78/EG av den 27 november 2000 om inrättande av en allmän ram för likabehandling (EGT L 303, 2.12.2000, s. 16).

(8) FRA och Europarådet (2018).

(9) Se not 8, s. 43.

(10) Rådets direktiv 2000/78/EG av den 27 november 2000 om inrättande av en allmän ram för likabehandling (EGT L 303, 2.12.2000, s 16) (direktivet om likabehandling i arbetslivet) se även FRA och Europarådet (2018), s. 53.

För att kunna bedöma om indirekt diskriminering har förekommit krävs i regel statistik om huruvida en enskild person i praktiken har blivit behandlad på ett mindre förmånligt sätt på grund av att han eller hon tillhör en grupp med särskilda skyddade egenskaper.

Exempel

I samband med en rutinkontroll beslutar den brottsbekämpande myndigheten att stoppa var tionde bil i staden X mellan klockan 21.00 och 1.00. Den del av stadens befolkning som kör mellan dessa tider utgörs till 60 procent av personer med afrokaribiskt ursprung, medan den afrokaribiska befolkningen i hela staden och dess omgivning inte överstiger 30 procent. Eftersom denna grupp sannolikt kommer att påverkas mer negativt än andra innebär kontrollen en indirekt diskriminering.

Hantering av diskriminering mot bakgrund av enda grund speglar inte de olika uttrycken för ojämlik behandling på ett tillfredsställande sätt. **Diskriminering på flera grunder** beskriver diskriminering som sker på flera olika grunder som uttrycks separat. En person kan till exempel utsättas för diskriminering inte bara på grund av sitt etniska ursprung, utan även sin ålder och sitt kön ⁽¹¹⁾. **Intersektionell diskriminering** avser en situation där flera grunder påverkar och samverkar med varandra samtidigt på ett sätt som gör att de är oskiljaktiga och leder till specifika typer av diskriminering (se rutan med exempel).

Exempel

En polis stoppar och visiterar en ung man av afrikansk härkomst utan rimlig misstanke om att han har begått ett brott. Han blir inte bara diskriminerad på grund av sin ålder – alla unga personer stoppas inte – eller sitt etniska ursprung – alla personer av afrikansk härkomst stoppas inte, utan just för att han både är ung och av afrikansk härkomst.

Diskriminering kan även uppstå vid automatisk behandling av personuppgifter och användning av algoritmisk profilering. Diskriminering kan förekomma under utformningen och genomförandet av algoritmer, genom fördomar som införlivats

(11) FRA och Europarådet (2018), s. 59.

– medvetet eller ej – i algoritmen, och när beslut ska fattas på grundval av den information som erhållits.

I artikel 9.1 i den allmänna dataskyddsförordningen fastslås uttryckligen att behandling av särskilda kategorier av personuppgifter som avslöjar personliga egenskaper, däribland ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, ska vara förbjuden (se figur 9 i avsnitt 2.2.4 för en fullständig förteckning över skyddade grunder). Detta förbud kan upphävas i särskilda fall, till exempel för att skydda ett allmänt intresse, under förutsättning att undantaget har en rättslig grund, är proportionerligt och nödvändigt samt omfattas av lämpliga skyddsåtgärder ⁽¹²⁾.

På liknande sätt, inom ramen för förebyggande, utredning, avslöjande och lagföring av brott, innehåller artikel 11.3 i polisdirektivet om automatiserat individuellt beslutsfattande ett förbud mot "[p]rofilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter", däribland uppgifter som avslöjar ras eller etniskt ursprung och religiös övertygelse samt genetiska och biometriska uppgifter ⁽¹³⁾. Även här kan undantag från förbudet beviljas i vissa fall, men de måste vara nödvändiga, omfatta lämpliga skyddsåtgärder och antingen ha en rättslig grund eller syfta till att skydda intressen som är av grundläggande betydelse för den enskilda personen ⁽¹⁴⁾.

Förbud mot diskriminerande profilering: vad säger lagen?

"Profilering som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden på de villkor som fastställs i artiklarna 21 och 52 i stadgan [om de grundläggande rättigheterna]."

Skäl 38 i polisdirektivet

(12) Allmänna dataskyddsförordningen, artikel 9.2 g.

(13) Mer information finns i artikel 29-gruppen (2017b).

(14) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89) (polisdirektivet).

”Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 (*) **ska förbjudas** i enlighet med unionsrätten.”

Artikel 11.3 i polisdirektivet

(*) *Artikel 10 i polisdirektivet: ”personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning”.*

”När gränskontrolltjänstemän utför in- och utresekontroller **får de inte diskriminera** personer på grund av något av följande: kön, ras eller etnisk tillhörighet, religion eller övertygelse, funktionshinder, ålder eller sexuell läggning.”

Artikel 7 i kodexen om Schengengränserna

Förbudet mot diskriminering innebär inte att personliga egenskaper inte får användas som berättigade faktorer för profilering i samband med brottsutredningar eller gränskontroller (se [avsnitt 2.3](#)). Det måste emellertid finnas rimliga skäl till misstanke som bygger på annan information än de skyddade grunderna. En person kan till exempel passa in på en specifik beskrivning av en misstänkt gärningsperson eller ha ett utseende som inte stämmer överens med informationen i personens resehandlingar ⁽¹⁵⁾.

Fokus på diskriminering på grund av nationalitet

I artikel 21 i EU-stadgan om de grundläggande rättigheterna är **förbudet mot diskriminering på grund av nationalitet begränsat till EU-medborgare**. I direktivet om likabehandling oavsett ras ingår inte nationalitet bland de skyddade grunderna.

Medlemsstaterna har emellertid utvidgat tillämpningsområdet för förbudet mot diskriminering så att det omfattar nationalitet på olika sätt. Detta bygger på en medvetenhet om att nationalitet ibland används som substitut för ras,

(15) Förenade kungariket, Överhuset (2006), Lord Scott, *Opinions of the Lords of appeal for judgment in R (on the application of Gillan (FC) and another (FC)) v. Commissioner of Police for the Metropolis and another (Respondents)*, UKHL 12, 8 mars 2006, punkt 67.

etniskt ursprung eller religion. I vissa sådana fall kan skillnader i behandling på grund av nationalitet förekomma i strid med lagstiftning som förbjuder diskriminering på dessa grunder (se Europeiska nätverket av juridiska experter på jämställdhet och icke-diskriminering, 2016, s. 99). I praktiken är det ofta svårt att särskilja mellan diskriminering på grund av nationalitet och diskriminering på grund av etniskt ursprung.

Det faktum att nationalitet inte uttryckligen nämns som en möjlig grund för diskriminering i artikel 21 i EU-stadgan återspeglar främst skillnaden i status mellan EU-medborgare (och andra personer som har rätt till fri rörlighet enligt unionsrätten) och tredjelandsmedborgare enligt unionsrätten. Detta har särskilt stor betydelse vid gränsförfaranden där nationaliteten är den avgörande faktorn för om en enskild person ska genomgå en fördjupad kontroll eller måste ha ett visum för att komma in i – eller resa genom – Schengenområdet.

Samtidigt finns det en risk för att en systematisk hänvisning till fördjupade kontroller av personer med en viss nationalitet blir diskriminerande. Nationalitet kan vara en berättigad del av riskprofiler för att upptäcka olaglig migration eller möjliga offer för människohandel, men får inte vara den enda eller huvudsakliga utlösande faktorn för en fördjupad kontroll. Precis som i andra sammanhang är särskiljande behandling på grund av nationalitet diskriminerande och därmed olaglig om den används som ett substitut för diskriminering på skyddade grunder med nära koppling till nationalitet, däribland ras, etniskt ursprung eller religion.

I 2014 års rekommenderade principer och riktlinjer avseende mänskliga rättigheter vid internationella gränser från kontoret för FN:s högkommissarie för mänskliga rättigheter ingår nationalitet som en av de skyddade grunder som inte får användas för profilering av migranter (princip 8).

Rättspraxis

I målet *Rosalind Williams Lecraft mot Spanien* blev en kvinna stoppad av en polis på en tågstation i Spanien och ombads att visa upp sina identitetshandlingar. Kvinnan frågade polisen varför hon var den enda personen som stoppades och fick beskedet: "Det beror på att du är svart." I sin dom underströk FN:s råd för mänskliga rättigheter att det i många fall

är berättigat att utföra identitetskontroller för att värna om allmänhetens säkerhet, förebygga brottslighet och övervaka irreguljär invandring. Samtidigt konstaterade rådet att myndigheterna vid utförandet av dessa kontroller inte bör betrakta de utvalda personernas fysiska eller etniska särdrag som ett tecken på att dessa personer eventuellt vistas olagligt i landet. Enligt rådet bör identitetskontroller inte heller utföras på ett sådant sätt att endast personer med vissa fysiska egenskaper eller en viss etnisk bakgrund drabbas. Detta skulle inte bara påverka de drabbades värdighet på ett negativt sätt, utan även bidra till att sprida främlingsfientliga attityder bland befolkningen i allmänhet och stå i strid med en effektiv politik för att bekämpa rasdiskriminering.

Under 2017 lämnades ett liknande klagomål in till Europeiska domstolen för de mänskliga rättigheterna angående behandlingen av en pakistansk medborgare under och efter en polisinsats i Spanien. Domstolen ska fatta beslut om huruvida målsäganden blev diskriminerad på grund av sitt etniska ursprung under identitetskontrollen och om det förekom överträdelser av artikel 8 (rätten till privatliv och familjeliv) eftersom de spanska myndigheterna inte vidtog alla rimliga åtgärder för att utreda eventuella rasistiska motiv i samband med incidenten. Domen har i skrivande stund ännu inte fastställts.

För mer information, se UNHCR, Rosalind Williams Lecraft mot Spanien, meddelande nr 1493/2006 och Europeiska domstolen för de mänskliga rättigheterna, Zeshan Muhammad mot Spanien, nr 34085/17, som ingavs den 6 maj 2017. Se även FRA och Europarådet (2018).

I *B.S. mot Spanien* uppgav en kvinnlig sexarbetare från Nigeria, som vistades lagligt i Spanien, att den spanska polisen hade misshandlat henne fysiskt och verbalt på grund av hennes ras, kön och sysselsättning. Hon hävdade att hon, till skillnad från andra sexarbetare med europeiskt ursprung, utsattes för upprepade poliskontroller och fick utstå rasistiska och sexistiska förolämpningar. Genom två tredjepartsinterventioner från AIRE Centre och den avdelningen för europeisk social forskning vid universitetet i Barcelona ombads Europeiska domstolen för de mänskliga rättigheterna att utreda om intersektionell diskriminering hade förekommit. Domstolen konstaterade en överträdelse av artikel 3 (förbud mot omänsklig och förnedrande behandling), men gick ännu längre för att utreda om man även hade underlåtit att utreda ett möjligt orsakssamband mellan den påstådda rasistiska attityden och

polisens våldsamma handlingar. I denna fråga konstaterade Europeiska domstolen för de mänskliga rättigheterna en överträdelse av artikel 14 (förbud mot diskriminering), eftersom de inhemska domstolarna inte hade tagit hänsyn till målsägandens särskilda utsatthet som prostituerad afrikansk kvinna. Även om domen byggde på ett intersektionellt perspektiv användes inte begreppet "intersektionalitet".

För mer information, se Europeiska domstolen för de mänskliga rättigheterna, B.S. mot Spanien, nr 47159/08, 24 juli 2012.

Fokus på bevisbördan

År 2016 utfärdade Frankrikes högsta domstol för första gången en dom i frågan om diskriminerande identitetskontroller. I sitt *beslut av den 9 november 2016* fastslog domstolen att polisen hade utfört diskriminerande identitetskontroller av 3 av 13 män med afrikanskt eller arabiskt ursprung. Domstolen konstaterade att staten var skyldig i dessa fall och ålade staten att betala en ersättning till de tre målsägandena. I de åtta andra fallen fastslog domstolen att identitetskontrollerna var lagliga, eftersom de hade grundats på objektiva och därmed icke-diskriminerande faktorer. Domstolarna utfärdade inte någon dom i två av fallen, utan hänvisade dem till lägre instanser för förnyad prövning.

Domstolen klargjorde även bevisbördan i liknande fall. Identitetskontroller registreras inte om de inte leder till rättsliga eller administrativa förfaranden. Domstolen förklarade att målsägandena borde ge domstolarna bevis för att diskriminering hade förekommit. Polisen måste antingen bevisa att det inte hade förekommit någon särskiljande behandling vid genomförandet av identitetskontrollerna eller att den särskiljande behandlingen var motiverad på objektiva grunder.

Vidare drog domstolen slutsatsen att domare kan använda bevis i form av undersökningar och statistisk information som bekräftar frekvensen av identitetskontroller som, på diskriminerande grunder, utförts inom samma befolkningsgrupp som målsäganden (dvs. synliga minoriteter baserat på fysiska egenskaper till följd av verkligt eller förmodat etniskt ursprung). Denna bevisning är emellertid i sig inte tillräcklig för att påvisa diskriminering.

Domstolen fastslog därför att en identitetskontroll baserad på fysiska egenskaper som förknippas med ett verkligt eller förmodat etniskt ursprung, utan någon föregående objektiv motivering, är diskriminerande och utgör en allvarlig försummelse som, i dessa tre fall, omfattas av statens ansvar.

För mer information, se Frankrikes högsta domstol (Cour de Cassation), Décision 1245, 9 november 2016.

1.2.2. Rätten till respekt för privatlivet och skydd av personuppgifter

Enligt unionsrätten är rätten till respekt för privatlivet (artikel 7 i EU-stadgan) och skydd av personuppgifter (artikel 8 i EU-stadgan) väl avgränsade men ändå närstående rättigheter. Rätten till privatliv (eller rätten till integritet) är en bredare rättighet som innebär att *all inblandning* i en enskild persons privatliv är förbjuden. Med privatliv avses inte bara sådant som en person vill hålla för sig själv, utan även de sätt på vilka personen uttrycker sin personlighet, till exempel genom att välja umgänge eller klädstil. Skyddet av personuppgifter är begränsat till bedömningen av lagligheten när det gäller *behandlingen av personuppgifter* ⁽¹⁶⁾. Om ingen specifik hänvisning görs till unionsrätten används de två utan åtskillnad vid tillämpning av denna vägledning. Dessa rättigheter är inte absoluta och kan begränsas under vissa omständigheter (se artikel 8 i Europeiska konventionen om de mänskliga rättigheterna och artikel 52 i EU-stadgan).

Rätten till integritet och skydd av personuppgifter: vad säger lagen?

”1. Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.

2. Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välbefinnande, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.”

Artikel 8 i Europeiska konventionen om de mänskliga rättigheterna

(16) FRA, Europeiska datatillsynsmannen och Europarådet (2018).

”Var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer.”

Artikel 7 i EU-stadgan om de grundläggande rättigheterna

”1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. [...]”

Artikel 8 i EU-stadgan om de grundläggande rättigheterna

”1. Den registrerade ska ha rätt att inte bli föremål för ett beslut **som enbart grundas på automatiserad behandling**, inbegripet profilering, och som **har rättsliga följder** för honom eller henne **eller** på liknande sätt **i betydande grad påverkar honom eller henne**.

2. Punkt 1 ska inte tillämpas om beslutet

- a) är nödvändigt för ingående eller fullgörande av ett avtal [...],
- b) tillåts enligt [...] rätt [...] som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller
- c) grundar sig på den registrerades uttryckliga samtycke.”

Artikel 22.1 och 22.2 i den allmänna dataskyddsförordningen

”Medlemsstaterna ska föreskriva att beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida.”

Artikel 11.1 i polisdirektivet

Tabell 2: Dataskyddskrav – skillnader mellan polisdirektivet och den allmänna dataskyddsförordningen

Dataskyddsprincip	Allmänna dataskyddsförordningen	Polisdirektivet
Laglighet, korrekthet, öppenhet	Personuppgifter ska behandlas korrekt, lagligt och på ett öppet sätt.	Personuppgifter ska behandlas korrekt och lagligt.
Ändamålsbegränsning	Personuppgifter som samlats in för ett ändamål ska inte senare behandlas för ett oförenligt ändamål. Ytterligare behandling för vetenskapliga, historiska eller statistiska ändamål får inte vara oförenlig med de ursprungliga ändamålen.	Personuppgifter som samlats in för ett ändamål ska inte behandlas ytterligare för ett oförenligt ändamål. Andra ändamål får inte vara oförenliga med det ursprungliga ändamålet om sådan behandling har godkänts enligt lag och är nödvändig och proportionerlig.
Uppgiftsminimering	Personuppgifter som samlats in ska vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål för vilka de samlades in.	Personuppgifter som samlats in ska vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de samlades in.
Lagringsminimering	Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade under den period som är nödvändig för att uppfylla de ändamål för vilka uppgifterna samlades in. Personuppgifter får lagras under längre perioder för vetenskapliga, historiska eller statistiska ändamål.	Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade under den period som är nödvändig för att uppfylla de ändamål för vilka uppgifterna samlades in.
Korrekthet	De insamlade personuppgifterna ska vara korrekta och uppdaterade. Felaktiga personuppgifter ska raderas eller rättas.	
Integritet och konfidentialitet	Personuppgifter ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse.	

Källa: FRA, 2018.

I EU:s sekundärrätt beskrivs rätten till integritet och skydd av personuppgifter på ett mer ingående sätt. Två olika rättsakter innehåller närmare regler för hur

personuppgifter får samlas in och behandlas. I förordning (EU) 2016/679, den allmänna dataskyddsförordningen, fastställs allmänna principer och skyddsåtgärder för behandlingen av personuppgifter. Direktiv (EU) 2016/680, som även kallas polisdirektivet, är mer specifikt och innehåller ett antal regler för behandling av personuppgifter i samband med brottsbekämpande insatser i syfte att förebygga, utreda, avslöja eller lagföra brott. De viktigaste principerna och några av de viktigaste skillnaderna mellan de två rättsakterna anges i [tabell 2](#). De rättsakter som har utarbetats för inrättandet av de stora EU-databaser som används vid gränsförvaltning, däribland informationssystemet för viseringar (VIS), in- och utresesystemet (EES) och EU-systemet för reseuppgifter och resetillstånd (Etias), innehåller också särskilda regelverk för dataskydd (se [avsnitt 3.2](#) om stora databaser).

Exempel

En gränsvakt skickar en förteckning över flygpassagerare till obehöriga personer. När dessa personuppgifter har delats kan de användas för andra och/eller privata ändamål. Detta är ett uppenbart brott mot dataskyddsprinciperna.

En polis lämnar sitt kontor med en förteckning över personuppgifter för misstänkta personer på sin dataskärm. Detta undergräver principen om skydd av personuppgifter och utgör därför ett brott mot dataskyddsprinciperna.

Rättspraxis

Domstolarnas domar ger vägledning om hur dessa principer tillämpas i praktiken.

Ändamålsbegränsning

I målet *Heinz Huber mot Bundesrepublik Deutschland* granskade EU-domstolen legitimiteten hos Tysklands centrala utlänningsdatabas (*Ausländerzentralregister, AZR*), som innehåller vissa personuppgifter för utlänningar – både EU-medborgare och medborgare utanför EU – som har bott i Tyskland under mer än tre månader. EU-domstolen drog slutsatsen att uppgifter som samlats in för ett särskilt ändamål inte får användas för ett annat ändamål. Domstolen ansåg att AZR är ett lagligt instrument

för tillämpning av uppehållsregler och att skillnaden i behandling mellan utlänningar och tyska medborgare, om vilka färre uppgifter lagras, är motiverad med tanke på det avsedda ändamålet. EU-domstolen konstaterade emellertid att de uppgifter som lagras i AZR inte får användas för bekämpning av brott i allmänhet, eftersom detta skiljer sig från det ändamål för vilket uppgifterna ursprungligen samlades in.

För mer information, se EU-domstolen, mål C-524/06, Heinz Huber mot Bundesrepublik Deutschland, 16 december 2008.

Lagringsminimering

I målet *S. och Marper mot Förenade kungariket* bad målsägandena att deras uppgifter (fingeravtryck, cellprover och DNA-profiler) skulle raderas från den DNA-databas som används för identifiering av gärningspersoner i Förenade kungariket. Deras rättegångar hade slutat med frikännande domar, och de var oroliga för hur deras uppgifter skulle användas i framtiden. Polismyndigheten vägrade. Europeiska domstolen för de mänskliga rättigheterna drog slutsatsen att en obegränsad lagring av DNA-prover från personer som arresterats och senare frikänts eller vars åtal har lagts ner är ett brott mot rätten till integritet. Domstolen betonade risken för stigmatisering, eftersom uppgifterna för personer som inte dömts för något brott behandlades på samma sätt som uppgifterna för dömda personer. Domstolen konstaterade även att den skada som kan orsakas om uppgifterna lagras är särskilt allvarlig för barn med tanke på vikten av deras utveckling och integrering i samhället.

För mer information, se Europeiska domstolen för de mänskliga rättigheterna, S. och Marper mot Förenade kungariket, nr 30562/04 och 30566/04, 4 december 2008.

För att få samla in och behandla personuppgifter i samband med profilering måste myndigheterna inom brottsbekämpning och gränsförvaltning uppfylla fyra grundläggande rättsliga principer:

- **Insamlingen och behandlingen ska vara definierad och reglerad i lag (rättslig grund).** Varje begränsning av rätten till skydd av privatliv och personuppgifter ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter. Lagstiftningen ska uppfylla standarderna för tydlighet och

kvalitet, vilket innebär att allmänheten ska ha tillgång till den och att den ska vara tillräckligt tydligt för att allmänheten ska kunna förstå dess tillämpning och konsekvenser.

- **Insamlingen och behandlingen ska ha ett giltigt, lagligt och lämpligt syfte (*berättigat ändamål*).** Berättigade ändamål fastställs i lagen och kan inte utökas ytterligare. De kan gälla nationell säkerhet, hälsa, allmän ordning eller förebyggande av brottslighet.
- **Insamlingen och behandlingen ska vara oundgänglig för att uppnå detta syfte (*nödvändighet*).** Behandlingen av personuppgifter bör vara begränsad till vad som är nödvändigt för syftet med insamlingen av uppgifter.
- **Insamlingen och behandlingen ska inte vara för omfattande (*proportionalitet*).** Myndigheter som behandlar personuppgifter bör sträva efter att uppnå en rättvis balans mellan syftet och de metoder som används. Med andra ord bör mervärdet av behandlingen inte väga tyngre än dess möjliga negativa konsekvenser.

I [kapitel 3](#) förklaras hur dessa principer kan tillämpas i praktiken.

[Figur 2](#) visar hur dessa principer kan användas för att bedöma om en insats kan begränsa rätten till respekt för privatliv och familjeliv och skydd av personuppgifter (se även [avsnitt 2.3.3](#) om klagomålsmekanismen). Målet *Gillan och Quinton mot Förenade kungariket* visar hur Europeiska domstolen för de mänskliga rättigheterna tillämpar dessa principer för att fastställa om det har förekommit någon överträdelse av rätten till skydd av personuppgifter och integritet (se rutan om rättspraxis).

Figur 2: Överträdelse av rätten till integritet och skydd av personuppgifter – bedömningsprocessen



Källa: FRA, 2018 (baserat på Europarådet (2003), *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human rights*) (Rätten till respekt för privatliv och familjeliv: en vägledning till genomförandet av artikel 8 i Europakonventionen om de mänskliga rättigheterna).

Rättspraxis

I målet *Gillan och Quinton mot Förenade kungariket* ifrågasatte de två målsägandena, två brittiska medborgare, de kontroll- och visiteringsbefogenheter som utövats mot dem genom en domstolskontroll.

Har den åtgärd som vidtagits föreskrivits i lag? Åtgärden stämde överens med avsnitten 44–47 i 2000 års terrorismlag, där det fastställdes 1) att polisbefäl kunde bemyndiga alla uniformerade poliser i ett visst område att utföra kontroller och visiteringar för att förhindra terroristhandlingar, 2) att bemyndigandena skulle bekräftas av ministern och var tidsbegränsade, men kunde förnyas utan begränsningar, 3) att kontrollerna och visiteringarna inte

behövde baseras på en misstanke om att den/de stoppade personerna bar på föremål som kunde användas för terroristhandlingar, även om syftet med kontrollen var att hitta sådana föremål och 4) att personer som vägrade att genomgå en kontroll kunde fängslas, bötfällas, eller både och (*Gillan och Quinton*, punkt 76–80).

Inskränker den åtgärd som vidtagits rätten till skydd av integritet och/eller personuppgifter? De brottsbekämpande myndigheternas användning av tvångsmedel för att stoppa en person och söka igenom dennes kläder och tillhörigheter utgör en tydlig inskränkning av rätten till respekt för privatlivet. Allvarlighetsgraden förstärks av den allmänna exponeringen av personuppgifter, vilken medför en känsla av förödmjukelse och förnedring (*Gillan och Quinton*, punkt 63).

Bedömning av proportionalitet och nödvändighet: Domstolen uttryckte ett antal farhågor om lagens proportionalitet och nödvändighet (*Gillan och Quinton*, punkt 80–86):

- Den lagstadgade standarden för bemyndigandet av kontroller var inte betungande.
- Omfattningen av befogenheten att utfärda bestämmelser är sådan att enskilda personer möter stora hinder om de vill visa att ett bemyndigande eller en bekräftelse ligger utanför de relevanta myndigheternas befogenheter (*ultra vires*) eller innebär maktmissbruk.
- De geografiska områden som omfattades av bemyndigandet var mycket stora, och tidsgränsen förlängdes fortlöpande, vilket begränsade bemyndigandets avsedda karaktär.
- Begränsningarna av de enskilda polisernas utrymme för egen bedömning var mer formella än verkliga.
- Möjligheten att få tillgång till rättsmedel var begränsad eftersom den polis som utförde kontrollen inte behövde visa att misstanken hade varit rimlig, och därför var det nästan omöjligt att bevisa att befogenheten hade utövats på ett felaktigt sätt.

Dessa överväganden fick Europeiska domstolen för de mänskliga rättigheterna att dra slutsatsen att de relevanta avsnitten i terrorismlagen varken var tillräckligt avgränsade eller föremål för adekvata rättsliga

skyddsåtgärder mot missbruk, och att de därmed innebar en överträdelse av artikel 8 i Europakonventionen

För mer information, se Europeiska domstolen för de mänskliga rättigheterna, Gillan och Quinton mot Förenade kungariket, nr 4158/05, 12 januari 2010.

De rättsliga krav för profilering som fastställs i EU:s omarbetade rättsliga ram för skydd av personuppgifter beskrivs i kapitel 3.

1.3. Vilka effekter kan olaglig profilering få för brottsbekämpning och gränsförvaltning?

Profilering som endast bygger på breda kategorier som ras, etniskt ursprung eller religion är inte bara olaglig, utan kan även medföra nackdelar för de brottsbekämpande och gränsförvaltande myndigheterna. I detta avsnitt beskrivs två möjliga negativa effekter:

- Den största svårigheten gäller den påfrestning som kan uppstå på relationerna till olika samhällsgrupper. Profilering kan leda till fientlighet bland de grupper som är särskilt påverkade och minska förtroendet för polisen och gränsmyndigheterna. Detta kan i sin tur begränsa effektiviteten i de metoder som bygger på samarbete med allmänheten.
- Det råder även tvivel om hur effektivt det är att använda breda kategorier av profiler vid gränsförvaltning och brottsbekämpning, till exempel om det leder till att en person misstänks på falska grunder ⁽¹⁷⁾.

Om profileringen utförs på ett olagligt sätt kommer myndigheterna dessutom att utsättas för klagomålsförfaranden eller rättsliga åtgärder. Detta kan ha formen av tillsyn på intern nivå genom polismyndighetens klagomålsinstans, särskilda klagomålsinstanser, tillsynsmyndigheter eller det civilrättsliga och straffrättsliga systemet (se [avsnitt 2.3](#)). Enskilda tjänstemän och chefer på mellannivå kan omfattas av administrativa och/eller straffrättsliga påföljder om de är inblandade i eller

(17) FRA (2017d), s. 51.

samtycker till olaglig profilering. Detta kan tära på resurserna och försämra myndigheternas moral och anseende.

Huvudpunkter

- **Olaglig profilering undergräver förtroendet** för de brottsbekämpande och gränsförvaltande myndigheterna och kan leda till att relationerna till lokala befolkningsgrupper försämras.
- Det råder **tvivel om huruvida användningen av bred profilering verkligen är effektiv** för att upptäcka brott eller skydda gränser. Bevisen är tvetydiga när det gäller huruvida en sådan profilering kan öka framgången för insatser inom brottsbekämpning eller gränsförvaltning.

1.3.1. Inverkan på förtroendet för polisen och gränsförvaltningen och relationerna till samhället

Forskning visar att användningen av breda profiler kan ha en negativ inverkan på de personer som utsätts och de samhällsgrupper de tillhör ⁽¹⁸⁾. I nedanstående ruta presenteras några personers vittnesmål efter att ha blivit stoppade och visiterade.

Exempel

Inverkan av kontroll- och visiteringsinsatser och gränskontroller på enskilda personer

1. Poliskontroller – Keskinen, S. et al (2018)

Mellan 2015 och 2017 intervjuade Svenska social- och kommunalhögskolan vid Helsingfors universitet 185 personer om deras upplevelser av etnisk profilering. Undersökningen visade att de flesta av de svarande uppfattade kontrollerna som obehagliga, irriterande eller förödmjukande. Här följer några utdrag ur svarandenas vittnesmål.

“Lite senare stoppade en annan polis mig igen [...] när jag gick längs gatan med två ljushyade vänner, en från Finland och en från Nederländerna. Och

(18) FRA (2017d).

gjorde precis samma sak ... ställde samma frågor. Jag blev arg eftersom jag inte förstod varför polisen valde ut just mig. Jag frågade dem, men de sa bara att de gjorde sitt jobb.” (Kvinna, 30-årsåldern, afrikanskt land)

”En gång när min mamma och min bror var ute och promenerade på stan kom två poliser fram och sa: ”Visa era pass!”. Jag anser att det är etnisk profilering. Då sa min bror [på finska]: ”Vi har inte våra pass, vi brukar inte alltid ha dem med oss”. När poliserna hörde att han pratade flytande finska verkade de inte längre bry sig. Jag blev arg eftersom jag vet att etnisk profilering är olaglig, men det visste inte min mamma och min bror. Så jag tyckte att de hade blivit dåligt behandlade. Jag blev förstas jättearg. När jag berättade för dem att det som hänt var olagligt så insåg de förstas att de hade blivit stoppade eftersom de [...] såg utländska ut och inte finska.” (Kvinna, 20-årsåldern, Somalia och Finland)

”De har alltid en liknande beskrivning. Jag tänker att om de har letat efter samma person i 11 år och inte har lyckats få tag på honom, då gör de inte ett särskilt bra jobb, eftersom deras beskrivning [gränskontrollens] alltid är samma och eftersom jag alltid passar in på den beskrivningen [skratt].” (Man, 30-årsåldern, afrikanskt land och Finland)

För mer information, se Keskinen, S. et al (2018), The Stopped – Ethnic Profiling in Finland (De kontrollerade – etnisk profilering i Finland).

2. Gränskontroller – FRA (2014a och 2014b)

”Jag förstår varför [gränsvakten] stoppade mig, men han behövde inte skicka mig hit [fördjupad kontroll/polisstation] eller behandla mig som en brottsling. De gör detta med alla från Östeuropa”. (Passagerare från Serbien, man, intervjuad på Frankfurts flygplats)

Fråga: *”Hur tycker du att de behandlade dig vid den första kontrollen?”*

Svar: *”Jag tycker inte att de behandlade mig bra. Det var förnedrande. Han behandlade mig dåligt. Han bara tog mitt pass, tittade på det och ringde direkt till immigrationsavdelningen. Han ställde några frågor och höjde sin röst, men jag förstod ingenting. De ledde bort mig från kön, men de visade inte någon respekt och de skrämde mig.”*

Fråga: "Varför kände du dig rädd eller förnedrad?"

Svar: "Jag visste inte vad som skulle hända och de förklarade inte någonting. Där var massor med folk runtomkring och vakten pratade med de andra vakterna utan att prata med mig. Sedan fick jag vänta och jag vet fortfarande inte varför jag var där." (Passagerare från Angola, man, intervjuad på flygplatsen Schiphol)

"Jag kan verkligen förstå [...] gränsvakterna. Det är ju jobbigt för dem också att sitta i sitt bås timme efter timme! Så det händer ibland att de har ett negativt beteende och skriker på folk som oss." (Man, turkisk medborgare, lastbilschaufför som ofta korsar gränsen, Kipi)

Slutresultatet av dessa enskilda personers erfarenheter kan dock få negativa effekter för en hel grupp ⁽¹⁹⁾. Detta kan bidra till en betydande försämring av relationen mellan tjänstemännen inom polisen och gränsförvaltningen och medlemmarna i de minoritetsgrupper som utsätts för många kontroll- och visiteringsinsatser eller fördjupade gränskontroller.

Fallstudie

Kontroller och visiteringar vid störning av den allmänna ordningen (Förenade kungariket 2011 och Frankrike 2005)

Efter de upplopp som inträffade i flera stora brittiska städer i augusti 2011 intervjuade London School of Economics och tidningen The Guardian 270 upprosmakare om varför de hade deltagit i upploppen. Undersökningen visade att misstro och motvilja mot polisen var en betydande faktor och att "[d]e vanligaste klagomålen gällde personernas vardagliga upplevelser av polisarbetet. Många uttryckte en djup frustration över hur personer i deras samhällsgrupper utsattes för kontroller och visiteringar".

För mer information, se London School of Economics (2011).

En liknande dynamik har identifierats i andra av EU:s medlemsstater. Upploppen i Frankrike i november 2005 utlöstes av en olycka där två

(19) Förenta nationerna (FN) (2007), punkt 57.

ungdomar från en minoritetsgrupp omkom efter en påstådd polisjakt (se Jobard, 2008 och Body-Gendrot, 2016).

För mer information, se Hörnqvist (2016).

Kopplat till detta kan profilering leda till ökade nivåer av fientlighet vid andra kontakter mellan enskilda personer och polisen eller andra brottsbekämpande organ. En ökad fientlighet ökar risken för att rutinärenden utvecklas till aggression och konflikter och skapar säkerhetsproblem för både tjänstemän och samhällsmedborgare.

Mer övergripande visar den senaste forskningen att personer som har kontrollerats, arresterats, dömts eller fängslats ofta undviker andra offentliga tjänster vid sidan av rättsväsendet, till exempel hälso- och sjukvård, arbetsförmedlingar och utbildningsinstitutioner ⁽²⁰⁾. Utan att ifrågasätta de berättigade orsaker som leder till arrestering av dömda personer bör det påpekas att uteslutningen av redan marginaliserade delar av befolkningen från sådana institutioner kan undergräva minoritetsgruppernas sociala delaktighet och integration.

Fokus på resultaten av FRA:s undersökning EU-Midis II

Under 2015 och 2016 samlade FRA in uppgifter från fler än 25 500 intervjupersoner från olika etniska minoriteter och invandrabakgrunder i de 28 EU-medlemsstaterna.

Vilka uppgifter samlades in?

När det gäller profilering tillfrågades intervjupersonerna om de trodde att de hade stoppats av polisen på grund av sin invandrabakgrund eller bakgrund i en etnisk minoritet, och om hur de hade behandlats av polisen, bland annat om de hade utsatts för fysiska angrepp. Undersökningen omfattade inte några frågor om kontakter med gränsförvaltningen.

Vad visar resultaten?

Kontroller och etniskt ursprung: Resultaten visar att 26 procent av alla som svarade på EU-Midis II hade stoppats och kontrollerats av polisen under de

(20) Brayne, S. (2014), s. 367–391.

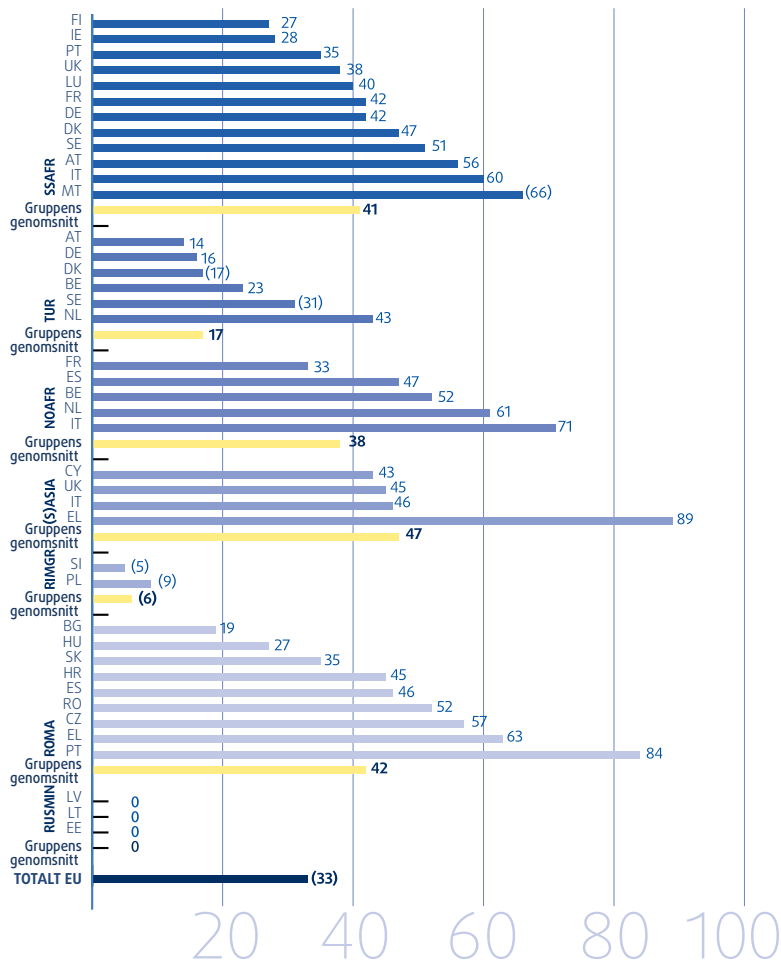
fem senaste åren före undersökningen. Av dem som hade stoppats under de fem åren före undersökningen uppgav 33 procent att det berodde på deras etniska ursprung och invandrarbakgrund.

Uppfattning av diskriminering: Nästan varannan av de svarande med ursprung i Asien (47 procent), Afrika söder om Sahara (41 procent) och Nordafrika (38 procent) som hade stoppats inom denna tidsram uppgav att de hade stoppats på grund av sin invandrarbakgrund eller sitt ursprung i en etnisk minoritet. Likaså ansåg nästan varannan av de romer som hade stoppats (42 procent) att det berodde på deras etniska bakgrund. Däremot är denna procentsats mycket lägre bland de personer med turkisk bakgrund som stoppades (17 procent) (se figur 3).

Respekt: Resultaten visar att en majoritet (59 procent) av alla intervjupersoner som hade stoppats av polisen under de senaste fem åren före undersökningen tyckte att de hade behandlats med respekt (25 procent "mycket respektfullt", 34 procent "ganska respektfullt"). En av fyra (24 procent) uppgav att polisens behandling "varken var respektfull eller respektlös". Samtidigt uppgav 17 procent att polisen behandlade dem respektlöst (8 procent "ganska respektlöst" och 9 procent "mycket respektlöst"). Personer med romskt eller nordafrikanskt ursprung som hade stoppats uppgav att de hade upplevt ett respektlöst beteende från polisens sida under den senaste kontrollen (25 procent respektive 21 procent), oftare än de andra målgrupperna.

För mer information, se FRA (2017b).

Figur 3: De senaste poliskontrollerna som uppfattades som etnisk profilering av dem som stoppades under de fem åren före EU-Midis II-undersökningen, per EU-medlemsstat och målgrupp (%)^{a,b,c,d}



Anm.: ^a Av de intervjupersoner som stoppades av polisen under de fem åren före undersökningen (n=6 787), viktade resultat.

- b Resultat som baseras på ett litet antal svar är mindre tillförlitliga statistiskt sett. Resultat som baseras på 20–49 oviktade observationer i en gruppsumma eller baseras på celler med färre än 20 oviktade observationer återges därför inom parentes. Resultat som baseras på färre än 20 oviktade observationer i en gruppsumma offentliggörs inte.*
- c Frågor: "Har du blivit stoppad, kroppsvisiterad eller förhörd av polisen under de senaste fem åren i [LAND] (eller sedan du kom till [LAND])?". "Anser du att du stoppades DEN SENASTE GÅNGEN på grund av din etniska bakgrund eller invandrarbakgrund?"*
- d Förkortningarna för målgrupper avser första och andra generationens invandrare från [land/region]: TUR = Turkiet, SSAFR = Afrika söder om Sahara, NOAFR = Nordafrika, SASIA = Sydasiien, ASIA = Asien, ROMA = Romska minoriteten.*

Källa: FRA, 2017b.

Fokus på vikten och nyttan av att samla in uppgifter om poliskontroller

Av de 28 EU-medlemsstaterna är Förenade kungariket för närvarande den enda där insamlingen av uppgifter om poliskontroller systematiskt omfattar information om de stoppade personernas etniska ursprung (se även [avsnitt 2.2.5](#) och [avsnitt 2.3.1](#)).

De insamlade uppgifterna ligger till grund för en mätning av frekvensen av kontroll och visitering för olika etniska grupper i England och Wales. De etniska kategorier som används är de som förtecknas i Förenade kungarikets folkräkning 2001. I denna folkräkning identifierades 16 kategorier, som sammanställdes i fem bredare grupper:

- Vita: Engelsk/walesisk/skotsk/nordirländsk/brittisk, irländsk och annan vit bakgrund.
- Blandade/varierade etniska grupper: Vit och svart karibisk, vit och svart afrikansk, vit och svart asiatisk och annan bakgrund i blandade/varierade etniska grupper.
- Asiatisk/asiatisk brittisk: Indisk, pakistansk, bangladeshisk och annan asiatisk bakgrund.

- Svart/afrikansk/karibisk/svart brittisk: Afrikansk, karibisk och annan svart/afrikansk/karibisk bakgrund.
- Övriga etniska grupper: Kinesisk och andra etniska grupper.

Med hjälp av de uppgifter om kontroller och visiteringar som samlats in jämförs antalet personer från en viss etnisk grupp som stoppats och visiterats med det totala antalet personer från den berörda etniska gruppen som bor i området, varefter en andel beräknas per 1 000 personer.

För åren 2016–2017 visar analysen av de insamlade uppgifterna att polisen hade utfört fyra kontroller per 1 000 vita personer, jämfört med 29 kontroller per 1 000 svarta personer. Uppgifterna visar även att den högsta andelen förekom bland de tre svarta etniska grupperna – övriga svarta (70 kontroller per 1 000 personer), svart karibisk (28 per 1 000 personer) och svart afrikansk (19 per 1 000 personer).

Utan belägg i form av disaggregerade data är det svårt att bevisa om det finns några skillnader i polisens insatser mot vissa etniska grupper och – om så är fallet – om dessa skillnader kan vara ett resultat av diskriminerande profileringsförfaranden. Disaggregerade data är allmänt tillgängliga i England och Wales, uppdelade per polisstyrka. Detta gör det möjligt att identifiera olika förfaranden bland polisstyrkorna som antingen kan förklaras som berättigade eller som kan användas för att identifiera en möjlig diskriminering i polisernas metoder. Uppgifterna används även på nivån för enskilda polistjänstemän för att identifiera diskriminerande förfaranden i deras arbete.

*För mer information, se regeringens [webbplats om kontroller och visiteringar](#), [webbplatsen för Independent Office for Police Conduct](#) och [inrikesministeriets webbplats med öppna data om brott och polisarbete](#). Se även *Förenade kungariket (2018)*. För vägledning om registreringsmetoder, se *Open Society Justice Initiative (2018b)*.*

Fallstudie

Undersökning om relationerna mellan polisen och allmänheten i Frankrike

Under 2016 genomförde den franska ombudsmannen (*Défenseur des droits*) en undersökning om tillgången till rättigheter. *Défenseur des droits* fungerar även som den nationella polisens klagomålskommission. Undersökningen omfattade ett representativt urval av fler än 5 000 personer.

I den första delen av rapporten presenteras resultaten för de brottsbekämpande myndigheternas beteende. Undersökningen visade att relationerna mellan allmänheten och polisen generellt sett är goda. En stor andel av de svarande uppgav att de hade förtroende för polisen (82 procent).

En mer specifik analys av undersökningen visar att de flesta inte utsätts för identitetskontroller: 84 procent av de svarande uppgav att de inte hade kontrollerats under de föregående fem åren (90 procent av kvinnorna och 77 procent av männen). De som uppgav att de hade blivit kontrollerade rapporterade få fall av beteenden som stred mot säkerhetsstyrkornas yrkesetiska regler under de senaste kontrollerna, däribland informella tilltalsätt (16 procent), brutalitet (8 procent) eller förolämpningar (7 procent). Däremot rapporterade 29 procent en bristande artighet, och mer än hälften av de svarande (59 procent) som hade kontrollerats uppgav att de inte hade fått någon förklaring av skälen till kontrollen. I allmänhet uppfattas identitetskontrollerna som mer berättigade om säkerhetsstyrkorna tar sig tid att förklara skälen till kontrollerna.

Uppgifterna visar även att vissa grupper av personer rapporterar mer negativa upplevelser. Unga män i åldern 18–24 år löper nästan sju gånger större risk att utsättas för täta identitetskontroller (dvs. mer än fem gånger under de senaste fem åren) än den allmänna befolkningen, och män som uppfattas som svarta eller arabiska utsätts för mellan sex och elva gånger mer av täta identitetskontroller än resten av den manliga befolkningen. Om vi kombinerar dessa två kriterier har 80 procent av männen som är yngre än 25 år och som uppfattas som arabiska eller svarta kontrollerats minst en gång under de senaste fem åren (jämfört med 16 procent av övriga intervju personer). Jämfört med den allmänna befolkningen löper denna grupp 20 gånger större risk att utsättas för identitetskontroller.

Unga män som uppfattas som svarta eller arabiska rapporterade dessutom fler fall av problematiskt beteende under de senaste identitetskontrollerna, däribland användning av informella tilltalssätt (40 procent jämfört med 16 procent av det totala urvalet), förolämpningar (21 procent jämfört med 7 procent av det totala urvalet) eller brutalitet (20 procent jämfört med 8 procent av det totala urvalet). Dessa negativa upplevelser och de täta kontrollerna förknippas med lågt förtroende för polisen. Denna grupp rapporterade också om försämrade relationer till polisen.

Slutligen visar resultaten att endast ett fåtal av de svarande (5 procent) som uppgav att polisen hade brutit mot de yrkesetiska reglerna under identitetskontrollerna har rapporterat denna situation. De flesta uppgav att de inte rapporterar sina upplevelser eftersom de tycker att det verkar meningslöst.

För mer information, se Défenseur des droits (2017).

Om breda profiler tillämpas på en minoritetsgrupp kan det, i kombination med andra stigmatiserande polisinsatser, leda till att denna grupp utvecklar en negativ syn på sig själv. Dessutom kan en negativ uppfattning om gruppen spridas bland allmänheten. Minoritetsgruppen kan bli en så kallad "misstänkt samhällsgrupp", som allmänheten förknippar med kriminalitet⁽²¹⁾. Detta kan leda till ökade fördomar.

Minoritetsgruppen kan bli föremål för ett oproportionerligt högt antal polisinsatser, vilket i sin tur sannolikt leder till ett högre antal arresteringar eller gränskontroller. Som en följd av detta kan ett självuppfyllande förhållande uppstå mellan ett intensivt polisarbete och ett ökat antal arresteringar (se rutan)⁽²²⁾.

Fokus på risken för en "självuppfyllande profetia"

Om polistjänstemännen inte baserar sin profilering på rimliga grunder utan på fördomar kommer de sannolikt att tolka information på ett sätt som bekräftar deras egna fördomar. Detta kallas "konfirmeringsbias" eller "bekräftelsefördom". Detta inträffar när polisernas fördomar gör att de förväntar sig att en individ ska bete sig på ett olagligt sätt på grund av

(21) Europeiskt centrum för övervakning av rasism och främlingsfientlighet (2006), s. 54.

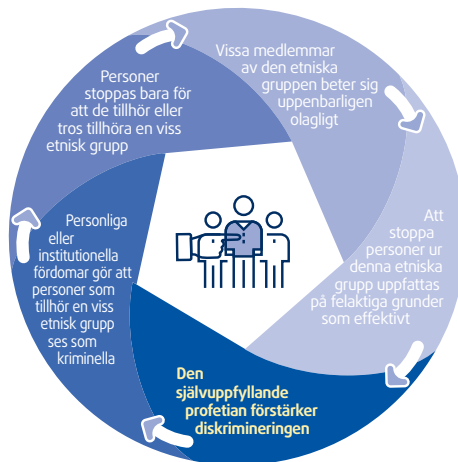
(22) Harcourt, B. (2004), s. 1329-1330; Underhusets kommitté för inrikesfrågor (2009), punkt 16 och FN (2007).

personens verkliga eller förmodade ras, etniska ursprung, kön, sexuella läggning, religion eller andra skyddade grunder. Denna typ av snedvridning gör att tjänstemän med sådana fördomar sannolikt väljer ut fler personer som passar in på en viss beskrivning.

Eftersom det är mer sannolikt att bevis för brottsliga handlingar påträffas hos individer som kontrolleras än hos dem som inte kontrolleras kan denna fördomsbaserade profilering förstärka befintliga stereotyper. Detta falska "bevis" för att beslutet att stoppa personerna var korrekt kallas "självuppfyllande profetia". Sådan fördomsbaserad profilering är diskriminerande, olaglig och ineffektiv, och den förstärker befintliga stereotyper.

I figur 4 beskrivs hur den "självuppfyllande profetian" förstärker kriminaliseringen av enskilda personer.

Figur 4: Den självuppfyllande profetians cykel



Källa: FRA, 2018.

1.3.2. Profileringens effektivitet

Det råder även tvivel om effektiviteten i att använda profilering baserad på breda kategorier för att upptäcka brott. Det är oklart om profilering verkligen ökar framgångskvoten (eller "träffkvoten") i de brottsbekämpande insatserna.

Vissa uppgifter antyder att den frekvens med vilken enskilda personer stoppas inte nödvändigtvis motsvarar andelen överträdelser bland olika etniska grupper (se rutan). Det bör noteras att uppgifterna om rättskipning i de flesta av EU:s medlemsstater inte möjliggör någon överblick över hanteringen av enskilda fall i det straffrättsliga systemet. Därför går det inte att fastställa om en arrestering leder till åtal och straff.

Fallstudie

Förändrade kontrollmönster leder till en högre "träffkvot" (1998–2000, USA)

Under 1998 var 43 procent av den amerikanska tullens kontroller inriktade på personer med afroamerikanskt eller latinamerikanskt ursprung, en avsevärt större andel än deras andel av resenärerna. En särskilt stor andel av kontrollerna, däribland röntgenkontroller och kroppsbesiktningar, gällde kvinnor som misstänktes vara narkotikakurirer. Detta grundades på en profil som i stor utsträckning byggde på nationalitet och etniskt ursprung. Träffkvoterna för dessa kontroller var låga för samtliga grupper: 5,8 procent för "vita", 5,9 procent för "svarta" och 1,4 procent för "latinamerikaner". Den var särskilt låg för latinamerikanska kvinnor, som i själva verket var minst benägna att transportera droger på eller i kroppen. Under 1999 förändrade den amerikanska tullen sina förfaranden och uteslöt ras från de faktorer som skulle ligga till grund för kontrollerna. I stället började man använda tekniker som var inriktade på beteende, till exempel nervositet och osammanhängande förklaringar, mer underrättelseinformation och en noggrannare övervakning av besluten om kontroller och visitering. År 2000 hade rasskillnaderna i tullens kontroller nästan eliminerats helt. Antalet utförda kontroller sjönk med 75 procent. Samtidigt förbättrades träffkvoten från under 5 procent till över 13 procent och blev nästan likvärdig för alla etniska grupper.

För mer information, se Harris (2002), USA (2000).

Ineffektivitet på grund av olaglig profilering (2007–2008, Ungern)

Forskning som utförts i Ungern visade att romer i oproportionerligt hög grad valdes ut för identitetskontroller. Omkring 22 procent av alla som kontrollerades av polisen tillhörde den romska samhällsgruppen, samtidigt som romernas andel av hela befolkningen endast var 6 procent. Det oproportionerligt höga antalet identitetskontroller av romer återspeglades inte i några bevis på olagligt beteende: 78 procent av identitetskontrollerna av romer ledde inte till att någon åtgärd vidtogs av polisen, och 19 procent kunde kopplas till mindre förseelser (*) (jämfört med 18 procent av kontrollerna av den allmänna befolkningen). Dessutom var arresteringsgraden ungefär densamma för den romska samhällsgruppen och befolkningen i allmänhet.

För mer information, se Tóth, B.M. och Kádár, A. (2011).

(*) Mindre förseelser är kvasikriminella överträdelser vars allvarsgrad inte når upp till kriminell nivå (dvs. de regleras inte i strafflagen). De mindre förseelserna varierar mellan brott som bestraffas med ett 60-dagars fängelsestraff, däribland prostitution eller fysiska hot, och sådana som bestraffas med mindre stränga åtgärder (t.ex. böter, konfiskering av varor eller förbud mot att delta i vissa evenemang). Exempel på sådana brott är snatteri eller trafiköverträdelser. *Se Kádár, A., Körner, J., Moldova, Z. och Tóth, B. (2008), s. 23.*

Det uppstår även frågor kring skälen till att vissa enskilda personer stoppas. En undersökning i Förenade kungariket visade att 27 procent (2 338) av de kontroller och visiteringar som granskades inte byggde på några rimliga grunder, även om många av insatserna hade godkänts av ledningen ⁽²³⁾. Enligt undersökningen antyder detta att polisstyrkorna inte alltid uppfyller sin skyldighet att säkerställa likabehandlingen inom den offentliga sektorn, vilken innebär att de måste ta vederbörlig hänsyn till behovet att eliminera olaglig diskriminering och främja likabehandling i fråga om möjligheter, skapa goda relationer och för detta ändamål säkerställa att de samlar in, analyserar och offentliggör uppgifter på ett lämpligt sätt för att visa att de har tillräcklig information för att förstå följderna av sitt arbete.

(23) Förenade kungariket, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), s. 6.

2

Laglig profilering: princip och praktik

I detta kapitel behandlas profilering som används av poliser i yttre tjänst, i synnerhet vid kontroller och visiteringar, och av tjänstemän inom gränsförvaltningen, i synnerhet vid hänvisningar till fördjupade kontroller. I kapitlet förklaras de huvudsakliga principer och metoder som kan bidra till att minska risken för olaglig profilering. Dessa åtgärder kan vidtas både på ledningsnivå och på operativ nivå. De utgår från de olika rättsliga och praktiska förutsättningarna vid kontroll- och visiteringsinsatser och gränskontroller.

När det gäller gränsförvaltning innehåller kodexen om Schengengränserna (förordning (EU) nr 2016/399) ⁽²⁴⁾ enhetliga regler för gränskontroller vid EU:s yttre gräns. Detta innebär att vissa av de principer som beskrivs i detta kapitel – till exempel angående den information som måste ges till tredjelandsmedborgare vid fördjupade kontroller – är föreskrivna i lag och bindande för medlemsstaterna. Dessutom har Frontex en viktig roll när det gäller att främja en genomgående hög standard för gränskontrollerna. I 2016 års förordning om den europeiska gräns- och kustbevakningen föreskrivs att medlemsstaterna ska följa de gemensamma läroplaner som har utarbetats av Frontex i samband med utbildning av gränsbevakningspersonal. Den gemensamma läroplanen offentliggjordes 2012 och innehåller en del om grundläggande rättigheter som även omfattar profilering (se [avsnitt 2.2.3](#) om målinriktad utbildning).

(24) Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 77, 23.3.2016, s. 1).

Fokus på grunderna för en fördjupad kontroll vid gränsen

Gränskontrollernas systematiska karaktär innebär att varje resenär genomgår en grundläggande första kontroll där resehandlingar och eventuella andra inresevillkor kontrolleras. Vissa resenärer kan dessutom hänvisas till en ytterligare fördjupad kontroll. Detta kan bero på en rad olika orsaker: en träff i en databas, en misstänkt resehandling, matchning av en riskprofil eller misstänkt beteende.

Under den inledande kontrollen kan gränsvakten fatta beslut på grundval av information som erhållits genom att uppgifter i den maskinläsbara resehandlingen (vilken omfattar biometriska kännetecken) jämförts med uppgifter som lagrats i nationella, europeiska eller internationella databaser, däribland Schengens informationssystem, informationssystemet för viseringar samt Europols och Interpols databaser. I praktiken fattas beslut om en fördjupad kontroll ofta till följd av en träff i någon av databaserna.

En person kan emellertid även hänvisas till en fördjupad kontroll av andra orsaker, till exempel om personen passar in på en riskprofil eller om tjänstemannen har andra misstankar om personen. I katalogen över rekommendationer för en korrekt tillämpning av Schengenregelverket och bästa metoder fastställs att målet med inledande kontroller, förutom att utföra gränskontroller enligt kodexen om Schengengränserna, bör vara att profilera passagerare och välja ut misstänkta personer för en ingående fördjupad kontroll (*). Gränsvakterna måste därför bedöma en kombination av andra indikatorer och kriterier för att fastställa om en person kan försöka komma in i EU på ett olagligt sätt, om personen kan utgöra en säkerhetsrisk eller om personen till exempel kan ha fallit offer för människohandel. Oavsett om de tillämpar en specifik befintlig riskprofil eller inte i dessa situationer använder gränsbevakningspersonalen sig av profilering.

Behovet av att säkerställa ett jämt flöde av resenärer innebär att gränsvakterna har begränsat med tid för att utföra en objektiv bedömning av vilka personer som ska hänvisas till en fördjupad kontroll. Uppgifter från Frontex visar att tjänstemännen i EU:s medlemsstater i genomsnitt bara har 12 sekunder på sig att besluta om de ska välja ut en person för ytterligare kontroll (**). Detta innebär att de är hårt pressade att fatta snabba och korrekta beslut.

(*) *Europeiska unionens råd (2009), rekommendation 43.*

(**) *Europeiska gräns- och kustbevakningsbyrån (Frontex) (2015).*

Principerna och de praktiska verktygen i detta kapitel erbjuder information om hur diskussioner och handlingar kan uppmuntras för att hjälpa tjänstemännen och deras övergripande organisationer att utföra sin profilering inom lagens gränser. De tre viktigaste principer som diskuteras är följande:

- Visa respekt för den personliga värdigheten.
- Se till att profileringen baseras på rimliga och objektiva grunder.
- Garantera ansvarighet.

Till var och en av principerna kopplas den underliggande vikten av att säkerställa att poliser och gränsvakter agerar inom lagens gränser när de använder profilering.

2.1. Visa respekt för den personliga värdigheten

Huvudpunkter

- Att säkerställa ett **möte med bra kvalitet** innebär inte i sig att diskriminerande profilering elimineras. Det är dock sannolikt att mötet blir mer framgångsrikt och att risken för möjliga negativa konsekvenser av kontroll- och visiteringsinsatsen minskar. Inom gränsförvaltningen är ett yrkesmässigt och respektfullt uppträdande en rättslig skyldighet.
- Ett **yrkesmässigt och respektfullt uppträdande** förstärker i allmänhet personens nöjdhet efter mötet.
- **En förklaring av skälen** till att en person stoppas ökar förtroendet för polisen och gränsbevakningen, samtidigt som misstankarna om diskriminerande profilering minskar.
- Respekt och artighet kan **aldrig motivera olagliga gränskontroller eller kontroll- och visiteringsinsatser**.

Respekt för den personliga värdigheten är inte bara en grundläggande rättighet i sig, utan en grundprincip för allt polisarbete och all gränsförvaltning. Vid insatser i frontlinjen är det mycket viktigt att tjänstemän inom polisen och gränsförvaltningen talar och samverkar med de personer som stoppas och att de ger rätt information.

Oavsett hur vänligt och professionellt tjänstemännen uppträder är det viktigt att komma ihåg att utpekandet av enskilda personer är en påträngande upplevelse som alltid måste bygga på lagliga grunder. Uppfattningen av diskriminerande profilering kopplas även till antalet interaktioner med polisen och gränsmyndigheterna. Detta understryker vikten av att säkerställa att det alltid finns objektiva och rimliga grunder för att kontrollera en person.

Vad säger normerna?

”In- och utresekontroller bör genomföras på ett sådant sätt att mänsklig värdighet respekteras fullt ut. Gränskontroll bör genomföras på ett professionellt och respektfullt sätt och stå i proportion till de syften som eftersträvas.”

Skäl 7 i kodexen om Schengengränserna

”Alla resenärer har rätt att informeras om kontrollens art och skall behandlas på ett yrkesmässigt, vänligt och artigt sätt, i enlighet med tillämplig internationell och nationell lagstiftning och gemenskapslagstiftning.”

Avsnitt 1.2 i Praktisk handledning för gränsbevakningspersonal (Schengenhandboken)

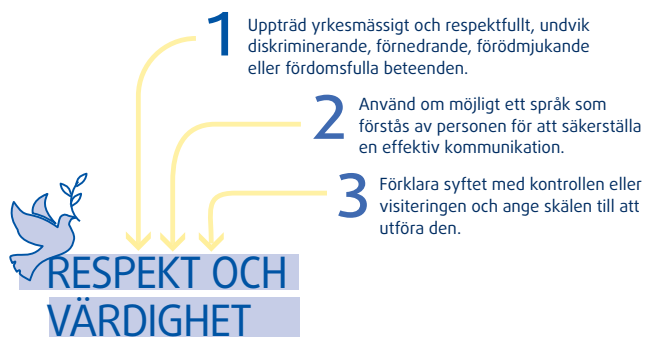
”Polisens personal ska agera med integritet och respekt gentemot allmänheten och med särskild hänsyn till situationen för personer som tillhör särskilt utsatta grupper.”

Rekommendation 44 i den europeiska yrkesetiska koden för polisen

Det är inte alltid lätt att säkerställa att polistjänstemän och gränsbevakningspersonal är artiga och hjälpsamma i stressiga och svåra situationer. Tillgängliga uppgifter visar emellertid att en respektfull ton avsevärt förbättrar nöjdheten efter mötet ⁽²⁵⁾. I figur 5 beskrivs några förutsättningar för ett respektfullt möte.

(25) FRA (2014b).

Figur 5: Tre förutsättningar för ett respektfullt möte



Källa: FRA, 2018.

Vissa delar av gränskontrollerna regleras genom kodexen om Schengengränserna, däribland kravet att utföra en kontroll på ett professionellt och respektfullt sätt eller att ge information om syftet med och förfarandet för kontrollen (kodexen om Schengengränserna, skäl 7, artikel 7 och artikel 8.5). Användning av ett gemensamt språk är å andra sidan inte något absolut krav i samband med gränskontroller på grund av gränstrafikens mycket varierande karaktär. Enligt kodexen om Schengengränserna ska medlemsstaterna under alla omständigheter uppmuntra sin gränsbevakningspersonal att lära sig de språk de behöver för att kunna utföra sina uppgifter (artikel 16.1). I Schengenkatalogen, som innehåller ett antal rekommendationer och exempel på bästa praxis för kontroller vid de yttre gränserna, rekommenderas även att gränsbevakningspersonalen ska ha möjlighet att kommunicera på främmande språk i sitt dagliga arbete. Som ett exempel på bästa praxis anges en tillräcklig kunskap om de angränsande ländernas språk, såväl som andra språk beroende på gränstrafikens karaktär. I idealiska fall bör det finnas tjänstemän med tillräckliga språkkunskaper på varje skift ⁽²⁶⁾.

Bristande hänsyn och respekt under poliskontroller kan ha en direkt inverkan på polisarbetets effektivitet (se [avsnitt 1.3.2](#)). I den uppförandekod som utarbetats i Förenade kungariket enligt lagen om polisarbete och bevismaterial fastställs följande: Alla kontroller och visiteringar måste utföras med artighet, hänsyn och respekt för den berörda personen. Detta har stor betydelse för allmänhetens

(26) Europeiska unionens råd (2009), rekommendationerna 27 och 41.

förtroende för polisen. Varje rimlig ansträngning måste göras för att minimera de besvär som en person kan uppleva vid en visitering ⁽²⁷⁾.

Vissa viktiga metoder för att respektera värdigheten, däribland att förklara skälen till kontrollen och se till att den berörda personen får möjlighet att uttrycka sina åsikter, är grundläggande delar av polisens och gränsförvaltningens förfaranden. Formulär för kontroller och visiteringar kan göra det lättare att lämna denna information på ett strukturerat sätt (se [avsnitt 2.3.1](#)).

I samband med gränsförvaltning är standardformulär ett användbart verktyg för att informera resenärer om syftet med och förfarandet för den fördjupade kontrollen. De kan underlätta kommunikationen med resenärerna under förutsättning att de lämnas ut och kompletteras med muntliga förklaringar vid behov. Enligt kodexen om Schengengränserna bör personer som väljs ut för en fördjupad kontroll få skriftlig information på ett språk som de förstår, eller som de rimligen kan antas förstå, om syftet med och förfarandet för kontrollen. Informationen ska

- vara tillgänglig på unionens alla officiella språk och språken i de länder som gränsar till den berörda medlemsstaten,
- ange att resenären får begära att få veta namnet eller tjänsteidentifikationsnumret på de gränskontrolltjänstemän som utför den noggranna fördjupade kontrollen samt namnet på gränsövergångsstället och datum för gränspassagen.

De aspekter av ett respektfullt möte som gäller kommunikation och social kompetens är svårare att fastställa i operativa förfaranden och kan kräva ytterligare utbildning. Svårigheter med att slå an en positiv ton för mötet kan bero på

- begränsad kommunikationsförmåga,
- oförmåga att förklara skälen till insatsen, och
- ovilja att övervinna personliga och institutionella fördomar och negativa stereotyper, såväl som fientlighet som byggts upp i delar av samhället.

(27) Förenade kungariket, inrikesministeriet (2014a), avsnitt 3.1.

2.2. Rimliga och objektiva grunder

Huvudpunkter

- Brottbekämpning och gränsförvaltning som baseras på specifika och uppdaterade underrättelser är sannolikt mer objektiva.
- För att vara lagliga måste kontroll- och visiteringsinsatser och hänvisningar till fördjupade gränskontroller baseras på **rimliga och objektiva skäl till misstanke**. "Magkänsla" är inte någon rimlig och objektiv grund för att stoppa och visitera en person eller hänvisa en person till en fördjupad gränskontroll.
- Skyddade egenskaper som ras, etniskt ursprung, kön eller religion kan ingå bland de faktorer som de brottbekämpande myndigheterna och gränsbevakningspersonalen tar hänsyn till när de utövar sina befogenheter, men **de får inte vara det enda eller huvudsakliga skälet till att en individ väljs ut**.
- Profilering som endast eller huvudsakligen baseras på en eller flera av de skyddade grunderna utgör direkt diskriminering och är därmed olaglig.

Objektivitet är en viktig princip för polisens och gränsförvaltningens arbete. När det gäller profilering bör enskilda personer endast stoppas och visiteras eller väljas ut för fördjupade gränskontroller på grundval av rimliga och objektiva skäl till misstanke. Objektiva motiveringar kan omfatta personens beteende, särskilda underrättelser eller omständigheter som gör att en eller flera personer kan kopplas till misstänkt olaglig verksamhet.

För att säkerställa objektiviteten i samband med profilering är det nödvändigt att

- undvika fördomar, bland annat genom tydlig vägledning och målinriktad utbildning, och
- använda underrättelseinformation på ett effektivt sätt.

2.2.1. Undvika fördomar

Den europeiska yrkesetiska koden för polisen ger vägledning när det gäller polisens agerande inom områden som insatser och ingripanden, ansvarighet och

övervakning⁽²⁸⁾. I koden betonas den allmänna principen att "[p]olisen ska utföra sina uppgifter på ett rättvist sätt, och i synnerhet följa principerna om opartiskhet och icke-diskriminering"⁽²⁹⁾.

Att välja ut enskilda personer genom att *som den enda eller avgörande faktorn* använda deras verkliga eller förmodade ras, etniska ursprung, kön, sexuella läggning, religion, funktionshinder eller andra förbjudna grunder innebär en kränkning av de grundläggande rättigheterna. Det kan även få betydande negativa konsekvenser både för de offentliga myndigheterna och samhället (se [avsnitt 1.3](#)).

Diskriminerande profilering kan spegla både personliga och institutionella fördomar. Förutom personliga fördomar kan stereotyper och diskriminerande beteenden mot enskilda personer uppstå på grund av särskilda förfaranden inom myndigheterna för brottsbekämpning och gränsförvaltning. Genom att institutionella förfaranden och metoder görs mer synliga kan hanteringen av diskriminering och stereotyper underlättas.

Att erkänna djupt rotade fördomar kan vara svårt. Poliser och gränsbevakningspersonal kanske tror att de väljer ut enskilda personer på rimliga och objektiva grunder (t.ex. beteende) när besluten i själva verket speglar deras fördomar.

Tjänstemän som utför kontroller kopplar ofta orsaken till valet att stoppa en viss person till en "magkänsla" eller "intuition". Denna känsla beror sannolikt på en kombination av sakkunskap och tidigare erfarenheter, men den kan även spegla medvetna eller omedvetna fördomar från tjänstemannens sida. För att undvika olaglig profilering bör tjänstemännen överväga om deras beslut kan motiveras med objektiv information. En "magkänsla" är i sig inte någon rimlig eller objektiv grund för att stoppa och visitera en person eller utsätta en person för en ytterligare kontroll vid gränsen.

2.2.2. Tydlig vägledning för tjänstemän

Praktisk, lättförståelig och användbar vägledning är av särskilt stor vikt för att hjälpa tjänstemän inom brottsbekämpning och gränsförvaltning att undvika olaglig profilering. Vägledningen kan ha många former: den kan bifogas till lagstiftningen, utfärdas

(28) Europarådet, ministerkommittén (2001), [Recommendation Rec\(2001\)10 of the Committee of Ministers to Member States on the European Code of Police Ethics](#), 19 september 2001.

(29) Se not 28, punkt 40.

av de brottsbekämpande och gränsförvaltande myndigheterna eller tillhandahållas av högre tjänstemän på daglig basis. Att använda verkliga exempel som visar vad man bör göra i särskilda situationer är sannolikt effektivare än att förklara reglerna och förfarandena.

Tjänstemän med ledande befattningar måste informera personalen om att verklig eller förmodad ras, etniskt ursprung, kön, sexuell läggning, religion eller andra förbjudna grunder för diskriminering inte får vara den avgörande faktorn för att inleda insatser för brottsbekämpning eller gränsförvaltning riktade mot en person. Ett klargörande av när och hur personliga egenskaper får användas kan bidra till att minska risken för olika tolkningar såväl som inverkan av stereotyper och fördomar. Vägledningen bör även omfatta frågor angående skydd av privatliv och personuppgifter.

I tabell 3 visas några av de typer av vägledning som kan användas och vilka viktiga funktioner som bör beaktas.

Tabell 3: Typer av vägledning, deras egenskaper och berörda parter medverkan

Typer av vägledning	Vägledningens egenskaper	De berörda parternas medverkan
<ul style="list-style-type: none"> • standardförfaranden • uppförandekoder • regelbunden vägledning av ansvariga chefer 	<ul style="list-style-type: none"> • detaljerad och specifik • omfattar all verksamhet där fördomsbaserad profilering kan förekomma: <ul style="list-style-type: none"> • kontroll och visitering • arresteringar • gränskontroller • användning av tvångsmedel etc. 	<ul style="list-style-type: none"> • utvecklar vägledningen med andra berörd parter • gör vägledningen tillgänglig för samhällsgrupper • uppmuntrar feedback från samhällsgrupper om vägledningen

Källa: FRA, 2018.

Fallstudie

Uppförandekod och ambassadörsmetoden (Nederländernas polismyndighet)

Den nederländska polisen har utarbetat en uppförandekod tillsammans med civilsamhällets organisationer, däribland Amnesty International, för att beskriva de fyra principerna för en yrkesmässig kontroll:

- Ett berättigat och motiverat urval av personer.
- En förklaring av skälen till kontrollen och visiteringen.
- Användning av yrkesmässig kommunikation.
- Tjänstemännen diskuterar sina metoder och ger feedback till varandra.

Det är svårt att ändra metoder som inte uppfattas som problematiska, till exempel användningen av förebyggande polisarbete som kan leda till etnisk profilering. Polisen i Amsterdam har utarbetat en bottom-up-strategi med grupper som inbegriper tjänstemän i yttre tjänst (ambassadörer) som får stöd av sina chefer och utbildare. Det första steget är att öka medvetenheten genom att visa och diskutera vilka effekter förebyggande kontroller har på de utvalda personerna och genom att införa ett alternativt regelverk som är rättvist och effektivt. Det andra steget är att se till att tjänstemännen tillägnar sig den nya strategin.

För mer information på nederländska, se [polisens webbplats](#).

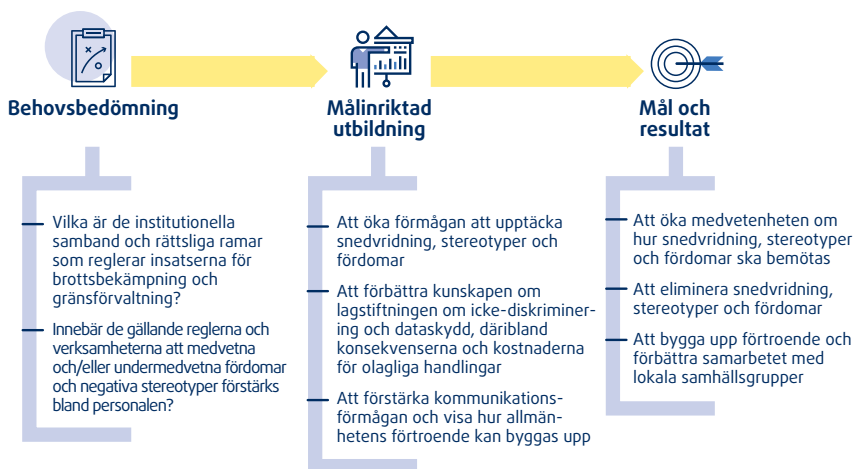
2.2.3. Målinriktad utbildning

Utbildning av poliser och gränsbevakningspersonal är ett annat viktigt verktyg för att minimera risken för olaglig profilering. Det finns många olika typer av utbildning som kan genomföras i olika steg av en tjänstemans karriär, däribland inledande rekryteringsutbildning, fortbildning och fortlöpande yrkesmässig utveckling. Oavsett vilken typ som används bör utbildningsmodulerna utgå från den organisatoriska kulturen och erbjuda kurser som omfattar strategier för att ersätta och motverka stereotyper. Slutligen är det viktigt att utvärdera effekterna av utbildningen för att se hur den har bidragit till att ändra tjänstemännens uppfattning och förbättra deras

metoder och för att identifiera områden där mer utbildning behövs. I figur 6 visas några faktorer som bör beaktas när den målinriktade utbildningen planeras.

Vissa typer av utbildning inom brottsbekämpning och gränsförvaltning har redan utvecklats i vissa länder, däribland "mångfaldsutbildning" och "känslighetsutbildning". Syftet med mångfaldsutbildning är att diskutera personliga uppfattningar om etniskt ursprung, skillnader och stereotyper, och hur dessa påverkar våra dagliga liv. I vissa mångfaldsutbildningar ingår emellertid inte någon diskussion om diskriminering. Vissa studier har visat att kultur- och mångfaldsutbildning i själva verket kan konkretisera och förstärka skillnader som ökar stereotypiseringen i stället för att minska den⁽³⁰⁾. "Utbildning i kulturell känslighet" (till skillnad från "allmän mångfaldsutbildning") syftar till att utbilda poliser och tjänstemän inom brottsbekämpningen om kulturen hos de etniska grupper som de ofta möter men inte alltid vet så mycket om. I sådana utbildningar behandlas regler och riktlinjer för hur artighet kan uttryckas ur olika etniska, religiösa eller nationella perspektiv. Utbildningar i kulturell känslighet är effektivast om de utvecklas och genomförs tillsammans med personer från de berörda samhällsgrupperna.

Figur 6: Processen och målen för utarbetandet av målinriktad utbildning



Källa: FRA, 2018.

(30) Wrench, J. (2007).

Fallstudie

Utbildning om laglig profilering

Utbildning om profilering för polistjänstemän (Italien)

Sedan 2014 har det italienska observationsorganet för säkerhet mot diskriminering (Osservatorio per la sicurezza contro gli atti discriminatori) genomfört en utbildningsmodul om etnisk profilering för polistjänstemän och aspiranter. Utbildningen är särskilt inriktad på olika fördomar som kan påverka profileringen, konsekvenserna för polisarbetets effektivitet och den negativa inverkan på relationerna till olika samhällsgrupper. Hittills har omkring 5 000 personer deltagit i utbildningen. Sedan 2017 har även en e-utbildning erbjudits inom ramen för polisens fortbildning.

För mer information, se [den italienska polisens webbplats](#).

Verktyg för grundläggande rättigheter i utbildningen av gränsbevakningspersonal (EU)

I den gemensamma läroplanen för europeisk gränsbevakningspersonal fastställs minimikrav för den nivå av färdigheter och kunskap som varje gränsbevakningstjänsteman måste uppnå. Läroplanen omfattar kapitel om sociologi och grundläggande rättigheter. Det finns särskilda avsnitt om icke-diskriminering (1.5.4) och etnisk profilering (1.7.10) som utbildarna kan använda. I den gemensamma läroplanen betonas de potentiella riskerna med fördomar, rasism, rasdiskriminering, främlingsfientlighet, islamofobi, homofobi och andra exempel på intolerans i samband med profilering. I 2017 års uppdatering av läroplanen ingår avsnitt om nya kompetenser, särskilt inom området för grundläggande rättigheter.

Dessutom har Frontex utarbetat en handbok för utbildare i samråd med universitet och internationella organisationer (se Frontex, 2013). Handboken innehåller metoder som utbildare kan använda för att förbättra gränsbevakningspersonalens kunskaper om grundläggande rättigheter och internationellt skydd. I ett särskilt avsnitt om profilering fastställs grundläggande regler för att undvika diskriminering. Utbildningen sker regelbundet, men det finns inte någon permanent mekanism för att bedöma vilka utbildningsmål som har uppnåtts.

För mer information, se Frontex (2012).

Studiedagar om profilering för högre tjänstemän (Belgien)

År 2015 anordnade centret för polisarbete och säkerhet (CPS) i Gent (Belgien), tillsammans med det belgiska likabehandlingsorganet (Unia), en studiedag om etnisk profilering (*Profilage ethnique: l'égalité sous pression?*). Utbildningen omfattade flera olika aspekter av frågan, däribland om och hur poliser med migrantbakgrund kan förbättra relationerna till etniska minoriteter, hur ofta etnisk profilering används av polistjänstemän och hur resultaten utvärderas.

Under 2016 anordnade Unia två studiedagar för polisbefäl från norra Bryssel för att öka medvetenheten om etnisk profilering och främja insikten om hur profilering används av poliser i yttre tjänst. Polistjänstemän från Spanien och Förenade kungariket presenterade exempel på god praxis för en publik bestående av tjänstemän inom brottsbekämpningen, forskare och icke-statliga organisationer. De visade framför allt att en minskad profilering baserad på etniskt ursprung ledde till ett ökat antal arresteringar av efterlysta personer. Grunden till detta var att varje kontroll registrerades och att öppenheten säkerställdes angående motiven bakom kontrollerna. Syftet med utbildningen var att nå en samsyn om metoderna för etnisk profilering för att stödja den framtida utvecklingen av forskningen om de metoder som används av polisen i området.

För mer information, se Belgien (2015 och 2017).

Utbildningen bör vara inriktad på de fördomar och stereotyper som kan finnas inom institutionerna för brottsbekämpning och gränsförvaltning. Den övergripande institutionella miljön och de interna regler som införts – t.ex. befintliga klagomålsmekanismer, förekomsten av en "tystnadskultur" bland medarbetarna etc. – bör undersökas innan en utbildning för att förebygga olaglig profilering påbörjas. Läroplanerna bör omfatta fördomar och stereotyper som kan vara rotade i polisinsatser som kontroll och visitering, arrestering, kvarhållande och användning av våld.

Tjänstemän på högre nivå och mellannivå har en viktig roll för att säkerställa en framgångsrik utbildning, både genom sitt eget deltagande och den vikt de fäster vid utbildningen ⁽³¹⁾. Som mottagare kan högre tjänstemän lära sig nya metoder och färdigheter som de kan föra vidare till tjänstemännen i yttre tjänst.

(31) Se Europeiska kommissionen (2017b).

Organisationens kultur bestäms till stor del av ledningen och har en stor inverkan på polisernas och gränsvakternas vardagliga beteenden, däribland hur de samverkar med allmänheten.

Högre tjänstemän kan även säkerställa att utbildningen upplevs på ett positivt sätt. Beteendet hos personal i ledande ställning, till exempel hur handledarna framställer syftet med utbildningen för tjänstemännen eller om tjänstemännen tror att de har valts ut slumpmässigt eller på grund av att de har ett "problematiskt" beteende, kan påverka intresset och engagemanget för utbildningen. Om tjänstemännen uppmuntras att delta aktivt i utbildningen och vara öppna för att förbättra sitt dagliga arbete genom att ändra sitt beteende kommer effekterna av utbildningen sannolikt att förstärkas ⁽³²⁾.

När utbildningen har slutförts bör den granskas och utvärderas för att bedöma om den har ökat medvetenheten och skapat ändrade beteenden.

Fokus på de vägledande principerna för utbildningen

Specialutbildning är mycket viktig för att säkerställa en laglig användning av profilering. Europeiska kommissionen har sammanställt ett antal vägledande principer för hur effektiv utbildning av hög kvalitet kan säkerställas när det gäller hatbrott. Samma principer gäller för utbildning om laglig profilering.

Utbildning om hatbrott för brottsbekämpande myndigheter och åklagarmyndigheter: 10 viktiga vägledande principer

Säkerställ en god inverkan och hållbarhet:

- Införliva utbildningen i en övergripande strategi för att bekämpa diskriminering.
- Utarbeta en metod för att hantera utbildningsbehoven.

Identifiera mål och bygg upp synergier:

- Anpassa programmen till din personal.
- Samarbeta med civilsamhället på ett strukturerat sätt.

(32) Miller, J. och Alexandrou, B. (2016).

Välj rätt metod:

- Kombinera olika metoder.
- Utbilda utbildarna.

Förmedla ett innehåll med hög kvalitet:

- Utforma en undervisningsplan med hög kvalitet.
- Utarbeta utbildningsmoduler med inriktning på diskriminering.

Övervaka och utvärdera resultaten:

- Koppla utbildningen till processer för prestationsöversyn.
- Säkerställ en regelbunden övervakning och utvärdering av dina utbildningsmetoder.

För mer information, se Europeiska kommissionen (2017a).

En helt fristående utbildning kommer emellertid inte att vara effektiv för att motverka tjänstemännens förutfattade meningar. Vad som behövs är ett helt nytt institutionellt tankesätt. Myndigheterna måste därför överväga mångfacetterade insatser för att bemöta personliga och institutionella fördomar (se fallstudien).

Fallstudie

Motverkande av "institutionell rasism" inom polisen

Efter att farhågor om rasism hade väckts angående polisens bristande hantering av utredningen av mordet på Stephen Lawrence inledde den brittiska regeringen en omfattande undersökning för att identifiera vilka lärdomar som kunde dras angående utredning och lagföring av brott med rasistiska motiv.

I utredningsrapporten, som offentliggjordes 1999, framhövs problemet med "institutionell rasism" inom poliskåren, däribland skillnader i kontroll och visitering, som en orsak till stor oro bland de berörda samhällsgrupperna. Rekommendationerna efter utredningen varierade från utbildning för att öka medvetenheten om rasism till rapportering och registrering av incidenter

inom ramen för en övergripande uppmaning att öka öppenheten, utkräva ansvar och återupprätta förtroendet för polisen.

En granskning som offentliggjordes 2009, tio år efter utredningen, visade att polisens samverkan med etniska minoriteter och utredningen av brott med rasistiska motiv hade förbättrats. I granskningen konstaterades dock att mörkhyade personer fortfarande löper mycket större risk att utsättas för kontroller och visiteringar än sina ljushyade medmänniskor.

För mer information, se Förenade kungariket, inrikesministeriet (1999), Förenade kungariket, kommissionen för lika möjligheter och mänskliga rättigheter (2009) och Förenade kungarikets underhus, utskottet för inrikes frågor (2009).

2.2.4. Rimliga skäl till misstanke: användning av underrättelser och information

När polistjänstemän och gränsbevakningspersonal väljer ut en enskild person grundar de vanligen sitt beslut på en kombination av faktorer. Dessa kan omfatta mer "objektiv" information, som särskilda underrättelser, beteenden, kläder eller föremål som personerna bär med sig, såväl som "subjektiv" kunskap baserad på erfarenhet.

Alla dessa faktorer kan utgöra en "signal" om illegal verksamhet. Informationen måste emellertid kombineras och användas med försiktighet. Undersökningar har visat att tjänstemän ibland tycker att det är svårt att skilja mellan objektiva och subjektiva faktorer i praktiken, vilket illustreras av exemplet i rutan.

Exempel

”Det är mycket subjektivt. Det handlar om personliga känslor som rör en person och ett ärende, men det finns även bevisfrågor som kan gälla motsägelsefulla uttalanden, motsägelser mellan dem and vad deras referensperson säger, motsägelser mellan vad de säger och deras handlingar, mellan vad de säger och allt de har i sina väskor. Så även om det finns bevis kan [dessa faktorer i sig] inte användas mot någon. Tjänstemannen måste bygga upp en komplett bild av personen och utgå från den.”

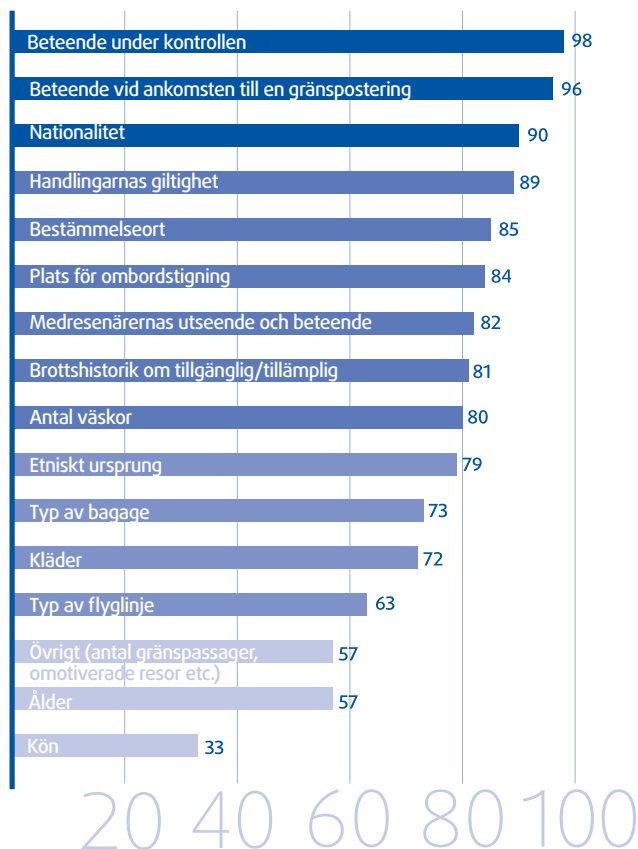
(Tjänsteman vid invandringsmyndigheten vid en stor flygplats i Förenade kungariket)

För mer information, se FRA (2014a), s. 46.

Fokus på identifiering av personer som försöker resa in i ett land på ett olagligt sätt

Undersökningar som FRA utförde 2012 vid ett antal stora flygplatser visade att gränsbevakningspersonal tar hänsyn till många olika faktorer när de ska avgöra om en person kan försöka resa in i landet på ett olagligt sätt. Dessa omfattar ofta en kombination av ”objektiva” kriterier – till exempel personernas beteende när de närmar sig gränsposteringen och under själva kontrollen, typen och mängden av bagage och resehandlingarnas giltighet – och personliga erfarenheter av tidigare gränskontroller, vilket framgår av figur 7.

Figur 7: Indikatorer som betraktas som användbara eller mycket användbara för att känna igen personer som försöker resa in i landet på ett olagligt sätt innan tjänstemännen pratar med dem (%)



Anm.: De giltiga svaren varierar mellan 206 och 216 av 223. Intervjupersoner som inte gav något svar på en viss fråga har uteslutits vid beräkningen av resultaten. Beroende på frågan valde mellan 7 och 17 personer att inte lämna något svar.

Källa: FRA, Undersökning av gränsbevakningspersonal, 2012 (fråga 17).

Gränsbevakningspersonalen uppgav att beteendet under kontrollen eller vid ankomsten till en gränspostering var de mest användbara faktorerna för att känna igen personer som försöker resa in i landet på ett olagligt sätt.

Faktorer som nationalitet och etniskt ursprung, som kan vara tecken på diskriminerande profilering, ansågs emellertid också vara viktiga.

Klädstilen, som också betraktades en användbar indikator, är ett exempel på hur skenbart "objektiv" information kan användas på ett fördomsfullt sätt i praktiken. Vissa typer av kläder kan kopplas till specifika riskprofiler. Exempelvis bär personer av en viss nationalitet som fallit offer för människohandel ofta en viss typ av kläder. Klädstilen kan emellertid även visa att en person tillhör en viss etnisk eller religiös grupp. Även om det finns tillräckligt med andra skäl som motiverar en fördjupad kontroll kan personer som identifierar sig starkt med sin etniska eller religiösa bakgrund, har tidigare negativa erfarenheter eller inte får någon tillräcklig förklaring av tjänstemannen uppleva behandlingen som diskriminerande.

För mer information, se FRA (2014a). När det gäller profiler för offer för människohandel, se Frontex (2017).

Utförliga underrättelser om beteendemönster eller händelser kan öka profileringens objektivitet. Detta kan gälla kriminell verksamhet eller, när det gäller gränsförvaltning, olaglig migration eller gränsöverskridande brott. Om insatser för brottsbekämpning och gränsförvaltning bygger på specifika och aktuella underrättelseuppgifter, t.ex. information om en viss person eller ett visst sammanhang, är de sannolikt mer objektiva och mindre påverkade av stereotyper.

Vid sidan av underrättelser och objektiva faktorer kan information om skyddade egenskaper, som verklig eller förmodad ras, etniskt ursprung, nationalitet, kön eller religion, användas på ett lagligt sätt som en extra del av profileringen under vissa omständigheter. För att användningen av denna information ska vara laglig måste den vara reglerad i lag, vara förenlig med de väsentliga delarna av de rättigheter och friheter som påverkas och vara både proportionerlig (dvs. uppfylla kravet på intresseavvägning) och nödvändig (dvs. det bör inte finnas några mindre begränsande metoder). Tjänstemännen måste även ha ett giltigt skäl, vid sidan av de skyddade grunderna, för att behandla en enskild person på ett annat sätt än andra personer i allmänheten. Skälet måste även vara direkt kopplat till den berörda personen, som i det exempel som beskrivs i rutan.

Exempel

Vittnen rapporterar att den rånmisstänkte hade röda löparskor och en svart keps, var mellan 1,60 och 1,70 meter lång och uppfattades vara av kinesisk härkomst. Under dessa omständigheter kan de brottsbekämpande myndigheterna ha rätt att betrakta den etniska bakgrunden som relevant för misstankarna mot en viss person, eftersom den kombineras med specifika underrättelser.

Fokus på detaljerade beskrivningar av misstänkta

Bra beskrivningar av misstänkta personer kan minska risken för olaglig profilering. En beskrivning av en misstänkt omfattar detaljer om personen, till exempel hud-, hår- och ögonfärg, vikt och längd samt klädstil. Dessa uppgifter lämnas av offret eller vittnena till brottet, eller på grundval av andra specifika underrättelser. En bra beskrivning av en misstänkt kan användas av tjänstemän som en grund för kontroller och visiteringar i syfte att frihetsberöva misstänkta eller för att hänvisa personer till en fördjupad kontroll vid en gränskontroll.

Om tjänstemännen får en alltför allmän beskrivning som omfattar ras, etniskt ursprung eller liknande egenskaper bör de emellertid inte använda beskrivningen som grund för insatserna. I sådana fall kommer insatserna sannolikt att leda till många kontroller av oskyldiga personer som råkar ha samma egenskaper. Tjänstemännen bör i stället efterfråga specifika operativa underrättelser som kan leda utredningen framåt.

För mer information, se Europeiska kommissionen (2017b).

Information som verkar objektiv kan i själva verket bygga på fördomar. Uppenbarligen objektiva faktorer som tidpunkt, dag, plats etc. kan användas som substitut för förbjudna diskrimineringsgrunder, t.ex. verklig eller förmodad ras, nationellt ursprung, kön, sexuell läggning eller religion, vilket nedanstående exempel visar.

Exempel

En kontroll- och visiteringsinsats utförs en fredag vid middagstid i område X. Denna tidpunkt är emellertid den viktigaste bönetiden för muslimer. Eftersom område X ligger nära en moské skulle de förment objektiva faktorerna tidpunkt, dag och plats i själva verket kunna fungera som fullmakt för en kontroll- och visiteringsinsats på grundval av religion, som är en förbjuden diskrimineringsgrund.

Att leta efter vissa misstänkta beteenden kan på liknande sätt förefalla som en objektiv metod för att identifiera möjliga förseelser. Tjänstemän kan emellertid tolka en persons beteende på olika sätt beroende på andra av den berörda personens egenskaper. Det finns bevis för att yrkeskunskapen och förståelsen för underrättelser kan variera avsevärt bland tjänstemännen och att den ofta inte motsvarar verkliga brottsmönster ⁽³³⁾.

Aktuella och detaljerade underrättelseuppgifter till tjänstemännen, till exempel under en genomgång i början av varje skift, minskar utrymmet för godtycke och hjälper tjänstemännen att inrikta sina befogenheter mer specifikt mot faktiska brottsmönster och identifierade säkerhetsproblem. Detta gör att effekterna av eventuella fördomar minskar. Förbättringar av underrättelseuppgifternas kvalitet och användning så att de inriktas på beteendemässiga faktorer eller specifik information är effektivast i kombination med ökad tillsyn och övervakning över hur tjänstemännen använder sina befogenheter.

Fallstudie**Objektivitet i samband med profilering****Genomgång före skiften (EU)**

I Schengenkatalogen rekommenderas att tjänstgörande befäl ska tillhandahålla information om eventuella riskindikatorer och riskprofiler före varje skift. Överlappningar av skiften kan ge tillräckligt med tid för genomgångar och utbyte av information bland personalen.

För mer information, se Europeiska unionens råd (2009).

(33) United Kingdom National Policing Improvement Agency (NPIA) (2012).

Utbildningsprogrammet SDR (Nederländerna)

Utbildningsprogrammet "Search, Detect and React" (SDR) syftar till att förebygga brott eller terroristhandlingar innan de inträffar genom att förstärka säkerhetspersonalens kapacitet när det gäller beteendeprofilering. Detta innebär att uppmärksamheten riktas bort från oföränderliga egenskaper som hudfärg och i stället inriktas på individuella beteenden när polisåtgärderna ska fastställas. Eftersom indikatorerna för misstänkta beteenden beror på sammanhanget anpassas utbildningen till miljön. Utbildningen utgår från att det inte finns någon lösning som passar alla. När de har upptäckt relevanta beteendemönster är tjänstemännen skyldiga att uppträda på ett "känsligt" sätt. I de flesta fall har de ett informellt samtal med den misstänkte i stället för att använda formella polisbefogenheter. Programmet omfattar lektioner i klassrum vid sidan av tillämpad och praktisk utbildning.

Mer information finns på [SDR-akademiens webbplats](#).

Kontroll- och visiteringsverktyget Authorised Professional Practice (APP) (Förenade kungariket)

Polishögskolan i Förenade kungariket har utarbetat en vägledning för auktoriserad yrkesutövning (Authorised Professional Practice, APP) som omfattar olika aspekter av polisarbetet. Genom APP-verktyget förklaras vad kontroll och visitering innebär, varför det är viktigt att använda dessa befogenheter på ett korrekt sätt och vilka delar som ingår i lagliga kontroller och visiteringar. I verktyget förklaras att kontrollernas och visiteringarnas laglighet och effektivitet förstärks om följande säkerställs:

- **Korrekthet.** Tjänstemannens beslut att kontrollera och visitera en person måste bygga på lämpliga, objektiva faktorer. En person får aldrig stoppas enbart eller huvudsakligen på grundval av skyddade egenskaper eller faktorer som tidigare domar.
- **Laglighet.** Kontrollen och visiteringen måste ha en rättslig grund som tillämpas på ett lagligt sätt.
- **Yrkesmässighet.** Under kontrollen och/eller visiteringen måste tjänstemännen uppfylla yrkesmässiga ordningsregler, i synnerhet etiska

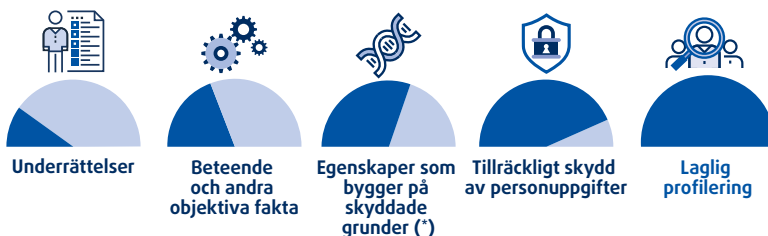
regler, kommunicera med personer på ett effektivt sätt och behandla alla med värdighet och respekt.

- **Öppenhet.** Det enskilda mötet måste registreras på ett korrekt sätt. En effektiv tillsyn och övervakning av kontroller och visiteringar måste säkerställas, liksom en offentlig granskning.

För mer information, se Förenade kungariket, College of Policing (2016).

I figur 8 visas de olika faktorer som kan användas vid laglig profilering. Möjligheterna att kombinera dem beror på omständigheterna i varje enskilt fall.

Figur 8: Kombination av faktorer



(*) I figur 9 finns en förteckning över de skyddade grunderna enligt unionsrätten. Profilering får aldrig enbart eller huvudsakligen baseras på skyddade egenskaper.

Källa: FRA, 2018.

I figur 9 visas hur dessa faktorer kan kombineras för att säkerställa att profileringen inte är diskriminerande.

Figur 9: Faktorer för icke-diskriminerande profilering



Anm.: Förteckningen över skyddade grunder varierar mellan medlemsstaterna. En översikt över de grunder för diskriminering som ingår i varje medlemsstats straffrättsliga lagstiftning finns i FRA (2018d). Se även [Equinets webbplats](#) (Europeiska nätverket för likabehandlingsorgan) som innehåller en förteckning över de grunder för diskriminering som omfattas av nationella likabehandlingsorgan.

Källa: FRA, 2018.

2.2.5. Formulär för kontroll och visitering vid profilering inom brottsbekämpning

Formulär för kontroll och visitering kan hjälpa tjänstemännen att avgöra huruvida de kontroller som utförs bygger på rimliga grunder och gör att de ansvariga cheferna kan övervaka eventuella diskriminerande förfaranden i de enskilda tjänstemännens användning av kontroller och visiteringar. Även om formulären ibland upplevs som betungande innehåller de uppgifter om kontroller som, när de sammanställs, kan visa om kontrollerna har genomförts på ett lagligt sätt ⁽³⁴⁾. Detta kan bidra till att främja öppenhet och ansvarighet. Förutom formulär i pappersform kan nya tekniker som mobilappar användas för att registrera denna information.

Några viktiga punkter som bör ingå när formulär för kontroll och visitering utformas beskrivs i fokusrutan.

Fokus på bra formulär för kontroll och visitering

Formulär för kontroll och visitering måste vara väl utformade för att vara användbara. För det första innebär ifyllandet av formulären en extra arbetsbörda för tjänstemännen. Om de inte har utformats på ett tydligt och koncist sätt är risken att tjänstemännen inte fyller i hela formuläret eller endast anger kortfattade uppgifter. För det andra gör bra formulär att uppgifterna kan sammanställas som stöd till övervakningen och utvärderingen av kontroll- och visiteringsinsatserna.

Om det är möjligt bör formulär för kontroll och visitering

- bestå av flervalssält som är snabbare att fylla i och lättare att bearbeta statistiskt,
- innehålla en omfattande lista med alternativ för varje post,
- sakna tvetydiga poster,
- vara lätta att förstå, både för tjänstemannen och personen som kontrolleras.
- Formulären bör omfatta

(34) Förenade kungariket, Stop Watch (2011).

- den rättsliga grunden för visiteringen, företrädesvis med enkla förklaringar i stället för en förteckning med regler,
- datum, tidpunkt och plats där personen eller fordonet visiterades,
- syftet med visiteringen, t.ex. vilka föremål som tjänstemännen letar efter,
- resultatet av visiteringen,
- namnen på tjänstemännen som utförde visiteringen och deras polisstation,
- personuppgifter för den eller de personer som visiterades, däribland namn, adress och nationalitet. Visiterade personer kan emellertid vägra att uppgive denna information.

För att vara effektiva bör formulären fyllas i medan kontrollen utförs.

En kopia bör överlämnas till den kontrollerade personen eller till den person som är ansvarig för det kontrollerade fordonet. I Förenade kungariket har personer som kontrolleras rätt att begära en kopia av registret inom tre månader efter kontrollen. På så sätt utgör formuläret inte bara en bekräftelse av kontrollen för polisen, utan även för den kontrollerade personen.

För mer information, se Förenade kungariket, West Midlands Police (2012), s. 7 och Förenade kungariket, inrikesministeriet (2014a).

Fallstudie

Formulär för kontroll och visitering (Förenade kungariket)

Det formulär för kontroll och visitering som används av poliskåren West Midlands Police i Förenade kungariket återges nedan.

Det visar att den person som stoppas blir ombedd att identifiera sig själv som tillhörande någon av de angivna kategorierna av etniskt ursprung eller något av alternativen "Övrigt" eller "Anges ej". Den tjänsteman som utför kontrollen kan lägga till sin uppfattning om den skiljer sig från den stoppade personens egen identifiering.

I uppförandekoden för utövandet av befogenheter i samband med kontroll och visitering i Förenade kungariket anges att tjänstemännen bör förklara för den som ska kontrolleras att informationen om etniskt ursprung behövs för att skapa en verklig bild av kontrollen och visiteringen och för att förbättra den etniska övervakningen, förebygga diskriminerande behandling och främja en effektiv användning av befogenheterna.

WC332
02/17

Stop and Search

Call: 805 6666



<p>Power</p> <ol style="list-style-type: none"> 1 Drugs 2 Section 1 PACE <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>A typical response would be "2,5" if the Power was "S1 PACE & Object 'Fireworks'. The Object of search will default if there is only 1 option.</p> </div> <ol style="list-style-type: none"> 3 S47 Firearms Act 4 Section 60 CJPO Act 1994 5 Section 43 Terrorism Act 6 New Psychoactive Substances Act 2016 7 Other (a Search contains list of additional powers) 	<p>Object</p> <ol style="list-style-type: none"> 1 Search for Drugs 1 Stolen Items 2 Offensive Weapon/Bladed Article 3 Articles for Burglary/Theft/Fraud/TWOC 4 Items for Criminal Damage 5 Fireworks 1 Firearms 1 Dangerous Items/Offensive Weapons 1 Evidence of Terrorism 1 Search for NPS 		
<p>Self Assessed Ethnicity (16+1)</p> <p>A1 Asian - Indian</p> <p>A2 Asian - Pakistani</p> <p>A3 Asian - Bangladeshi</p> <p>A9 Asian - Any Other Asian background</p> <p>B1 Black - Caribbean</p> <p>B2 Black - African</p> <p>B9 Black - Any Other Black background</p> <p>M1 Mixed - White & Black Caribbean</p> <p>M2 Mixed - White and Black African</p> <p>M3 Mixed - White & Asian</p> <p>M9 Mixed - Any Other Mixed Background</p> <p>O1 Other - Chinese</p> <p>O9 Other - Any Other Ethnic Group</p> <p>W1 White - British</p> <p>W2 White Irish</p> <p>W9 White - Any Other White background</p> <p>NS Not Stated</p>	<p>Officer assessed Ethnicity (PNC)</p> <p>IC1 White North European</p> <p>IC2 White South European</p> <p>IC3 Black</p> <p>IC4 Asian</p> <p>IC5 Chinese/Japanese/South East Asian</p> <p>IC6 Middle Eastern</p> <p>IC9 Other</p>		
<p>Grounds for Search - Multi Select</p> <ol style="list-style-type: none"> 1 Acting Suspiciously 2 Stopped in tasking area 3 Stopped in high crime area 4 Could not give reasonable explanation 5 Tried to avoid police 6 Seen to discard an item 7 Seen to conceal item 8 Smell of controlled drug 9 Current Intelligence 10 Matches Description <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <p>Grounds will be supported by a free text explanation</p> </div>			
<p style="text-align: center;">Outcome</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 1 Arrested - Consequence of Stop & Search 2 Arrested - Unrelated Offence including Warrant/PNC 3 Community Resolution 4 Fixed Penalty 5 Cannabis Warning 6 Street Bail </td> <td style="width: 50%; vertical-align: top;"> <ol style="list-style-type: none"> 7 Street Summons 8 Conditional Bail 9 Out of custody Caution 10 Substance seized, person not arrested 11 NFA </td> </tr> </table>		<ol style="list-style-type: none"> 1 Arrested - Consequence of Stop & Search 2 Arrested - Unrelated Offence including Warrant/PNC 3 Community Resolution 4 Fixed Penalty 5 Cannabis Warning 6 Street Bail 	<ol style="list-style-type: none"> 7 Street Summons 8 Conditional Bail 9 Out of custody Caution 10 Substance seized, person not arrested 11 NFA
<ol style="list-style-type: none"> 1 Arrested - Consequence of Stop & Search 2 Arrested - Unrelated Offence including Warrant/PNC 3 Community Resolution 4 Fixed Penalty 5 Cannabis Warning 6 Street Bail 	<ol style="list-style-type: none"> 7 Street Summons 8 Conditional Bail 9 Out of custody Caution 10 Substance seized, person not arrested 11 NFA 		

För mer information, se Förenade kungariket, West Midlands Police (2017a) och Förenade kungariket, inrikesministeriet (2014a), s. 19.

Många poliskontor har slutat att samla in uppgifter om kontroller och visiteringar på formulär och i stället börjat använda tekniker som telefonappar, radiobaserade system, terminaler för mobildata eller bärbara datorer. Dessa tekniker kan påskynda registreringsprocessen och minska byråkratin, men de medför även nya risker, i synnerhet när det gäller algoritmisk användning av personuppgifter (se [kapitel 3](#)).

Fallstudie

Registrering i realtid av kontroller och visiteringar

"eSearch" (West Midlands Police, Förenade kungariket)

Detta system antogs i april 2014 och bygger på ett samtal mellan en polis i yttre tjänst och en medarbetare i en kontaktcentral. Uppgifterna om kontrollen och visiteringen registreras omedelbart i kontrollrummet och förs in i en databas. Denna information kan sedan hämtas och användas för att granska kontrollernas och visiteringarnas effektivitet, både internt och externt. eSearch har förändrat registreringen av kontroll- och visiteringsinsatser. Uppgifterna i registren kan hämtas mycket snabbare i polisens system, vilket underlättar integreringen av underrättelser i det operativa polisarbetet.

För mer information, se Förenade kungariket, West Midlands Police (2014) och Förenade kungariket, West Midlands Police (2016).

Mobilapp för poliser i yttre tjänst (West Midlands Police, Förenade kungariket)

En ny mobilapp lanserades i oktober 2017 för att möjliggöra snabbare och effektivare kontroller och visiteringar. eSearch-appen gör att poliserna kan registrera uppgifter om insatser på gatan direkt i appen via en smarttelefon, utan att behöva ringa till personalen i kontaktcentralen. Varje kontroll får ett unikt referensnummer, och platsen registreras automatiskt via GPS. Appen förväntas minska antalet samtal till kontaktcentralen med närmare 1 000 samtal i månaden.

För mer information, se Förenade kungariket, West Midlands Police (2017b).

Högre tjänstemän spelar en viktig roll för att säkerställa att kontroller och visiteringar är lagliga. Exemplet nedan visar hur högre tjänstemän kan upprätthålla tillsynen. De bör även säkerställa att kontroll- och visiteringsinsatserna inte används som en prestationsmätning baserad på antalet kontrollerade personer.

Fallstudie

Underteckning av kontroll- och visiteringsregister (Förenade kungariket)

Sedan augusti 2014 måste varje kontroll och visitering i Förenade kungariket undertecknas av chefen för den tjänsteman som utförde visiteringen. I registret anges om insatsen uppfyller de relevanta normerna. I det senare fallet måste den rapporterande tjänstemannen ange varför i registret över kontroller och visiteringar.

För mer information, se Förenade kungariket, inrikesministeriet (2014a).

2.3. Ansvarighet

Huvudpunkter

- Tjänstemän inom brottsbekämpning och gränsförvaltning är **ansvariga** för att hålla profileringen inom lagens gränser.
- **Insamling av tillförlitliga, korrekta och aktuella uppgifter** om profileringsverksamheten är avgörande för att säkerställa ansvarigheten.
- **Effektiva klagomålsmekanismer** kan både avskräcka från maktmissbruk och säkerställa och återställa allmänhetens förtroende för polisens och gränsmyndigheternas verksamheter.
- **Återkopplingsmöten med företrädare för allmänheten** för att ta del av åsikter, diskutera profilering och samla in feedback om verksamheten gör det möjligt att dra viktiga lärdomar och förbättra profileringarna.

Ansvarighet är en viktig princip för demokratisk samhällsstyrning. I mycket allmänna ordalag innebär detta att svar måste ges till dem som har rätt att begära en redogörelse ⁽³⁵⁾. Ansvarigheten gäller inte bara enskilda personers beslutsfattande, utan även institutionens (så kallat "institutionellt ansvar"). Som offentliga tjänstemän och organ är tjänstemän inom brottsbekämpning och gränsförvaltning, såväl som deras organisationer, ansvariga för sina beslut och handlingar inför allmänheten. Detta

(35) Bovens, M., Schillermans, T. och Goodlin, R.E. (2014), s. 1-11.

innebär att de är ansvariga för att säkerställa att all profilering utförs inom lagens gränser.

Insamling av tillförlitliga, korrekta och aktuella uppgifter är avgörande för att säkerställa ansvarigheten. Eftersom många av uppgifterna innehåller känsliga personuppgifter måste de hanteras i enlighet med reglerna och förfarandena för dataskydd (se kapitel 3).

Checklista för ansvarighet

Nedanstående checklista innehåller en grundläggande översikt över de åtgärder som myndigheter inom brottsbekämpning och gränsförvaltning kan vidta för att säkerställa att de är ansvariga för sina beslut och handlingar i samband med profilering. Förteckningen kan hjälpa tjänstemännen att öka sin ansvarighet, men de olika stegen ska inte betraktas som obligatoriska för tjänstemän inom både brottsbekämpning och gränsförvaltning. Beroende på sammanhanget kan det hända att vissa rekommendationer inte är tillämpliga på de specifika förutsättningarna inom gränsförvaltningen.

1. Identifiera

- Skapa förståelse för och **erkänn** problemet med olaglig profilering. Fördomar och stereotyper förekommer och utgör risker för dem som är inblandade, däribland tjänstemän och lokala samhällsgrupper.
- Samla in och använd disaggregerade data**. De är ett viktigt verktyg för att bedöma effektiviteten och resultaten.
- Delta i externa paneler som anordnas av det civila samhället för att få **feedback** om era metoder och förstärka förtroendet för era insatser.

2. Samla in information

- Säkerställ ansvarigheten genom att **föra register** över profileringarna.
- Om nödvändiga skyddsåtgärder iakttas kan **videoövervakning** och/eller **kroppsburna kameror** förstärka ansvarigheten och fungera som stöd till åtgärder för att ändra på mönster av fördomsfulla beteenden.
- Skapa **formulär för kontroll och visitering** som ska fyllas i av polistjänstemännen efter varje kontroll.

3. Agera och förhindra

- ☑ Gör **bedömningar** för att ta reda på om det finns regler eller metoder som förstärker medvetna och/eller undermedvetna fördomar och negativa stereotyper.
- ☑ Inför särskilda kurser och/eller **utbildningar** med inriktning på personliga och institutionella fördomar och stereotyper.
- ☑ **Ge information** till personer som stoppas för att förstärka upplevelsen av en rättvis kontroll, och ge personerna tillräcklig information om deras möjligheter att begära prövning. Vid hänvisningar till fördjupad kontroll vid gränspassager är tillhandahållandet av information en rättslig skyldighet.
- ☑ Visa **nolltolerans** mot fördomsfullt beteende inom organisationen.
- ☑ Inrätta **interna mekanismer** för övervakning och kontroll, t.ex. interna paneler för att diskutera om kontrollerna utförs på rimliga grunder.
- ☑ Se till att **prestationsindikatorer** kopplas till undvikande av fördomar och stereotyper.
- ☑ Inrätta **klagomålsmekanismer** för att avskräcka från maktmissbruk och säkerställa ansvarighet.

Källa: FRA, 2018.

2.3.1. Intern övervakning

Ledningen och förvaltningen av myndigheterna inom brottsbekämpning och gränsförvaltning spelar en viktig roll när det gäller att skapa en kultur som upprätthåller individuella rättigheter och principen om icke-diskriminering, både inom organisationen och i dess kontakter med allmänheten. De bidrar även till att skapa ett klimat av ansvarighet och öppenhet. Öppen kommunikation bland personalen (både horisontell och vertikal) och tydliga normer för beteenden, däribland yrkesmässiga uppförandekoder, är två av de interna åtgärder som bör vidtas för att förstärka ansvarigheten. Rekrytering och utbildning kan också spela en viktig roll (se [avsnitt 2.2.3](#)).

Enligt unionsrätten måste alla offentliga myndigheter och organ utse ett **dataskyddsombud**. Han eller hon ska informera polistjänstemän och gränsbevakningspersonal om deras skyldigheter, däribland om att de ska föra register över

behandlingen av personuppgifter och genomföra konsekvensbedömningar avseende dataskydd. När det gäller profilering ska dataskyddsombudet till exempel ge råd om och se till att de personuppgifter som samlas in före eller under profilering behandlas och lagras på ett lagligt sätt.

Fokus på dataskyddsombudens roll

I **polisdirektivet** föreskrivs att medlemsstaterna ska utse ett dataskyddsombud som ska ha följande uppgifter:

- Övervaka efterlevnaden av den tillämpliga lagstiftningen om skyddet av personuppgifter, däribland genom
 - tilldelning av ansvarsområden,
 - medvetandehöjande insatser och fortbildning av personal,
 - revisioner.
- Ge råd om konsekvensbedömningen avseende dataskydd och övervaka dess genomförande.
- Fungera som kontaktpunkt för tillsynsmyndigheten.

Dataskyddsombudet ska delta fullt ut och i god tid i alla frågor som rör skyddet av personuppgifter.

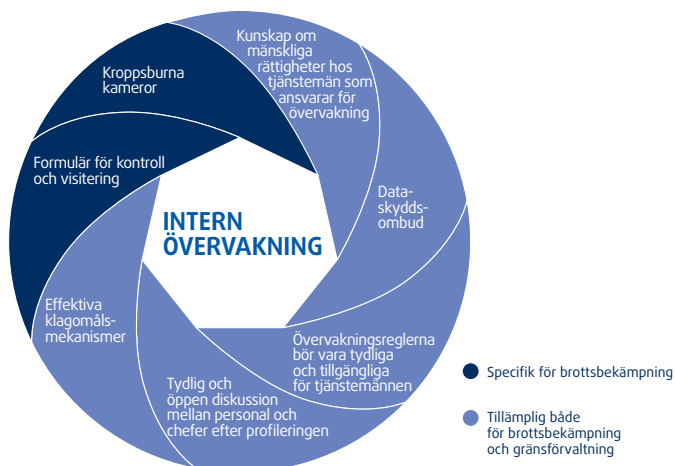
Se artiklarna 32-34 i polisdirektivet.

Inom polismakten kan profileringen övervakas internt som en del av en bred uppsättning av andra åtgärder för att registrera möten mellan myndigheterna och allmänheten (se [figur 10](#)). Dessa åtgärder omfattar användningen av

- **formulär för kontroll och visitering**, ett användbart och praktiskt verktyg som uppmuntrar tjänstemännen att utföra välgrundade kontroller och främjar öppenheten och ansvarigheten gentemot allmänheten (se [avsnitt 2.2.5](#)),
- **kroppsburna kameror**, ett verktyg som, om de nödvändiga skyddsåtgärderna iakttas, kan förstärka förtroendet mellan olika samhällsgrupper och polisen och fungera avskräckande mot missbruk av våld och diskriminering (se [avsnitt 2.3.2](#)).

Dessa åtgärder kan även användas vid den interna övervakningen av organisationer för gränsförvaltning. I Schengenkatalogen rekommenderas till exempel att antalet av och skälen till fördjupade kontroller ska registreras. Dessutom skapar de olika förutsättningarna för gränskontroller, infrastrukturen vid gränspassagerna och närvaron av överordnade chefer ytterligare möjligheter för intern övervakning. Exempelvis kan videoövervakning eller annan teknisk utrustning finnas tillgänglig.

Figur 10: Åtgärder i samband med intern övervakning



Källa: FRA, 2018.

Om de nödvändiga skyddsåtgärderna iakttas kan videoinspelningar ligga till grund för bedömningen av hur profileringen genomförs och användas som bevis i samband med särskilda klagomål. Inspelningarna kan till exempel bekräfta om en persons beteende i väntan på den inledande kontrollen gav tillräckliga skäl för en fördjupad kontroll.

I motsats till kontroller och visiteringar är videoövervakning något som resenärerna förväntar sig vid gränspassager på grund av deras offentliga karaktär och överväganden rörande säkerhet. Användningen av sådana verktyg måste likväl uppfylla rätten till integritet och de tillämpliga dataskyddsbestämmelserna.

Att föra register kan ha både kortsiktiga och långsiktiga fördelar. Exemplet med formulär för kontroll och visitering visar följande:

- På **kort sikt** kan formulär för kontroll och visitering säkerställa ansvarigheten på plats. I Förenade kungariket ska varje person som stoppas få en redogörelse för formuläret eller ett kvitto där det står var de kan hämta en kopia. Redogörelsen omfattar information om orsaken till kontrollen och möjligheten att lämna in klagomål. Detta gör att personen kan granska skälen och bestrida dem om de uppfattas som orättvisa.
- På **lång sikt** kan polisen analysera registren för att fastställa om befogenheterna i samband med kontroller och visiteringar har varit oproportionerligt inriktade mot medlemmar av en viss minoritetsgrupp och anpassa de riktlinjer som ges till tjänstemännen i enlighet med detta. Dessa register kan göras offentliga för att förstärka öppenheten och främja allmänhetens förtroende för användningen av kontroll- och visiteringsbefogenheter.

Att föra register: Vad säger lagen?

För att säkerställa att databehandlingen är laglig föreskrivs i polisdirektivet att brottsbekämpande myndigheter ska föra ett register över alla kategorier av behandling inom sitt ansvarsområde. Om de använder automatiserade databehandlingssystem måste de dessutom föra loggar för att kunna fastställa vem som har läst eller lämnat ut personuppgifter, när det ägde rum, vem som fick uppgifterna och motiveringen till behandlingen (se [avsnitt 3.1.3](#)).

Artiklarna 24 och 25 i polisdirektivet

Fallstudie

Användning av register för att upptäcka oproportionerliga kontroll- och visiteringsåtgärder (Förenade kungariket)

I den uppförandekod som utarbetats i England och Wales (Förenade kungariket) enligt lagen om polisarbete och bevismaterial fastställs att polisen har en lagstadgad skyldighet att övervaka användningen av kontroll- och visiteringsbefogenheter för att fastställa om de utövas på grundval av stereotypa bilder eller olämpliga generaliseringar. Varje uppenbart oproportionerlig användning av befogenheterna som enskilda tjänstemän eller grupper av tjänstemän gör sig skyldiga till eller som sker mot särskilda delar av samhället bör identifieras och utredas för att lämpliga åtgärder ska kunna vidtas. Polisen måste dessutom se till att registren kan granskas

av företrädare för allmänheten och förklara användningen av kontroll- och visiteringsbefogenheter på lokal nivå.

För mer information, se Förenade kungariket, inrikesministeriet (2014a).

Polisen i Förenade kungariket har utvecklat flera verktyg för att öka öppenheten genom att göra uppgifter om kontroller och visiteringar lättillgängliga. På webbplatsen www.police.uk kan användare skriva in sitt postnummer för att se detaljerad information om antalet kontroller och deras karaktär i det lokala området. Den information som offentliggörs bygger på ifyllda formulär för kontroll och visitering. Metropolitan Police har även en [anslagstavla för kontroller och visiteringar](#) med uppgifter om alla kontroller och visiteringar i London, däribland andelen kontrollerade personer med bakgrund i en etnisk minoritet i förhållande till hela befolkningen. Användare kan komma åt detaljerade uppgifter på olika sätt via internet, till exempel

- en karta som för varje månad visar den exakta platsen för de kontroller och visiteringar som utförts i ett visst område. Verktöget ger även detaljerad information om kontrollen (syfte, typ, resultat, om kontrollen ingick i en polisinsats), om personen (kön, åldersgrupp, självdefinierat etniskt ursprung, ursprung som definierats av tjänstemannen) och om den lagstiftning som ligger till grund för kontrollerna och visiteringarna (se [figur 11](#)), samt
- en översikt med statistik och diagram som visar polisens kontroll- och visiteringsinsatser. Detta gör att informationen kan aggregeras och laddas ner.

Även om detta ökar öppenheten och förtroendet kan det påverka rätten till integritet och dataskydd för de berörda personerna. En kombination av tillgängliga uppgifter i detta eller andra onlineverktyg kan användas för att fastställa en enskild persons identitet. Sådana risker måste bedömas och i relevanta fall förhindras.

Figur 11: Onlineverktyg som visar uppgifter om kontroller och visiteringar i London

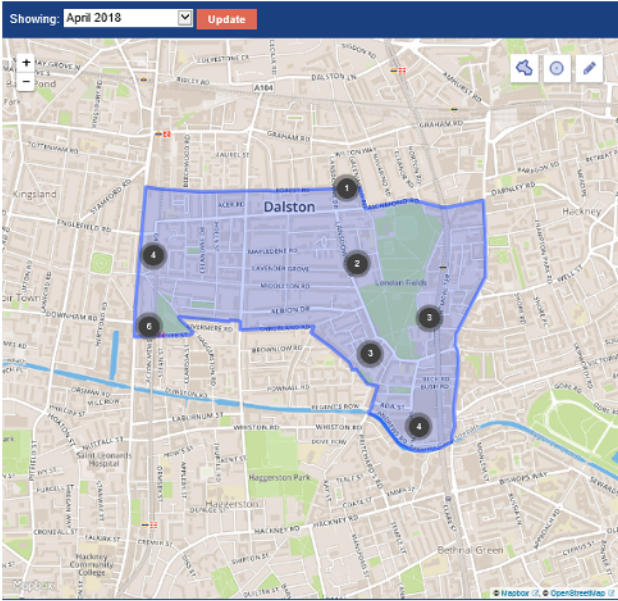
POLICE.UK Find your neighbourhood 🔍 Share this page ➦

Home > Metropolitan Police Service > London Fields > Stop and search >

Stop and search map

Click on the dots on the map for information about individual stop and searches.

Showing: April 2018



[View A-Z list of stop and search locations](#)

[View the crime map for London Fields](#)

1076 stop and searches were carried out by Metropolitan Police Service this month that could not be mapped to a location.

The British Transport Police are responsible for policing railways in the Metropolitan Police Service area. [View summary information for stop and searches conducted by the British Transport Police.](#)

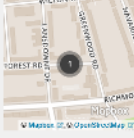
Location anonymisation is accurate to 2012 population and housing developments. [Learn more.](#)

Please [contact us](#) about any privacy concerns, or feedback about how useful and useable you find this stop and search information.

Källa: Förenade kungariket, inrikesministeriet, webbplats med *karta över kontroller och visiteringar.*

POLICE.UK Find your neighbourhood Search this page Menu

Home > Metropolitan Police Service > London Fields > Stop and search > Map >



Stop and searches on or near Forest Road in April 2018

In this neighbourhood

- Overview
- Crime map
- Stop and search
- Policing team
- News and events
- Performance
- Community Feedback

Stop and search at 29 April 2018, 12:20 p.m.

<p>Object of search: Articles for use in criminal damage</p> <p>Type of search: Person search</p> <p>Outcome: A no further action disposal</p> <p>Part of a policing operation: No</p> <p>Gender: Male</p> <p>Age range: over 34</p>	<p>Self-defined ethnicity: Black/African/Caribbean/Black British - Any other Black/African/Caribbean background</p> <p>Officer-defined ethnicity: Black</p> <p>Removal of more than just outer clothing: Unknown</p> <p>Legislation: Police and Criminal Evidence Act 1994 (section 1)</p> <p>Outcome linked to object of search: Unknown</p>	<p>Next steps</p> <ul style="list-style-type: none"> View stop and search overview for Metropolitan Police Service Contact us regarding a privacy request or to provide stop and search feedback Contact your local policing team Attend your next beat meeting <p>Related links</p> <ul style="list-style-type: none"> Stop and search FAQs
--	--	---

Källa: Förenade kungariket, inrikesministeriet, [webbplats med specifika kontroller](#).

2.3.2. Kroppsburna kameror

Polisen använder kroppsburna kameror i allt större utsträckning. De kan vara viktiga för att säkerställa ansvarigheten, förbättra kvaliteten i de enskilda mötena och ändra på mönster av fördomsfulla beteenden. De kan även bidra till att förhindra farliga situationer. Vid sidan av det bildmaterial som samlas in av polisen använder personer i allmänheten allt oftare sina kameror för att filma polisens ingripanden. Detta material kan också användas för att granska polisens arbete.

Fallstudie

Effekterna av kroppsburna kameror

I Förenade kungariket utfördes 2015 en undersökning av hur 500 kameror användes av 814 polistjänstemän inom Metropolitan Police. Resultaten visade ingen övergripande inverkan på antalet eller typerna av kontroller

och visiteringar, ingen effekt på andelen arresteringar för våldsbrott och inga bevis för att kamerorna förändrade tjänstemännens sätt att bemöta vare sig brottsoffer eller misstänkta. Rapporter om liknande försök av andra poliskårer innehåller inga eller endast fåtaliga bevis för att kamerorna hade någon positiv effekt för att minska antalet brott, antalet klagomål mot tjänstemän eller användningen av våld.

För mer information, se Big Brother Watch (2017).

I Frankrike användes kroppsburna kameror på 300 platser under en tvåårig försöksperiod. Inrikesministeriet utförde i juni 2018 en granskning där de positiva effekterna och resultaten av försöket lyftes fram. I rapporten betonades framför allt de kroppsburna kamerornas avskräckande effekt för att hindra personer från att kränka eller förolämpa polisen. Rapporter från olika kommuner visade att användningen av kameror minskade det aggressiva och kränkande beteendet mot polistjänstemännen. Några av kommunerna påpekade att användningen av kroppsburna kameror verkade ha förhindrat situationer som annars hade kunnat leda till att polistjänstemännen utsattes för brott. Dessa rapporter visar att kroppsburna kameror främst har varit användbara för att skapa en avskräckande effekt, men en del av bildmaterialet har kunnat användas som bevis under domstolsförhandlingar för att identifiera gärningsmän. Slutligen betonade flera av kommunerna att kamerorna hade pedagogiska fördelar, eftersom polistjänstemännen kunde använda inspelningarna för att lära sig olika förfaranden och tekniker vid ingripanden. Efter försöksperioden lades ett lagförslag fram för det franska parlamentet för att harmonisera användningen av kroppsburna kameror i alla poliskårer och utöka användningen till brandsoldater och fängelsepersonal.

För mer information, se Frankrike, inrikesministeriet (2018).

En 12 månader lång försöksperiod med kroppsburna kameror utfördes 2012–2013 i Rialto i USA för att utröna om kamerorna skulle leda till socialt önskvärda beteenden bland polistjänstemännen. Resultaten visade att användningen av våld under 12-månadersperioden minskade från 60 till 25 fall jämfört med 2011 och att klagomålen mot polisen minskade från 28 till 3 ärenden.

För mer information, se Farrar, T. (2018).

Polisens användning av kroppsburna kameror väcker emellertid även farhågor när det gäller de grundläggande rättigheterna. Tydliga skyddsåtgärder och användningsregler är nödvändiga för att hantera dessa problem.

- Vilken **roll kroppsburna kameror har för att upptäcka och avskräcka från olaglig profilering** är oklar. Kamerorna fångar enskilda incidenter, vilket gör att det inte går att samla in statistiska uppgifter som kan användas för att fastställa om kontrollerna och visiteringarna är diskriminerande. I stället kan de användas för att granska och diskutera enskilda händelser och bidra till att förbättra deras kvalitet.
- Användningen av kroppsburna kameror kan ha **negativa effekter på relationerna till minoritetsgrupper** som känner sig särskilt utsatta. Om skyddsåtgärder och användningsregler utarbetas i samråd med lokala samhällsgrupper kan kroppsburna kameror ses som ett verktyg för att förbättra ansvarigheten i stället för att stigmatisera minoritetsgrupper.
- Användningen av kroppsburna kameror **har konsekvenser för rätten till integritet och dataskydd**, såväl som för andra grundläggande rättigheter. De kan till exempel påverka friheten att delta i fredliga sammankomster om de används för att övervaka offentliga demonstrationer. Det är ofta oklart när kamerorna bör vara igång eller avstängda och vad som händer om en tjänsteman glömmer eller beslutar att inte sätta på sin kamera. Tydlig vägledning behövs inom detta område. Privata företag som tillhandahåller denna tjänst måste vara tydliga med att de inte använder bildmaterialet för egna ändamål. Användningen av kroppsburna kameror bör regleras i lag för att säkerställa att den uppfyller de grundläggande rättigheterna.

Fokus på effektiv användning av kroppsburna kameror

Uppfylldandet av tre viktiga principer kan bidra till att säkerställa att kroppsburna kameror används på ett effektivt sätt:

- **Äkthet.** Bilderna måste kunna knytas direkt till händelsen. Datum och tidpunkt (t.ex. genom tidsstämpling) och exakt plats (t.ex. via GPS) för incidenten bör registreras.
- **Tillförlitlighet.** Bilderna bör laddas upp i det centrala systemet på ett noggrant, säkert och konfidentiellt sätt. Dessa bilder bör uppfylla

principerna för dataskydd och respekt för integriteten, och bör därför inte lagras under längre tid än vad som föreskrivs i lagen.

- **Tillåtlighet.** För att vara användbart i straffrättsliga förfaranden måste bildmaterialet kunna förevisas vid domstolsförfaranden. Detta kan innebära att
 - undvika kontinuerlig videoinspelning som utgör en oacceptabel inskränkning av rätten till integritet, både för polistjänstemannen och den filmade personen,
 - informera dem som kan bli filmade och få deras samtycke (vid behov),
 - lagra bilder med tillräcklig säkerhetsnivå och hålla reda på tillgången till bilderna för både polistjänstemän och medborgare.

För mer information, se Coudert et al. (2015), s. 8.

Ytterligare teknikutveckling kommer att kräva att nya skyddsåtgärder utarbetas för att säkerställa att kroppsburna kameror används på ett lagligt sätt. Till exempel kan kameror som automatiskt känner igen en persons ansikte genom att jämföra det med tidigare poster i en befintlig databas medföra nya utmaningar för rätten till integritet och dataskydd.

Fallstudie

Poliser som använder kroppsburna kameror: En bedömningsmall (USA)

För att öka öppenheten och ansvarigheten vid användning av kroppsburna kameror utvecklade paraplyorganisationen Leadership Conference on Civil and Human Rights & Upturn i USA ett verktyg för att bedöma och strukturera den information som finns i bildmaterial från kroppsburna kameror. I verktyget föreslås åtta olika kriterier för bedömningen av sådant material:

1. Om bildmaterialet offentliggörs och görs tillgängligt av polismyndigheten.
2. Om tjänstemännens godtycke om vad som ska registreras framgår tydligt.
3. Om farhågor kring skyddet av personuppgifter beaktas.

4. Om tjänstemännen måste granska bildmaterialet innan de utarbetar sin inledande skriftliga rapport.
5. Om oskyddat bildmaterial ska raderas inom en förutbestämd tidsperiod.
6. Om bildmaterialet skyddas mot manipulering och missbruk.
7. Om bildmaterialet görs tillgängligt för personer som inger klagomål.
8. Om användningen av biometriska tekniker för att identifiera enskilda personer i bildmaterialet är begränsad eller inte.

Sådana initiativ kan bidra till att förstärka ansvarigheten genom att fastställa normer och uppmuntra genomförandet av mekanismer för att bedöma om bildmaterialet samlas in och används på ett korrekt sätt.

För mer information, se Leadership Conference on Civil and Human Rights & Upturn, [webbplatsen om bedömningsmallen](#).

2.3.3. Klagomålsmekanismer

Effektiva klagomålsmekanismer kan både avskräcka från maktmissbruk och bidra till att säkerställa och återställa allmänhetens förtroende för polisens och gränsmyndigheternas verksamheter. De används vanligen vid sidan av formella rättsliga kanaler som gör att enskilda personer kan överklaga en handling eller ett beslut av en offentlig myndighet inför en oberoende och opartisk domstol.

För att mekanismerna ska vara effektiva bör följande förutsättningar vara uppfyllda:

- **Det bör vara lätt för enskilda personer att komma åt klagomålsmekanismerna.** Det finns entydiga bevis för att många är ovilliga att lämna in klagomål, till exempel på grund av att processen är för lång eller dyr eller för att de är oroliga för negativa konsekvenser. Användningen kan uppmuntras om klagomålsmekanismerna finns tillgängliga via internetplattformar som webbplatser eller appar. Dessutom kan organisationer hjälpa enskilda personer att lämna in klagomål, antingen genom att framföra klagomålen för deras räkning eller genom de principer för kollektiv prövning som avses i artikel 80.2 i den allmänna dataskyddsförordningen.

- **Klagomålen bör hanteras på ett öppet sätt.** Detta bidrar till att öka förtroendet för klagomålsmekanismerna.
- **Klagomålsinstanserna bör vara oberoende** av organisationen eller den del av organisationen mot vilken klagomålet framförs.

Det finns en mängd olika mekanismer som hanterar olika typer av klagomål. I [figur 12](#) ges en översikt över vissa av de klagomålsmekanismer som finns tillgängliga i medlemsstaterna och på EU-nivå.

Figur 12: Översikt över klagomålsmekanismer i EU:s medlemsstater



Källa: FRA, 2018.

Mekanismer där polistjänstemän möter personer i allmänheten för att lyssna på deras klagomål, diskutera profilering och få feedback på sin verksamhet gör det möjligt att dra viktiga lärdomar för att förbättra de processer som reglerar profileringen. De gör även att allmänheten kan bli delaktig i den brottsbekämpande verksamheten (se fallstudien).

Fallstudie

Offentliga klagomålsmekanismer inom brottsbekämpningen

Paneler för offentlig granskning (West Midlands Police – Förenade kungariket)

De åtta polisdistrikten inom West Midlands Police (WMP) anordnar varannan månad en panel för granskning av kontroller och visiteringar, där personer i allmänheten fungerar som ordförande. Dessa paneler granskar rapporter om kontroller och visiteringar, säkerställer att WMP respekterar lagen och ger olika samhällsgrupper möjlighet att lämna in klagomål och framföra åsikter. Mötenas dagordning och protokoll offentliggörs online. WMP har infört ett antal metoder för att öka samhällsengagemanget i ett försök att göra kontrollerna mer rättvisa och målinriktade och utöka tjänstemännens ansvarighet.

För mer information, se West Midlands Police, [webbplatsen om kontroller och visiteringar](#) och Her Majesty's Inspectorate of Constabulary (2016).

Paneler om rimliga grunder (Northamptonshire Police – Förenade kungariket)

Polisen i Northamptonshire har inrättat paneler om rimliga grunder för att göra allmänheten delaktig i förbättringen av kontroller och visiteringar. Dessa paneler fungerar som en kanal för diskussioner om användningen av kontroll- och visiteringsbefogenheterna och deras inverkan på samhällsgrupperna. Panelerna leds av en poliskommissarie och består av en polistjänsteman och två personer i allmänheten, i vissa fall före detta gärningspersoner. Förutom att förbättra kommunikationen mellan polisen och allmänheten har panelen befogenhet att inskränka polistjänstemännens befogenheter och besluta om ytterligare utbildning för att förbättra deras kontroll- och visiteringsinsatser.

För mer information, se Northamptonshire Police, webbplatsen om panelen och [Open Society Justice Initiative](#) (2018a).

Informellt nätverk av klagomålsmekanismer för polisen

Independent Police Complaints Authorities' Network (IPCAN) är ett informellt nätverk för utbyte och samarbete mellan oberoende instanser som är ansvariga för den externa kontrollen av säkerhetsstyrkor. Nätverket skapades 2013 och sammanför klagomålsmyndigheter från omkring 20 olika länder. Dessa organ, som främst kommer från EU:s medlemsstater, tar emot och behandlar klagomål mot offentliga säkerhetsstyrkor och, i vissa fall, privata styrkor.

För mer information, se IPCAN:s [webbplats](#).

När det gäller gränsförvaltning kan offentliga klagomålsmekanismer genomföras genom möjligheten att lämna in klagomål på plats eller i efterhand. Möjligheten att komma åt sådana mekanismer ökar öppenheten och ansvarigheten, och främjar en ömsesidig respekt och en god relation mellan gränsbevakningspersonalen och allmänheten. Alternativet att inge klagomål i efterhand till ett ledande organ i stället för (endast) direkt vid gränspassagen förstärker graden av tillsyn och kan öka resenärernas benägenhet att rapportera möjliga incidenter ⁽³⁶⁾.

Fallstudie

Klagomålsmekanismer i samband med gränsförvaltning

Intern klagomålsmekanism vid Manchesters flygplats (Förenade kungariket)

Vid Manchesters flygplats fungerar Central Allocation Hub som en enda kontaktpunkt för alla passagerare som vill framföra klagomål. Klagomål kan lämnas in via e-post, brev, telefon eller fax, eller personligen, på antingen engelska eller walesiska. I riktlinjerna för Förenade kungarikets gränsstyrka beskrivs olika metoder för att hantera klagomål. Mindre överträdelser som oartighet, bryskhet eller dåligt beteende kan vanligen lösas lokalt. Bland

(36) FRA (2014b).

de olika möjligheterna ingår att klargöra problemet med kunden, förklara det operativa förfarandet, komma överens om ytterligare åtgärder och erbjuda en ursäkt i förekommande fall. Klagomål om allvarliga överträdelser hänvisas vanligen till enheten för yrkesstandarder. Gränsbevakningens riktlinjer omfattar ett test för att fastställa tecken på möjlig diskriminering som kan utgöra en allvarlig överträdelse. Om det finns starka bevis för att behandlingen av en resenär kan förklaras med andra faktorer än ras hänvisas fallet vanligen till ett lokalt beslut.

För mer information, se FRA (2014a), s. 74.

Frontex mekanism för individuella klagomål (EU)

Efter antagandet av den nya förordningen om den europeiska gräns- och kustbevakningsbyrån (Frontex) 2016 inrättade Frontex en mekanism för individuella klagomål för att övervaka respekten för grundläggande rättigheter inom byråns verksamhet. Mekanismen omfattar pilotstudier, återvändandeinsatser, gemensamma insatser, snabba gränsinsatser, utplacering av stödgrupper för migrationshantering och återvändandeinterventioner. Alla personer vars rättigheter har påverkats direkt av den personal som deltar i Frontex verksamheter, däribland nationella offentliga myndigheter, kan lämna in klagomål till Frontex ombud för grundläggande rättigheter. Han eller hon beslutar om huruvida klagomålet kan tas upp till prövning och skickar det till Frontex verkställande direktör samt till myndigheterna i den berörda medlemsstaten om nationell personal deltog i den anmälda överträdelsen. Klagomålet kan lämnas in på vilket språk som helst via e-post, brev eller via ett klagomålsformulär på Frontex webbplats: <http://frontex.europa.eu/complaints/>.

Fokus på rättigheterna för tjänstemän inom brottsbekämpningen

Poliser har precis samma rättigheter och friheter som andra personer och skyddas av människorättsnormer under sin tjänsteutövning. De kan åberopa de rättigheter som har fastställts i olika internationella människorättsdokument, t.ex. Europeiska konventionen om de mänskliga rättigheterna eller Internationella konventionen om medborgerliga och politiska rättigheter. I den europeiska yrkesetiska koden för polisen klargörs att polispersonal som regel ska ha samma medborgerliga och politiska rättigheter som andra medborgare. Inskränkningar i dessa

rättigheter får endast ske om det krävs för att utöva polisens funktioner i ett demokratiskt samhälle i enlighet med lagen och i enlighet med Europeiska konventionen om de mänskliga rättigheterna. Ett undantag finns i artikel 11 i Europakonventionen och gäller rätten till mötes- och föreningsfrihet.

När poliser utför polisuppgifter, och framför allt när de utövar polisens befogenheter, agerar de inte som privatpersoner utan som ett statligt organ. Statens skyldighet att respektera och skydda mänskliga rättigheter får därför direkta konsekvenser för den enskilda polisens möjlighet att svara på aggressioner. Poliser som kan riskera att skadas eller dö under tjänstgöringen har också rättigheter som ska respekteras och skyddas. Detta görs t.ex. genom att erbjuda skyddsutrustning, noggrant planera polisinsatser eller vidta förebyggande åtgärder. När polisens uppgifter utförs kan det bli nödvändigt att inskränka den enskilda polisens rättigheter, men alla sådana inskränkningar måste ske enligt proportionalitetsprincipen. Eftersom polisen har en särskild roll som statligt organ kan rättigheterna inskränkas mer för en polis än för en "vanlig medborgare". Som exempel kan nämnas en demonstration som övergår i våldsamheter. En "vanlig medborgare" kan springa därifrån eller söka hjälp, medan en polis är skyldig att skydda andra personers mänskliga rättigheter och återställa allmän ordning.

För mer information, se FRA (2013).

3

Algoritmisk profilering



Med algoritmisk profilering avses varje form av stegvis datoriserad teknik som analyserar data för att identifiera utvecklingstrender, mönster eller sammanhang ⁽³⁷⁾. Genom profilering väljs en enskild person ut på grundval av kopplingar till andra som identifierats av algoritmen i stället för personens verkliga beteende, och enskilda individers val struktureras i enlighet med information om gruppen i stället för deras egna personliga val ⁽³⁸⁾.

Algoritmisk profilering kan hjälpa organisationer inom gränsförvaltning och brottsbekämpning att använda data för att förebygga, upptäcka och utreda brott på ett effektivt sätt. Insamlingen och behandlingen av stora dataset väcker emellertid farhågor angående de grundläggande rättigheterna. Utöver vikten av att undvika diskriminering medför algoritmisk profilering nya risker, särskilt när det gäller rätten till skydd av integritet och personuppgifter. I detta avsnitt behandlas dessa risker i första hand. Avsnittet innehåller även en beskrivning av de utmaningar för de grundläggande rättigheterna som förknippas med användningen av algoritmisk profilering i stora databaser för gränsförvaltning och säkerhetsinsatser och förslag på hur dessa risker kan minimeras.

(37) För mer information om vad algoritmer är, se FRA (2018b), s. 4.

(38) Mittelstadt, BD, Allo, P., Taddeo, M., Wachter, S. och Floridi, L. (2016).

Fokus på prognostiserat polisarbete

De brottsbekämpande myndigheterna använder flera olika programvaror för att kunna förutse när och hur ett brott kommer att begås. Några exempel på detta är PredPol i Förenade kungariket och USA, Criminality Awareness System (CAS) i Nederländerna samt Precobs i Tyskland och Schweiz. Hur effektiva dessa prediktionsmetoder är när det gäller att förebygga brottslighet har emellertid ännu inte utvärderats ordentligt. Än så länge är bevisen motsägelsefulla, vilket följande exempel visar.

Fältstudier i samband med prognostiserat polisarbete i Kent (Förenade kungariket) och Los Angeles (USA)

Polisen i Förenade kungariket och USA genomförde ett experiment för att jämföra en helt automatisk algoritm för identifiering av brottsplatser och efterföljande planering av polispatruller med ett mer traditionellt tillvägagångssätt.

Resultatet visade att den automatiska algoritmen fungerade bättre för att identifiera framtida brottslighet. Den förutsåg mellan 1,4 och 2,2 gånger fler kriminella handlingar än en brottsanalytiker som använde traditionella metoder med underrättelser och kartläggning. Dessutom är de patrulleringsinsatser som bygger på det prediktiva verktyget effektivare, vilket leder till en genomsnittlig minskning av antalet brott med 7,4 procent.

För mer information, se Mohler, G.O. et al. (2016).

Programmet PILOT (Predictive Intelligence Led Operational Targeting) i Shreveport (USA)

Inom detta program används en prediktiv modell för att identifiera små områden med ökad risk för egendomsbrott och införa en interventionsmodell för att förhindra sådana brott. Resultat från tre distrikt som använder PILOT-programmet jämfördes med tre distrikt där polisarbetet utfördes på ett traditionellt sätt. Inga statistiskt säkerställda bevis kunde påvisas för en större minskning av egendomsbrotten i de tre PILOT-distrikten.

För mer information, se Hunt, P. et al (2014).

Programvaran Beware (USA)

Beware är en programvara som gör att nödsamtal kan färgkodas (röd, gul eller grön) för att visa hotnivån för den berörda personen eller platsen. Programvaran söker igenom databaser med arresteringsrapporter, fastighetsregister, kommersiella databaser, djupgående webbsökningar, inlägg på sociala medier och andra offentligt tillgängliga databaser.

Systemets styrkor och svagheter har ännu inte utvärderats. Bristen på tillsyn över beslutsprocessen och det faktum att algoritmen skyddas av yrkeshemligheter har emellertid väckt farhågor om ansvarigheten. Dessutom kan de potentiella felaktigheterna i de insamlade uppgifterna och/eller den information som härleds från analysen minska verktygets övergripande effektivitet.

För mer information, se American Civil Liberties Union (2016).

Fallstudie

Bedömning av effekter och risker med prognostiserat polisarbete – bedömningsverktyget ALGO-CARE

De möjliga negativa effekterna av prognostiserat polisarbete måste beaktas för att säkerställa en balanserad och öppen översikt över dess konsekvenser för samhället. Efter en analys som utfördes av en grupp av akademiker och polistjänstemän drogs slutsatsen att prognostiserat polisarbete fortfarande är i en experimentfas i Förenade kungariket och att dess konsekvenser för samhället och enskilda personer måste utvärderas ingående. Forskarna hävdar att vissa beslut skulle kunna medföra alltför stora konsekvenser för samhället och enskilda personer för att man ska låta dem påverkas av ny teknik. Dessa fall bör inte omfattas av ett algoritmiskt beslutsfattande.

För att styra upp användningen av algoritmiska bedömningsverktyg i polisarbetet utvecklade gruppen en beslutsram som kallas ALGO-CARE. Syftet med denna ram är att hjälpa polistjänstemännen när de bedömer de möjliga riskerna med prognostiserat polisarbete. Den är även ett försök att överföra grundläggande principer för offentlig rätt och mänskliga rättigheter

till praktiska överväganden och riktlinjer som kan hanteras av organ i den offentliga sektorn.

Polistjänstemännen kan använda verktyget för att bedöma användningen av prognostiserat polisarbete genom åtta kompletterande steg:

- **Rådgivande:** för att bedöma omfattningen av mänskligt ingripande.
- **Laglig:** för att bedöma den rättsliga motiveringen för användning av algoritmen.
- **Granularitet:** för att bedöma om algoritmen kan användas med tillräcklig detaljrikedom i det specifika ärendet.
- **Ansvarighet:** för att säkerställa att polismakten har det rättsliga ansvaret och den tekniska kapaciteten för att bedöma, upprätthålla, uppdatera och korrigera källkoden med regelbundna mellanrum.
- **Kontrollerbar:** för att säkerställa att mekanismer för tillsyn och granskning finns tillgängliga.
- **Noggrannhet:** för att bedöma om algoritmen är anpassad till syftet med polisarbetet och kan valideras periodvis, och att sannolikheten för och inverkan av felaktigheter utgör en godtagbar risk.
- **Rättvisande:** för att bedöma algoritmens korrekthet, ansvarighet och öppenhet.
- **Förklarbar:** för att bedöma tillgången till information om både reglerna för beslutsfattande och den inverkan varje faktor har på det slutliga resultatet.

För mer information, se Oswald, M. et al. (2017).

3.1. Ramen för dataskydd som styr algoritmisk profilering

Utvecklingen och den ökande användningen av nya tekniker – däribland användningen av stora dataset som stöd i beslutsfattandet – föranledde EU att göra en omfattande omarbetning av de regler som styr behandlingen av personuppgifter under 2016. I de två nya instrumenten, den allmänna dataskyddsförordningen och

polisdirektivet, fastställs viktiga principer och normer för varje beslut som baseras på datoriserade beslutsprocesser, däribland algoritmisk profilering.

Dataskyddsförordningen och polisdirektivet trädde i kraft i maj 2018, vilket innebär att det i skrivande stund endast finns ett fåtal praktiska exempel på genomförandet. I [avsnitt 1.2.2](#) finns en beskrivning av de rättsliga normer som styr rätten till integritet och dataskydd och en förklaring av de viktigaste skillnaderna mellan dataskyddsförordningen och polisdirektivet (se [tabell 2](#)). I detta kapitel beskrivs och förklaras de rättsliga krav för algoritmisk profilering som infördes genom dataskyddsförordningen och polisdirektivet. Några exempel:

- Uppgifterna måste behandlas för ett särskilt syfte med en specifik rättslig grund.
- Enskilda personer måste informeras när deras personuppgifter behandlas.
- Uppgifterna måste förvaras på ett säkert sätt.
- Olaglig databehandling måste upptäckas och förebyggas.

Polistjänstemän och gränsbevakningspersonal som vill ha mer information om de rättsliga krav som beskrivs i detta kapitel bör vända sig till dataskyddsombudet i sina organisationer. I den handbok över den europeiska dataskyddslagstiftningen som tagits fram av FRA, EDPS och Europarådet finns ytterligare vägledning om tillämpningen av polisdirektivet och dataskyddsförordningen ⁽³⁹⁾.

(39) FRA, EDPS och Europarådet (2018).

Huvudpunkter

- Algoritmisk profilering måste vara **berättigad, nödvändig** och **proportionerlig**.
- Uppgifter får inte behandlas utan ett **särskilt syfte med en specifik rättslig grund**.
- Enskilda personer har särskilda rättigheter som beskrivs i detalj i bestämmelserna i dataskyddsförordningen och polisdirektivet, däribland
 - **rätten till insyn i personregister**, däribland meningsfull information om logiken bakom algoritmen,
 - rätten **att få tillgång till personuppgifter**,
 - rätten **att inge klagomål** till en tillsynsmyndighet, och
 - rätten till ett **effektivt rättsmedel**.
- Uppgifterna ska samlas in, behandlas och lagras på ett **säkert** sätt.
- Olaglig databehandling måste **förebyggas** och **upptäckas**.

3.1.1. Uppgifterna måste behandlas för ett särskilt syfte

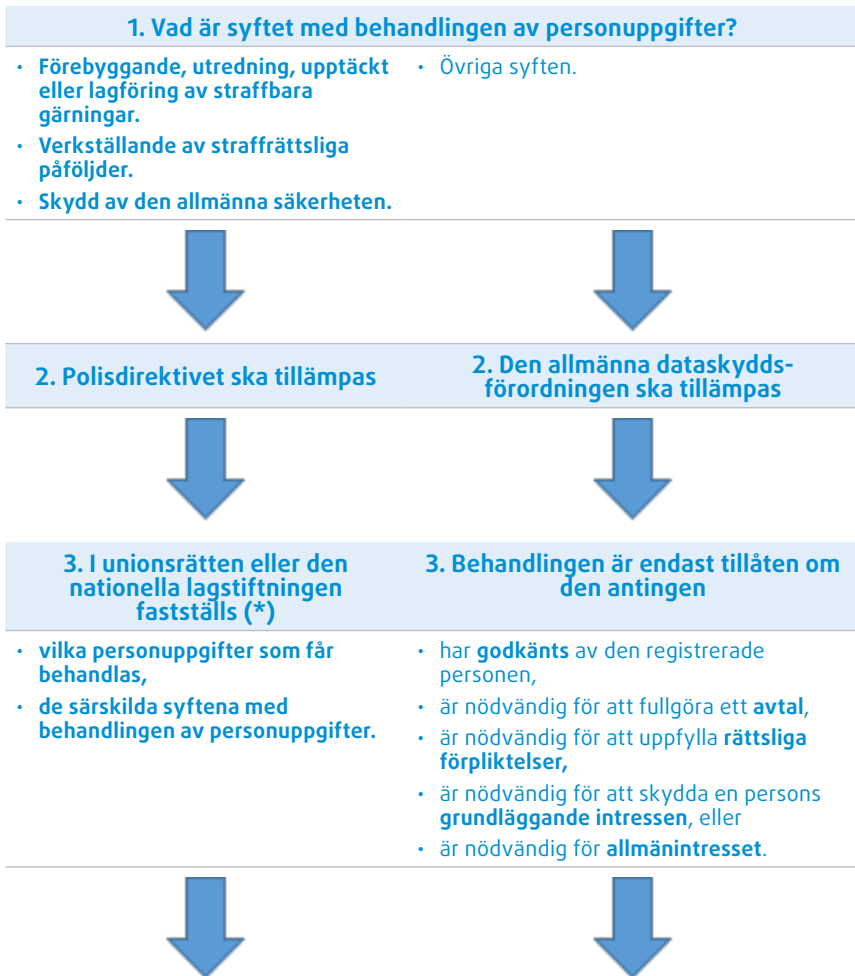
All behandling av personuppgifter måste ha en rättslig grund. Detta innebär att den måste utföras för att uppnå **ett särskilt syfte** som fastställs i lagen.

Innan en behandling påbörjas måste en tjänsteman känna till dess syfte. Detta kan bland annat omfatta följande frågeställningar:

- Ska uppgifterna behandlas för att upptäcka en straffbar gärning?
- Ska de behandlas för att upprätthålla den allmänna säkerheten?
- Ska de behandlas för att bekämpa terrorism?

När syftet har fastställts på ett korrekt sätt kommer tjänstemännen att veta vilken rättslig ram som är tillämplig och vilka rättsliga skyldigheter som måste uppfyllas. I [tabell 4](#) anges hur den tillämpliga rättsliga ramen ska fastställas.

Tabell 4: Identifiering av den korrekta rättsliga ramen beroende på syftet med behandlingen av personuppgifter



4. Är syftet med profileringen undantaget från polisdirektivet?

Rätten att bli informerad, att få tillgång till personuppgifter och att begära att uppgifterna ändras eller raderas kan vara begränsad (helt eller delvis) i följande fall:

- För att inte hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden.
- För att undvika en menlig inverkan på möjligheten att förebygga, upptäcka, utreda, eller lagföra straffbara gärningar eller verkställa straffrättsliga påföljder.
- För att skydda den allmänna säkerheten.
- För att skydda den nationella säkerheten.
- För att skydda andra personers fri- och rättigheter.

4. Är syftet med profileringen undantaget från dataskyddsförordningen?

De skyldigheter (att vara öppen, att informera och att anmäla överträdelser) och rättigheter (att få tillgång till och erhålla rättelse eller radering av personuppgifter, att ha rätt att göra invändningar eller att inte omfattas av automatiserat beslutsfattande) som fastställs i den allmänna dataskyddsförordningen **kan begränsas** av den nationella lagstiftningen eller unionsrätten för att säkerställa

- nationell säkerhet, försvar eller allmän säkerhet,
- förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder, inbegripet skydd mot och förebyggande av hot mot den allmänna säkerheten,
- andra av unionens eller en medlemsstats viktiga mål av generell allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,
- rättsväsendets oberoende och rättsliga förfaranden,
- förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,
- en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i de särskilda fallen,
- skyddet av den registrerade eller andras rättigheter och friheter,
- verkställigheten av civilrättsliga krav.

Anm.: (*) Nationella rättsakter som införlivar polisdirektivet finns tillgängliga på [webbplatsen EUR-Lex](#).

Källa: FRA, 2018.

3.1.2. Enskilda personer måste informeras

Enligt artikel 13 i polisdirektivet och artiklarna 13 och 14 i den allmänna dataskyddsförordningen ska enskilda personen informeras när deras personuppgifter behandlas. I tabell 5 beskrivs hur och när informationen ska lämnas till den person vars uppgifter behandlas.

Tabell 5: Skyldighet att ge enskilda personer information om profilering: typ av uppgifter, kommunikationssätt och undantag

Anmälningsskyldighet – Checklista	
Till vem?	Person vars uppgifter behandlas
Hur?	<ul style="list-style-type: none"> • tydligt och enkelt språk • lättillgänglig form • i samma form som begäran – <i>företrädesvis elektroniska metoder</i>
Vad?	<p>Om behandlingen:</p> <ul style="list-style-type: none"> • namn och kontaktuppgifter till din myndighet • kontaktuppgifter till ditt dataskyddsombud • syftena med behandlingen • den rättsliga grunden för behandlingen • den längsta tillåtna perioden för lagring av uppgifterna • typerna av personer/organisationer som kommer att få tillgång till uppgifterna <p>Om den enskilda personens rättigheter:</p> <ul style="list-style-type: none"> • rätten att inge klagomål till en tillsynsmyndighet, och tillsynsmyndighetens kontaktuppgifter • rätten att begära tillgång till sina personuppgifter • rättelse och/eller annullering av personuppgifter • rätten att begära en begränsning av bearbetningen
Undantag	<ul style="list-style-type: none"> • För överdrivna (dvs. upprepade) eller uppenbart ogrundade begäranden • Om den begärande personens identitet inte kan bekräftas • Om tillhandahållandet av information skulle hindra en utredning • Om tillhandahållandet av information skulle inverka menligt på förebyggandet/utredningen av straffbara gärningar • För att skydda den allmänna eller nationella säkerheten • För att skydda andra personers rättigheter

Källa: FRA, 2018.

Fokus på "rätten till förklaring"

När det gäller profilering fastställs i dataskyddsförordningen att "meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna" av behandlingen ska lämnas till den registrerade. Denna information bör lämnas både när uppgifterna samlas in (anmälan) och om personen begär ytterligare information (rätt till tillgång). Denna rättighet nämns inte uttryckligen i polisdirektivet. I skäl 38 fastställs emellertid att "automatiserad behandling [...] bör [...] omfattas av lämpliga skyddsåtgärder, inbegripet skild information till den registrerade [...], särskilt [...] rätten att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätten att överklaga beslutet".

Denna "rätt till förklaring" kan vara svår att genomföra i praktiken. Vissa personer kan ha tillräcklig digital kompetens för att förstå koden till en algoritm, medan andra kan behöva förenklad information om syftet med behandlingen och kopplingen mellan uppgifterna. Nyckeln till bedömningen av den lämnade förklaringens meningsfullhet är dess mål. Varje person bör få tillräcklig information för att förstå syftet, motiveringen och kriterierna bakom ett beslut.

Rätten till en förklaring är inte absolut (se steg 4 i [tabell 4](#)). Medlemsstaterna kan i flera fall begränsa denna rättighet i lagen, däribland mot bakgrund av nationell säkerhet och försvar; allmän säkerhet; förebyggande, utredning, upptäckt eller lagföring av straffbara gärningar; verkställande av straffrättsliga påföljder; skydd av den registrerade eller andras rättigheter och friheter eller verkställande av civilrättsliga krav.

Tillhandahållande av rimlig information om syftet med och de väntade konsekvenserna av behandlingen är under alla omständigheter rekommenderad god praxis. Enkla metoder för att förklara den ingående logiken och de kriterier som använts för att komma fram till ett beslut kommer i slutändan att förstärka öppenheten och ansvarigheten.

Mer information finns i den allmänna dataskyddsförordningen, artiklarna 13–15 (rätt till information och rätt till tillgång), artikel 22 (automatiserat individuellt beslutsfattande, inklusive profilering) och artikel 23 (begränsningar) samt i polisdirektivet, artikel 11 (automatiserat

individuellt beslutsfattande, inklusive profilering) och artiklarna 13–15 (rätt till information och rätt till tillgång).

Se även artikel 29-gruppen (2018a).

3.1.3. Säker förvaring av uppgifter: register, loggar och lagringsregler

Myndigheter som samlar in och behandlar personuppgifter i profileringssyfte måste inte bara behandla uppgifterna på ett lagligt sätt, utan även säkerställa att uppgifterna inte

- finns tillgängliga för obehöriga personer,
- används för andra syften än det ursprungliga syftet, eller
- lagras under längre tid än vad som är nödvändigt.

För detta ändamål måste myndigheter och tjänstemän inom brottsbekämpning och gränsförvaltning säkerställa att lämpliga åtgärder har vidtagits för att skydda uppgifternas integritet och säkerhet. De måste registrera varje åtkomst till, och användning av, uppgifterna genom att skapa och upprätthålla register över all behandling eller alla kategorier av behandling (artikel 30 i den allmänna dataskyddsförordningen och artikel 24 i polisdirektivet). Registren måste omfatta

- myndighetens och dataskyddsombudets **namn** och **kontaktuppgifter**,
- **syftet** med behandlingen,
- de **kategorier av mottagare** till vilka personuppgifterna har lämnats eller ska lämnas ut,
- en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter,
- **användningen av profilering**,
- information om den **rättsliga grunden** för behandlingen,

- om möjligt, de planerade **tidsfristerna** för annullering av de olika kategorierna av personuppgifter,
- om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 i dataskyddsförordningen eller artikel 29.1 i polisdirektivet.

Om datorbaserad profilering genomförs för syften som omfattas av polisdirektivet (se [avsnitt 3.2](#)) måste myndigheterna dessutom föra loggar över insamling, ändring, läsning, utlämning, inbegripet genom överföring, sammanförande och radering av uppgifter.

Dessa register och loggar hjälper tjänstemännen att visa att de uppfyller de rättsliga kraven under intern och extern övervakning. Om, till exempel, en enskild person lämnar in ett klagomål är myndigheterna för brottsbekämpning och gränsförvaltning skyldiga att göra registren och loggarna tillgängliga för de nationella dataskyddsmyndigheterna.

Personuppgifter bör inte lagras under längre tid än vad som är nödvändigt för att uppnå det berättigade syftet. Lagring under längre perioder måste motiveras på ett tillfredsställande sätt. I sådana fall bör myndigheterna säkerställa att lagringen granskas regelbundet för att garantera uppgifternas integritet och säkerhet.

3.1.4. Olaglig behandling måste upptäckas och förebyggas

Det kan vara svårt att upptäcka och förebygga olaglig behandling av personuppgifter. Den specialkunskap som behövs för att förstå komplicerade algoritmer och stora databaser gör det svårt att säkerställa ordentliga kontroller.

För att avhjälpa detta innehåller både dataskyddsförordningen och polisdirektivet skyddsåtgärder för att hjälpa tjänstemän inom brottsbekämpning och gränsförvaltning före, under och efter databehandlingen. Dessa avser

- konsekvensbedömningar avseende dataskydd, och
- inbyggt dataskydd och dataskydd som standard.

Konsekvensbedömningar

I EU:s rättsliga ram föreskrivs att polismyndigheter och gränsmyndigheter ska genomföra konsekvensbedömningar innan de utför en databehandling som sannolikt leder till en hög risk för enskilda personers rättigheter (artikel 35 i dataskyddsförordningen och artikel 27 i polisdirektivet). Detta innebär att konsekvensbedömningar inte bara ska genomföras om resultatet av behandlingen kan strida mot normerna för dataskydd eller integritet, utan i varje situation som kan leda till en överträdelse av *en grundläggande rättighet*. Detta kan omfatta rätten till lika-behandling och icke-diskriminering; yttrande- och informationsfrihet; tankefrihet, samvetsfrihet och religionsfrihet; utbildning; hälso- och sjukvård; asyl samt skydd i händelse av avlägsnande, utvisning eller utlämning.

Konsekvensbedömningar är särskilt viktiga om profileringen kan leda till rättsliga konsekvenser för enskilda personer. I sådana fall föreskriver dataskyddsförordningen och polisdirektivet att konsekvensbedömningar ska genomföras.

Konsekvensbedömningarna måste utföras innan den automatiska databehandlingen påbörjas. Det finns emellertid två syften med dessa konsekvensbedömningar:

- Före behandlingen av personuppgifter kan utförandet av en konsekvensbedömning av kvaliteten på uppgifterna och/eller algoritmen bakom behandlingen göra det lättare att upptäcka och, i relevanta fall, åtgärda eventuella överträdelser av de grundläggande rättigheterna.
- När uppgifterna har behandlats kan tjänstemannen vara skyldig att visa att han/hon har agerat enligt lagen. Konsekvensbedömningen kan hjälpa honom/henne att bevisa att alla nödvändiga åtgärder för att säkerställa efterlevnaden av lagen hade vidtagits.

Konsekvensbedömningar kommer även att hjälpa tjänstemännen att upptäcka dolda fördomar som kan strida mot rätten till skydd av personuppgifter och icke-diskriminering, och därmed påverka profileringens kvalitet (se [avsnitt 1.3.2](#)).

Fokus på riskerna med användningen av "dynamiska algoritmer"

"Dynamiska algoritmer" är algoritmer som hela tiden omdefinieras och "förbättras" baserat på "återkopplingslingor". Dessa slingor skapas av de algoritmiska systemen själva och kan inte förklaras eller ens uttryckas på ett enkelt språk (se artikel 35 i dataskyddsförordningen och artikel 27 i polisdirektivet). Till skillnad från "statiska algoritmer", som bygger på förutbestämda kriterier, genererar "dynamiska algoritmer" **nya sammanhang** genom att ständigt omdefiniera sig själva.

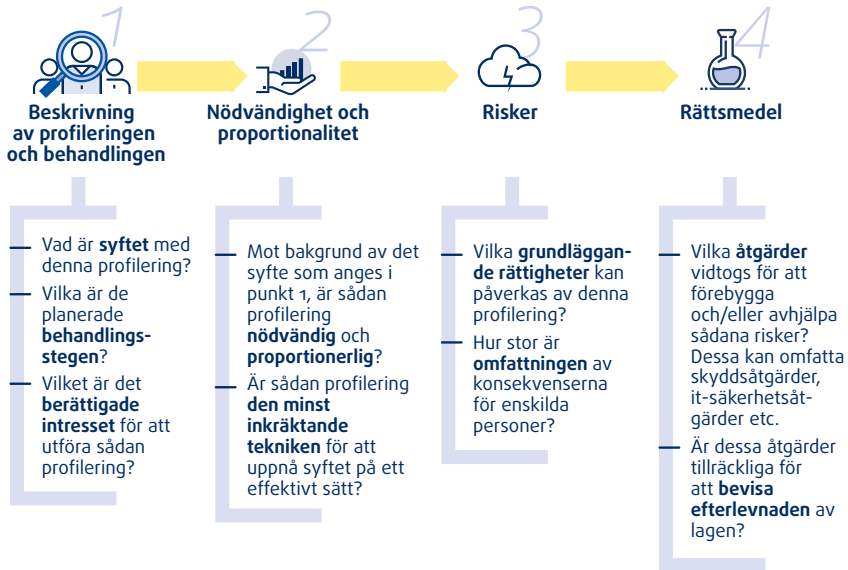
Med dynamiska algoritmer uppstår risken att expertutvecklare vid en viss punkt inte längre känner till logiken bakom algoritmen. Detta skapar en betydande **risk för att befintliga fördomar återskapas på ett okontrollerat sätt** och att den sociala ojämlikheten och stigmatiseringen av enskilda grupper förstärks. I sådana fall blir det mycket svårt att säkerställa ansvarighet och tillgång till domstolsprövning för de berörda personerna.

Användningen av "dynamiska algoritmer" bör därför **undvikas eller begränsas** för att minimera risken för att förlora kontrollen över bedömningskriterierna. Detta ger interna och externa revisorer en möjlighet att utvärdera algoritmerna och ändra dem om de är olagliga. Om användningen av dynamiska algoritmer är motiverad ska riskindikatorerna granskas och provas så att det säkerställs att de inte leder till olaglig profilering.

För mer information, se Gandy, O. (2010) och Korff, D. (2015).

En konsekvensbedömning kan variera avsevärt beroende på typen och volymen av personuppgifter som behandlas såväl som typen av och syftet med behandlingen. Den kan omfatta en kontroll av uppgifternas kvalitet, tekniska kontroller av de algoritmer som bearbetar uppgifterna och/eller en heltäckande granskning av målen med behandlingen, etc. I [figur 13](#) anges de minimikriterier som bör granskas.

Figur 13: Minimikrav för konsekvensbedömningar



Källa: FRA, 2018.

Artikel 29-gruppen (som nu har ersatts av [Europeiska dataskyddsstyrelsen](#)) arbetar med att sammanföra de nationella dataskyddsmyndigheterna i EU:s medlemsstater och har tagit fram riktlinjer med ytterligare information om konsekvensbedömningar avseende dataskydd. Dessa riktlinjer omfattar en detaljerad kartläggning av de kriterier som ska användas vid konsekvensbedömningar ⁽⁴⁰⁾.

Inbyggt laglighet och laglighet som standard

Oavsett om möjliga överträdelser av de grundläggande rättigheterna har konstaterats vid en konsekvensbedömning kan åtgärder genomföras för att ytterligare förebygga den eventuella risken för olaglighet. Dessa åtgärder kallas "inbyggt

(40) Artikel 29-gruppen (2017a).

dataskydd” och ”dataskydd som standard” (artikel 25 i dataskyddsförordningen och artikel 20 i polisdirektivet).

Inbyggt dataskydd syftar till att säkerställa att tekniska och organisatoriska åtgärder genomförs både *före* och *under* behandlingen av personuppgifter för att uppfylla dataskyddsprinciperna. Personuppgifter kan till exempel ”pseudonymiseras” vid behov. Pseudonymisering är en åtgärd genom vilken personuppgifter inte kan kopplas till en enskild person utan ytterligare information, som lagras separat. Den ”nyckel” som gör det möjligt att på nytt identifiera personen måste hållas avskild och säker⁽⁴¹⁾. I motsats till anonymiserade uppgifter är pseudonymiserade uppgifter fortfarande personuppgifter och måste därför uppfylla reglerna och principerna för dataskydd.

Dataskydd som standard säkerställer att ”endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas”⁽⁴²⁾. Detta får konsekvenser för

- mängden av personuppgifter som samlas in och lagras,
- typerna av behandling som kan inbegripa personuppgifter,
- den maximala lagringsperioden,
- antalet personer som har tillstånd att komma åt sådana personuppgifter.

Fokus på ansvarighet

Det huvudsakliga målet med inbyggt dataskydd och dataskydd som standard är att hjälpa myndigheter och tjänstemän inom brottsbekämpning och gränsförvaltning att utforma program för algoritmisk profilering som uppfyller kraven på grundläggande rättigheter, i synnerhet principerna om **laglighet, öppenhet** och **säkerhet**.

Sådana åtgärder kan emellertid även visa hur myndigheterna uppfyller de rättsliga kraven avseende **ansvarighet**. Myndigheter som behandlar personuppgifter ska enligt lag genomföra ”lämpliga tekniska och organisatoriska åtgärder” för att visa att de uppfyller kraven i unionsrätten.

(41) FRA, EDPS och Europarådet (2018), s. 83.

(42) Den allmänna dataskyddsförordningen, artikel 25.

Om till exempel en person lämnar in ett klagomål kan den nationella rättsliga myndigheten och dataskyddsmyndigheten kräva att de berörda myndigheterna påvisar var och en av följande punkter:

- Den datorbaserade profileringens legitimitet, nödvändighet och proportionalitet.
- Syftets laglighet.
- Vilken information som lämnats till enskilda personer.
- Uppgifternas integritet och säkerhet.
- Vilka kvalitetsåtgärder och kontroller som har utförts före och under profileringen.

3.2. Stora databaser för gränsförvaltning och säkerhetsinsatser

EU har utvecklat flera stora it-system och mekanismer för insamling och behandling av personuppgifter som kan användas vid gräns- och migrationsförvaltning och, i viss utsträckning, vid brottsbekämpning. De kan fungera som exempel för att visa några av de gemensamma utmaningar som kan kopplas till användningen av algoritmisk profilering, såväl som de möjliga skyddsåtgärderna.

I [tabell 6](#) finns en kortfattad presentation av dessa it-system och mekanismer. I [bilagan](#) finns en mer detaljerad översikt över befintliga och planerade stora it-system inom EU, som läget var i mars 2018.

Tabell 6: Utvalda EU-instrument för behandlingen av stora mängder personuppgifter för gränsförvaltning och brottsbekämpning

Databas	Förkortning	Huvudsakligt syfte
Schengens informationssystem	SIS II	Att lägga in och behandla larmmeddelanden om eftersökta eller försvunna personer för att skydda säkerheten, registrera och behandla larmmeddelanden om tredjelandsmedborgare i syfte att neka inresa eller vistelse samt registrera och behandla larmmeddelanden om tredjelandsmedborgare som omfattas av ett beslut om återvändande.
Informationssystemet för viseringar	VIS	Att underlätta utbytet av uppgifter om viseringsansökningar mellan Schengenmedlemsstaterna.
Europeiska daktyloskopisystemet	Eurodac	Att fastställa vilken medlemsstat som är ansvarig för att granska ansökningar om internationellt skydd och bistå vid kontrollen av irreguljär invandring och sekundär förflyttning.
In- och utresesystemet	EES	Att beräkna och övervaka varaktigheten av tredjelandsmedborgares tillåtna vistelser och identifiera personer som överskridit den tillåtna vistelsen.
Passageraruppgifter	PNR	Att samla in, behandla och utbyta passageraruppgifter för flygförbindelser från tredjeländer (flygförbindelser utanför EU) (*). Uppgifterna används i strikt mening endast för brottsbekämpning.
Förhandsinformation om passagerare	API	Att samla in och bearbeta passageraruppgifter för flygförbindelser från tredjeländer (flygförbindelser utanför EU) för gränsförvaltning och brottsbekämpning.
EU-system för reseuppgifter och resetillstånd	Etiás	Att bedöma om en tredjelandsmedborgare utan viseringskrav utgör en risk när det gäller säkerhet, olaglig migration eller folkhälsa.
Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister om tredjelandsmedborgare	Ecris-TCN	Att utbyta information om tredjelandsmedborgares tidigare fällande domar.

Anm.: (*) Dessutom ger artikel 2 i direktiv (EU) 2016/681 medlemsstaterna möjlighet att behandla uppgifter från flygförbindelser inom EU.

Källa: FRA, 2018.

EU:s stora it-system används i flera migrationsrelaterade processer, däribland vid riskbedömning före ankomst, vid handläggning av asylansökningar och viseringsansökningar, under gränskontroller, vid utfärdande av uppehållstillstånd, vid gripanden av migranter i en irreguljär situation, under återvändandeförfaranden och vid utfärdande av inreseförbud. It-system som inrättats av EU, däribland de som ursprungligen skapades för asyl- och migrationshantering, används också allt oftare inom ramen för intern säkerhet, till exempel vid poliskontroller och i kampen mot allvarliga brott och terrorism.

De flesta av de system som inrättats genom unionsrätten är inriktade på att identifiera en specifik person genom att matcha alfanumeriska eller biometriska uppgifter (för närvarande fingeravtryck) med information som redan finns i systemet. Med vissa noterbara undantag (se "Fokus på algoritmisk profilering i EU-instrument") innehåller de inte i sig någon algoritm som kan göra att en person matchas med en profil. Trots det kan de användas för att ta fram anonymiserad statistik, däribland om egenskaper som betraktas som skyddade grunder, till exempel kön eller ålder (se [avsnitt 1.2.1](#)).

Sådan statistik skulle kunna användas för att upprätta riskprofiler som kan tillämpas vid framtida beslut i samband med gränsförvaltning eller polisarbete. Som en del av det bredare programmet för interoperabiliteten mellan EU:s it-system kommer Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-Lisa) att vara ansvarig för förvaltningen av den centrala databasen för rapporter och statistik. Denna databas kommer att byggas upp med uppgifter från befintliga EU-databaser (in- och utresesystemet, Etias, Schengens informationssystem och informationssystemet för viseringar) för att generera statistik och analysrapporter för EU-organ och nationella organ ⁽⁴³⁾.

(43) Europeiska kommissionen (2017), [Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem \(gränser och viseringar\) och om ändring av rådets beslut 2004/512/EG, förordning \(EG\) nr 767/2008, rådets beslut 2008/633/RIF, förordning \(EU\) 2016/399 och förordning \(EU\) 2017/2226](#), COM(2017) 793 final, Strasbourg, 12 december 2017; Europeiska kommissionen (2017), [Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem \(polisarbete och rättsligt samarbete, asyl och migration\)](#), COM(2017) 794 final, Bryssel, 12 december 2017.

Fokus på algoritmisk profilering i EU-instrument

För vissa befintliga EU-instrument föreskrivs att statistik som härleds från deras uppgifter ska användas för att skapa riskprofiler. Förutom att möjliggöra upptäckt av "kända" misstänka personer innehåller de en funktion för algoritmisk profilering som identifierar "okända" individer som kan vara av intresse för myndigheterna inom brottsbekämpning och gränsförvaltning.

EU-systemet för reseuppgifter och resetillstånd (Etias) ⁽⁴⁴⁾, som antogs i september 2018 men som ännu inte tagits i drift när denna vägledning slutfördes, kommer att användas för att bedöma om tredjelandsmedborgare utan viseringskrav utgör en risk när det gäller olaglig migration, säkerhet eller folkhälsa innan inresetillståndet utfärdas. Information som lämnats av resenärer under ansökningsprocessen kommer att jämföras automatiskt med relevanta EU-databaser och internationella databaser och med en uppsättning av riskindikatorer ("sökregler") i Etias-systemet. En algoritm som utvecklats av Frontex kommer att jämföra resenärens individuella profil (baserat på indikatorer som ålder, kön, nationalitet, bostadsort, utbildningsnivå och yrke) med dessa riskindikatorer för att fastställa om ansökan bör hänvisas till manuell granskning.

Passageraruppgifter samlas in av lufttrafikföretag utifrån den information som lämnats av passagerarna i flygbokningssystemen, däribland resedatum och resplan, kontakt- och betalningsuppgifter, bagageinformation och andra "allmänna anmärkningar", t.ex. önskemål om kost. Det finns inte någon central EU-databas som används för att samla in dessa uppgifter, men enligt direktivet om passageraruppgifter ⁽⁴⁵⁾ ska lufttrafikföretagen tillhandahålla uppgifterna till de nationella enheterna för passagerarinformation, som sedan analyserar informationen i syfte att bekämpa terrorism och allvarliga brott. Förutom att upptäcka kända personers förflyttningar över gränserna kan dessa uppgifter användas för att identifiera tidigare okända hot genom behandling av passagerarnas uppgifter gentemot särskilda riskindikatorer ("på förhand fastställda kriterier"). Dessa kriterier fastställs av enheterna för passagerarinformation och uppdateras på grundval av nya uppgifter och mönster som finns tillgängliga i systemet.

(44) Europeiska kommissionen (2018), [Europaparlamentets och rådets förordning \(EU\) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd \(Etias\) och om ändring av förordningarna \(EU\) nr 1077/2011, \(EU\) nr 515/2014, \(EU\) 2016/399, \(EU\) 2016/1624 och \(EU\) 2017/2226, COM\(2016\) 731 final](#), Bryssel, 16 november 2016, artikel 33.5.

(45) [Europaparlamentets och rådets direktiv \(EU\) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar \(PNR-uppgifter\) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet \(EUT L 119, 4.5.2016, s. 132\)](#).

3.2.1. Minimering av riskerna för de grundläggande rättigheterna vid behandling av uppgifter i stora databaser

Omfattande uppgifter om resenärer, däribland om nationalitet, kön och ålder, kommer att användas för profilering, inklusive algoritmisk profilering, i en omfattning som tidigare inte har varit möjlig. Även om dessa uppgifter är anonymiserade är behandlingen inte helt riskfri. Medvetna eller omedvetna fördomar i urvalet av riskindikatorer, utformningen av algoritmer eller tolkningen av resultaten skulle kunna leda till operativa åtgärder som kan innebära att vissa kategorier av personer diskrimineras ⁽⁴⁶⁾.

Detta avsnitt innehåller en genomgång av några av dessa risker och förslag på hur de kan minimeras. Avsnittet bygger på FRA:s dokument *Twelve operational fundamental rights considerations for law enforcement when processing PNR data* (tolv riktlinjer för grundläggande rättigheter vid behandling av passageraruppgifter i samband med brottsbekämpning) (se fallstudien). Även om de har utarbetats inom den specifika ramen för behandling av passageraruppgifter är vissa av dessa överväganden mer allmänt tillämpliga och kan betraktas som skyddsåtgärder för att minska riskerna med algoritmisk profilering.

Fallstudie

FRA:s operativa vägledning för inrättande av nationella system för passageraruppgifter

År 2014 fick FRA i uppdrag av Europeiska kommissionen att tillhandahålla praktisk vägledning om behandlingen av passageraruppgifter för brottsbekämpning till de medlemsstater som planerade att inrätta egna nationella system för passageraruppgifter. Vägledningen var inriktad på rätten till respekt för privatlivet (artikel 7 i EU-stadgan), skydd av personuppgifter (artikel 8 i EU-stadgan) och icke-diskriminering (artikel 21 i EU-stadgan). Vissa av de skyddsåtgärder som föreslogs infördes senare i EU:s direktiv om passageraruppgifter.

(46) För mer information, se FRA (2017e) och FRA (2018a).

De tolv riktlinjerna för grundläggande rättigheter vid behandling av passageraruppgifter i samband med brottsbekämpning är följande:

- Använd endast passageraruppgifter för att bekämpa terrorism och allvarlig gränsöverskridande brottslighet.
- Begränsa åtkomsten till databasen med passageraruppgifter till en specialenhet.
- Begär inte direkt åtkomst till flygbolagens databaser.
- Radera känsliga passageraruppgifter.
- Inrätta strikta skyddsåtgärder för säkerhet och spårbarhet mot missbruk.
- Minska sannolikheten för att flagga falska positiva resultat.
- Var öppen mot passagerarna.
- Se till att alla personer kan komma åt och ändra sina passageraruppgifter.
- Tillåt inte någon identifiering av registrerade personer eller lagring av uppgifter under längre tid än nödvändigt.
- Överför endast uppgifter från PNR-systemet till behöriga nationella offentliga myndigheter.
- Överför endast uppgifter från PNR-systemet till tredjeländer på stränga villkor.
- Genomför objektiva och öppna utvärderingar av PNR-systemet.

För mer information, se FRA (2014c).

Behandling av personuppgifter som avslöjar skyddade egenskaper bör vara nödvändig och proportionerlig

Den algoritmiska profileringens karaktär innebär att användningen av personliga egenskaper som är kopplade till skyddade grunder medför särskilt hög risk för diskriminering⁽⁴⁷⁾. Inom EU är det enligt lagstiftningen om Etias och PNR förbjudet att basera riskindikatorer på kriterier som medför hög risk för diskriminering, inbegripet på grund av ras, etniskt ursprung eller religiös övertygelse. Även om det inte finns

(47) Europeiska datatillsynsmannen (2018).

några sådana uppgifter kan emellertid andra typer av uppgifter vara starkt förknippade med dessa egenskaper och i praktiken fungera som substitut för sådana skyddade egenskaper. Exempelvis kan kategorin "allmänna anmärkningar" i PNR-systemet innehålla resenärernas önskemål om kost och därmed avslöja vissa religiösa övertygelser.

En specifik kombination av uppgifter som används av algoritmen kan även vara till nackdel för en kategori av personer. Den kan till exempel göra att personer hamnar i ett ofördelaktigt läge på grund av sitt etniska eller sociala ursprung eller sin tillhörighet i en nationell minoritet, vilka är skyddade egenskaper enligt artikel 21 i EU-stadgan. Om till exempel en riskprofil i Etias angående risken för olaglig migration baseras på kombinationen av en viss nationalitet och yrkesgrupp kan det leda till att en insats inriktas på en etnisk grupp eller nationalitet som i ett visst land ofta arbetar inom en viss ekonomisk sektor, t.ex. byggnadsarbete eller jordbruk ⁽⁴⁸⁾.

- Behandling av uppgifter som avslöjar egenskaper som är skyddade enligt artikel 21 i EU-stadgan bör begränsas till vad som är strikt nödvändigt och proportionerligt, och får aldrig leda till diskriminering. Innan behandlingen påbörjas bör den behöriga myndigheten bedöma uppgifterna för att fastställa om de innehåller skyddade egenskaper och ta bort uppgifter som inte kan behandlas på ett lagligt sätt. Detta bör kompletteras med ett program för matchning och borttagning med en regelbundet uppdaterad ordlista över "känsliga begrepp".

Kriterierna för profileringen bör vara specifika och målinriktade

En annan risk kan uppstå vid användning av **breda profileringskriterier**. Befintliga EU-instrument ger ett betydande utrymme för skönsmässig bedömning vid utveckling av profileringsalgoritmer. För att bedöma risken för olaglig migration bygger användningen av Etias på EU-statistik och nationell statistik om överskridanden av den tillåtna vistelsen och nekade inresor. När det gäller säkerhetsrisker hänvisar systemet emellertid vanligtvis till information om specifika säkerhetsindikatorer och hot. Direktivet om passageraruppgifter innehåller allmänna riktlinjer för utformningen av algoritmer, utan att specificera vilka kriterier som bör användas för att identifiera personer som kan vara delaktiga i ett terroristbrott eller någon annan allvarlig brottslighet, eller vilken vikt som bör tilldelas ett visst kriterium.

(48) Se även FRA (2017a).

Alltför breda kriterier leder till ett stort antal "falsa positiva resultat", vilket innebär att personer matchas felaktigt med en viss riskprofil. Vissa av dessa "falsa positiva resultat" kan även vara diskriminerande till sin karaktär. En bred definition av kriteriet "tidigare brottmålsdom" innebär till exempel att hbtq-personer skulle vara tvungna att uppvisa ett kriminalregister över vissa sexuella beteenden som är straffbelagda i vissa länder utanför EU.

- Bedömningskriterierna bör vara förutbestämda, målinriktade, specifika, proportionerliga och faktabaserade. Bedömningskriterierna bör provas med anonymiserade stickprov. De bör granskas regelbundet av en internrevisor i syfte att fastställa om de fortfarande är motiverade med tanke på deras specifika mål.
- Innan ett larmmeddelande baserat på automatisk behandling skickas vidare för ytterligare åtgärder bör den behöriga myndigheten granska uppgifterna manuellt tillsammans med annan information för att fastställa om personen matchar riskprofilen och eliminera falska positiva resultat. Uppgiftsmottagaren bör ge feedback om vilka åtgärder som vidtagits på grundval av larmet.

Uppgifter som behandlas bör vara korrekta och tillförlitliga

FRA:s undersökningar har bekräftat att de befintliga stora it-systemen innehåller en stor mängd felaktiga uppgifter ⁽⁴⁹⁾. **Felaktiga eller otillförlitliga uppgifter** kan ha flera olika negativa effekter i samband med algoritmisk profilering för brottsbekämpning eller gränsförvaltning. Felaktiga uppgifter kan påverka enskilda personer på ett negativt sätt, men även leda till felaktiga sammanhang och en förvrängd bild som försämrar polisens och gränsbevakningspersonalens arbete.

Detta är särskilt relevant om uppgifterna läggs in av personer i allmänheten, till exempel i systemet för passageraruppgifter eller Etias, eftersom de kan innehålla fler felaktigheter än officiella register. På liknande sätt medför en granskning av sociala medier, vilket föreskrivs av vissa system för resetillstånd utanför EU, en hög risk för att otillförlitliga uppgifter ingår i profileringsprocessen. Det medför även en särskild risk för insamling av information som avslöjar känsliga personuppgifter som skyddas av EU-stadgan, till exempel politiska åsikter eller sexuell läggning.

- Ge korrekt information till enskilda personer om insamlingen, lagringen och behandlingen av deras uppgifter och om de tillämpliga dataskyddsprinciperna.

(49) Se FRA (2018c), s. 81-98.

Varje person bör få kännedom om sina rättigheter, däribland vilka mekanismer för domstolsprövning som finns tillgängliga.

- Se till att enskilda personer kan ändra sina uppgifter om de är felaktiga och att de får information om uppgifterna har ändrats eller raderats.
- Säkerställ tillgången till effektiv administrativ och rättslig prövning i de fall då rätten till skydd av personuppgifter har kränkts, däribland om åtkomst har nekats eller om felaktiga uppgifter inte har ändrats eller raderats.

Slutsats

Profilering är ett legitimt verktyg som används av tjänstemän inom brottsbekämpning och gränsbevakning för att förebygga, utreda och lagföra brottslig verksamhet samt för att förebygga och upptäcka irreguljär invandring.

För att vara laglig, rättvis och effektiv måste profileringen användas inom lagens gränser. I synnerhet måste profileringen respektera kraven på likabehandling och skydd av personuppgifter.

Detta uppnås genom en kombination av faktorer. Varje profilering bör

- behandla enskilda personer på ett likvärdigt, respektfullt och värdigt sätt,
- undvika profilering av enskilda personer baserad på fördomar,
- vara rimlig, objektiv och baserad på underrättelser,
- säkerställa ett tillräckligt skydd av individens personuppgifter och privatliv.













Olika verktyg finns tillgängliga för att säkerställa att polistjänsteman och gränsbevakningspersonal känner till, förstår och upprätthåller dessa principer i praktiken.

- Innan en profilering genomförs bör tjänstemännen få vägledning och utbildning.
- Under profileringen bör uppgifter om verksamheten registreras och lagras.
- Efter profileringen bör tjänstemännens handlingar övervakas och bedömas för att identifiera förbättringsområden.




Om olaglig profilering förhindras kommer inte bara tjänstemännen inom brottsbekämpning och gränsförvaltning att hålla sig inom lagens gränser, utan deras handlingar kommer även att förstås och accepteras av allmänheten. Ett ökat förtroende för brottsbekämpningen och gränsförvaltningen förbättrar effektiviteten i polisarbetet och gränsbevakningen och bidrar därmed till en ökning av säkerheten och tryggheten i samhället som helhet.

Bilaga






Tabell 7: Befintliga och planerade stora it-system inom EU

It-system	Huvudsakligt syfte	Personer som omfattas	Tillämplighet	Rättsligt instrument/förslag	Biometrisk kännetecken
Europeiska daktyloskopisystemet (Eurodac)	Att fastställa vilken medlemsstat som är ansvarig för att granska en ansökan om internationellt skydd <i>Att bistå vid kontrollen av irreguljär invandring och sekundära förflyttningar</i>	Personer som sökt och beviljats internationellt skydd, <i>migranter i en irreguljär situation</i>	28 EUMS + SAC	Förordning (EU) nr 603/2013 (Eurodac-förordningen) <i>COM(2016) 272 final (förslag om Eurodac)</i>	 
Informationssystemet för viseringar (VIS)	Att underlätta utbytet av uppgifter om viseringsansökningar mellan Schengenassocierade länder	Personer som ansöker om visering och referenspersoner	24 EUMS (ej CY, HR, IE, UK) ⁽¹⁾ + SAC	Förordning 767/2008/EG (VIS-förordningen)	
Schengens informations-system (SIS II) – polis	Att skydda säkerheten inom EU:s medlemsstater och Schengenassocierade länder	Försvunna eller efterlysta personer	26 EUMS (ej CY, IE) ⁽²⁾ + SAC	Rådets beslut 2007/533/RIF (SIS II-beslutet) <i>COM(2016) 883 final (förslag om SIS II för polisen)</i>	  
Schengens informations-system (SIS II) – gränsbevakning	Att registrera och behandla larmmeddelanden för att neka inresa till eller vistelse i Schengenassocierade länder	Migranter i en irreguljär situation	25 EUMS (ej CY, IE, UK) ⁽²⁾ + SAC	Förordning 1987/2006 (SIS II-förordningen) <i>COM(2016) 882 final (förslag om SIS II för gränsbevakning)</i>	  
Schengens informations-system (SIS II) – återvändande	<i>Att registrera och bearbeta larmmeddelanden för tredjelandsmedborgare som omfattas av ett beslut om återvändande</i>	<i>Migranter i en irreguljär situation</i>	25 EUMS (ej CY, IE, UK) ⁽²⁾ + SAC	<i>COM(2016) 881 final (förslag om SIS II för återvändande)</i>	  

Förebyggande av olaglig profilering idag och i framtiden: en vägledning

<p>In- och utresesystemet</p>	<p>Att beräkna och övervaka varaktigheten av tredjelandsmedborgares tillåtna vistelser och identifiera personer som överskridit den tillåtna vistelsen</p>	<p>Resenärer som anländer för en kort vistelse</p>	<p>22 EUMS (ej BG, CY, HR, IE, RO, UK) ⁽³⁾ + SAC</p>	<p>Europaparlamentets och rådets förordning (EU) 2017/2226 (EES-förordningen)</p>	
<p>EU-systemet för reseuppgifter och resetillstånd (Etias)</p>	<p>Att bedöma om en tredjelandsmedborgare utan viseringskrav utgör en risk när det gäller säkerhet, olaglig migration eller folkhälsa</p>	<p>Resenärer utan viseringskrav</p>	<p>26 EUMS (ej IE, UK) ⁽³⁾ + SAC</p>	<p>COM(2016) 731 final (förslag om Etias)</p>	<p>Inga</p>
<p>Det europeiska informations-systemet för utbyte av uppgifter ur kriminalregister om tredjelandsmedborgare (Ecris-TCN)</p>	<p>Att utbyta information om tredjelandsmedborgares tidigare fällande domar</p>	<p>Tredjelandsmedborgare med ett kriminalregister</p>	<p>27 EUMS (ej DK) ⁽⁴⁾</p>	<p>COM(2017) 344 final (förslag om Ecris-TCN)</p>	
<p>Interoperabilitet – Gemensam databas för identitetsuppgifter</p>	<p>Att upprätta en ram för interoperabilitet mellan EES, VIS, Etias, Eurodac, SIS II och Ecris-TCN</p>	<p>Tredjelandsmedborgare som omfattas av Eurodac, VIS, SIS II, EES, Etias och Ecris-TCN</p>	<p>28 EUMS ⁽⁵⁾ + SAC</p>	<p>COM(2017) 793 final (förslag om interoperabilitet för gränser och viseringar) COM(2017) 794 final (förslag om interoperabilitet för polisarbete, asyl och migration)</p>	

Anm.: Planerade system och planerade ändringar inom systemen anges i kursiv stil.

 : Fingeravtryck, : Handavtryck, : Ansiktsbild, : DNA-profil.

EUMS: EU-medlemsstater

SAC: Schengenassocierade länder, dvs. Island, Liechtenstein, Norge och Schweiz.

¹ Irland och Förenade kungariket deltar inte i VIS. Danmark är inte bundet av förordningen, men har valt att ansluta sig till VIS. VIS är ännu inte tillämpligt för Kroatien och Cypern och endast delvis tillämpligt för Bulgarien och Rumänien enligt rådets beslut (EU) 2017/1908 av den 12 oktober 2017.

² Cypern och Irland har ännu inte anslutit sig till SIS. Danmark är inte bundet av förordningen eller rådets beslut, men har valt att ansluta sig till SIS II och måste åter besluta om huruvida landet ska omfattas efter antagandet av förslagen om SIS II. Förenade kungariket deltar i SIS, men får inte använda eller komma åt registreringar om nekad inresa till eller vistelse i Schengenområdet. Bulgarien, Rumänien och Kroatien får inte utfärda Schengenövergripande registreringar i

syfte att neka inresa eller vistelse i Schengenområdet, eftersom de ännu inte ingår i Schengenområdet.

- ³ *Danmark kan besluta att ansluta sig till EES och Etias.*
- ⁴ *Ecris-TCN är inte tillämpligt för Danmark. Förenade kungariket och Irland kan besluta att ansluta sig.*
- ⁵ *Danmark, Irland och Förenade kungariket kommer att delta, eftersom de deltar i de it-system som gjorts interoperabla.*

Källa: FRA, baserat på befintliga och föreslagna rättsliga instruments, 2018.

Hänvisningar

Akhgar, B., Saathoff, G.B., Arabnia, H.R., Hill, R., Staniforth, A. och Bayerl, P. S. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016), *Eight Problems With Police "Threat Scores"*, 13 januari 2016.

Artikel 29-gruppen (2014), *Yttrande 01/2014 om tillämpning av principerna om nödvändighet och proportionalitet samt uppgiftsskydd inom brottsbekämpningssektorn*, 536/14/SV, WP 211, Bryssel, 27 februari 2014.

Artikel 29-gruppen (2017a), *Riktlinjer om konsekvensbedömning avseende data-skydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679*, WP 248 rev.01, 4 oktober 2017.

Artikel 29-gruppen (2017b), *Yttrande om vissa centrala frågor gällande direktivet om brottsbekämpning (EU 2016/680)*, 7 december 2017.

Artikel 29-gruppen (2018a), *Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679*, WP251rev.01, 6 februari 2018.

Artikel 29-gruppen (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Bryssel, 23 april 2018.

Belgium, Unia, *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Bryssel, 2015.

Belgium, Unia, *Rapport annuel 2016*, Bryssel, september 2017.

Big Brother Watch, *Smile you're on body worn camera Part II – Police, The use of body worn cameras by UK police forces*, augusti 2017.

Body-Gendrot, S. (2016), *"Making sense of French urban disorders in 2005"*, *European Journal of Criminology*, vol. 13, nr 5, s. 556–572.

Bovens et al. (2014), "Public accountability", i: Bovens, M., Schillermans, T. och Goodlin, R.E. (red.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), "Surveillance and system avoidance: criminal justice contact and institutional attachment", *American Sociological Review*, vol. 79, nr 3, s. 367–391.

Buolamwini, J., Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab and Microsoft Research, 2018.

Center on Privacy and Technology at Georgetown Law (2016), *The Perpetual Line-up, Unregulated Police Face Recognition in America*, 18 oktober 2016.

Centre d'analyse stratégique (2006), *Enquête sur les violences urbaines - Comprendre les émeutes de novembre 2005 : les exemples de Saint-Denis et d'Aulnay-Sous-Bois*, Paris, La Documentation française, 2006.

Coudert, F., Butin, D. och Le Metayer, D. (2015), "Body-worn cameras for police accountability: opportunities and risks", *Computer Law and Security Review*, vol. 31, s. 749–762.

De Hert, P. och Lammerant, H. (2016), "Predictive profiling and its legal limits: effectiveness gone forever?", i van der Sloot, B., Broeders, D. och Schrijvers, E. (red.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, s. 145–173.

Défenseur des droits (2017), *Enquête sur l'accès aux droits. Volume 1. Relations police / population : le cas des contrôles d'identité*, 2017.

Dinant, J.-M., Lazaro, C., Pouillet Y., Lefever, N. och Rouvroy, A. (2008), *Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD)*, Doc. T-PD 01, s. 3.

Europarådet, ministerkommittén (2001), *Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics adopted by the Committee of Ministers*, 19 september 2001.

Europeiska datatillsynsmannen (EDPS) (2015), *Opinion 5/2015. Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use*

of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Bryssel, 24 september 2015.

Europeiska datatillsynsmannen (EDPS) (2018), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Bryssel, 18 april 2018.

Europeiska gräns- och kustbevakningsbyrån (Frontex) (2012), *Common core curriculum, EU border guard basic training*, mars 2012.

Europeiska gräns- och kustbevakningsbyrån (Frontex) (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Europeiska gräns- och kustbevakningsbyrån (Frontex) (2015), *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Europeiska gräns- och kustbevakningsbyrån (Frontex) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Europeiska kommissionen (2017a), *Utbildning om hatbrott för brottsbekämpande myndigheter och åklagarmyndigheter*, februari 2017.

Europeiska kommissionen (2017b), *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, december 2017.

Europeiska kommissionen mot rasism och intolerans (Ecri) (2007), *ECRI General Policy Recommendation No 11 on combating racism and racial discrimination in policing*, antagen den 27 juni 2007, Strasbourg, 4 oktober 2007.

Europeiska kommissionen, undergruppen för metoder för registrering och insamling av uppgifter om hatbrott (2017), *Improving the recording of hate crime by law enforcement authorities - Key guiding principles*, Bryssel, december 2017.

Europeiska nätverket av juridiska experter på jämställdhet och icke-diskriminering (2016), *Links between migration and discrimination - A legal analysis of the situation in EU Member States*, juli 2016.

Europeiska unionens råd (2009), *EU:s uppdaterade Schengenkatalog om kontroll av de yttre gränserna, återvändande och återtagande*, 19 mars 2009.

Europeiskt centrum för övervakning av rasism och främlingsfientlighet (2016), *Perceptions of discrimination and islamophobia – Voices from members of Muslim communities in the European Union*, 2006.

Farrar, T. (2018), *Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force*, Police Foundation, 2018.

FRA (2013), *Polisutbildning om grundläggande rättigheter – En handbok för polisutbildare*, Luxemburg, Publikationsbyrån, december 2013.

FRA (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Luxemburg, Publikationsbyrån, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luxemburg, Publikationsbyrån, 2014.

FRA (2014c), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, februari 2014.

FRA (2016), *Rapport om grundläggande rättigheter 2016*, Luxemburg, Publikationsbyrån, 2016.

FRA (2017a), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, yttrande från FRA – 2/2017 [Etias], juni 2017.

FRA (2017b), *Second European Union Minorities and Discrimination Survey - Main results*, Luxemburg, Publikationsbyrån, december 2017.

FRA (2017c), *Rapport om grundläggande rättigheter 2017*, Luxemburg, Publikationsbyrån, maj 2017.

FRA (2017d), *Europeiska unionens andra undersökning av minoriteter och diskriminering. Muslimer: resultat i urval*, Luxemburg, Europeiska unionens publikationsbyrå, september 2017.

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxemburg, Publikationsbyrån, maj 2017.

FRA (2018a), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, yttrande från FRA – 1/2018 [Interoperabilitet], april 2018.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, FRA Focus Paper, maj 2018.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxemburg, Publikationsbyrån, februari 2018.

FRA (2018d), *Hate crime recording and data collection practice across the EU*, Luxemburg, Publikationsbyrån, juni 2018.

FRA (2018e), *Rapport om grundläggande rättigheter 2018*, Luxemburg, Publikationsbyrån, juni 2018.

FRA, Europeiska datatillsynsmannen (EDPS) och Europarådet (2018), *Handbook on European data protection law – 2018 edition*, Luxemburg, Publikationsbyrån, maj 2018.

FRA och Europarådet (2018), *Handbook on European non-discrimination law – 2018 edition*, Luxemburg, Publikationsbyrån, februari 2018.

Frankrike, inrikesministeriet (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 juni 2018.

Förenade kungariket, Camden och London Prepared (2006), *Major Incident Procedures: What businesses and the voluntary sector need to know*, april 2006.

Förenade kungariket, College of Policing (2016), *Stop and Search, Authorised Professional Practice (APP)*, 29 september 2016.

Förenade kungariket, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), *Stop and search powers: Are the police using them effectively and fairly?*, 2013.

Förenade kungariket, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), *PEEL: Police legitimacy 2015. An inspection of West Midlands Police*, februari 2016.

Förenade kungariket, inrikesministeriet (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, februari 1999.

Förenade kungariket, inrikesministeriet (2014a), *Revised code of practice for the exercise by: police officers of statutory powers of stop and search; police officers and police staff of requirements to record public encounters. Code A*, Norwich, The Stationery Office (TSO), 2014.

Förenade kungariket, inrikesministeriet (2014b), *Best use of stop and search scheme*, 2014.

Förenade kungariket, kommissionen för de mänskliga rättigheterna (2009), *Police and racism: what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

Förenade kungariket, London School of Economics (2011), *Reading the Riots*, december 2011.

Förenade kungariket, National Policing Improvement Agency (NPIA) (2012), *Stop and search, the use of intelligence and geographic targeting. Findings from case study research*, 2012.

Förenade kungariket, Northamptonshire Police (2018), *Get Involved – Reasonable Grounds Panel*, hämtad i april 2018.

Förenade kungariket, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), *An Independent Report into Stop & Search Encounters by Staffordshire Police*, januari 2015.

Förenade kungariket, Stop Watch (2011), "Carry on Recording": Why police stops should still be recorded, maj 2011.

Förenade kungariket, Underhusets kommitté för inrikesfrågor (2009), *The Macpherson Report – Ten Years On*, den tolfte rapporten från sammanträde 2008–09, 22 juli 2009.

Förenade kungariket, West Midlands Police (2012), *Stop and Search Policy*, november 2012.

Förenade kungariket, West Midlands Police (2016), *Stop and Search Recommendations*, juli 2015 (senast ändrad i juni 2016).

Förenade kungariket, West Midlands Police (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, april 2017.

Förenade kungariket, West Midlands Police (2017b), *New "app" set to speed up Stop & Search process*, augusti 2017.

Förenade kungariket, West Midlands Police (2018), *Stop and Search Scrutiny Panels*, hämtad i april 2018.

Förenade kungariket, West Midlands Police and Crime Commissioner (2014), *Stop and Search Action Plan – Outcome of consultation*, januari 2014.

Förenade kungariket, Överhuset (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents)*, [2006] UKHL 12, 8 mars 2006.

Förenta nationerna (FN) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29 januari 2007.

Gandy, O. (2010), "Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems", *J Ethics Inf Technol*, vol. 12, nr 1, s. 29–42, 2010.

Gross, S. R. (2002), "*Racial Profiling under Attack*", D. Livingston, medförfattare, *Colum. L. rev.* 102, nr 5, s. 1413–1438.

Harcourt, B. (2004), "Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally", *University of Chicago Law Review*, vol. 71, 2004.

Harris, D. (2002), "Flying While Arab: Lessons from the Racial Profiling Controversy", *Civil Rights Journal*, vol. 6, nr 1, vinter 2002.

Harris, D. (2003), *Profiles in Injustice; Why Racial Profiling Cannot Work*, The New Press, 2003.

Hildebrandt, M. och de Vries, K. (2013), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, New York, Routledge, 2013.

Hildebrandt, M. och Gutwirth, S. (red.) (2008), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlin, Springer, 2008.

Hunt, P., Saunders, J. och Hollywood, J.S. (2014), *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.

Hörnqvist, M. (2016), "*Riots in the welfare state: The contours of a modern-day moral economy*", *European Journal of Criminology*, vol. 13, nr 5, s. 573–589.

Jobard, F. (2008), "The 2005 French urban unrests: data-based interpretations", *Sociology Compass*, vol. 2, nr 4, s. 1287–1302.

Kádár, A., Körner, J., Moldova, Z. och Tóth, B. (2008), *Control(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS) Project*, Budapest, s. 23.

Keskinen, S. et al (2018), *The Stopped – Ethnic Profiling in Finland*, Svenska social- och kommunalhögskolan, Helsingfors universitet, Helsingfors, 3 april 2018.

Kontoret för FN:s högkommissarie för mänskliga rättigheter (OHCHR) (2014), *Recommended Principles and Guidelines on Human Rights at International Borders*, 23 juli 2014.

Korff, D. (2015), *Passenger Name Records, data mining & data protection: the need for strong safeguards*, T-PD(2015)11, Strasbourg, 15 juni 2015.

Miller, J. och Alexandrou, B. (2016), *College of policing stop and search training experiment: Impact evaluation*, College of Policing Limited, 2016.

Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. och Floridi, L. (2016), "[The ethics of algorithms: Mapping the debate](#)", Big Data & Society, 1 december 2016.

Mohler, G.O., Short, M.B., Malinowski, S., Johnson, M., Tita, G.E., Bertozzi, A.L., Brantingham, P.J., *Randomized Controlled Field Trials of Predictive Policing*, 15 januari 2016.

Nisbet, R., Elder, J. och Miner, G. (2009), *Handbook of Statistical Analysis & Data Mining Applications*, Sydney (Kanada), Elsevier, 2009.

Open Society Justice Initiative (2018a), *Regulating Police Stop and Search: An Evaluation of the Reasonable Grounds Panel*, december 2018.

Open Society Justice Initiative (2018b), *The Recording of Police Stops: Methods and Issues*, december 2018.

Oswald, M., Grace, J., Urwin, S. och Barnes, G., "[Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality](#)", *Information & Communications Technology Law*, 31 augusti 2017.

Schauer, F. (2003), *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007), "United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism", *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/26, 29 januari 2007.

The Guardian (2015), [Northamptonshire police ban stop and search by officers who abuse powers](#), 18 augusti 2015.

Tóth, B.M. och Kádár, A. (2011), "Ethnic profiling in ID checks by the Hungarian police", *Policing and Society*, vol. 21, nr 4, s. 383-394.

USA, GAO (General Accounting Office) (2000), *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results*, GAO/GGD-00-38, mars 2000.

Van Brakel, R. (2016), "Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing", i: van der Sloot, B., Broeders, D. och Schrijvers, E. (red.), *Nederländernas vetenskapliga råd för offentlig politik (Wetenschappelijke Raad voor het Regeringsbeleid), Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, s. 117–141.

Wrench, J. (2007), *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T.Z. (2011), "Governmental Data Mining and its Alternatives", *Penn State Law Review*, vol. 11, nr 2, s. 285–330.

Unionslagstiftning

Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012, s. 391).

[Förklaringar avseende stadgan om de grundläggande rättigheterna](#) (EUT C 303, 14.12.2007, s. 17).

Icke-diskriminering

[Rådets direktiv 2000/43/EG](#) av den 29 juni 2000 om genomförandet av principen om likabehandling av personer oavsett ras eller etniskt ursprung (EGT L 180, 19.7.2000, s. 22).

[Rådets direktiv 2000/78/EG](#) av den 27 november 2000 om inrättande av en allmän ram för likabehandling (EGT L 303, 2.12.2000, s. 16).

Dataskydd

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 (allmän dataskyddsförordning) (EUT L 119, 4.5.2016).

Europaparlamentets och rådets [direktiv \(EU\) 2016/680](#) av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller

verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

Gränsförvaltning

[Rådets beslut 2007/533/RIF](#) av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

Europaparlamentets och rådets [direktiv \(EU\) 2016/681](#) av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (EUT L 119, 4.5.2016, s. 132).

Europaparlamentets och rådets [förordning \(EG\) nr 1987/2006](#) av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 381, 28.12.2006, s. 4).

Europaparlamentets och rådets [förordning \(EG\) nr 767/2008](#) av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) (EUT L 218, 13.8.2008, s. 60).

Europaparlamentets och rådets [förordning \(EG\) nr 603/2013](#) av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 180, 29.6.2013, s. 1).

Europaparlamentets och rådets [förordning \(EU\) 2016/1624](#) av den 14 september 2016 om en europeisk gräns- och kustbevakning och om ändring av Europaparlamentets och rådets förordning (EU) 2016/399 och upphävande av Europaparlamentets och rådets förordning (EG) nr 863/2007, rådets förordning (EG) nr 2007/2004 och rådets beslut 2005/267/EG (EUT L 251, 16.9.2016, s. 1).

Europaparlamentets och rådets [förordning \(EU\) nr 1052/2013](#) av den 22 oktober 2013 om inrättande av ett europeiskt gränsövervakningssystem (Eurosur) (EUT L 295, 6.11.2013, s. 11).

Europaparlamentets och rådets [förordning \(EU\) 2016/399](#) av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 77, 23.3.2016, s. 1).

Rättspraxis

Frankrikes högsta domstol (*Cour de Cassation*), Décision 1245, 9 november 2016.

Förenade kungariket, Överhuset (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents)*, UKHL 12, 8 mars 2006.

EU-domstolens dom av den 16 december 2008, [Heinz Huber mot Bundesrepublik Deutschland](#), C-524/06, ECLI:EU:C:2008:724.

Europeiska domstolen för de mänskliga rättigheterna, [B.S. mot Spanien](#), nr 47159/08, 24 juli 2012.

Europeiska domstolen för de mänskliga rättigheterna, [S. och Marper mot Förenade kungariket](#), nr 30562/04 och 30566/04, 4 december 2008.

Europeiska domstolen för de mänskliga rättigheterna, [Gillan och Quinton mot Förenade kungariket](#), nr 4158/05, 12 januari 2010.

FN:s råd för mänskliga rättigheter, *Rosalind Williams Lecraft mot Spanien*, Comm. nr 1493/2006, 30 juli 2009.

KONTAKTA EU

Besök

Det finns hundratals Europa direkt-kontor i hela EU.

Hitta ditt närmaste kontor på https://europa.eu/european-union/contact_sv.

Telefon eller mejl

Tjänsten Europa direkt svarar på dina frågor om EU. Kontakta tjänsten på något av följande sätt:

- Ring det avgiftsfria telefonnumret 00 800 6 7 8 9 10 11 (en del operatörer kan ta betalt för samtalet).
- Ring telefonnumret +32 22999696.
- Mejla via webbplatsen (https://europa.eu/european-union/contact_sv).

EU-INFORMATION

På nätet

På webbplatsen Europa finns det information om EU på alla officiella EU-språk (https://europa.eu/european-union/index_sv).

EU-publikationer

Ladda ned eller beställ både gratis och avgiftsbelagda EU-publikationer (<https://op.europa.eu/sv/publications>). Om du behöver flera kopior av en gratispublikation kan du kontakta Europa direkt eller ditt lokala informationskontor (https://europa.eu/european-union/contact_sv).

EU-lagstiftning och andra rättsliga handlingar

Rättsliga handlingar från EU, inklusive all EU-lagstiftning sedan 1951, finns på alla officiella EU-språk på EUR-Lex (<http://eur-lex.europa.eu>).

Öppna data från EU

På EU:s portal för öppna data (<http://data.europa.eu/euodp/sv>) finns dataserier från EU. Dataserierna får laddas ned och användas fritt för kommersiella och andra ändamål.

Den tekniska utvecklingen har medfört en ökad användning av profilering inom en rad olika områden. Användningen av profileringsverktyg för att underlätta arbetet för tjänstemän inom brottsbekämpning och gränsförvaltning har under senare år rönt allt större uppmärksamhet bland EU:s medlemsstater. Profilering används lagligt för att förebygga, utreda och lagföra brott samt för att förebygga och upptäcka irreguljär invandring. Olaglig profilering kan emellertid undergräva förtroendet för myndigheterna och stigmatisera enskilda samhällsgrupper.

I denna vägledning förklaras vad profilering innebär, vilken rättslig ram som utgör dess grund och varför en laglig profilering både är nödvändig för att uppfylla de grundläggande rättigheterna och helt avgörande för att effektivisera polisarbetet och gränsförvaltningen. Vägledningen innehåller även praktiska riktlinjer om hur olaglig profilering kan undvikas vid insatser inom polisverksamheten och gränsförvaltningen.



FRA – EUROPEISKA UNIONENS BYRÅ FÖR GRUNDLÄGGANDE RÄTTIGHETER

Schwarzenbergplatz 11 – 1040 Wien – Österrike

Tfn +43 158030-0 – Fax +43 158030-699

fra.europa.eu

facebook.com/fundamentalrights

linkedin.com/company/eu-fundamental-rights-agency

twitter.com/EURightsAgency



Europeiska unionens
publikationsbyrå