



GEAUTOMATISEERDE DISCRIMINATIE

'PREDICTIVE' POLICING EN DATAPROFILERING IN BELGIË

Foto voorpagina:
Hoofdkwartier politiekorps Antwerpen
CC-BY-SA 2.0 Fred Romero, 2016



GEAUTOMATISEERDE DISCRIMINATIE

'PREDICTIVE' POLICING EN DATAPROFILERING IN BELGIË

APRIL 2025

 STATEWATCH



LIGA VOOR
MENSEN
RECHTEN

European
Artificial Intelligence
& Society Fund



tac
tic



Inhoudstafel

Methodologie	9
Samenvatting	11
Inleiding	17
I. 'Predictive' policing bij lokale politiekorpsen	20
1. Geografisch informatiesysteem (GIS) Orbit	20
2. Politiekorps Westkust	21
3. Politiekorps Zennevallei	23
4. Antwerpse politie	27
II. Gegevensbanken van de Belgische politie	31
1. Korte presentatie van de verschillende types gegevensbanken	31
a. De Algemene Nationale Gegevensbank (ANG)	31
b. Basis gegevensbanken	32
c. Speciale gegevensbanken	33
d. De Gemeenschappelijke gegevensbank Terrorisme, Extremisme, Radicaliseringsproces (GGB T.E.R.)	34
e. Technische gegevensbanken	35
2. De risico's van politionele gegevensbanken: casussen	36
a. Gegevensbanken en profilering sekswerkers	38
b. Gegevensbanken en profilering 'stadsbendes'	42
c. Gegevensdiscriminatie bij sollicitatiescreenings en veiligheidsmachtigingen	45
d. Gegevensscreening voor 'terrorismebestrijding'	48
e. Het indirecte recht op toegang aanvechten	50
3. De toekomst van Belgische politionele gegevensbanken	51
III. Het federale project 'i-Police'	53
1. Gegevens i-Police	56
2. Videobewaking	57
3. Open-Source Intelligence (OSINT), algoritmische analyse en onderaannemers	60
4. Het programma i-Police: staat van vooruitgang	65
Automatisering van justitie in België: kleine stappen, grote problemen	68
Conclusie: Garbage in, garbage out	69
1. Samenvatting	69
2. Discussie	71
Acroniemen en afkortingen	75

Methodologie

Hoofdauteur: Corentin Debailleul.

Toezicht, redactie en nagelezen door Griff Ferris en Sofia Lyall.

Onderzoek door Griff Ferris, Sofia Lyall, Nathalie Vandeveld, Maria Karantoumani, en Corentin Debailleul.

Vragen over het gebruik van specifieke databases werden verstuurd naar een selectie van lokale politiekorpsen die als strategische doelgroep werden vastgelegd.

De commissie voor privacy van de *Ligue des droits humains (LDH)* stuurde verzoeken om bestuursdocumenten te raadplegen naar alle Franstalige lokale politiekorpsen en gemeenten, en naar de grootste Vlaamse steden (Gent en Antwerpen), met betrekking tot surveillanceapparatuur en de locatie ervan, gerelateerde openbare aanbestedingsdocumenten en gerelateerde Data Protection Impact Assessments (DPIA's). Er werden ook verzoeken verstuurd naar de Federale Politie, met betrekking tot 'i-Police' en gezichtsherkenning.

De informatie werd afgetoetst door het controleren van beschikbare informatie in de pers, op websites over openbare aanbestedingen, in de notulen van parlementaire debatten en politie- en gemeenteraden.

Interviews afgenomen door Griff Ferris en Sofia Lyall:

Datum	Naam en/of functie
2023-02-17	Frank Schuermans, voorzitter Controleorgaan op de politionele informatie (coc)
2023-04-04	Catherine Forget, advocaat en universiteitsonderzoeker, gespecialiseerd in politiedatabanken

Interviews afgenomen door Corentin Debailleul:

Datum	Naam en/of functie
2023-06-16	Hoofdcommissaris bij de Gerechtelijke Federale Politie, Senior raadgever voor Onderzoek & Ontwikkeling en ICT-strategie bij de Algemeen Directeur van de Gerechtelijke Federale Politie.
2023-06-28	Gregory Lewkowicz, ULB-professor in de rechten betrokken bij een onderzoeksprogramma om een AI-systeem te ontwikkelen
2023-07-03	Data protection officer (dpo) van een lokaal politiekorps
2023-08-04	Coördinator van een non-profit organisatie die mannelijke en trans sekswerkers ondersteunt (Brussel)
2023-08-08	Nina Henkens & Onur Cevik, maatschappelijk werkers van Kif Kif (Antwerpen)
2023-08-17	Vakbondsafgevaardigden, Federale Politie

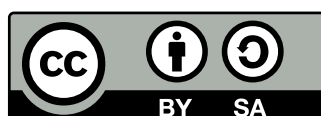
2023-09-19	Een juridisch deskundige, voorheen werkzaam bij de Federale politie
2023-09-28	Farah Kassem, KU Leuven-onderzoeker over (de)radicalisering
2023-10-11	Frank Schuermans, voorzitter Controleorgaan op de politionele informatie (COC)

Tot slot werden informele gesprekken gevoerd met leden van de commissie Privacy en ICT van LDH; leden van het Brusselse collectief Technopolice; een maatschappelijk werker uit Antwerpen die werkt met trans sekswerkers; een beleidsadviseur van de Belgische Vereniging van sekswerkers UTSOPI; een bron binnen de Federale Politie; en een advocaat, lid van *het Observatoire international des prisons - section belge*.

Met dank aan Emmanuelle de Buisseret Hardy, Manuel Lambert, Rémy Farge, Fien De Meyer, Chris Jones, and Sarah De Laet.

Vertaling: Ruben Bogaerts, Maud Boey

Layout: Margaux Hallot



<https://creativecommons.org/licenses/by-sa/4.0/deed.fr>

Samenvatting

De politie in België maakt, net als elders in de wereld, steeds meer gebruik van geavanceerde data-analysetechnieken om criminaliteit te proberen 'voorspellen'. De veronderstelde voordelen hiervan zijn een verhoogde 'efficiëntie' en 'effectiviteit' van de politie door de beheersing van algoritmen, gegevens en 'innovatie'.

Dit nieuwe digitale tijdperk van misdaadbeheersing kent echter problemen. Politie-data zijn vaak onnauwkeurig en weerspiegelen systemische vooroordelen binnen de politie en de bredere samenleving – in het bijzonder racisme, islamofobie en klassenongelijkheid. De huidige wet- en regelgeving, procedures en systemen bieden onvoldoende controle op de wijze waarop deze gegevens worden verzameld, opgeslagen, gedeeld en gebruikt. Betrokkenen hebben weinig mogelijkheden om verhaal te halen en de mogelijkheden die er wel zijn, zijn vaak zo gebrekkig dat ze niet doeltreffend zijn.

Dit rapport belicht deze ernstige tekortkomingen aan de hand van een analyse van drie ruime onderwerpen:

- Locatiegerichte 'voorspellende' politiesystemen die worden gebruikt door lokale Belgische politiekorpsen;
- Databanken die gebruikt (zullen) worden om deze systemen te informeren; en
- het 'i-Police'-project van de Belgische federale politie, dat is ontworpen om gegevens van de politie en andere openbare agentschappen, alsook andere databronnen, te gebruiken om de besluitvorming en activiteiten van de politie te voeden.

'Predictive policing'

'Predictive' policing (= 'voorspellende' politietechnieken) en dataprofilering berusten op data-analyse en algoritmen om potentiële criminele activiteiten zogenaamd te 'voorspellen' en vervolgens te 'voorkomen'. De vermeende doelen zijn:

- een efficiëntere toewijzing van politiemiddelen mogelijk maken;
- individuen en locaties te 'voorspellen' of te profileren als crimineel;
- politie-interventies rechtvaardigen, waaronder surveillance en toezicht, onder-vragingen, stop and search interventies of zelfs arrestaties.

Lokale Belgische politie

Lokale Belgische politiekorpsen gebruiken verschillende tools en systemen om deze doelstellingen te bereiken. Het Geografisch Informatiesysteem van het bedrijf Columba is bijzonder opmerkelijk. Het maakt gebruik van geografische gegevens uit historische misdaadrapporten om vermeende 'hotspots' van criminaliteit

te identificeren. Het bedrijf stelt dat het door bijna 100 politiekorpsen in België wordt gebruikt. Andere tools die het bedrijf aanbiedt zijn bedoeld voor «misdaadanalyse» en openbare ordehandhaving (bijvoorbeeld bij protesten).

De Politiezone Westkust omvat de Vlaamse gemeenten De Panne, Koksijde en Nieuwpoort en was een voorloper in het digitaliseringsproces van de Vlaamse politie. Een bezoek van de politiecommissaris aan de Verenigde Staten leidde tot een plan om politiedata te gebruiken om, in de woorden van de commissaris, “ruwweg te voorspellen waar het mogelijk mis zou kunnen gaan.” Het locatiegebaseerde systeem heeft naar verluidt geleid tot een vermindering van 40% van het aantal criminele incidenten, maar een objectieve evaluatie van het systeem of de werking ervan ontbreekt.

De Politiezone Zennevallei omvat de gemeenten Beersel, Halle en Sint-Pieters-Leeuw in de Vlaamse zuidwestelijke randgemeenten van Brussel. Interesse in ‘predictive’ policing leidde tot een project met de Universiteit Gent om inbraken te ‘voorspellen’. Hierbij werden zowel historische criminaliteitsgegevens als andere gegevens, zoals weersomstandigheden, gebruikt.

Het systeem is gebaseerd op een methode die bekend staat als *Risk Terrain Modeling*, die wordt gebruikt om gebieden te identificeren die waarschijnlijk een hoger risico op criminaliteit lopen vanwege zogenaamde ‘omgevingsfactoren’ en ruimtelijke kenmerken. De criminologische theorieën die aan deze aanpak ten grondslag liggen zijn alom bekritiseerd omdat ze geen rekening houden met de meervoudige, complexe en structurele oorzaken van criminaliteit. De onderzoekers achter het project hebben opgeroepen tot het gebruik van nog meer gegevens om de werking van het systeem te verbeteren, en ontvingen financiële steun van de EU om dit te doen.

Politieagenten van de grote havenstad Antwerpen en, met uitbreiding het hele land, hebben bodycams gekregen door een deal tussen Antwerpen en het Zweedse bedrijf Securitas. Het bedrijf heeft ook bepaalde activiteiten van de Antwerpse politie overgenomen, zoals het monitoren van CCTV-beelden.

Daarnaast heeft de politie van Antwerpen haar eigen smartphoneapplicatie ontwikkeld, genaamd FOCUS. Hiermee krijgen politieagenten op straat toegang tot federale databanken en tot verschillende andere functionaliteiten, zoals rapporterings- en berichtendiensten. Daarnaast verzamelt de politiezone gegevens uit verschillende bronnen op één platform: ANPR-systemen, locaties van politiewagens, CCTV-camera’s en crowd management via tracking van mobiele telefoons. Ze hebben ook geavanceerde analysetechnieken toegepast op CCTV-beelden, waaronder tekstherkenning, gedragsprofilering en het volgen van objecten.

Deze systemen, tools en technieken roepen een aantal vragen op met betrekking tot de bescherming van maatschappelijke vrijheden en mensenrechten. Van locatiegericht ‘hotspot’-policing is in meerdere contexten aangetoond dat het discriminerende patronen en buitensporig politieoptreden ten aanzien van bepaalde individuen of wijken in stand houdt. De theorieën die hieraan ten grondslag liggen zijn

schaars en bekritiseerd. De integratie van een toenemend aantal databronnen maakt deze problemen nog groter en werpt nog meer vragen op met betrekking tot privacy, dataminimalisatie en het risico van misbruik of lekken.

‘Voorspellende’ systemen zoals die gebruikt worden door lokale politiekorpsen in België schenden belangrijke principes van recht(vaardigheid), waaronder het recht op vrijheid, het recht op een eerlijk proces en het vermoeden van onschuld. Individuen, groepen en locaties worden voortijdig bestempeld als potentieel bedreigend. Dit kan leiden tot preventieve sanctiemaatregelen, zoals ongerechtvaardigde vrijheidsberovingen. Dit holt het essentiële principe uit dat individuen als onschuldig worden beschouwd tot het tegendeel is bewezen, en vormt een ernstig risico op gerechtelijke dwalingen.

Politiedatabanken

Veel van de gegevens die in deze systemen worden gebruikt, zijn afkomstig uit politionele databanken. Deze vormen een fundamentele uitdaging voor ‘voorspellende’ politietools. Er is een groot aantal politiedatabanken in gebruik in België, maar er is weinig effectieve controle of toezicht op hun structuur of gebruik. De wetten op de gegevensbescherming worden niet of nauwelijks gehandhaafd. Agenten die illegaal toegang krijgen tot of gegevens gebruiken, krijgen weinig tot geen betekenisvolle sancties.

Dit gebrek aan controle en toezicht is des te opvallender gezien het aantal politiedatabanken in België en de enorme hoeveelheid gegevens die ze kunnen bevatten. Officiële politionele en strafrechtelijke gegevens zijn gestructureerd volgens de systemische vooroordelen van de politie en de maatschappij waarin ze werken. Ze zijn ook vaak onnauwkeurig.

Informeel data zijn soms gebaseerd op niet meer dan roddels, geruchten, speculatie of zelfs verzinsels – zoals in het geval van een man waarover in de database vermeld stond dat hij van plan was om politieagenten te besmetten met HIV. Bovendien kunnen dataverzamelingssystemen ook dienen om mensen in reeds kwetsbare situaties verder te marginaliseren. Dat probleem wordt in dit rapport aangetoond door het voorbeeld van een app voor het registreren van sekswerkers. Zogenaamd om de veiligheid van sekswerkers te garanderen, betekende de databank dat sekswerkers in precarie migratiesituaties verder werden weggedreven van ondersteunende diensten en organisaties, omdat registratie in de app uiteindelijk zou kunnen leiden tot hun uitzetting.

Politiedatabanken worden ook voor steeds meer verschillende doeleinden gebruikt. Het zal weinig mensen verbazen dat ze gebruikt worden om toekomstige werknemers te controleren, bijvoorbeeld wanneer deze werknemers toegang zouden krijgen tot geclassificeerde informatie of gevoelige gebieden zoals nucleaire sites. Het gebruik ervan om mensen te controleren die op muziekfestivals solliciteren, kan echter de wenkbrauwen doen fronsen.

Dit rapport vermeldt de ervaring van een jonge man die de baan die hij zocht

werd geweigerd omdat hij ten onrechte werd beschuldigd van deelname aan een protest. Die beschuldiging (en arrestatie) leidt er nog steeds toe dat hij op luchthavens wordt aangehouden en ondervraagd. In onafhankelijke rapporten wordt ook melding gemaakt van een onevenredig groot aantal geweigerde veiligheidsmachtigingen voor werknemers van Noord-Afrikaanse afkomst.

De gevolgen van dit vooringenomen beleid zijn wijdverspreid en divers. Individuen hebben financiële verliezen geleden en moeilijkheden ondervonden bij het vinden van werk door de weigering van financiële diensten. Deze financiële moeilijkheden vergroten hun vatbaarheid voor verdere schade en marginalisatie. Bovendien biedt de Belgische wet mensen geen zinvol recht op toegang tot hun data, waardoor het uiterst moeilijk – zo niet onmogelijk – is om onjuistheden te corrigeren of te verwijderen.

Het i-Police systeem

Aan het i-Police-systeem wordt al minstens tien jaar gewerkt. Het is momenteel in handen van de federale politie en het bedrijf Sopra Steria, met ondersteuning van het internationale adviesbureau KPMG en een reeks onderaannemers. Onder deze onderaannemers bevinden zich een aantal Israëlische bedrijven, waaronder bedrijven waarvan de oprichters of CEO's voormalige functionarissen zijn van de Israëlische militaire inlichtingendienst. Dit roept ernstige vragen op over de ethische verplichtingen van de Belgische autoriteiten, evenals de mogelijkheid van mogelijke 'achterdeurtjes' die illegale toegang tot gegevens mogelijk maken.

In een officiële aankondiging staat dat het systeem:

«automatische analyse en kruising van data, zoals camerabeelden, foto's, vingerafdrukken, sporen, documenten, ... Hierdoor worden criminelen en criminaliteitsfenomenen sneller en duidelijker in beeld gebracht. Onderzoekers ontvangen in real time een schat aan gefilterde informatie en kunnen snel en gericht optreden.»

Er staan een aantal locatiegerichte 'voorspellende' functies voor het systeem gepland. De mogelijkheid voor agenten om real-time updates te ontvangen over interessante personen – bijvoorbeeld wanneer die persoon wordt aangetroffen door een andere agent – werd tevens gepromoot.

Net als bij de lokale politiesystemen die in dit rapport zijn onderzocht, zijn deze plannen – hoe vergezocht ze ook mogen lijken – afhankelijk van de integratie en analyse van enorme hoeveelheden data. Deze data zijn afkomstig van internationale en nationale overheidsinstanties, particuliere bedrijven en openbaar toegankelijke bronnen zoals sociale media of de pers. Deze bronnen bevatten zowel geverifieerde als niet-geverifieerde informatie. Naast kwesties van proportionaliteit en noodzakelijkheid, steekt ook het probleem van geruchten, roddels of een gebrekkig algoritme weer de kop op wanneer die politie-interventies bepalen. Het automatiseren van de analyse van bewakingscamerabeelden voor 'verdachte' activiteiten roept vergelijkbare vragen op, naast vragen over de fundamentele wenselijkheid van deze technologieën voor een zogenaamde democratische samenleving.

Zoals bij veel IT-projecten van de overheid, is de toekomst minder zeker dan het leek toen het i-Police project voor het eerst werd aangekondigd. Er lopen campagnes tegen het gebruik van Israëlische technologieën en onderaannemers door de Belgische politie, toezichthoudende organen maken zich grote zorgen over de ongepaste verzameling en het ongepaste gebruik van gegevens en de Belgische federale politie zit bijna zonder geld. Elk van deze factoren zou voldoende moeten zijn om de noodzaak van een dergelijk project in vraag te stellen. De combinatie van deze drie factoren zou moeten volstaan om er voor eens en altijd een einde aan te stellen. Of het zo zal lopen, valt nog af te wachten.

Verbod, nu

Eerst en vooral staan ‘voorspellende’ AI-systemen gekend voor hun onevenredig richten op en discrimineren van gemarginaliseerde groepen en het versterken van bestaande structurele ongelijkheden. Data die worden ingevoerd op basis van ras, religie, sociaaleconomische status, migratieachtergrond en nationaliteit worden vaak bepalende factoren in een onredelijk en overdadig politieoptreden tegen, en surveillance en criminalisering van bepaalde gemeenschappen. Ze schenden en ondermijnen meerdere rechten: het recht op vrijheid, een eerlijk proces, vrijwaring van discriminatie, het vermoeden van onschuld, enzovoort.

Een gebrek aan transparantie en verantwoording, en het gebrek aan toegang tot effectieve rechtsmiddelen, vergroot deze problemen. ‘Voorspellende’ AI-systemen opereren achter technologische en commerciële barrières, waardoor beslissingen aan het oog worden onttrokken. Getroffen individuen tasten in het duister, zonder duidelijke en effectieve middelen om deze *black boxes* te openen en ondoorzichtige beslissingen aan te vechten.

De Belgische wetgeving biedt weinig zinvolle bescherming tegen, of verhaal voor, deze diepgewortelde problemen. Het is onwaarschijnlijk dat de recente wet van de EU inzake kunstmatige intelligentie veel zal bijdragen – en het is in ieder geval duidelijk dat de Belgische autoriteiten er niet in zijn geslaagd om de bestaande EU-wetgeving die bedoeld is om individuen te beschermen, zoals de regels rond gegevensbescherming, correct toe te passen.

De reeds bestaande wettelijke bescherming moet worden gehandhaafd en er moeten nieuwe wettelijke mechanismen worden ingevoerd om deze aan te vullen. Om echter volledig rekening te houden met de schade die het gevolg is van datagestuurd politiewerk in België, zijn dergelijke regelgevende voorstellen niet toereikend. Dit rapport heeft de structurele problemen van racisme, islamofobie en klassenvooroordelen bij de politie aan het licht gebracht. Deze problemen zijn systemisch en kunnen niet opgelost worden door regulering van politionele algoritmes of datagebruik alleen.

In het licht van deze dringende bezorgdheden is het noodzakelijk dat België het gebruik van ‘predictive’ policing en geautomatiseerde besluitvormingssystemen in politie- en strafrechtcontexten verbiedt. Door deze systemen te verbieden, kan België een belangrijke stap zetten in de richting van een meer rechtvaardige, even-

redige en democratische samenleving. Het is een kans om het engagement te bevestigen om fundamentele rechten te handhaven, gelijkheid te bevorderen en de principes van rechtvaardigheid en verantwoordingsplicht te handhaven.

Inleiding

De laatste jaren hebben politiekorpsen overal ter wereld hun gebruik van gegevensanalyse en dataprofilering aanzienlijk uitgebreid. Ze introduceerden *'predictive' policing* ('voorspellende' politietechnieken) en misdaadvoorspellende systemen in hun operaties en stelden ze voor als transformatieve methoden die het landschap van misdaadpreventie en onderzoek kunnen hertekenen. De zogenaamde 'politiwetenschappelijke' benadering beweert de veronderstelde 'efficiëntie' en 'effectiviteit' van politieactiviteiten te verbeteren door gebruik van algoritmes, gegevens en 'innovatie'. Dit lijkt het begin te zijn van een nieuw digitaal tijdperk voor misdaadcontrole.

'Predictive' policing en dataprofilering zijn aanpakken van wetshandhaving die berusten op gegevensanalyse en algoritmes voor machinaal leren om potentiële criminele activiteiten zogenaamd te 'voorspellen' en vervolgens te 'voorkomen'. Ze maken gebruik van historische misdaadcijfers, naast verscheidene sociodemografische en omgevingsfactoren, om patronen en tendensen te identificeren die aangeven waar en wanneer een misdrijf het meest waarschijnlijk zal plaatsvinden, of wie het misdrijf zou plegen.

De belangrijkste doelen van *'predictive' policing* en dataprofilering zijn:

- Politiemiddelen efficiënter toewijzen door criminele activiteiten te anticiperen en te voorkomen op bepaalde locaties en in bepaalde gebieden;
- Personen 'voorspellen' of profileren als (potentiële) criminelen om hen nauwgezet te monitoren;
- Politie-interventies zoals ondervragingen, aanhoudingen op straat en fouilleringen of arrestaties rechtvaardigen.

Maar dataprofilering en *'predictive' policing* geven aanleiding tot bezorgdheid over gegevensbias, discriminatie, mogelijke schendingen van mensenrechten en burgerlijke vrijheden. De betrouwbaarheid van de systemen kan in vraag worden gesteld, zeker wanneer de onderliggende theorieën twijfelachtig zijn. De aanpak brengt ook het risico op selffulfilling prophecies met zich mee. Verhoogde politieaanwezigheid in bepaalde gebieden leidt vaak tot politieacties en strafrechtelijke resultaten zoals aanhoudingen en fouilleringen op straat en mogelijke arrestaties. Die resultaten worden dan omgezet in gegevens en in het systeem ingevoerd. Bijgevolg zal de politie dezelfde gebieden herhaaldelijk viseren, wat voor een feedbackloop zorgt.

Gegevensgestuurde wetshandhaving kan ook leiden tot het viseren van personen met een bepaalde achtergrond of mensen die passen binnen een bepaald profiel. Vaak gaat het om mensen uit raciale of gemarginaliseerde groepen. Zij krijgen dan te maken met politie- of strafrechtelijke interventies zoals aanhoudingen op straat en fouilleringen of arrestaties. Wanneer dat op zijn beurt wordt omgezet in politiegegevens, wordt er een gelijkaardige feedbackloop gecreëerd waarbij de politie personen die aan een profiel voldoen viseert.

Er zijn ook problemen met betrekking tot transparantie. Algoritmes kunnen vaag en onbegrijpelijk zijn, hoewel aansprakelijkheid net cruciaal is voor mensen om deze systemen en hun resultaten te kunnen aanvechten. Hierdoor kunnen fundamentele mensenrechten in het gedrang komen, waaronder het vermoeden van onschuld, het recht op privacy, op vrijheid en op een eerlijk proces, de vrijheid van vergadering en vereniging en gelijke behandeling door de wet.¹

‘Predictive’ policing in België is een complex netwerk van evoluerende initiatieven bij federale en lokale instanties van rechtshandhaving. Dit verslag legt de meerlagige dimensies van gegevensgedreven en ‘*predictive*’ policing in België bloot. Het onderzoekt de onderliggende technologieën, theorieën en maatschappelijke implicaties.

Het verslag analyseert een grote hoeveelheid informatie, waaronder persberichten, publieke communicatie, officiële documenten en parlementaire vragen en debatten. Daarnaast doet het beroep op verslagen van overheidsdiensten en ngo’s, alsook privé-audits van de IT-afdeling van de Federale Politie. Het put ook uit academische literatuur over systemen van ‘*predictive*’ policing in België.

Het verslag put verder uit interviews met politiemedewerkers en vertegenwoordigers van mensenrechtenverenigingen of groepen die door de politie kunnen worden opgevolgd, zoals gemarginaliseerde groepen of sekswerkers. Aanvragen voor vrijheid van informatie werden ingediend, maar de politie gebruikte veiligheidsuitzonderingen om de verstrekte informatie te beperken tot wat al publiekelijk toegankelijk was.

Dit verslag bestaat uit vier delen. Het eerste deel bespreekt de voorspellende capaciteiten van de politie en behandelt initiatieven die door lokale politiekorpsen zijn genomen. Het tweede deel beschouwt de gegevensbanken van de Belgische politie, die een groot deel van de gegevens voor voorspellende systemen voorzien en beschrijft de risico’s die verbonden zijn aan het gebruik ervan. Deel drie beschouwt het i-Police-programma van de Federale Politie en zijn vele gevolgen. Het vierde en laatste deel beschrijft de weinige rudimenten van voorspellende rechtspleging in België. Het verslag sluit af met een beschouwende samenvatting van ons onderzoek.

Dit verslag heeft als doel om verder te gaan dan enkel technologie in actie te observeren. In een tijdperk waarin gegevens en algoritmes overheersen in het beslissingsproces, is ons doel om de uitdagingen en gevaren van deze transformatie bloot te leggen. De richting van ‘*predictive*’ policing is niet vooraf bepaald, maar wordt beïnvloed door de handelingen en keuzes van personen, gemeenschappen, beleidsmakers en activisten. Het is de gedeelde verantwoordelijkheid van ons allemaal om te garanderen dat de weg voorwaarts er een is van gerechtigheid, eerlijkheid en standvastige bescherming van fundamentele vrijheden.

¹ Thomas Marquenie. 2022. ‘Het gebruik van Ai-toepassingen binnen het politiewezen: voordelen, risico’s en best practices’. Staten Generaal over Artificiële Intelligentie. *Centre for IT & IP Law (CiTiP)*. 17 June 2022. URL: vaia.be/files/cursusmateriaal/presentaties/220617-3-Thomas-Marquenie.pdf

NB: Het gebruik van aanhalingstekens rond 'predictive' in dit verslag dient als herinnering dat de zogenaamde 'predictive' policing nooit volledig of nauwkeurig toekomstige gebeurtenissen zoals misdrijven kan voorspellen. In plaats daarvan benadrukken de aanhalingstekens dat het gaat om gegevensgestuurde algoritmes en statistische modellen die waarschijnlijkheden en tendensen weergeven, eerder dan zekere voorspellingen. Ondanks de beweringen of wensen van techliefhebbers blijft profetische zekerheid à la *'Minority Report'* beduidend fictie.

I. 'Predictive' policing bij lokale politiekorpsen

In België is de geïntegreerde politie (GPI) gestructureerd op twee niveaus: de Federale Politie en 183 lokale politiekorpsen. Die laatsten zijn verantwoordelijk voor alle gerechtelijke en administratieve basispolitietaken, terwijl de Federale Politie hen op verschillende manieren ondersteunt.

Verschillende lokale politiekorpsen hebben in de laatste jaren gebruik gemaakt van geografische 'predictive' policing en profileringsystemen en deelgenomen aan experimentele projecten in het kader van 'predictive' policing. Er bestaat weinig tot geen transparantie over deze initiatieven. Het is mogelijk dat andere politiekorpsen ook gebruik maken van 'voorspellende' systemen of dataprofilering, of gelijkaardige projecten hebben.

In 2020 voerden criminologen aan de KU Leuven een enquête uit bij politiekorpsen in Vlaanderen en het Brussels Hoofdstedelijk Gewest, waaruit bleek dat bijna de helft van alle respondenten gebruik maakt van een vorm van gegevensanalyse. Meer bepaald 43% gebruikte 'manuele gegevensanalyse', terwijl 31% 'geautomatiseerde gegevensanalyse' toepaste.²

1. GEOGRAFISCH INFORMATIESYSTEEM (GIS) ORBIT

Het Geografisch Informatiesysteem (GIS)³ van het bedrijf Orbit is de belangrijkste tool die politiekorpsen in Vlaanderen en het Brussels gewest gebruiken. Het bedrijf zelf stelt dat het systeem "reeds bij 115 zones geïmplementeerd" is.⁴ Orbit GIS biedt de mogelijkheid om historische misdaadverslagen ruimtelijk op te volgen, om zogenaamde geografische 'hotspots' van criminaliteit te identificeren.

Orbit biedt ook de tool 'Orbit Crime' aan voor "criminaliteitsanalyse". Het bedrijf geeft het voorbeeld van inbraak, winkeldiefstal, drugs (inclusief drugshandel en -cultuur), overlast en vandalisme (geïllustreerd door vandalisme "gepleegd door minderjarigen op een nieuwe bouwplaats").⁵ Het biedt aanvullende tools om "in realtime alle personeels- en actieplannen van evenementen op één scherm te visualiseren" en een specifieke tool gericht op openbare orde beschreven als "onderhandeld beheer van de openbare ruimte".⁶

² Lore Rooseleers en Jeroen Maesschalk. 2021. "Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?" *Panopticon*. Vol. 42, n° 5, p. 419-438. URL: lirias.kuleuven.be/3611651

³ Orbit GIS. *Politie*. URL: web.archive.org/web/20230930193822/https://www.orbitgis.com/nl/home/producten/politie

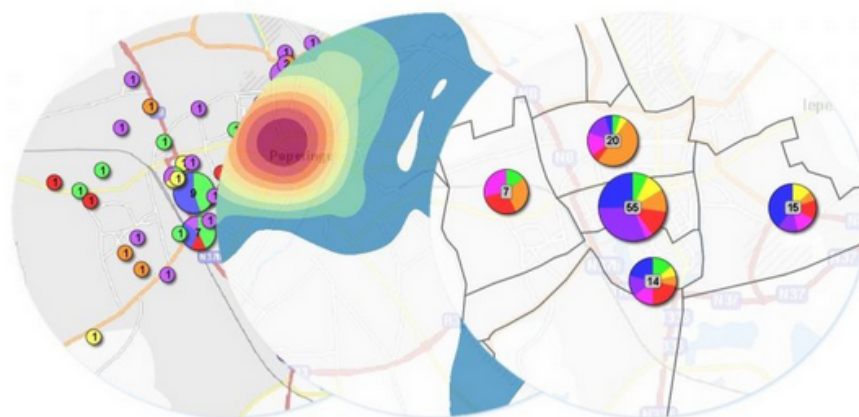
NB : Het programma kreeg in 2024 de nieuwe naam "Columba". URL: www.columbasoftware.be/software/veiligheidsdiensten

⁴ Orbit GIS. *Politie*. URL: web.archive.org/web/20230930193822/https://www.orbitgis.com/nl/home/producten/politie

⁵ Orbit GIS. *Politie - BeleidsTools*. URL: https://web.archive.org/web/20230930183829/https://www.orbitgis.com/nl/home/producten/politie/pz_beleid-tools

⁶ Orbit GIS. *Politie - Operationele tools*. URL: web.archive.org/web/20230930185818/https://www.orbitgis.com/nl/home/producten/politie/pz_operationele-tools

ORBIT CRIME



Figuur 1. Schermafbeelding van de Orbit-website met daarop 'Orbit Crime'
url: www.orbitgis.com/fr/zone-de-police/zp_strategie

In verschillende contexten is al aangetoond dat *'hotspots' policing* ervoor zorgt dat discriminatiepatronen worden verdergezet en excessief wordt opgetreden tegen specifieke individuen of gebieden, op basis van voorgaande interacties met de politie.⁷ Desondanks hebben verschillende Vlaamse politiekorpsen experimentele testprojecten met *'predictive' policing* gelanceerd.

2. POLITIEKORPS WESTKUST

Het politiekorps van de Westkust omvat de Vlaamse gemeentes De Panne, Koksijde en Nieuwpoort. Dit zijn gemeenten die grenzen aan Frankrijk, in het westen van de Belgische kust. Er wonen slecht een 45 000 mensen, maar het gebied is een toeristische trekpleister tijdens de vakantieperiode.



Figuur 2. Panoramische foto van het strand van De Panne
Copyleft Lokilech, 2008.

⁷ William Isaac and Kristian Lum, 'To Predict and serve?', *Royal Statistical Society*, 2016, doi:10.1111/j.1740-9713.2016.00960.x; Lyria Bennett Moses and Janet Chan, 'Algorithmic prediction in policing: assumptions, evaluation, and accountability', 2016, *Policing and Society*, 28:7, DOI: 10.1080/10439463.2016.1253695; Rashida Richardson, Jason Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', February 2019. 94, *N.Y.U. Law Review*. 192, URL: ssrn.com/abstract=3333423; Gizmodo, 2021. 'Crime prediction software promised to be free of biases, new data shows it perpetuates them', 2 December 2021, URL: gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977

Het lokale politiekorps van de Westkust was een voorloper in het digitaliseringsproces van de politie. Het korps begon al in 2016 met de uitrol van *systemen van 'predictive' policing*.⁸ Nicholas Paelinck, de lokale korpschef, bracht persoonlijk een bezoek aan Philadelphia in de Verenigde Staten om te observeren hoe de politie daar dergelijke systemen gebruikt en om te zien hoe ze zouden kunnen worden geïmplementeerd in de Westkust.

Het voorgewende doel van het lokale korps is om te gaan naar “minder blauw op straat”, waarmee minder patrouilles maar meer gegevensanalysten wordt bedoeld.⁹ De korpschef legde aan de pers uit hoe het project hoorde te werken:

“Wij werken nu al met drie datamanagers in ons korps. Via informatie die ze binnenkrijgen, voorspellen we grosso modo waar het mogelijk mis kan gaan. Daar sturen we dan proactief een interventieploeg heen. Het gaat niet alleen om het voorkomen van inbraken, maar de werkwijze dient ook voor preventieve acties tegen gauwdieven of drugsdealers. Het is de bedoeling om criminaliteit aan te pakken vooraleer de feiten gebeuren”.¹⁰

De eigenlijke werking van het programma werd enkel op volgende algemene wijze beschreven:

“De politie verzamelt een hoop verschillende gegevens, gaande van eerdere misdrijven, nummerplaten, gerechtelijke dossiers tot zelfs het weer, die in de computer ingegeven worden. Met behulp van algoritmes zouden data data-analisten precies kunnen voorstellen waar en wanneer misdrijven zich in de nabije toekomst zouden kunnen voordoen”.¹¹

De korpschef beweerde dat sinds de invoering van het programma bij de Westkust criminele incidenten met 40% zijn afgenomen. De politie beweerde dat de ‘voorspellende’ capaciteiten van de software het best in staat waren om inbraken en autodiefstal aan te pakken.¹²

De betrouwbaarheid van deze ongefundeerde statistieken moet echter in vraag worden gesteld. Er zijn geen objectieve evaluaties van het systeem openbaar beschikbaar. Informatie over het computerprogramma dat gebruikt wordt om de analyse uit te voeren en voorspellingen te doen of de daarvoor vrijgemaakte gelden blijft geheim.

De korpschef wenst op termijn de software ook te integreren met camera's voor automatische nummerplaatherkenning (ANPR).¹³

8 Rosamunde van Brakel. *Automating Society 2019: Belgium*. URL: algorithmwatch.org/en/automating-society-2019/belgium/

9 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit'. *De Standaard*. 17/05/2016. URL: standaard.be/cnt/dmf20160517_02292901

10 MVHB. 'De toekomst van de politie: minder blauw op straat, meer blauw achter de computer'. *De Morgen*. 17/05/2016. URL: www.demorgen.be/nieuws/de-toekomst-van-de-politie-minder-blauw-op-straat-meer-blauw-achter-de-computer~bd35acda/

11 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit'. *Op. Cit.*

12 *Ibid.*

13 Rosamunde van Brakel. *Automating Society 2019: Belgium*. *Op. Cit.*

Daarnaast is de korpschef van de Westkust ook de voorzitter van de Vaste Commissie van de Lokale Politie (VCLP), de overkoepelende organisatie van de lokale politiekorpsen in België. Dit betekent dat hij goed geplaatst is om de technieken van *'predictive' policing* die hij heeft getest in de Westkust verder uit te rollen naar andere politiekorpsen doorheen het land.¹⁴

3. POLITIEKORPS ZENNEVALLEI

Onder de politiezone Zennevallei vallen de gemeenten Beersel, Halle en Sint-Pieters-Leeuw in de Vlaamse zuidwestelijke randgemeenten van Brussel. In 2020 startte het korps er een tweejarig project over *'predictive' policing* op, samen met de Universiteit Gent. Deze aanpak omvat dat de politie 'voorspellende' inzichten gebruikt om gebieden die een verhoogd risico op criminaliteit vertonen, waaronder inbraken en andere misdrijven, te identificeren.¹⁵



Figuur 3. Luchtfoto van Bergensesteenweg in Sint-Pieters-Leeuw
CC-BY-SA 3.0 Wouters Hagens, 2014

Het politiekorps kondigde aan dat het in 2022 een prijs won voor haar initiatief met de volgende woorden:

“Daarom startte politiezone Zennevallei, samen met de UGent, in oktober 2019 een project op waarbij een big data policing model werd ontwikkeld en getest in de praktijk. Het project spitste zich voornamelijk toe op woninginbraak, dat immers het meest voorkomende misdrijf is in België en een grote psychologische impact heeft op de slachtoffers.

¹⁴ VCLP, 2019. Memorandum 2019-2023. Vaste Commissie van de Lokale Politie. <https://www.politie.be/5806/sites/5806/files/media/file/2025-05/Memorandum%20NL.pdf>

¹⁵ EDRI. 'Use cases: Impermissible AI and fundamental rights breaches'. August 2020. URL: edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf

Het project werd in de politiezone Zennevallei verder concreet gemaakt in de loop van de jaren 2020 en 2021. Zo werden risicokaarten opgesteld op basis van statistische modellen gevoed met big data die vervolgens gebruikt werden om politiepatrouilles proactief aan te sturen. Op korte termijn werden op deze manier risicoanalyses voorzien die de kans op criminaliteit aangaven en mensen en middelen konden dusdanig worden ingezet op deze risicogebieden. Op lange termijn beoogden we het efficiënter kunnen inzetten van politiemiddelen en een daling van de criminaliteit".¹⁶

Het systeem van '*predictive*' policing in de Zennevallei heeft de aandacht van de Belgische Senaat getrokken, die de overheid over de materie ondervroeg. Hierop antwoordde de minister van Binnenlandse Zaken dat de overheid de inspanningen van de Federale Politie steunt om haar analytische capaciteiten te verbeteren en benadrukte de minister het fundamentele belang van een sterke basis voor '*predictive*' policing, waaronder het vergaren van de nodige gegevens. De minister van Binnenlandse Zaken erkende echter ook dat de politiestatistieken voornamelijk betrekking hebben op activiteiten van wetshandhaving en dus niet noodzakelijk een volledig beeld schetsen van het eigenlijke criminele landschap binnen een rechtsgebied.¹⁷

Aan de voorhoede van het programma van de Zennevallei stond Anneleen Rummens, doctoraatsstudente aan de Universiteit Gent, onder begeleiding van professor criminologie Wim Hardyns. Ze verzamelden op grote schaal 'big data' voor een breed gamma aan variabelen, waaronder locatie en tijd, maar ook aanvullende factoren zoals weersomstandigheden tijdens specifieke incidenten. Het doel was om dit kluwen aan informatie nauwkeurig in beeld te brengen.¹⁸

Hun methode is gebaseerd op Risk Terrain Modelling (RTM), een methode van ruimtelijke '*predictive*' policing die put uit geografische informatiesystemen (GIS) en criminologische theorie in een poging om gebieden te identificeren die waarschijnlijk een hoger risico op criminaliteit lopen. RTM berust op het idee dat specifieke omgevingsfactoren, ook bekend als 'risk terrains', een invloed hebben op criminele incidenten.

De criminologische theorieën die aan de grondslag liggen van RTM en bijgevolg RTM zelf worden alom bekritiseerd.¹⁹ De fundamentele theorie achter RTM is dat bepaalde geografische gebieden inherent criminaliteit aantrekken of genereren.²⁰ Deze veronderstelling is niet empirisch onderbouwd. Criminaliteit is het gevolg van een complexe wisselwerking tussen verschillende sociale, economische en individuele factoren. Door de nadruk te leggen op geografische factoren, laat RTM de onderliggende socio-economische, culturele en structurele oorzaken van crimina-

16 'Derde prijs voor Big Data Policing'. *Lokale Politie Zennevallei*. 18/03/2022. URL: www.politie.be/5905/nieuws/derde-prijs-voor-big-data-policing

17 Antwoord van de minister van Binnenlandse Zaken op 09/07/202 op schriftelijke vraag n°7-591. Belgische Senaat. URL: senate.be/www/?Mlval=/Vragen/SVPrintNLFR&LEG=7&NR=591

18 Anneleen Rummens & Wim Hardyns. 2020. 'Comparison of near-Repeat, Machine Learning and Risk Terrain Modeling for Making Spatiotemporal Predictions of Crime'. *Applied Spatial Analysis and Policy*, Vol. 13, no. 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2

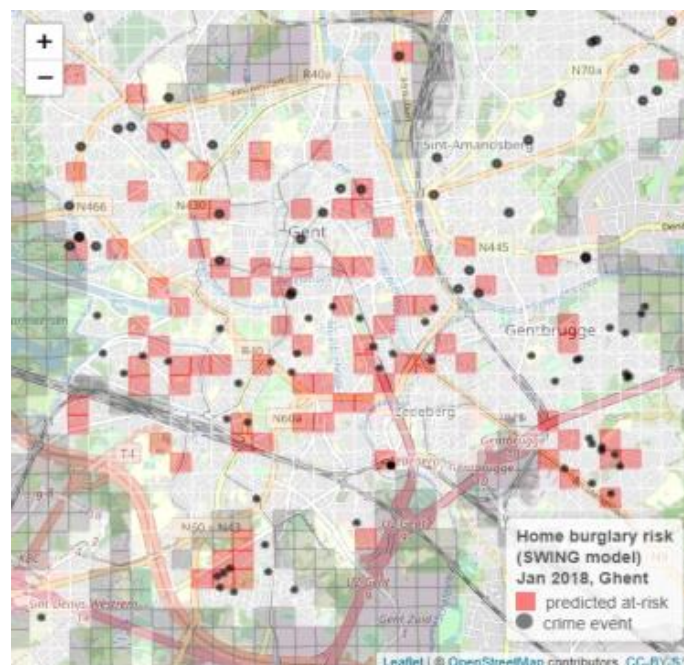
19 Brian Jefferson. 2020. 'Crime Mapping'. In: *International Encyclopedia of Human Geography*. Elsevier. pp. 11-15.

20 Henri Buccine-Schraeder & Leslie W. Kennedy, 2021. 'Risk Terrain Modeling (RTM)'. In: *The Encyclopedia of Research Methods in Criminology and Criminal Justice*, edited by J.C. Barnes & David R. Forde, Wiley, pp. 873–74. Wiley, 2021. DOI: 10.1002/9781119111931.ch169

liteit vaak links liggen.

De criminologen van de UGent menen los te staan van deze kritiek door socio-economische factoren op te nemen in hun criteria. Hun model bevat daarom variabelen zoals het percentage jongeren en migranten of de dichtheid van sociale woningen en snackbars.²¹ Zulke kaarten behandelen verre van de structurele oorzaken van criminaliteit en kunnen ongewenst ruimtelijke bias versterken, door disproportioneel bepaalde wijken te viseren. Dit kan excessief politieoptreden in achtergestelde gemeenschappen in stand houden en zo bestaande ongelijkheden versterken. Zoals de antikolonialistische geograaf Brian Jefferson uitlegt:

“De effecten van politie bias, jury bias en bias in de toekenning van straffen op criminaliteitspatronen worden in geen enkele van deze technieken systematisch onderzocht. Evenmin onderzoeken deze technieken hoe wetten, beleidsmaatregelen of politiepraktijken de geografische patronen in criminaliteitsgegevens beïnvloeden. Crime maps bieden geen definitief, objectief beeld van illegaal gedrag, maar roepen eerder vragen op over hoe dit soort gedrag wordt gemonitord en geregistreerd.”²²



Figuur 4. Voorspelde inbraken (rode vierkanten) en effectieve inbraken (zwarte stippen) in Gent
Source: Rummens & Hardyns. CPS international conference 'Street policing in a smart society'. 17/09/2019.

Hardyns en Rummens lijken weinig aandacht te schenken aan de mogelijks discriminerende gevolgen van hun systeem, des te meer gezien de overvloed aan gevoelige gegevens die door het systeem worden gebruikt. Tijdens een conferentie probeerde Hardyns de bezorgdheid omtrent discriminatie weg te nemen door te benadrukken dat technologie neutraal zou zijn. Om die neutraliteit te verduidelijken, zei Hardyns het volgende: “Wapens doden geen mensen. Domme mensen met wapens doden mensen”.²³ De redenering achter technologische neutraliteit

21 Anneleen Rummens & Wim Hardyns. 2020. “Comparison...”. *Op. Cit.*, Table 2.

22 Brian Jefferson. 2020. ‘Crime Mapping’, *Op. Cit.*, p. 14.

23 Wim Hardyns. Academic panel session: Predictive policing in the big data era. *CPS International Conference ‘Street Policing in a Smart Society’*. 17/09/2019. URL: policingandsecurity.be/wp-content/up-

is als volgt: technologie is niet inherent goed of slecht; de ethische waarde ervan hangt af van het gebruik. Die stelling is echter eenvoudig te weerleggen. Het potentieel voor kwaad is sterk bepaald door de technische eigenschappen van een bepaalde technologie, net zoals de productie ervan inherent deel uitmaakt van de sociale context en doelen.

Op basis van hun onderzoek kwamen de onderzoekers van de Universiteit Gent, Hardyns en Rummens, tot de conclusie dat:

“Predictive policing kan ertoe leiden dat we (big) data gericht gaan inzetten om zo te komen tot een meer datagestuurde (data driven) werking binnen politiediensten. Naast het gebruik van nieuwe databronnen kunnen ook nieuwe methoden zoals machine learning optimaal benut worden om ons meer dynamische inzichten te geven in hoe criminaliteitspatronen evolueren. Er zijn echter nog vele (big) databronnen en gerelateerde methoden die momenteel grotendeels onbenut zijn gebleven. Zo kan bijvoorbeeld gedacht worden aan sociale-mediadata en nieuwe methoden binnen het brede veld van machine learning (bijv. deep learning-modellen, de geavanceerde versie van neurale netwerken). Het potentieel van deze nieuwe bronnen en methoden blijft tot op heden onontgonnen terrein.”²⁴

Het team van Hardyns keek recent ook naar de criminaliteitscijfers in Brussel en probeerde patronen te identificeren. Hun onderzoek bracht hen tot een reeks aanbevelingen die het ‘voorspellende’ getijde volgen. Ze roepen op tot meer *big data* en geautomatiseerde analyse, naast de integratie van verschillende surveillantie- en gegevensbronnen:

“Criminaliteit in Brussel vertoont eerder een link met de mobiliteit van plegers en vereist daarom wellicht pleggergerichte technieken die zich toespitsen op de mobiliteit van plegers in real time, bijvoorbeeld door automatische nummerplaatlezers (ANPR) of bewakingssystemen te gebruiken. Algemeen gesproken kan het daarom nuttig zijn om de criminaliteitsgegevens regelmatig te monitoren en te analyseren, en zo een meer real time Intelligence-Led Policing-aanpak (ILP) te implementeren. In dat opzicht is het misschien ook aangeraden om plaatsgebonden en persoonsgebonden benaderingen tot policing te combineren, of om meer dynamische technieken toe te passen die rekening kunnen houden met de mate van criminaliteitsconcentratie, de ruimtelijke (in)stabiliteit van criminaliteit, de mobiliteit van daders en real time informatie (bijvoorbeeld plaatsgebonden benaderingen tot policing). [...]

Daarnaast is het cruciaal om de mogelijke integratie van alternatieve (grote) gegevensbronnen met officiële politieregistraties te onderzoeken. Door relevante informatie uit bronnen zoals sociale media te integreren (bijv. Twitter-gegevens) en textmining-technieken te gebruiken, kunnen we kwalitatieve inzichten in criminaliteitsgerelateerde incidenten voorzien. Dit zou ons inzicht in criminaliteitsconcentraties kunnen verrijken en zo bijdragen aan uitgebreidere en innovatievere analyses”.²⁵

loads/2020/05/2019-09-17_Studiedag_Street-policing_Hardyns_Academic-panel-session.pdf

24 Wim Hardyns & Anneleen Rummens. (2021). Predictive policing: een balans na zes jaar empirisch evaluatieonderzoek in België. Tijdschrift voor Veiligheid (20) 4, 9-23. URL: tijdschriften.boomcriminologie.nl/tijdschrift/tijdschriftveiligheid/2021/4/TvV-D-21-00005

25 Robin Khalfa, Thom Snaphaan, Lieven Pauwels, Ourania Kounadi and Wim Hardyns, 2023. ‘Crime within a Bandwidth: Testing “the Law of Crime Concentration at Place” in Brussels’. *European Journal on Crim-*

Gezien de invloed die Hardyns heeft in het veld van ‘*predictive*’ *modelling* voor wetshandhaving, is het belangrijk om toekomstig onderzoek van hem en zijn team op te volgen. In 2023 kreeg hij bijna twee miljoen euro van de EU voor een vijfjarig project, bigdatapol.²⁶ Het onderzoeksdoel is om “statistisch-methodologische, criminologische, juridische en ethische voorwaarden in één *evidence-based 3D-model* te integreren”. Dit zou “zowel academische als politiediensten richtlijnen en aanbevelingen” moeten geven inzake “het bestuderen, toepassen en implementeren van *big data policing*”.²⁷ Niet minder dan twintig Vlaamse politiekorpsen wilden deelnemen aan dit onderzoek.²⁸ Hardyns en zijn team hebben ook gewerkt met cijfers van de Antwerpse politie, wat in het volgende deel besproken wordt.

4. ANTWERPSE POLITIE

Antwerpen is de tweede grootste stad in België maar heeft maar één politiekorps. Brussel, de hoofdstad, heeft zes aparte politiekorpsen. Dat maakt van de Antwerpse politie een van de grootste en belangrijkste korpsen in het land,

wat wordt versterkt door het feit dat de Belgische politiekorpsen bestuurd worden door de lokale gemeente. De Antwerpse gemeente werd tussen 2013 en 2025 bestuurd door Bart De Wever, de voorzitter van de rechtse Vlaams-nationalistische partij N-VA (Nieuw-Vlaamse Alliantie). De Wever is een van de invloedrijkste politici in België en bekleedt momenteel de functie van eerste minister (2025).



Figuur 5. Stadsgezicht van Antwerpen
CC-BY-SA 3.0 Paul Hermans, 2012

inal Policy and Research. DOI: 10.1007/s10610-023-09556-8.

26 'Towards an evidence-based model for big data policing: Evaluating the statistical-methodological, criminological and legal and ethical conditions'. *cordis eu research results*. 2023. DOI: 10.3030/101088156

27 'Six Ghent University researchers win ERC Consolidation Grant'. *UGent*. 31/03/2023. URL: web.archive.org/web/20230814224751/https://www.ugent.be/en/news-events/six-ghent-university-researchers-win-erc-consolidator-grant

28 Bigdatapol. 'Kick-off field test Belgium'. *nwsltr*. no. 1. Summer 2024. URL: bigdatapol.com/wp-content/uploads/2024/08/SUMMER-2024-NWSLTR_LR.pdf

Een aantal openbare aanbestedingen die door de Antwerpse politie werden ondertekend zijn bijgevolg doorgetrokken naar andere politiekorpsen. Dit toont aan hoe groot de invloed van de Antwerpse politie is in de bredere digitalisering en automatisering van de politie in België.

Antwerpen heeft een contract voor twee miljoen euro getekend met het Zweedse bedrijf Securitas²⁹ om bepaalde politietaken te privatiseren, waaronder de bewaking van publieke evenementen en strategische perimeters en het monitoren van CCTV-beelden.³⁰ Datzelfde contract staat de aankoop van materiaal toe. Veel Belgische politiekorpsen hebben ingetekend om via die weg *bodycams* aan te kopen.

Naast de technologieën van Securitas heeft de Antwerpse politie haar eigen smartphoneapplicatie ontwikkeld, genaamd FOCUS. Hiermee hebben alle politieagenten toegang tot gegevensbanken van de politie. De app werd doorverkocht aan de Geïntegreerde Politie en uitgerold in het hele land.

De standaardapplicatie FOCUS, toegankelijk voor iedere Belgische politieagent, heeft verschillende modules. Waaronder:

- De module 'zoeken', waarmee agenten toegang krijgen tot alle beschikbare gegevensbanken. De module verschaft ook proactief informatie. Wanneer agenten een locatie opzoeken, haalt de app automatisch alle informatie op van individuen (en mogelijke wapens) die geregistreerd staan op dat adres, naast eerdere incidenten;
- De module 'incidenten' geeft agenten een geüpdatet overzicht van lopende gebeurtenissen in het veld;
- De module 'islp' (Integrated System for the Local Police) waarmee agenten snel een verslag kunnen opmaken op het terrein;
- De module 'berichten' biedt agenten een platform om met elkaar te communiceren;
- De module 'afbeeldingen' biedt agenten de mogelijkheid foto's te nemen en te uploaden;
- De module 'kaarten' heeft verschillende lagen waaronder: de locatie van veldeenheden, CCTV-camera's en een overzicht van de huidige verkeerssituatie.

Naast het basispakket kunnen de politiekorpsen ook aanvullende modules toevoegen aan FOCUS.³¹

29 Securitas Security company. URL: www.securitas.be

30 Lokale Politie Antwerpen. LPA/2017/295. URL: enot.publicprocurement.be/enot-war/preViewNotice.do?noticeId=319270

31 Lore Rooseleers en Jeroen Maesschalk. 2021. 'Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?' *Op. Cit.*, p. 10.



Figuur 6. De interface van de FOCUS-app

Source: Monkeyshot. 2018. 'Een typische zoekopdracht van een gebruiker van de Antwerpse politie – IxD18'. Slideshare.

Het systeem van FOCUS gebruikt ook algoritmes waarmee politiekorpsen gegevens van verschillende bronnen kunnen invoeren, waaronder de algemene politionele gegevensbank (ang); het anpr- en nummerplaatregister; het ISLP-systeem. Dat gegevens van islp worden gebruikt is bijzonder verontrustend. De informatie uit deze gegevensbank is niet geverifieerd en bestaat voornamelijk uit onbevestigde veldnotities van politieagenten, in grote mate gebaseerd op geruchten en meningen.

Een ander softwareplatform dat de politie van Antwerpen gebruikt, verzamelt gegevens van anpr-systemen, de locatie van politiewagens, CCTV-camera's en *crowd management* via tracking van mobiele telefoons.

De Antwerpse politie heeft ook geavanceerde analysetechnieken toegepast op CCTV-beelden, waaronder tekstherkenning, menselijke ontleding, gedragsprofilering, objecttracering.³²

Jo Forceville, specialist 'smart policing' bij de Antwerpse politie, voorziet een transitie naar methodologieën met kunstmatige intelligentie (AI) en open-source intelligentie (OSINT):

"Er zijn projecten lopende rond het 'scrapen' van sociale media, 'deep learning' modellen en het inzetten van Artificiële Intelligentie (ai) bij de analyse van bijvoorbeeld camerabeelden. Scraping van sociale media gebeurt bijvoorbeeld bij onderzoeken naar radicalisme, ai zoekt naar verdachte patronen of routes in het verkeer".³³

³² Jo Forceville. 2023. 'Big Data en politie, evolutie in versnelling: Een blik voorbij data en technologie'. In Snaphaan et al. (eds.), *Cahiers Politiestudies*, no. 66: Big Data Policing. Antwerpen: Gompel&Svacina. pp. 107-120.

³³ Ibid.

Antwerpen is duidelijk koploper wanneer het gaat om nieuwe technologieën te implementeren. Het zal belangrijk zijn om kritisch te blijven kijken naar het politiekorps van de stad en om geïnformeerd te blijven over ontwikkelingen in het gebruik van technologie bij de Belgische politie.

II. Gegevensbanken van de Belgische politie

Politiegegevensbanken zijn de primaire gegevensbron voor *'predictive' policing* en dataprofileringsystemen. Daarom is het nodig om hun gebruik en inhoud te beschrijven.

Politiegegevensbanken in België zijn officieel onderverdeeld in vijf categorieën:

- a) De Algemene Nationale Gegevensbank (ANG);
- b) Basis gegevensbanken;
- c) Speciale gegevensbanken;
- d) De Gemeenschappelijke Gegevensbank (GGB);
- e) Technische gegevensbanken.

Private gegevensbronnen, met name sociale netwerken en geolocatiegegevens verschaft door telefonieoperators,³⁴ spelen ook een belangrijke rol en zullen later besproken worden.

1. KORTE PRESENTATIE VAN DE VERSCHILLENDE TYPES GEGEVENS BANK

A. DE ALGEMENE NATIONALE GEGEVENS BANKEN (ANG)

De Algemene Nationale Gegevensbank (hierna ANG genoemd) is de belangrijkste politiegegevensbank en is verdeeld in drie delen: verkeer; administratief; en gerechtelijke politie. Deze gegevensbank wordt vaak gebruikt voor politieonderzoek. In 2019 bevatte de ANG informatie van maar liefst drie miljoen mensen - een kwart van de Belgische bevolking.³⁵ De betrouwbaarheid van deze informatie schommelt en kan gaan over verdachten, getuigen of slachtoffers en kan verwijzen naar eender welk soort incident. Sinds 2019 en de onderdrukkende maatregelen van de coronapandemie is dat cijfer zeker niet gedaald.

Het Controleorgaan op de politiegegevensinformatie (COC) publiceerde recent een scherp rapport over het gebruik van de ANG.³⁶ Officiële protocollen vereisen dat niet-geverifieerde gegevens door een tweede partij moeten worden gecontroleerd alvorens ze worden toegevoegd aan de ANG. Toch zijn er gevallen van dubieuze opgeslagen informatie in de gegevensbank vast te stellen.

³⁴ Corentin Debailleul. 2021. 'Pistage dans le cyberspace'. *Culture & Démocratie*. no. 53. URL: www.cultureetdemocratie.be/articles/pistage-dans-le-cyberspace

³⁵ Olivier Bailly. 'bng, la base non gérée'. *Médor*. 14/04/2021. URL: medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/bng-la-base-non-geree-25

³⁶ COC, 2023. *Rapport concernant les infractions commises par des membres de la police intégrée dans le cadre de traitements dans la bng*. Organe de contrôle de l'information policière. DIO23001. URL: www.organe-decontrôle.be/files/DIO23001_F.pdf

Er bestaat een cultuur van veronderstelde legitimiteit van opzoeken in politionele gegevensbanken en een zekere graad van soepelheid ten aanzien van de agenten die de protocollen overzien. De politie heeft slechts recentelijk archiveringsprocedures opgestart om achterhaalde gegevens te verwijderen, wat een wettelijke verplichting is.³⁷ Zoals vaak wanneer de politie van het wettelijk pad afdaalt, zijn straffen beperkt of onbestaand. Het COC legt de situatie als volgt uit:

“Als lid van Comité P [Het Vast Comité van Toezicht op de politiediensten] heb ik in 2007 or 2008 een onderzoek uitgevoerd, een analyse van alle sancties en uitspraken die aan politieagenten zijn opgelegd. En het werd duidelijk dat politieagenten in feite zeer licht werden beoordeeld door de onderzoeksinstanties en dat er vaak geen vervolging werd ingesteld.”³⁸

Een Belgische advocate en juridisch academica, Catherine Forget, constateerde dat “de ANG gegevens gedurende dertig jaar archiveert, alvorens ze definitief te verwijderen. Maar, opmerkelijk is dat in principe de gegevens die in politionele en gerechtelijke gegevensbanken zijn verwerkt gearhiveerd moeten worden wanneer ze ongeschikt, irrelevant of overbodig worden geacht, ongeacht het bewaarbeleid.”³⁹

In de praktijk worden bewaarperiodes echter vaak langdurig verlengd, wat als gevolg heeft dat gegevens voor onbepaalde duur worden bewaard zonder ze te archiveren of verwijderen.⁴⁰ De huidige functionaris voor gegevensbescherming (Data Protection Officer, DPO) van het politiekorps van Charleroi zei dat hij bij zijn aanstelling in 2014 geconfronteerd werd met duizenden onafgewerkte procedures in de ANG. Het duurde verschillende jaren om alle achterstallige procedures bij te werken.⁴¹

B. BASIS GEGEVENS BANKEN

Basis gegevensbanken worden gebruikt door de Geïntegreerde Politie om veldnotities van agenten tijdens operaties op te slaan. Zij omvatten de gegevens die voor administratieve en gerechtelijke politieprocedures worden verwerkt, inclusief kennisgeving van straf en verslagen over de gebeurtenissen, wat een brede waaier aan situaties omvat.

De ANG put uit de verslagen van de basis gegevensbanken. Dit gebeurt aan de hand van applicaties zoals:

- IsIp (Information System for the Local Police), wat gebruikt wordt om officiële processen-verbaal te encoderen;
- Feedis (Feeding Information System) voor de Federale Politie; en
- GES/Itinera, dat “alle federale onderzoeksdiensten de mogelijkheid biedt om, bijna in realtime, de status van dossiers bij het gerecht op te volgen”.⁴²

37 COC, 2023. DIO23001. *Op. Cit.*

38 Hoorzitting van het COC in het Federaal Parlement na zijn rapport over de ANG. 28/06/2023. Belgische Kamer van Volksvertegenwoordigers. Doc 55 3467/001.

39 Catherine Forget. ‘L’effacement des données policières et judiciaires : un parcours du combattant ?’. *e-legal, Revue de droit et de criminologie de l’ULB*, vol. 6, March 2022. URL: e-legal.ulb.be/medias/pdfs/178-l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant.pdf

40 *Ibid.*

41 Interview met de dpo van het politiekorps Charleroi. 3/07/2023.

42 Police Fédérale. ‘La gestion de l’information au cœur de notre organisation’. 2017 *Annual Report of the*

C. SPECIALE GEGEVENS BANKEN

Speciale gegevensbanken worden gecreëerd en gebruikt door politiedepartementen voor specifieke, toegewezen doeleinden. Volgens de wet op het politieambt:

“In specifieke omstandigheden kunnen de korpschefs, de commissaris-generaal, de directeurs-generaal en de directeurs, voor bijzondere behoeften, bijzondere gegevensbanken oprichten waarvoor ze de verwerkingsverantwoordelijke zijn, teneinde de erin vervatte gegevens verder te verwerken in het kader van de uitoefening van hun opdrachten en doeleinden van bestuurlijke en gerechtelijke politie”.⁴³

Aangaande de gebieden die speciale gegevensbanken meestal dekken, vertelt de voorzitter van het COC het volgende:

“Het kan echt alles zijn. Jeugdbendes bijvoorbeeld. Die zijn zeker aanwezig in de Brusselse regio. Er zijn zes lokale politiekorpsen in het Brussels Gewest. Hoogstwaarschijnlijk heeft elk van hen een databank specifiek voor jeugdbendes, of een databank gericht op terrorisme en/of radicalisering. Dat zijn dus allemaal mensen gekend voor bijvoorbeeld inbraak, recidivisten. Dat zijn allemaal mogelijke databanken voor wanneer het over speciale databanken gaat”.⁴⁴

Deze gegevensbanken worden vaak op lokaal niveau gebruikt, maar de Federale Politie maakt er ook gebruik van. Zo is de administratieve tak van de Federale Politie verantwoordelijk voor het opvolgen van protesten, waarvoor gegevensbanken van vermeende extreemrechtse en extreemlinkse activisten worden gebruikt.⁴⁵

Vele van deze speciale gegevensbanken bestaan onder de radar. Ze kunnen zelfs actief zijn buiten het toezicht van het COC, wiens hoofd zei:

“Ik denk dat er ongeveer 1600 van die gegevensbanken zijn waarvan we weet hebben. Maar ik ken natuurlijk niet elke specifieke gegevensbank. Er is in principe geen systeem voor directe toegang, zeker niet wat betreft directe toegang tot speciale gegevensbanken. Maar hier is het uiteindelijk de lokale politiechef die beslist wie toegang krijgt en wie niet. [...]. Dat is het grote verschil tussen de drie types gegevensbanken. Voor de basis en algemene gegevensbanken zijn ministers van Binnenlandse Zaken en Justitie verantwoordelijk voor de gegevensbescherming, maar voor de lokale, deze speciale gegevensbanken, is dat de politiechef of -directeur. [...] En dus is het voor ons natuurlijk veel ingewikkelder om goed zicht te krijgen op die speciale gegevensbanken. Er is maar één manier om dat echt te weten te komen en dat is door naar de lokale politie te gaan en hen te vragen ons deze gegevens te tonen”.⁴⁶

Het COC heeft ook kritiek geuit op het gebrek aan toezicht op en aansprakelijkheid van speciale gegevensbanken:

Federal Police. URL: police.be/5998/sites/5998/files/downloads/RA2017_web_FR.pdf

43 Art. 44/11/3. Wet op het politieambt. URL: ejustice.just.fgov.be/eli/loi/1992/08/05/1992000606/justel

44 Interview met Frank Schuermans (COC), 17/02/2023.

45 Interview met afgevaardigden van de politievakbond, 17/08/2023.

46 Interview met Frank Schuermans (COC), 17/02/2023.

“Wat speciale gegevensbanken betreft, denk ik dat het echt een probleem is, want het merendeel daarvan wordt niet geregistreerd. De politiekorpsen die hier correct mee proberen om te gaan, ondernemen die pogingen al gaandeweg. De systemen zijn zeer specifiek en soms is het niet meer dan een Excel-bestand, wat voor een groot verschil in gebruikersnamen zorgt. Maar voor ons wordt het in de toekomst een groot probleem, en daarom is het belangrijk dat we dit op orde krijgen, terwijl dat op dit moment helemaal niet het geval is”.⁴⁷

Over de mogelijkheid om zulke gegevensbanken te gebruiken, is het COC duidelijk:

“Bij proactieve audits zullen we altijd zeggen: “Geef me een lijst met al jullie speciale gegevensbanken, en leg me uit waarom die gegevensbanken nodig zijn.” En in 99% van de gevallen beginnen we met, bijvoorbeeld, 25-30 speciale gegevensbanken, [maar] is de helft daarvan verdwenen tegen dat we vertrekken of wanneer ons onderzoek is afgerond”.⁴⁸

Dit standpunt werd bevestigd door de DPO van de politie van Charleroi. Het is misschien niet verwonderlijk dat hij van mening is dat de ANG verschillende voordelen heeft: de gegevensbank is toegankelijk voor andere politiekorpsen, wordt beter beheerd op gemonitord en de ingegeven gegevens moeten worden gevalideerd. Hij meent dat speciale gegevensbanken enkel in uitzonderlijke gevallen de moeite lonen. Zo kan er in de ANG niet met *high-definition* foto's worden gewerkt. In het algemeen is de DPO van de politie van Charleroi echter van mening dat de ANG de voorkeur geniet.

Vanuit het perspectief van mensenrechten is de vraag een kansloze affaire: beide vormen van gegevensbanken brengen aanzienlijke risico's met zich mee. Kiezen tussen een buitengewoon grote gecentraliseerde gegevensbank en een slecht beheerde lokale gegevensbank is als kiezen voor de hamer of het aambeeld. Deze risico's zullen in een later hoofdstuk van dit verslag behandeld worden.

D. DE GEMEENSCHAPPELIJKE GEGEVENS BANK TERRORISME, EXTREMISME, RADICALISERINGS-PROCES (GGB T.E.R.)

De GGB T.E.R. staat politie en inlichtingendiensten toe om informatie te delen, voornamelijk in het kader van terrorismebestrijding. Volgens de operator van de gegevensbank, het Coördinatieorgaan voor de dreigingsanalyse (OCAD), is de gemeenschappelijke deler van alle individuen die zijn opgenomen in de GGB T.E.R. 'extremisme', 'terrorisme', of 'potentieel tot geweld'.⁴⁹

De GGB omvat vijf categorieën, als volgt gedefinieerd:

- “Foreign Terrorist Fighters (FTF): personen die naar een conflictgebied zijn vertrokken om er een terreurgroep te vervoegen of hiervan terugkeerden, of waarbij het vertrek is verhinderd of die de intentie hebben om dit te doen (opgenomen sinds de oprichting van de ggb in 2016);

⁴⁷ Hoorzitting van het COC in het Federaal Parlement na zijn rapport over de ANG. 28/06/2023. Belgische Kamer van Volksvertegenwoordigers. Doc 55 3467/001.

⁴⁸ Interview met Frank Schuermans (COC), 17/02/2023.

⁴⁹ ‘De Gemeenschappelijke gegevensbank Terrorisme, Extremisme, Radicaliseringsproces (GGB T.E.R.)’. OCAD. URL: ocad.belgium.be/de-gemeenschappelijke-gegevensbank-ggb-t-e-r

- Homegrown Terrorist Fighters (HTF): personen die niet de intentie hebben om naar een terreurorganisatie in het buitenland te vertrekken, maar die verkiezen om hier terroristische acties te plegen of om ze te ondersteunen;
- Haatpropagandisten (HP): personen die het gebruik van geweld willen rechtvaardigen omwille van ideologische doeleinden. Met hun invloed willen ze hun omgeving doen radicaliseren en schade toebrengen aan de rechtstaat;
- Potentieel Gewelddadige Extremisten (PGE): personen met extremistische opvattingen die ze eventueel willen concretiseren via geweld, maar die nog geen concrete stappen daartoe hebben ondernomen;
- Terrorismeveroordeelden (TV): personen die veroordeeld, geïnterneerd of onder beschermingsmaatregel geplaatst zijn voor terrorisme in België of in het buitenland”.⁵⁰

Sommige categorieën zijn duidelijk omschreven, maar anderen zijn voor interpretatie vatbaar. Het Comité Terrorismebestrijding (Comité T) stelt de graduele uitbreiding van de GGB T.E.R. naar steeds bredere en vagere categorieën aan de kaak.⁵¹ Dit is des te meer problematisch aangezien deze gegevensbank gebruikt kan worden om veiligheidsmachtigingen te geven of ontzeggen.⁵²

In 2022 waren er zo’n 700 personen opgenomen in de GGB T.E.R. De overheid beweert dat 87% van de personen op de gegevensbank “een jihadistische ideologie volgen”, 10% rechts-extremistisch zijn en 2% links-extremistisch. Anderen in de gegevensbank zijn “verscheidene bedreigingen”, waaronder “anti-establishment gevoelens ten gevolge van de coronapandemie of een buitenlandse politieke context”.⁵³

E. TECHNISCHE GEGEVENS BANKEN

De laatste categorie gegevensbanken is die van de zogenaamde ‘technische’ gegevensbanken en staat los van de andere. Deze gegevensbanken bevatten persoonlijke gegevens en informatie die automatisch worden verzameld; momenteel gebeurt dat enkel door camera’s met automatische nummerplaat herkenning (ANPR). Deze anpr-camera’s hebben rechtstreeks toegang tot de Dienst Inschrijving Voertuigen (DIV), waardoor specifieke voertuigen van belang, zoals gestolen of onverzekerde voertuigen, kunnen worden geïdentificeerd. Het COC zei onlangs dat “voor het gebruik van anpr, we niet kunnen zien wie de gegevens op welk moment heeft geraadpleegd, er is geen register, wat in feite een gerechtelijk probleem is”⁵⁴ - een understatement om te zeggen dat het illegaal is.⁵⁵

50 *Ibid.*

51 Comité T. Rapport 2021. *Comité de vigilance en matière de lutte contre le terrorisme*. pp. 18-20. URL: comitet.be/wp-content/uploads/2021/03/Comite-T-Rapport-2021-Verslag.pdf

52 Arrêté royal du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l’exécution d’une vérification de sécurité. URL: beroepsorgaan.be/images/boor/6_1/Veiligheids_verificaties_gegevens.pdf

53 ‘700 extremisten prioritair opgevolgd in ons land’. ocad. 28/07/2023. url: ocad.belgium.be/700-extremisten-prioritair-opgevolgd-in-ons-land

Europol has similar concerns at the European level. See URL: www.statewatch.org/news/2021/june/eu-growing-online-censorship-of-presumed-violent-extremism-of-all-ideological-varieties

54 Hoorzitting van het COC in het Federaal Parlement na zijn rapport over de ANG. 28/06/2023. Belgische Kamer van Volksvertegenwoordigers. Doc 55 3467/001.

55 Zie artikel 25 van de AVG. URL : eur-lex.europa.eu/eli/dir/2016/680/oj/art_25



Figuur 7. Een Macq ANPR-CAMERA (LINKS) EN OFFICIËLE BORDEN (RECHTS) IN SINT-GILLIS, BRUSSELS HOOFDSTEDELIJK GEWEST. FOTO'S DOOR CORENTIN DEBAILLEUL, CC-BY-SA.

ANPR-camera's nemen een belangrijke plaats in bij de Belgische bewakingsinspanningen. Ze zijn gerechtvaardigd voor een reeks redenen, van terrorismebestrijding tot de naleving van lage-emissiezones (LEZ). Hun dubbelzinnige doel roept vragen op omtrent functieverhuizing, d.w.z. het gebruik van een technologie buiten haar oorspronkelijke doelen. De Brusselse anpr werd ook gelijktijdig aangekondigd als antiterrorismemaatregel en als deel van de lez, met als doel vervuiling tegengaan en de gezondheid verbeteren. Al snel werden er echter vergunningen uitgeschreven voor het gebruik van de camera's voor wetshandhaving in voetgangerszones.

Door videoanalyses te combineren met technische gegevensbanken, zijn anpr-camera's een cruciaal precedent. Het zou uitermate verontrustend zijn als hetzelfde verband werd gelegd met gezichtsherkenning - wat zou neerkomen op het systematisch controleren van de identiteit van alle voorbijgangers.

2. DE RISICO'S VAN POLITIONELE GEGEVENS BANKEN: CASUSSEN

Politionele gegevensbanken dragen een ernstig potentieel tot discriminatie met zich mee vanwege de gehanteerde categorieën, de opgeslagen informatie en het gebrek aan regelgeving inzake hun bestaan, gebruik en inhoud. In de woorden van de criminoloog Jan Van Dijk: politiegegevens "reflecteren het probleem van criminaliteit zoals het wordt gezien door de ordehandhavers en de politici, aanklagers of rechters die het werk opvolgen." Deze instellingen zijn zelf "onderworpen aan hun eigen bias".⁵⁶

Volgens de wet op het politieambt kunnen de ANG, basis gegevensbanken en speciale gegevensbanken gebruikt worden om persoonlijke gegevens van personen in specifieke categorieën voor administratieve politionele en gerechtelijke doe-

⁵⁶ Van Dijk. 2009. 'Approcher la Vérité en matière de délinquance: La comparaison des données d'enquêtes en population générale avec les statistiques de police sur la délinquance enregistrée'. In: *Mesurer la délinquance en Europe*. L'Harmattan. Geciteerd in: Rémy Farge, 2020. 'Police du futur et nouvelles technologies du profilage ethnique'. *La chronique des droits humains*. pp. 13-16.

leinden te verwerken.⁵⁷

Voor administratieve redenen, omvat dit:

- De contactgegevens van vertegenwoordigers van organisaties;
- Personen die betrokken zijn geweest bij incidenten van verstoring van de openbare orde;
- Leden van nationale of internationale groepen die een bedreiging zijn voor de openbare orde;
- Personen die schade kunnen berokkenen aan anderen of eigendom die bescherming vereisen; en
- Personen onderhevig aan administratieve maatregelen uitgeschreven door een bevoegde administratieve instantie en onder politietoezicht geplaatst.⁵⁸

Advocate en onderzoekster Catherine Forget beschrijft de schadelijke gevolgen die kunnen voortvloeien uit het bewaren van informatie over personen in een politionele gegevensbank:

“Deze problematiek is relevant voor iedereen die gekend is bij de politie wanneer bepaalde informatie met betrekking tot hen in gegevensbanken worden geregistreerd, potentieel zelfs zonder dat ze hiervan op de hoogte zijn of ooit betrokken waren bij een strafrechtelijke procedure. Dit soort registraties kan niet alleen de nodige verwarring scheppen, maar kan ook rechtstreeks leiden tot onaangename of zelfs verontrustende omstandigheden voor de betrokkene. Zo kan de persoon in kwestie tot verscherpte identiteitscontroles op de luchthaven worden ontworpen, inclusief ondervragingen, of het onderwerp worden van ongerechtvaardigde fouilleringen. Het kan er ook voor zorgen dat ze geen veiligheidscertificaat voor hun professionele bezigheden kunnen verkrijgen, en zo dus de facto worden belemmerd in het uitoefenen van hun job.”⁵⁹

Het lijkt misschien schadeloos dat gegevens in deze gegevensbanken worden bewaard, maar het kan verregaande gevolgen hebben. In haar jaarverslag van 2022 stelt het COC dat:

“De kwaliteit (nauwkeurigheid en precisie) van politiedatabanken laat nog steeds veel te wensen over, met potentieel zeer schadelijke gevolgen voor burgers. Burgers kunnen rechtstreeks of onrechtstreeks schade oplopen door incorrecte, verouderde of anderszins ongepaste gegevensverwerking. Rechtstreekse schade, omdat de gegevensverwerking waaraan de burger wordt onderworpen (fouilleren, arrestatie, politietechnieken, koppeling met ANPR-technische gegevensbanken, enz.) niet correct kan zijn als deze gebaseerd is op incorrecte informatie. En onrechtstreekse schade, omdat de toegang tot bepaalde beroepen onrechtmatig wordt belemmerd of geblokkeerd [...] veiligheidsagenten, militair personeel, privé security, werknemers in kerncentrales en anderen worden allemaal beoordeeld op

57 Art. 44/5 of the Police Act. URL: ejustice.just.fgov.be/eli/loi/1992/08/05/1992000606/justel

58 Catherine Forget. ‘L’effacement des données policières et judiciaires : un parcours du combattant ?’. *e-legal, Revue de droit et de criminologie de l’ULB*, vol. 6, March 2022. URL: e-legal.ulb.be/medias/pdfs/178-l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant.pdf

59 *Ibid.*

basis van hun 'politiedossier'.⁶⁰

Comité P, het Vast Comité van Toezicht op de politiediensten, stelde verschillende gevallen vast waarin deze informatie gebruikt werd zonder de nodige voorzorgsmaatregelen.⁶¹ Bijvoorbeeld, in één van deze gevallen ging het om informatie dat een persoon hiv-positief zou zijn en zou plannen om politieagenten te besmetten tijdens een operatie. Uit het onderzoek van Comité P en het COC bleek dat het om zuivere geruchten ging, met geen wettelijke of administratieve verantwoording om ze te bewaren. De informatie werd niet volledig geëvalueerd en er was geen duidelijke reden om ze in de gegevensbank op te slaan.⁶²

Sinds de invoering van een hervorming uit 2019⁶³ hebben wetshandhavingsinstanties de toestemming om specifieke categorieën van gegevens te verwerken, inclusief gevoelige gegevens zoals gezondheids-, biometrische en genetische gegevens, als deel van hun administratieve en juridische politietaken. Dit kan ook in de context van internationale politiesamenwerking. Biometrische gegevens verwijzen naar persoonlijke gegevens over de fysieke of fysiologische kenmerken van een persoon. Het omvat bijvoorbeeld vingerafdrukken, uiterlijke gezichtskenmerken, stempatronen en oorafdrukken. Het verzamelen van zulke informatie vereist voorzichtigheid, gezien de risico's verbonden aan het bekendmaken van gevoelige informatie, zoals de etniciteit of gezondheid van een persoon.⁶⁴

We bespreken nu verschillende casussen die de specifieke risico's van het gebruik van politionele gegevensbanken illustreren. Eerst nemen we speciale gegevensbanken voor sekswerkers aan de ene kant en stedelijke 'bendes' aan de andere kant onder de loep. Daarna bespreken we de zogenaamde antiradicaliseringsmaatregelen, screenings en veiligheidsmachtigingen. We sluiten dit deel af met een analyse van recente rechtspraak die de huidige aanpak in België omtrent persoonlijke toegang tot de eigen politiedossiers aan banden kan leggen.

A. GEGEVENSbanken EN PROFILERING SEKSWERKERS

Sinds 2022 is sekswerk gedecriminaliseerd in België.⁶⁵ Het leveren van seksuele diensten was nooit an sich verboden, maar het aanzetten tot en verkrijgen van die diensten waren wel strafbaar. Daarnaast bestond er een vorm van indirecte criminalisering. Dat betekent dat iedereen die geld verdiende met sekswerk, zelfs met verschillende scheidingsniveau's, gezien werd als een pooier. Bijgevolg kon

60 COC. *Rapport d'activité 2022*. Organe de contrôle de l'information policière. URL: organedecontrôle.be/files/Rapport-dActivit%C3%A9_COC_2022.pdf

61 Rosamunde van Brakel. 2021. 'How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium'. *Surveillance & Society*, vol. 19, no. 2, pp. 228-240. URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779

62 Rapport d'activité 2003 du Comité permanent de contrôle des services de police. Belgische Kamer van Volksvertegenwoordigers en Senaat. 30/07/2004. URL: comitep.be/document/jaarverslagen/2003.pdf

63 Wet tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft. Belgisch Staatsblad. 22/05/2019. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=19-06-19&numac=2019013125

64 Catherine Forget. 'L'effacement des données policières et judiciaires : un parcours du combattant ?' *Op. Cit.*

65 Wet houdende wijzigingen aan het Strafwetboek met betrekking tot het seksueel strafrecht. Belgisch Staatsblad. 21/03/2022. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-03-30&numac=2022031330

een huisgenoot, een chauffeur, een boekhouder, etc. veroordeeld worden voor prostitutie.⁶⁶

Mensenhandel en bepaalde diensten die als misbruik worden gezien, blijven strafbaar. Desondanks laat de federale overheid in België de lokale overheden een grote vrijheid in hun regulering van de sector. Verschillende lokale regelgevingen leggen vaak beperkingen op aan het uitvoeren van sekswerk.

In Antwerpen bijvoorbeeld is sekswerk voornamelijk beperkt tot een specifieke wijk, het Schipperskwartier. Een politieteam bestaande uit 15 leden, bekend onder de naam prostitutieteam, is verantwoordelijk voor het monitoren van de wijk. De politie voert inspecties uit op sekswerklocaties en stelt strafvervolgning in voor de zwaarste overtredingen, zoals vermeende mensenhandel. Voor kleinere overtredingen zoals geluidsoverlast, grijpt de stad in door maatregelen af te dwingen zoals administratieve sancties, boetes of sluitingen als er sprake is van overlast of andere verstoringen van de openbare orde (waaronder gezondheid, veiligheid en rust).

In 2020 ontwikkelde Antwerpen een platform met de naam 'HookUp' om sekswerk te monitoren. Het doel van HookUp is om onderdrukking van sekswerkers en inmenging van tussenpersonen te voorkomen. HookUp is een platform voor de eigenaars en/of managers van sekswerkondernemingen en voor sekswerkers zelf. Een profiel aanmaken op het platform HookUp is een verplichting voor personen die een werkruimte in het Schipperskwartier wensen te huren. Ook bestaan er voorwaarden voor een bekwaamheidscertificaat en specifieke vergunningen om een ruimte te verhuren aan sekswerkers. Om die documenten te bekomen moeten aanvragers hun informatie in het aanvraagformulier van HookUp ingeven. Die informatie wordt dan tot vijf jaar lang bewaard.

De applicatie verzamelt gegevens en geeft die door aan de lokale overheden, inclusief informatie over de locatie waar sekswerkers actief zijn en wie de eigenaar is van de ruimte. De website van de stad stelt dat informatie over sekswerkers enkel toegankelijk is voor de politie, naar verluidt om hun veiligheid te kunnen garanderen.⁶⁷

HookUp biedt de politie inzichten in vervolledigde huurovereenkomsten, is bedoeld om sekswerkers een platform te geven waar ze misbruik kunnen melden en dient als een middel voor de politie om informatie uit te wisselen zoals de foto van plegers van seksueel geweld. Aanvullend gebruikt de politie het platform om de identiteit van sekswerkers te bevestigen, samen te werken met de stad met als vermeend doel het onderverhuren van ruimtes, mensenhandel en andere criminele activiteiten aan te pakken.

Maar de politie gebruikt deze gegevens voor andere doeleinden. Het staat buiten kijf dat op het eerste gezicht de veiligheid van sekswerkers verzekeren en mensenhandel bestrijden positieve doelen zijn. Maar wanneer dit gebeurt aan de hand van monitoring en bewaking, kunnen sekswerkers worden blootgesteld aan gro-

⁶⁶ Interview met de coördinator van een vereniging die sekswerkers steunt in Brussel, 04/08/2023.

⁶⁷ 'Prostitutiebeleid'. *Stad Antwerpen*. URL: www.antwerpen.be/prostitutiebeleid

tere risico's, zeker de meest kwetsbaren onder hen.

Omdat het platform door de politie wordt opgevolgd en registratie verplicht is, worden mensen met afwijkende of preciaire migratiestatus ervan uitgesloten. Antropologe Anna Di Ronco, die onderzoek doet naar politiecontrole van sekswerk in Antwerpen, schrijft dat:

“Geïdentificeerde sekswerkers worden benaderd door politieagenten die zich voordoen als cliënten. Vervolgens worden ze geregistreerd in de politiedatabank tijdens een administratieve controle die samen met de stad wordt uitgevoerd. Tijdens deze administratieve controles controleert de politie ook zorgvuldig het statuut van migrantensekswerkers (bijvoorbeeld: ‘soms, wanneer ze hier illegaal verblijven – we zijn nog steeds politie dus we moeten onze job doen [...] dan moet er worden onderzocht of ze wel in België mogen blijven’).”⁶⁸

Zoals Di Ronco aanhaalt, duwt de verplichte registratie van sekswerkers op HookUp migrantensekswerkers in Antwerpen naar minder zichtbare ruimtes. Daar kunnen ze vaak op minder steun van sociale organisaties rekenen:

“Repressieve politieacties op straat hebben er ook voor gezorgd dat sekswerkers, en in het bijzonder niet-EU-migranten zonder visum, hun activiteiten naar binnen verhuizen en online websites en apps gebruiken, wat het voor maatschappelijk werkers veel moeilijker maakt om hen te bereiken. In een reactie op het Antwerpse prostitutiebeleid opperde een maatschappelijk werker: “[He]t heeft sommige sekswerkers naar de marge geduwd, en zelfs met de beste bedoelingen [...] Te veel proberen te controleren duwt mensen altijd meer naar onzichtbare ruimtes, zoals binnen-huiskamers, appartementen, het internet, waar het voor ons als maatschappelijke organisatie natuurlijk moeilijker is om hen te bereiken”.⁶⁹

Dit staat in schril contrast met de situatie in Brussel, waar de politie zich minder zorgen lijkt te maken over de migratiestatus van sekswerkers. De coördinator van een lokale vereniging die sekswerkers ondersteunt, beschreef de relatie tussen sekswerkers en de politie in de wijk de IJzer, gelegen tussen het stadscentrum en het Noordstation:

“Er is een groot verschil tussen wat ze de ‘Playmobils’ noemen en de agenten in burger. De agenten in burger behoren tot de zedenpolitie, terwijl de ‘Playmobils’ gewone jongens van de lokale Brusselse politie zijn... Het komt erop neer dat de agenten van de zedenpolitie een zeer paternalistische relatie met de sekswerkers in Yser hebben. Maar het is geven en nemen, in andere woorden, ze komen en zeggen: “Hoe gaat het met je? Vallen mensen je lastig? Word je beroofd? Zijn er drugs? Zijn er pooiers in de buurt?” Ze vissen naar informatie. [...] We hebben vertrouwen in de zedenpolitie; zij geven niet echt om mensen zonder papieren. Dat is niet hun probleem. Hun probleem is afpersing, [...] dat is wat de zedenpolitie interesseert, en waar hun interesse ligt: de meisjes leren kennen, uitzoeken waar ze werken en hen zover krijgen dat ze vertellen wat er aan de hand is. [...] De lokale politie is verschrikkelijk, want hun houding wisselt elke week. De ene week laten ze je met rust, de week daarop vragen ze je: “Kom, verhuis” ... [...] De stadsagenten zijn dus zeer onvoorspelbaar. [...] En eigenlijk is het enige wat de meisjes in Yser vragen: “Het

68 Anna Di Ronco. 2022. ‘Law in action: Local-level prostitution policies and practices and their effects on sex workers’. *European Journal of Criminology*. Vol. 19, no. 5, pp. 1078-96. DOI: 10.1177/1477370820941406.

69 *Ibid.*

kan ons niet schelen of de politie ons komt opzoeken, we willen gewoon weten wat er aan de hand is, we willen niet elke week iets anders te horen krijgen”.⁷⁰

De decriminalisering van sekswerk verhoogt de levensomstandigheden van sekswerkers beduidend en vermindert de kans dat migrantensekswerkers onderzocht worden. De decriminalisering mag dan wel op een breed draagvlak rekenen, de meningen zijn minder uitgesproken wanneer het gaat over de regulering van sekswerk. Sommige grassroots-initiatieven voeren bijvoorbeeld al lang actie voor de erkenning van een officieel statuut voor sekswerkers, terwijl anderen er minder enthousiast over zijn. Een plaatselijke maatschappelijk werker getuigt:

“99,99% van de mensen die we hier zien, geeft geen cent om hun status als sekswerker. Ze hebben geen papieren, ze hebben geen opvang, ze hebben geen ziektekostenverzekering. Dus als we hen vertellen dat je het officiële statuut van sekswerker kan krijgen, antwoorden ze: “maar ik heb geen papieren, het kan me niets schelen.” Dus ik ben blij dat ze het statuut kunnen krijgen, als dat is wat sekswerkers willen. Maar ik steun het niet, want ik ben zelf geen sekswerker en het is niet wat de mensen die wij zien willen. Dus al die vragen over of ik mijzelf nu wel of niet als sekswerker moet opgeven, die zien we hier niet veel. Dus dan denk ik bij mezelf, met het besef dat het profiel van mensen in Antwerpen min of meer hetzelfde is [...] Ik kan me inbeelden dat de applicatie in kwestie in Antwerpen [HookUp], als je geen rijksregisternummer hebt, als je geen papieren hebt, dan weet ik niet of je je dan wel op die app gaat registreren.”.⁷¹

Een nieuwe Federale wet werd in 2024 gestemd⁷² met als doel beschermingen te voorzien voor sekswerkers. Maar die wet geeft ook toestemming om grote hoeveelheden informatie te verzamelen om sekswerk te reguleren. Onlineplatformen voor sekswerk moeten bijvoorbeeld activiteiten op hun websites registreren en op aanvraag aan de politie verschaffen. Bovendien moeten mogelijke werkgevers een vergunning aanvragen, wat de weg vrijmaakt voor een register van erkende werkgevers. Het doel om ervoor te zorgen dat plegers van seksueel geweld nooit werkgevers worden is lofwaardig, maar sekswerk krijgt ook een eigen classificatienummer (NACE-code), waardoor sekswerkers officieel geregistreerd zijn en daardoor ook traceerbaar.⁷³ Desondanks lijkt het mogelijk (en legaal) om te registreren onder een andere code en zo de mogelijke negatieve effecten van de registratie te beperken.⁷⁴

Dit nieuwe wettelijke kader vraagt om extreme voorzichtigheid. Aangezien sommigen in het Federaal Parlement voorstellen om HookUp nationaal uit te rollen,⁷⁵ moeten de principes van minimale gegevensverzameling dringend worden opgelegd en moeten er minder gegevens worden verzameld. De scheiding van administratieve en politiedossiers moet gegarandeerd worden - zeker wanneer de veiligheid van de gegevens niet gegarandeerd kan worden.

⁷⁰ Interview met de coördinator van een vereniging die sekswerkers ondersteunt in Brussel, 04/08/2023.

⁷¹ *Ibid.*

⁷² utsopi, 2024. *Belgian labor law for sex workers: what and how?* URL: www.utsopi.be/our-work/decriminalisation/cadre-du-travail

⁷³ Interview met de coördinator van een vereniging die sekswerkers ondersteunt in Brussel, 04/08/2023.

⁷⁴ Volgens een vakbondsvertegenwoordiger van sekswerkers die zo vriendelijk was feedback te geven op dit onderdeel.

⁷⁵ Vraag n°1070 op 25/02/2022 door Ben Segers, een Vlaamse sociaaldemocraat, aan de minister van Justitie. URL: www.lachambre.be/QRVA/pdf/55/55K0082.pdf

In December 2022 kreeg de stad Antwerpen nog te maken met een serieus gegevenslek toen hackers haar systemen binnendrongen. Hierop moest het stadsbestuur tijdelijk terug stappen op pen en papier voor haar activiteiten. De hackers wisten meer dan 500 gigabytes aan gegevens te bemachtigen, waaronder persoonlijke informatie, paspoorten, identiteitskaarten, financiële documenten en meer.⁷⁶ Het is onduidelijk of informatie over sekswerk gelekt is, maar de applicatie HookUp is sindsdien niet meer actief.⁷⁷ De hackers vroegen om losgeld en waarschuwden dat de gegevens zouden worden vrijgemaakt als er niet werd betaald. De hackers zijn niet gearresteerd en de gegevens werden niet breed gelekt, wat wijst in de richting dat losgeld betaald zou zijn, hoewel de burgemeester dat ontkent.⁷⁸

Het politiekorps van Zwijndrecht, in de provincie Antwerpen, kreeg ook te kampen met een cyberaanval in 2022. Het resultaat was een lek van “nummerplaten, pv’s, onderzoeksverslagen en boetes van de laatste 16 jaar”.⁷⁹ Deze incidenten tonen de kwetsbaarheid van gegevensinfrastructuren en de risico’s die gepaard gaan met centrale gegevensopslag. Ze vragen ook voor een herevaluatie van de strategieën van gegevensbeheer en bevestigen dat de beste manier om met gevoelige informatie om te gaan het beperkt verzamelen ervan inhoudt.

B. GEGEVENSbanken EN PROFILERING ‘STADSBENDES’

Begin jaren 2010, maakte de Belgische politie van zogenaamde ‘stadsbendes’ een prioriteitskwes­tie na geweld en moorden die door die groepen zouden zijn gepleegd.⁸⁰ Een centraal aspect van de politieaanpak was het opzetten van gegevensbanken over deze vermeende ‘bendes’. De gegevensbanken bevatten informatie over vermeende ‘bendeleden’ om het monitoren, surveilleren en viseren te vereenvoudigen.

De beschrijving van deze groepen als zowel ‘stads-’ als ‘bende’ berust volledig op racisme. Racistische stereotypes en angstzaai­erij woedden. ‘Bendeleden’ werden vergeleken met ‘kindsoldaten’ en ‘sociale’ programma’s werden ontwikkeld om ‘bendeleden’ te leren dat “België Afrika niet is” - hoewel de meerderheid geboren of opgegroeid was in België.⁸¹

76 Michaël Temmerman. ‘Site van hackerscollectief Play dat stad Antwerpen viseerde, plots offline gehaald’. *gva*. 21/12/2022. URL: www.gva.be/cnt/dmf20221221_95447283

77 Volgens persoonlijke uitwisselingen met een maatschappelijk werker en met de medewerker die verantwoordelijk is voor sekswerk in Antwerpen in de zomer en herfst van 2023.

78 Belga. ‘Bart De Wever affirme ne pas avoir payé de rançon après la cyberattaque ayant visé Anvers’. *rtbf*. 18/12/2022. URL: www.rtbf.be/article/bart-de-wever-affirme-ne-pas-avoir-payé-de-rançon-après-la-cyberattaque-ayant-visé-anvers-11125227

79 Ionut Ilascu. ‘Antwerp’s city services down after hackers attack digital partner’. *Bleeping Computer*. 06/12/2022. URL: www.bleepingcomputer.com/news/security/antwerps-city-services-down-after-hackers-attack-digital-partner

80 GPI. *Plan national de sécurité 2012-2015 : Veiller ensemble à une société sûre et viable*. URL: www.police.be/5998/sites/5998/files/downloads/fr/Brochures%20informatives/PNS2012-2015.pdf

81 Mireille-Tsheusi Robert. ‘« Bandes Urbaines Africaines » : Un Produit Made in Belgium’. *Politique*, 01/06/2012. URL: www.revuepolitique.be/bandes-urbaines-africaines-un-produit-made-in-belgium

Het is alom erkend dat de ‘bende’-narratieven rusten op racistische en discriminerende ideologieën en gebruikt worden door de politie om jonge mensen van etnische minderheidsgroepen te viseren.⁸² Personen die werden geïdentificeerd als deel van deze ‘probleemgroepen’ hadden een gedeeld profiel: ze bevinden zich in een kwetsbare positie en zijn het slachtoffer van discriminatie.⁸³

De parameters die bepalen wie wordt opgenomen in de gegevensbanken over ‘stadsbendes’ zijn enorm onduidelijk. In de woorden van Rémy Farge van de *Ligue des droits humains* (LDH):

“Voor de politie omvat de veel ruimere definitie elke groep mensen die openbare orde en veiligheid verstoort. Het is die laatste definitie die wordt gebruikt als een instrument voor politieonderzoek en informatieverzameling”.⁸⁴

De vraag werd voorgelegd aan de DPO van het politiekorps Charleroi. Hij erkende dat informatieverzameling over ‘bendeleden’ gebaseerd is op correlaties eerder dan op feiten:

“Strikt genomen bestaat er geen formele definitie; het is een kwestie van misdrijven die worden geregistreerd, die regelmatig door dezelfde personen of op hetzelfde grondgebied worden gepleegd en die een probleem voor de openbare orde veroorzaken. De daarna vastgestelde correlaties (feiten en personen, relaties tussen personen) worden dan aan de bevoegde magistraat voorgelegd en bijgevolg wordt de ‘bende’ gecreëerd. Dit is voornamelijk vakjargon”.⁸⁵

Die vaagheid over inclusie in gegevensbanken van ‘stadsbendes’ zorgt voor een significant risico tot discriminatie op basis van afkomst en klasse. Zoals Farge uitlegt is de informatieverzameling van de politie over vermeende ‘bendeleden’ voornamelijk gesteund op racistische bias van individuele agenten:

“Een analyse van de politionele referentiedatabank waarin deze stadsbendes zijn geregistreerd, toont dat de cijfers, locatie en telling van deze bendes ‘in perspectief moet worden geplaatst, afhankelijk van hoe politieagenten naar hen kijken.’ De telling is ook afhankelijk van de agent die het delict rapporteert: ‘Deze categorisering hangt dus af van toeval, de perceptie van de politieagent, diens aangifte of de specifieke registratie in de databank’, terwijl ‘de media deze cijfers zeer vaak gebruikt om een bepaalde stijging aan te tonen of een nieuwsbericht te illustreren.’

Politiestatistieken zijn geen weerspiegeling van de realiteit, maar een momentopname van overtredingen of misdrijven, en worden beïnvloed door veel factoren. Hun registratie is deels afhankelijk van de representaties die slachtoffers of instellingen hebben van het strafrechtstelsel: ‘In dit systeem van representaties zijn bepaalde personen of groepen bijzondere kwetsbaar omdat ze, als gevolg van complexe ideologische structuren, op een gegeven moment het gevoel van drei-

82 Patrick Williams and Eric Kind. 2019. Data-driven Policing: The Hardwiring of discriminatory policing practices across Europe. enar. URL: raceandpolicing.issuelab.org/resources/36920/36920.pdf

83 Mireille-Tsheusi Robert. “« Bandes Urbaines Africaines » : Un Produit Made in Belgium”. *Op. Cit.*

84 Rémy Farge, 2020. ‘Police du futur et nouvelles technologies du profilage ethnique’. *La chronique des droits humains*, pp. 13-16.

85 DPO van het politiekorps Charleroi in zijn geschreven antwoorden op onze enquête. 2/03/2023.

De gevolgen van geregistreerd staan als ‘bendelid’ kunnen verregaand zijn. De DPO van het politiekorps Charleroi schreef: “The fact that the photo is available allows the police officer, during a security patrol, to identify the person to be monitored, searched or stopped”.⁸⁸

Gegevensbanken over ‘stadsbendes’ dienen om onderzoek te vereenvoudigen, aldus een politieagent. De ontmenselijkende taal die gebruikt wordt is toonaangevend voor het racisme dat hier bestaat:

“Bijvoorbeeld, men steelt een handtas van een oude dame en zij vertelt ons dat het een bende van drie of vier zwarten was. Zij kan een beschrijving van één van de zwarten geven. Wij hebben er dus al één. Wie zijn dan die drie anderen? Dat weten wij niet. Wij kijken dan onze computerbestanden na en zien wat die persoon al op zijn kerfstok heeft. Mogelijkerwijs heeft hij op andere momenten strafbare feiten met anderen gepleegd. Wij tonen dan foto’s, en zo maken wij stilaan vorderingen”.⁸⁹

Zoals in recent onderzoek naar het potentieel van discriminatie van i-Police (in detail besproken in deel III) blijkt, is het Belgische strafrechtelijke systeem meermaals bekritiseerd wegens racistische praktijken, zeker wanneer het gaat over etnische profilering.⁹⁰ Het Comité voor de uitbanning van rassendiscriminatie van de V.N. (CERD) waarschuwde in 2014 dat “personen met buitenlandse origine oververtegenwoordigd zijn in het strafrechtelijk systeem, ook wanneer het gaat over de mate en lengte van opsluiting”.⁹¹

De Belgische tak van Amnesty International publiceerde een verslag over etnische profilering in 2018.⁹² Dat verslag concludeerde dat de helft van de beschouwde politieagenten het probleem van etnische profilering bevestigt. Agenten begrijpen dat een legitieme reden voor een straataanhouding vereist is, maar onduidelijke begeleiding heeft ervoor gezorgd dat de wet breed geïnterpreteerd wordt en er in sterke mate op intuïtie wordt vertrouwd. Amnesty geeft echter aan dat intuïtie vaak geassocieerd is met stereotypen.

De publicatie van het verslag van Amnesty International leidde tot publieke debatten in het Federaal Parlement.⁹³ De situatie lijkt echter nog niet te zijn verbeterd, aangezien het CERD in een verslag in 2021 nog zei dat:

86 I. Ravier *et. al.* 2016. ‘Vers une image chiffrée de la délinquance enregistrée des jeunes en Région de Bruxelles-Capitale’. *Revue de Droit Pénal et de Criminologie*, no. 2, pp. 119-133.

87 Rémy Farge, 2020. ‘Police du futur et nouvelles technologies du profilage ethnique’. *Op. Cit.*

88 DPO van het politiekorps Charleroi in zijn geschreven antwoorden op onze enquête. 2/03/2023.

89 Sylvia Bruier Desmeth, Valérie Caprasse, Jenneke Christiaens, Dominique De Fraene, Els Enhus, Carla Nagels, Sybille Smeets. 2012. *Op onderzoek naar stadsbendes. Brussel. POD Maatschappelijke Integratie; Grootstedenbeleid*, p. 13. URL: www.mi-is.be/sites/default/files/documents/stadsbendes.pdf

90 Jérémiah Vervoort, 2021. *I-Police ou l’art de prédire la discrimination*. Travail de fin d’études. Brussels: Université libre de Bruxelles.

91 cerd. 2014. ‘Concluding observations on the sixteenth to nineteenth periodic reports of Belgium’. *United Nations Committee on the Elimination of Racial Discrimination*. cerd/c/bel/co/16-19. URL: tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F16-19

92 Amnesty International Belgium. 2018. ‘You Never Know With People Like You’, URL: www.amnesty-international.be/sites/default/files/bijlagen/ethnic_profiling_executive_summary_en.pdf

93 Nawal Ben Hamou. 2019. ‘Le profilage ethnique’. *Belgische Kamer van Volksvertegenwoordigers. 54K3683001*. URL: www.lachambre.be/FLWB/PDF/54/3683/54K3683001.pdf

“De Commissie maakt zich zorgen dat etnische profilering door de politie een hardnekkig probleem in de Staat [België] blijft en dat er geen wet is die dergelijke profilering expliciet verbiedt. De Commissie maakt zich ook zorgen dat er in de praktijk een risico op misbruik is door de interpretatie van de term “redelijke gronden” die wordt gebruikt in [...] de Wet op het Politieambt, in verband met de bevoegdheden van politieagenten om identiteitscontroles uit te voeren. Verder is de Commissie bezorgd over het gebrek aan volledige gegevens, uitgesplitst naar etniciteit of nationale afkomst, over personen die het doelwit zijn van identiteitscontroles en slachtoffers van raciale of etnische profilering”.⁹⁴

Een onderzoek uit 2021 verschaft verder bewijs van dit probleem. Een etnografisch onderzoek bij twee Belgische politiekorpsen toonde dat een identiteitscontrole van een persoon voornamelijk bepaald werd door wat de politieagenten hun “buikgevoel”, “zesde zintuig” of “radar” noemen. Politie-interventies tegen iemand blijken niet enkel door hun gedrag maar ook door persoonlijke kenmerken, waaronder gender, etniciteit, leeftijd, socio-economische status en kleding, te worden bepaald. Bovendien, “vanuit een zeker ideeënkader worden bepaalde (groepen) personen met andere woorden geassocieerd met het beeld van een ‘probleemmaker’, wat in de ogen van de interveniërende inspecteurs een hardere aanpak verantwoordt”.⁹⁵

Bias beïnvloedt politieacties, waardoor bepaalde groepen vaker worden tegengehouden, gearresteerd en opgesloten. In deze omstandigheden is het moeilijk om te zien hoe het Belgische strafrechtelijke systeem kan ontsnappen aan de kritiek dat wetshandhaving met big data discriminatie met zich meebrengt.

C. GEGEVENSDISCRIMINATIE BIJ SOLLICITATIESCREENINGS EN VEILIGHEIDSMACHTIGINGEN

Medewerkers in België kunnen worden onderworpen aan een veiligheidscontrole door hun werkgever of andere autoriteiten. Die controles kunnen in verscheidene omstandigheden plaatsvinden. Ze kunnen vereist zijn voor specifieke opdrachten of taken binnen een baan of om bepaalde privileges te verkrijgen die rusten op de beoordeling van de werkgever van iemands loyaliteit, integriteit, discretie en algeheel ‘goede karakter’.

Het kan gaan om politieonderzoek, veiligheids- en administratieve gegevensbanken en kunnen een vereiste zijn voor:

- “een ‘veiligheidsmachtiging’ te verkrijgen voordat kennis mag worden genomen van gevoelige informatie;
- een ‘veiligheidsattest’ te verkrijgen voordat bepaalde functies mogen worden uitgeoefend op diplomatieke evenementen (bijvoorbeeld een Europese top) of om tijdelijk toegang te verkrijgen tot gevoelige zones (bijvoorbeeld binnen nucleaire infrastructuur);

⁹⁴ CERD. 2021. ‘Concluding observations on the combined twentieth to twenty-second periodic reports of Belgium’. *United Nations Committee on the Elimination of Racial Discrimination*. cerd/c/bel/co/20-22. URL: tinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F20-22

⁹⁵ Inès Saudelli. 2021. *Mag ik uw identiteitskaart zien? Een kwalitatief onderzoek naar identiteitscontroles uitgevoerd door de Belgische lokale politie*. PhD Dissertation. Vrije Universiteit Brussel.

- een positief veiligheidsadvies te verkrijgen om bijvoorbeeld een luchthavenbadge te verkrijgen of zich kandidaat te stellen bij Defensie”.⁹⁶

Een brede waaier aan gegevensbanken kan worden geraadpleegd voor een veiligheidscontrole, waaronder:

- Het Schengeninformatiesysteem (SIS, een gegevensbank van de EU voor politie-, gerechtelijke en immigratieautoriteiten);
- de ANG (zie eerder);
- gemeenschappelijke gegevensbanken (zie eerder);
- gerechtelijke gegevensbanken;
- Limosa (het register voor buitenlandse arbeiders);
- een gegevensbank over illegale tewerkstelling en sociale-zekerheidsfraude;
- en de speciale operationele politionele gegevensbank die ontwikkeld en beheerd wordt door de ‘Centrale directie van de bestrijding van de zware en georganiseerde criminaliteit verbonden aan terrorisme, radicalisering en extremisme’.⁹⁷

Tijdens een interview met het COC vroegen we welke soorten informatie dit kan omvatten:

“Alles. Gerechtelijke informatie, harde informatie en ook zachte (administratieve of gerechtelijke) politie-informatie. Het kan gaan over meldingen dat je verdacht werd van [het plegen van] diefstal, maar dat je nooit bent veroordeeld, of dat je een transactie [een schikking] hebt aanvaard van het Openbaar Ministerie, enz. Die informatie wordt dan gebruikt om al dan niet een vrijgave te verlenen”.⁹⁸

De website van het beroepsorgaan stelt:

“[De onderzoekers] kunnen niet alleen bestaande bestanden raadplegen, maar ook een bijkomend onderzoek uitvoeren (buurtonderzoek, bij de werkgever enz.). In dit verband kan ook een onderzoek worden gevoerd naar de partner en andere volwassenen die met de aanvrager samenwonen.”.⁹⁹

In België is deze veiligheidscontrole verplicht voor mensen die in de havens, luchthavens of kerncentrales werken,¹⁰⁰ maar ze worden steeds breder toegepast. Zelfs medewerkers van grote muziekfestivals hebben veiligheidscontroles ondergaan, zoals hieronder besproken zal worden. Er zijn talloze voorbeelden van mensen die een baan ontzegd worden door informatie die over hen te vinden is in politionele gegevensbanken.

Zo werd in 2023 aangekondigd dat havenarbeiders in Antwerpen aan doorlichtingsprocedures zouden worden onderworpen, als onderdeel van een harde aanpak van drugshandel. Hoewel het onduidelijk blijft welke gegevensbanken ge-

⁹⁶ Beroepsorgaan inzake Veiligheidsmachtigingen, –attesten of -adviezen. URL: beroepsorgaan.be

⁹⁷ Koninklijk besluit tot bepaling van de lijst van de gegevens en informatie die geraadpleegd kunnen worden in het kader van de uitvoering van een veiligheidsverificatie. 8 mei 2018. URL: beroepsorgaan.be/images/boor/6_1/Veiligheids_verificaties_gegevens.pdf

⁹⁸ Interview met Frank Schuermans (COC), 17/02/2023.

⁹⁹ Beroepsorgaan inzake Veiligheidsmachtigingen, –attesten of -adviezen. URL: beroepsorgaan.be

¹⁰⁰ Interview met Frank Schuermans (COC), 17/02/2023.

bruikt worden voor deze procedures, is het aannemelijk dat de informatie uit politionele gegevensbanken hierbij horen. In Februari 2023 stond er op de officiële website van de eerste minister dat:

“De screening van het havenpersoneel is opgestart. Het gaat om zo’n 16.000 mensen op gevoelige posten binnen de haven die door de veiligheids- en inlichtingendiensten zullen gescreend worden op linken met de georganiseerde misdaad. Dit proces is de voorbije weken opgestart. De verschillende havenbedrijven duiden veiligheidsofficieren aan die zullen optreden als contactpersoon. Zij worden momenteel onderworpen aan een grondige doorlichting door de Veiligheid van de Staat. Daarna kunnen zij de gegevens van het te screenen personeel binnen hun bedrijf overmaken”.¹⁰¹

Dit scenario presenteert een grote uitdaging voor de gelijke rechten van burgers, zeker wanneer een screening verplicht wordt om toegang te krijgen tot steeds meer diensten en kansen. Het feit dat werkgevers toegang hebben tot politionele gegevensbanken, zij het indirect, brengt ook een enorm potentieel voor discriminatie met zich mee. Dit wordt goed geïllustreerd door de volgende getuigenis van een jonge man, die geen baan kreeg in een lokaal jeugdcentrum door de informatie die over hem in gegevensbanken van de politie te vinden is:

“Ik ben een man van 22. Drie jaar geleden werd ik slachtoffer van een steekpartij. Uit het niets werd ik neergestoken. Dat was niet alleen lichamelijk maar vooral mentaal een zware klap. Om daar bovenop te komen heb ik heel veel gehad aan mijn jeugdwerking. Ik ga daar al een achttal jaar heen. De laatste jaren ben ik van dichtbij betrokken bij een project waarbij we ingezet worden als steward op evenementen in de buurt. Ik doe dat heel graag en krijg veel verantwoordelijkheid. Ik vind het super belangrijk om mensen een veilig gevoel te geven omdat ik mij zelf zo onveilig gevoeld heb. [...]”

Al vier jaar lang doe ik vrijwilligerswerk bij een jongerencentrum van de stad als steward. Deze zomer solliciteerde ik voor een functie als verantwoordelijke. Via mail kreeg ik te horen dat ik was aangenomen. Maar de dag voor ik mijn contract ging tekenen, vertelde de coördinator me dat ik niet kon beginnen. Ik was niet door de screening geraakt. Hij verwees mij door naar een agent van de lokale politie, maar die kon mij niets meer vertellen dan dat de screening negatief was.

Toen mijn jeugdwerker ging polsen bij zijn contacten bij de politie, lieten die zelfs weten dat er geen screening gebeurd was. Het ergste was dat ik wel aan de slag mocht als steward in het jongerencentrum. Ik heb dat dan toch maar gedaan omdat ik het heel graag doe en al mijn vrienden ook naar het jongerencentrum komen.

Ik heb daar nooit iets van op papier gekregen. Ik heb geen strafblad en ben nooit met de politie in aanraking gekomen. Behalve één keer lang geleden, toen ik nog minderjarig was. Ik was toen met mijn oudere broer op stap in de buurt om inkopen te doen. Tegelijkertijd was er een verboden betoging aan de gang van een extremistische islamitische organisatie. We werden ingesloten door de politie. Mijn broer mocht naar huis gaan omdat hij toen werkte als journalist en een perskaart kon voorleggen. Ik werd meegenomen naar het politiebureau en moest nadien bij een GAS-ambtenaar komen. Die gaf me een werkstraf.

¹⁰¹ ‘Nationale drugscommissaris en meer politie in Antwerpse haven in strijd tegen drugsmafia’. 16/02/2023. URL: premier.be/nl/nationale-drugscommissaris-en-meer-politie-antwerpse-haven-strijd-tegen-drugsmafia

Ik heb nooit de bedoeling gehad om mee te betogen. Ik was gewoon op de foute plek op het foute moment. De GAS-ambtenaar heeft mij toen nog gezegd dat dit sowieso van mijn strafblad zou verdwijnen. Ik denk toch dat ik nu ergens in een databank zit en dat ik daarom niet door de screening geraak. Ook als ik naar het buitenland reis met het vliegtuig halen ze steeds mij uit de rij voor een controle en zeggen ze mij dat ik geseind sta.

In september ben ik van plan om mij in te schrijven voor de security-opleiding. Ik ben heel bang dat ik daar ook niet door de screening geraak. Het is nochtans mijn droom om in de veiligheidssector te werken.

Heel deze situatie raakt mij enorm. Ik vind dat de samenleving ondankbaar is. Ik heb al zo hard mijn best gedaan voor jongeren en het jeugdwerk. Ik heb al zo veel vrijwilligerswerk gedaan voor de stad. Gelinkt worden aan terrorisme doet pijn".¹⁰²

Deze getuigenis benadrukt de zware gevolgen van racistische en islamofobe vooroordelen bij de politie, die weerspiegeld worden in politionele gegevensbanken. De jongeman werd onterecht geregistreerd in een politionele gegevensbank en verbonden aan terrorisme door zijn huidskleur en omdat hij een moslim was of vermeend werd een moslim te zijn. Zijn ervaringen tonen ook hoe zulke gegevens in de gegevensbanken aanwezig blijven. Jaren na de gebeurtenissen zorgt de informatie die er over hem in te vinden is tot ondervragingen en fouilleringen in luchthaven en heeft het een invloed op zijn kansen op de arbeidsmarkt. Het verhaal benadrukt de verregaande schade die politionele gegevensbanken kunnen veroorzaken door bestaande discriminatie en onrechtvaardigheid te versterken.

D. GEGEVENSSCREENING VOOR 'TERRORISMEBESTRIJDING'

Naast de screening voor veiligheidsmachtigingen voert de politie ook bepaalde preventieve en geautomatiseerde analyses uit. Over dit onderwerp is maar beperkt informatie beschikbaar. In 2018 verklaarde een woordvoerder van de Federale Politie echter dat:

"Onze politie- en inlichtingendiensten gebruiken nu al software, zoals Radix en Vera 2, om risico's en dreigingen in de strijd tegen het terrorisme in te schatten. Daarvoor worden parameters en namen van verdachten tegen elkaar afgewogen om prioriteiten te kunnen stellen. Onze diensten gebruiken dezelfde parameters als die in andere landen, weliswaar aangepast aan de nationale context en met andere namen voor de tools, zoals Kim in Nederland en RADAR-iTE in Duitsland".¹⁰³

Deze kwesties kwamen naar de voorgrond na de aanslagen in Parijs in november 2015 en in Brussel in maart 2016. Maatregelen voor antiradicalisering werden in België ingevoerd onder het voorwendsel de nationale veiligheid te vrijwaren. Ze hebben een verregaande impact op individuen gehad. Nadia Fadil, professor sociologie aan de KU Leuven, coördineerde een onderzoek naar de effecten van antiterreurprocedures op moslims in België. Die gevolgen gaan onder andere

¹⁰² Geciteerd in Nina Henkens en Ikrame Kastit. *Het deradicaliseringsbeleid anders bekeken: Radicaal voor kinderrechten. Uit de Marge*. 2019. p. 26-27. URL: www.uitdemarge.be/?sdm_process_download=1&download_id=5743

¹⁰³ Lars Bové. 'Politie gaat criminaliteit via data voorspellen'. *De Tijd*. 30/08/2018. URL: tijd.be/politiek-economie/belgie/federaal/politie-gaat-criminaliteit-via-data-voorspellen/10044356.html

over negatieve veiligheidsbeoordelingen, obstakels in de toegang tot financiële diensten, weigering aan de grenzen, meerdere politie-invalen en overmatige identiteitscontrole.

Die voortdurende buitensporige controles zijn een vorm van voortdurende bewaking en intimidatie die niet alleen het persoonlijke leven van de betrokkenen verstoort, maar ook inbreuk maakt op hun burgerlijke vrijheden. Zulke praktijken zijn niet alleen een inbreuk op persoonlijke vrijheden en privacy, maar creëren ook een sfeer van angst en wantrouwen.¹⁰⁴

In veel gevallen was de eerste aanstoot voor de politie het feit dat een individu kennissen, vrienden of familieleden had die naar Syrië waren afgereisd en verdacht werden betrokken te zijn met Daesh (ook bekend als IS). Deze aanpak van schuld door associatie heeft onjuist personen verstrikt die mogelijk zelf niet betrokken waren.

Daarnaast is de aansluiting bij verenigingen, zeker activistische groepen voor sociale gerechtigheid of met kritische standpunten, ook een vertrekpunt om personen te viseren. Hiermee wordt een andere mening gegroepeerd met 'extremisme' en wordt het fundamentele recht op vrijheid van vereniging ondermijnd.¹⁰⁵ Verder contacteerde Comité T (het onafhankelijke Comité Terrorismebestrijding) advocatenbureaus die in beroep gingen tegen weigeringen van veiligheidsmachtingen. Ze benadrukten dat er bij de betrokken groep personen een "oververtegenwoordiging van mensen met een Belgisch-Marokkaanse of Noord-Afrikaanse afkomst" was, "zeker wanneer het gaat om luchthavenarbeiders".¹⁰⁶

De gevolgen van zulk beleid van vooroordelen zijn verregaand en gevarieerd. Betrokken personen hebben financiële verliezen geleden en konden maar moeizaam een baan vinden door de weigering van financiële dienstverlening. Die financiële tegenspoed versterkt hun vatbaarheid voor schade en marginalisatie.¹⁰⁷

Een ander verslag van Nadia Fadil en andere academici geeft aan dat het concept 'radicalisering' zelf kritisch bekeken moet worden. Professionals in het veld van preventie staan sceptisch tegenover de term en de toepassing ervan, wat wijst naar de nood voor een herevaluatie:

"De bevroegde actoren staan overwegend kritisch ten aanzien van het thema radicalisering. Ze geven aan dat dit discours bijdraagt tot de stigmatisering van jongeren, en stellen vragen bij het gegeven dat radicalisering een gevaar of probleem zou zijn. Enkel verdedigen, bijvoorbeeld, het recht van jongeren om zich tegen de samenleving te keren, om rechten op te eisen, of om problemen aan te kaarten, zonder dat dit onmiddellijk als gevaarlijk wordt gezien. Ook plaatsen praktijkwerkers vraagtekens bij de vroegdetectie van radicalisering. Ze hebben namelijk bedenkingen bij de wenselijkheid en mogelijkheid van vroegdetectie: niet alleen kan

104 Nadia Fadil, Arthemis Snijders, Kaoutar Boustani Dahan, Lore Janssens. 2022. Entre droits fondamentaux et surveillance: Les effets secondaires de la lutte contre la radicalisation sur les musulmans belges. Rapport de recherche. KU Leuven. ISBN: 9789071047244.

105 *Ibid.*

106 Comité T. Rapport 2021. *Op. Cit.* p. 41.

107 Fadil *et al.*, 2022, Entre droits fondamentaux et surveillance, *Op. Cit.*

het de vertrouwensrelatie hypothekeren, ook wordt er geopperd dat het profiel vaag is en gebaseerd is op stereotypen of karikaturen. Bovendien wordt een inschatting als een moeilijke tot onmogelijke opdracht gezien”.¹⁰⁸

Er bestaat een significant risico dat deze problemen meer zullen voorkomen in de toekomst. Lokale autoriteiten staan op het punt een nieuwe aanpak in te voeren, waarin ze politieverlagen in overweging nemen wanneer ze beslissen vergunningen voor handelsruimtes en bedrijven te verwerpen, schorsen of in te trekken of de ruimtes te sluiten.¹⁰⁹

Verder kan over de efficiëntie van wijdverspreide monitoring worden gedebatteerd. Veiligheidsdiensten screenen al jaren de gegevens van mensen die via het luchtruim reizen en verwerken de gegevens van tientallen miljoenen passagiers. Een verslag van het COC identificeert tal van problemen bij deze aanpak en stelt in vraag of deze “gigantische inbreuk op onze privacy” werkt in de strijd tegen terrorisme en georganiseerde misdaad.¹¹⁰ Het is ook illegaal volgens het precedentenrecht van het Europese Hof van Justitie en het Belgisch Grondwettelijk hof.¹¹¹

Als laatste maken deze screenings, ontworpen om veiligheid en geschiktheid te garanderen, gebruik van een grote hoeveelheid informatie. Er bestaat echter bezorgdheid over de waarheidsgetrouwheid van deze informatiebronnen. Sommige dossiers worden gegenereerd voor inlichtingendoeleinden en kunnen ongegronde of niet-bewezen implicaties, voorspellingen en inferenties bevatten. De kern van het probleem is de oorsprong van deze mogelijks onbetrouwbare bronnen, die vaak komen van wetshandhavinginstanties of inlichtingendiensten. Dat zorgt voor een dilemma. Individuen hebben geen directe toegang tot deze bronnen, waardoor ze foutieve informatie niet kunnen rechtzetten.

E. HET INDIRECTE RECHT OP TOEGANG AANVECHTEN

Het recht op toegang tot politionele gegevens is opgenomen in artikel 14 van de Europese ‘richtlijn gegevensbescherming bij rechtshandhaving’ - het equivalent van de AVG voor rechtshandhaving.¹¹² Artikel 14 stelt dat mensen het recht moeten hebben om “van de beheerder [van de gegevens] bevestiging te krijgen of persoonlijke gegevens al dan niet verwerkt worden en, wanneer dat het geval is, toegang te krijgen tot die persoonlijke informatie”, naast een lijst van informatie over zulke gegevens. Dit toegangsrecht stelt burgers in staat om zich te berusten

108 Lore Janssens, Nadia Fadil & Maryam Kolly. 2022. ‘Tussen geheimhouding en informatiedeling: De onderhandeling van het beroepsgeheim en informatiedeling in de aanpak van gewelddadige radicalisering’. Onderzoeksrapport *KU Leuven*. ISBN: 9789071047213. pp. 28. URL: <https://soc.kuleuven.be/anthropology/files/FARapport2-web-NL>

109 Projet de loi relatif à l’approche administrative communale, à la mise en place d’une enquête d’intégrité communale et portant création d’une Direction chargée de l’Évaluation de l’Intégrité pour les Pouvoirs publics. URL: lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=55&dossierID=3152

110 Lars Bové. ‘Waakhond betwijfelt of screening vliegtuigpassagiers doeltreffend is’. *De Tijd*. 28/12/2022. URL: [tijd.be/politiek-economie/belgie/algemeen/waakhond-betwijfelt-of-screening-vliegtuigpassagiers-doeltreffend-is/10437318.html](https://www.detijd.be/politiek-economie/belgie/algemeen/waakhond-betwijfelt-of-screening-vliegtuigpassagiers-doeltreffend-is/10437318.html)

111 La loi belge PNR « Passenger Name Record » recadrée par la Cour de justice de l’Union européenne. *Ligue des droits humains*. URL: www.liguedh.be/la-loi-belge-pnr-passenger-name-record-recadree-par-la-cour-de-justice-de-lunion-europeenne

112 ‘Law Enforcement Directive’. *EUR-Lex*. 27/04/2016. URL: data.europa.eu/eli/dir/2016/680/oj

op hun recht op gegevenswissing en rectificatie.¹¹³

Het toegangsrecht is in principe direct. België gebruikt echter indirecte toegang tot gegevens voor politiedoeleinden, in tegenstelling tot de meeste andere Europese landen. Dat betekent dat toegangsverzoeken worden ingediend bij het COC in plaats van de gegevensbeheerder of verwerker. Volgens artikel 42 van de Belgische Gegevensbeschermingswet geeft het COC de aanvrager enkel de informatie dat “de nodige controle is uitgevoerd”.¹¹⁴ Er bestaat geen wettelijk recht om de gegevens zelf te zien. Zulke beperkingen op toegang zijn zo ingrijpend dat ze het toegangsrecht in wezen tenietdoen.

Deze problematische situatie werd voor het Europese Hof van Justitie (EHJ) gebracht. De zaak werd opgestart door een persoon die niet aan de slag mocht bij een muziekfestival na een veiligheidsscreening. Advocate Catherine Forget, samen met de *Ligue des droits humains (LDH)*, vertegenwoordigde de eiser en behaalde een belangrijke overwinning bij het ehj. Uiteindelijk werd duidelijk dat de persoon werd geweigerd op basis van informatie over de deelname van de eiser bij tien betogingen (zonder daarbij wettelijk te zijn gearresteerd).

De aanklager gebruikte zijn toegangsrecht via het COC, dat antwoordde dat “alle controles zijn uitgevoerd”. Bijgevolg kon de aanklager zich niet bewust zijn van, laat staan ingaan tegen, de telastlegging. Bovendien blijft het onduidelijk waarom zijn uitoefening van een fundamenteel recht - het recht op betoging - werd opgenomen in een gegevensbank van de politie.

Het vonnis van het ehj was dat deze vorm van indirecte toegang tot politionele gegevensbanken ingaat tegen de Europese wetgeving.¹¹⁵ Het indirect uitoefenen van rechten was initieel bedoeld als een extra bescherming, waardoor rechten konden worden uitgeoefend wanneer beperkingen van toepassing zijn. Door er de enige vorm van verhaalrecht van te maken werd het toegangsrecht ondermijnd. Bijgevolg moet de Belgische staat de wet aanpassen om deze kwestie recht te zetten.

113 Art. 16 of Directive 2016/680. url: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

114 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. url: etaamb.openjustice.be/fr/loi-du-30-juillet-2018_n2018040581.html

115 ehj. Zaak C-333/22. Arrest van het hof (Vijfde kamer). *Curia*. 16/11/2023. url: curia.europa.eu/juris/document/document.jsf?text=&docid=279747&pageIndex=0&doclang=NL&mode=req&dir=&occ=-first&part=1&cid=874087

3. DE TOEKOMST VAN BELGISCHE POLITIONELE GEGEVENS BANKEN

Nadat het COC een erg kritisch verslag publiceerde over het beheer van gegevensbanken van de politie,¹¹⁶ werd het COC uitgenodigd in het Federaal Parlement om de kwestie te bespreken. Tijdens deze aangelegenheid presenteerde voorzitter Frank Schuermans de belangrijkste bevindingen:

- De IT-systemen van de politie dateren van “prehistorische” tijden en vragen enorm veel onderhoudswerk;
- er is een gebrek aan standaardisering en duidelijke richtlijnen. De verschillen in informatiebeheer tussen politiekorpsen zijn hierdoor erg groot. Sommige afdelingen en politiekorpsen hechten er veel belang aan terwijl er bij anderen nog veel moet gebeuren;
- bestaande opleidingen in politiescholen volstaan niet. Er bestaat geen curriculum, geen syllabus over gegevensbescherming. Daardoor zijn nieuwe rekruten onvoldoende opgeleid over de kwestie;
- er is een gebrek aan expertise bij de leidinggevendenden. Er zijn nog steeds lokale politiekorpsen zonder DPO of waar de DPO ook een andere rol uitoefent, zoals DPO en directeur operaties of IT-manager, wat voor een belangenconflict zorgt.¹¹⁷

Zoals hierboven is aangetoond, worden raciale en gemarginaliseerde groepen en individuen geconfronteerd met discriminatie en meer strafrechtelijke en andere gevolgen vanwege de gegevens in politionele gegevensbanken. Dit is bij uitstek het geval in de context van politieprocedures voor ‘bendes’ en terrorismebestrijding. Na het kritische verslag van Amnesty International in 2018¹¹⁸ volgden er debatten in het Federaal Parlement over etnische profilering bij de politie.¹¹⁹ Vandaag is er echter onvoldoende politieke wil om de uitdagingen van het beheer van gegevensbanken en de discriminerende gevolgen voor de meeste gemarginaliseerden van gegevensgestuurde wetshandhaving aan te kaarten.

116 COC, 2023. DIO23001. *Op. Cit.*

117 Hoorzitting van het COC in het Federaal Parlement na zijn rapport over de ANG. 28/06/2023. Belgische Kamer van Volksvertegenwoordigers. Doc 55 3467/001.

118 Amnesty International. 2018. Belgique : Le profilage ethnique, injuste et inefficace. URL: www.amnesty.be/infos/actualites/article/belgique-profilage-ethnique-injuste-inefficace

119 Nawal Ben Hamou. 2019. ‘Le profilage ethnique’. *Belgische Kamer van Volksvertegenwoordigers*. 54K3683001. URL: www.lachambre.be/FLWB/PDF/54/3683/54K3683001.pdf

III. Het federale project ‘i-Police’

Het project i-Police is een centraal aandachtspunt in dit verslag over ‘voorspellende’ en gegevensgestuurde wetshandhaving. Het federale project geniet van aanzienlijke subsidies en heeft verschillende implicaties voor de burgerlijke vrijheden en mensenrechten.

De commissaris-generaal van de Federale Politie zei in een officiële aankondiging aan de minister van Binnenlandse Zaken:

“i-Police zal van de Belgische politie één van de meest vooruitstrevende politiediensten in Europa maken inzake data-governance. Het systeem zal informatie analyseren, automatisch informatie ter beschikking stellen van politiediensten, onderzoeksvoorstellen doen en tal van tijdbesparende hulpmiddelen mogelijk maken, zoals automatische vertalingen. Met i-Police effenen we het pad naar een toekomstgerichte Geïntegreerde Politie en dat voor de burgers van wie wij ten dienste staan”.¹²⁰

In diezelfde aankondiging lezen we:

“i-Police zorgt voor een automatische analyse en kruising van data, zoals camerabeelden, foto’s, vingerafdrukken, sporen, documenten, ... Hierdoor worden criminaliteit en criminaliteitsfenomenen sneller en duidelijker in beeld gebracht. Onderzoekers ontvangen in real time een schat aan gefilterde informatie en kunnen snel en gericht optreden. [...] Daarnaast biedt het systeem de burgers garantie op privacy en op een transparante monitoring. Politied medewerkers krijgen een beperkte en gecontroleerde toegang tot gegevens van burgers, op basis van hun functie en opdracht op dat moment”.¹²¹

De eerste vermelding van het project i-Police die we konden vinden gaat terug naar de algemene beleidsnota van de minister van Binnenlandse Zaken van 2013. In die nota staat dat i-Police als doel heeft de IT-systemen van de Federale Politie (FEEDIS) en de lokale politie (ISLP) te harmoniseren aangezien beide achterhaald waren - en zijn - en hoge onderhoudskosten met zich meedragen.¹²² Islp werd aan het begin van de jaren 1990 ontwikkeld en feedis aan het begin van de jaren 2000.¹²³

Een haalbaarheidsstudie voor i-Police werd in 2014 uitgevoerd en daarmee vergrootte het opzet van het project. De minister van Binnenlandse Zaken zei in de beleidsnota van 2015:

“Het doel is via sensornetwerken, lokaal en federaal intelligent vergaarde informatie te integreren met bestaande (authentieke) gesloten en open bronnen en

120 Annelies Verlinden. *i-Police: de toekomst van de politie is digitaal*. 07/05/2022. URL: verlinden.belgium.be/nl/i-Police

121 *Ibid.*

122 Joëlle Milquet. *Algemene beleidsnota – Federale politie en geïntegreerde werking*. Belgische Kamer van Volksvertegenwoordigers. 6/11/2013. 53K3096012. URL: www.lachambre.be/FLWB/pdf/53/3096/53K3096012.pdf

123 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*.

vervolgens deze informatie maximaal te exploiteren door ze te verwerken met geautomatiseerde intelligente tools. Het uitrusten van de politie met “next generation” technologie in de politionele keten maakt intelligent policing, i.e. een fusie van gemeenschapsgerichte, probleemoplossende en informatiegestuurde politiezorg, mogelijk”.¹²⁴

In 2016 maakte de Belgische federale overheid geld vrij om de systemen van i-Police op te starten en alle politiegegevens binnen een cloud-infrastructuur te centraliseren. De operationele lancering van het systeem stond gepland in 2020 en zou het resultaat zijn van een samenwerking tussen de ministeries van Binnenlandse Zaken, Digitale Agenda en Justitie.¹²⁵ In het nationaal veiligheidsplan 2016-2019 stond:

“In het domein van de intelligent policing werkt de federale politie aan een nieuwe innovatieve oplossing (i-Police) waarbij de huidige mainframe verlaten wordt ten voordele van nieuwe en moderne technologieën. Ze moeten een betere koppeling, uitwisseling en analyse van informatie mogelijk maken en op een snelle manier. De politie moet immers kunnen werken en handelen op basis van een integrale analyse van gestructureerde en niet-gestructureerde informatie, van intern en extern beschikbare informatie”.¹²⁶

In september 2018 publiceerden de Federale en lokale politie een gemeenschappelijk persbericht waarin de plannen voor ‘predictive’ policing als deel van i-Police uit de doeken werden gedaan.¹²⁷ Ze voorzagen experimenten rond ‘predictive’ policing in Antwerpen en bij andere lokale politiekorpsen na de gemeenteraadsverkiezingen op 14 oktober 2018. Gegevens zouden van politionele gegevensbanken gehaald worden, inclusief de frequentie van specifieke misdrijven in specifieke gebieden. Externe gegevensbronnen werden even significant geacht.¹²⁸



Figuur 8. Logo i-Police¹²⁹

bron: *Rapport annuel 2022 de la Police Fédérale*, p. 82.

124 Jan Jambon. *Algemene beleidsnota – Federale politie en geïntegreerde werking*. Belgische Kamer van volksvertegenwoordigers. 4/11/2015. 54K1428004. URL: www.lachambre.be/FLWB/PDF/54/1428/54K1428004.pdf

125 Rosamunde Van Brakel. *Automating Society 2019: Belgium*. Op. Cit.

126 gpi. *Nationaal veiligheidsplan 2016-2019 : Samen, naar de kern van de zaak*. p. 86. URL: www.politie.be/5998/sites/5998/files/downloads/NVP2016-2019.pdf

127 Kathleen Heylen. ‘Politie wil in de toekomst criminele feiten “voorspellen” via algoritmes’. *VRT news*. 30/08/2018. URL: www.vrt.be/vrtnws/nl/2018/08/30/politie-wil-criminele-feiten-kunnen-voorspellen-aan-de-hand-van

128 Rosamunde van Brakel. *Automating Society 2019: Belgium*. Op. Cit.

129 According to a Senior Advisor r&d and ict Strategy Belgian Federal Judicial Police, the central orange line symbolises the collection of data; the light blue line the creation of value from it; while the whole process is protected by the thick dark blue shield.

In 2021 publiceerde de Federale Politie de aankondiging van de gegunde opdracht¹³⁰ voor het project. Het Franse IT- en consultancybedrijf Sopra Steria¹³¹ zou €300 miljoen krijgen over een periode van zeven jaar (2021-2027). Het zou vier jaar duren om het systeem te bouwen, waarna het contract nog drie jaar onderhoud dekte.¹³²

De aanbesteding voor het project omvatte een fictief scenario van een dag in het leven van 'Jan', een politieagent in een fictief politiekorps. De intentie om 'i-Police' uit te werken tot een programma van *'predictive' policing is duidelijk*:

"Op [het] scherm komt ook een 'pop-up' om te zeggen dat er een 'anomalie', iets vreemds dus, is vastgesteld. De politietoepassing merkte op dat er een hoog aantal fietsdiefstallen geregistreerd staan rond een bepaald punt en rond bepaalde tijdstippen. Het systeem kan dit herkennen omdat onze 'data scientists' in Brussel het systeem geprogrammeerd hebben om dit soort 'anomalieën' te herkennen. [...] Voorlopig plant [de hoofdinspecteur] een recurrente patrouille in".¹³³

Elders wordt er in de aanbesteding een 'preventief' plan voor het politiedistrict besproken:

"Via de geïnformatiseerde analyse van een aantal recente incidenten, verkeersongevallen, en de opening binnenkort van een nieuwe kmo-zone [kleine of middelgrote ondernemingen], wordt een 'predictive' model uitgewerkt en een plan opgezet voor preventief toezicht op de kmo-panden".¹³⁴

Later in de aanbesteding wordt een ander type 'voorspellende' toepassing voorgesteld:

"De dienst interventie en directie Operaties organiseren met enkele naburige politiezones een actie op vrijdagavond om een grootscheepse controle te doen in cafés en discotheken omdat er de laatste tijd een stijging is gerapporteerd op het aantal mesgerelateerde misdrijven op vrijdagavond".¹³⁵

Het systeem staat ook een grondigere opvolging van 'verdachte' personen toe:

"Jan krijgt op het einde van de dag nog een telefoontje van een onderzoeker uit Brussel. Uit zijn tekstbericht dat hij dicteerde bij een woonstcontrole, bleek dat er een ander persoon aanwezig was in dat huis. Deze persoon wordt opgevolgd in het kader van een terreuronderzoek. De collega uit Brussel – die een 'digitaal abonnement' had genomen op de persoon die Jan was tegen gekomen – wil graag van Jan wat extra info gezien hij automatisch een 'alert' had gekregen dat Jan, wijkagent in een zone ergens te lande, deze persoon toevallig was tegengekomen in het kader van zijn controles".¹³⁶

130 'i-Police tender'. *Tenders electronic daily*. 2021. URL: ted.europa.eu/udl?uri=TED:NO-TICE:675394-2021:TEXT:FR:HTML&src=0&tabId=4

131 Sopra Steria company. URL: www.soprasteria.be

132 Antwoord van minister Verlinden op vraag 1323 door Yngvild Ingels, Vlaams-nationalistisch lid van het Federaal Parlement.. 14/07/2022. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrv&language=fr&cfm=qrv&Xml.cfm?legislat=55&dossierID=55-B089-1192-1323-2021202215762.xml

133 GPI. 2020. *i-Police Selectiedossier*. Bijlage H. p. 35.

134 *Ibid*, p. 34.

135 *Ibid*, p. 35.

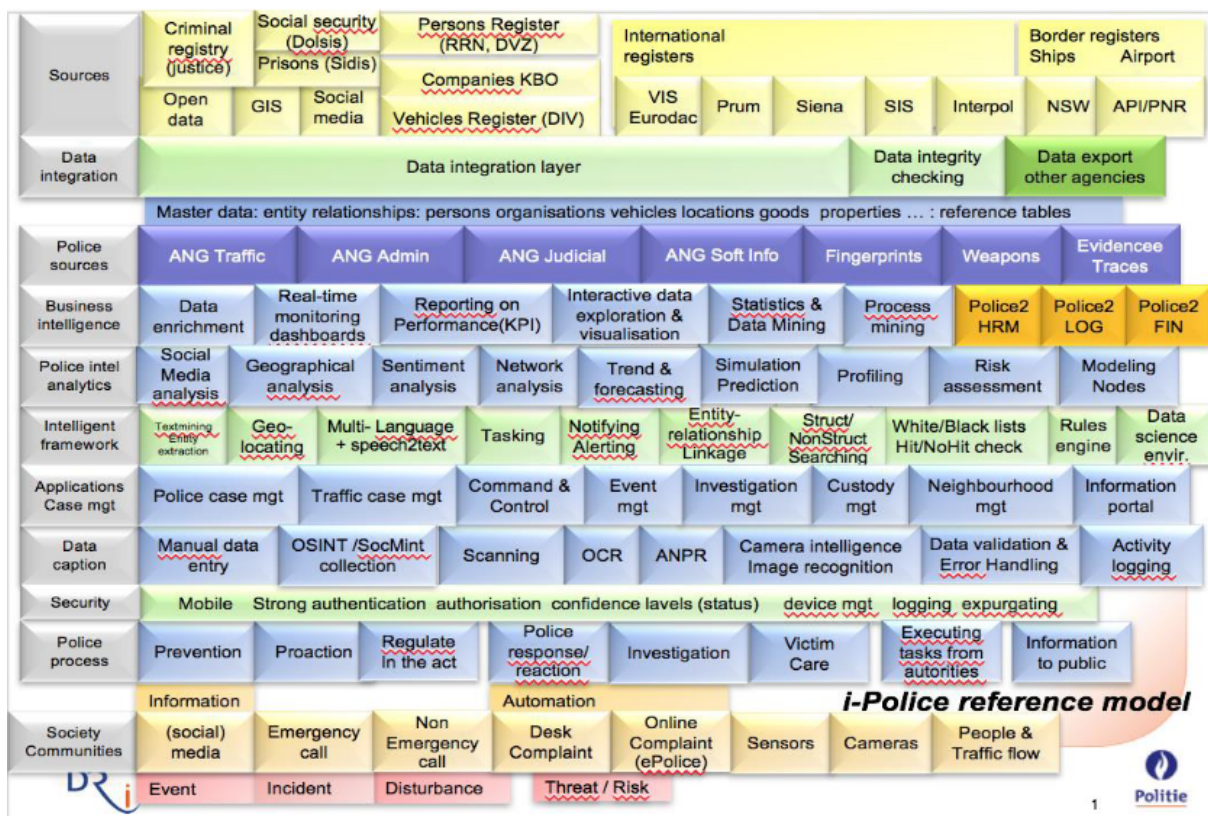
136 *Ibid*, p. 34-35.

1. GEGEVENS I-POLICE

Belgische politionele gegevensbanken zullen het toekomstige i-Police-programma voeden, naast vele andere gegevensbronnen. De aanbesteding voor i-Police bevat een fictief scenario na een identiteitscontrole:

“Hun systeem controleert automatisch 10 controle databanken (Rijksregister, politiedatabanken van binnen- en buitenland, gevangenenissen, foreign fighters,...) en geeft onmiddellijk aan op welke identiteiten er een ‘hit’ is”.¹³⁷

De politie plant om een brede waaier aan gegevensbronnen te integreren in i-Police, zoals in onderstaande figuur weergegeven.



Figuur 9. Toekomstige “business architecture” van het project i-Police

bron: aanbesteding i-Police Appendix H, p. 58.

Zowel de omvang als de types gegevens zijn onrustwekkend. Gegevens van verschillende gegevensbanken zullen worden samengebracht in een ‘data lake’: een bewaarplaats die meerdere bronnen gebruikt maar alle gegevens in hun originele formaat bewaart.

De politionele gegevensbanken maken meestal een onderscheid tussen ‘gevalideerde’ en ‘niet-gevalideerde’ informatie. ‘Gevalideerde’ informatie is geverifieerd, ‘niet-gevalideerde’ informatie is dat niet. De voorzitter van het COC heeft zijn bezorgdheden geuit over de combinatie van nagetrokken en niet nagetrokken informatie in het ‘data lake’ van i-Police:

¹³⁷ Ibid, p. 36.

“Er is ook veel niet-gevalideerde informatie. [...] Binnen het nieuwe concept van i-Police dreigt dat verschil tussen gevalideerde en niet-gevalideerde informatie, vrees ik, te verdwijnen in een data lake. De gemiddelde politieagent [...] zal dus toegang krijgen tot veel meer informatie en veel meer niet-gevalideerde informatie, wat natuurlijk een enorme zorg is, en niet alleen voor de persoon (de vermeende verdachte) zelf, maar ook voor het rechtssysteem als geheel. Het is een enorme zorg voor iedereen. [...] Maar dat is duidelijk de weg die niet alleen de politie, maar ook de politiek en de ministers, [...] willen inslaan: geef elke politieagent op elk moment zoveel informatie als hij nodig heeft [...]. In ons systeem is het heel goed mogelijk [...] [dat] je bent vrijgesproken door de rechtbank, maar nog steeds in de gegevensbank te vinden bent. En als je dan een politieagent tegenkomt, zou hij je kunnen confronteren met gegevens op basis waarvan je eigenlijk door de rechtbank bent vrijgesproken. En dat is dus een enorm probleem”.¹³⁸

De voorzitter van het COC heeft veel ervaring als criminoloog en als voormalig lid van Comité P. We vroegen hem naar zijn mening over de evolutie van het gebruik van informatie bij de politie:

“Ik heb het vaak over de ‘versnipperde politie’, omdat we er in de realiteit nog steeds niet zijn, zelfs in het beheer van politie-informatie, wat tot de eerste integratiegebieden zou moeten behoren. Gelukkig is de ANG gecentraliseerd, maar zelfs op dat niveau heersen er grote verschillen in de manier waarop mensen werken, in de manier waarop mensen gegevens coderen, in de manier waarop mensen de ANG gebruiken, enzovoort: het expertiseniveau is zeer laag. Dus als je me vraagt hoe ik naar de toekomst van informatiebeheer kijk, moet ik toegeven dat ik eerder pessimistisch ben. Neem bijvoorbeeld de ‘informatiekruispunten.’ Dat zijn diensten die politie-informatie zouden moeten integreren. Wanneer je in de praktijk echter van een politieagent af wilt, is dat vaak waar je hem parkeert. Dat is toch zeer tekenend, niet?”¹³⁹

Het ‘data lake’ van i-Police lijkt kwantiteit boven kwaliteit te verkiezen. Deze aanpak is onrustwekkend aangezien er geen rekening wordt gehouden met de betrouwbaarheid en nauwkeurigheid van de gegevens, hoewel de implicaties verregaand kunnen zijn. In de ambitie om zoveel mogelijk gegevens te verzamelen, zonder aandacht voor het principe van gegevensminimalisatie, kan de visie van i-Police als volgt worden samengevat: “Neem alles; laat het algoritme maar sorteren”.

2. VIDEOBEWAKING

Met het project i-Police zijn er plannen om ook videobewakingsbeelden te integreren. Hier bespreken we de verschillende soorten analysesoftware voor beelden, zoals gezichtsherkenning, die nu al gebruikt worden door de Belgische politiediensten.

Een daarvan is live detectiesoftware. De Belgische politie maakt hier gebruik van om meldingen te krijgen wanneer mogelijks ‘verdachte’ activiteiten door een camera worden gefilmd en worden opgemerkt door een algoritme. Relevante acti-

¹³⁸ Interview met Frank Schuermans (COC), 17/02/2023.

¹³⁹ Tweede interview met Frank Schuermans (COC), 11/10/2023.

viteiten zijn, onder andere: rook, graffiti, sluikstorten, mensen die nabij een wagen lopen of rondhangen en andere gelijkaardige zaken. In de praktijk identificeert de software verschillende 'problematische' gebeurtenissen in grote gebieden met een hoog percentage valse positieven, wat ervoor zorgt dat de operatoren de meldingen negeren. Desondanks kan het systeem een impact hebben op privacy en ervoor zorgen dat gebeurtenissen vertekend worden, omdat ze zijn vormgegeven door technische capaciteiten en de weergave van IT-ingenieurs, eerder dan door een democratisch debat.¹⁴⁰

De Belgische politie gebruikt ook de software BriefCam,¹⁴¹ van een Israëliisch bedrijf, voor beeldenanalyse na de feiten in onderzoek.¹⁴² Deze software maakt videosamenvattingen. De software bestudeert uren camerabeelden en categoriseert incidenten volgens bepaalde criteria zoals de bezittingen van de verdachte, de kleur van de kleding of gender. Deze functie roept vragen op over mogelijke onwettigheid. Het Belgische juridische kader inzake non-discriminatie staat toe om gericht te zoeken op basis van objectieve criteria, waaronder gevoelige fysieke kenmerken zoals gender, maar verbiedt om massaal personen in te delen op basis van zulke criteria.

BriefCam wordt gebruikt door zowel de lokale politiekorpsen als de Federale Ge-rechtelijke Politie. Het is uniek in die zin dat het gezichtsherkenningstechnologie integreert. Lokale politiekorpsen ontkennen vaak dat ze die functie gebruiken.¹⁴³ De Federale Politie, aan de andere kant, steekt niet onder stoelen of banken dat ze gebruik maakt van gezichtsherkenning: de aanbesteding die ze publiceerde om de vergunning van BriefCam te verlengen, vermeldt het expliciet.¹⁴⁴ Er is echter geen juridisch kader voor gezichtsherkenning in België.¹⁴⁵

Het gebruik van gezichtsherkenning heeft de laatste jaren voor de nodige aandacht in de Belgische pers gezorgd. In 2017 startte de Federale Politie een piloot-project in Brussels-Airport Zaventem om de technologie te testen.¹⁴⁶ Het systeem produceerde een aanzienlijk aantal valse positieven tijdens de test, waardoor het geschorst werd. Tijdens een later bezoek van het COC bleek echter dat het systeem nog steeds gedeeltelijk operationeel was, buiten de wettelijke kaders. Na het onderzoek van het COC, werd het project uiteindelijk volledig stopgezet.¹⁴⁷

140 Sarah Brayne. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

141 BriefCam company. URL: www.briefcam.com

142 Nicolas Bocquet. 2021. 'The Brussels Smart City: how "intelligence" can be synonymous with video surveillance'. *Brussels Studies*. URL: journals.openedition.org/brussels/5678

143 'Kortrijkse politie is één stap verwijderd van gezichtsherkenning'. *Datapanik*. 24/05/2019. URL: www.datapanik.org/2019/05/24/kortrijkse-politie-is-een-stap-verwijderd-van-gezichtsherkenning

We stelden dezelfde vraag aan politiekorpsen die BriefCam gebruiken in Brussel en over het algemeen gaven zij ons hetzelfde antwoord.

144 Cahier spécial des charges n° procurement 2024 R3 005 relatif à la maintenance de la solution d'analyse d'images de vidéo surveillance « Briefcam » au profit de la Police Judiciaire Fédérale, p. 37. URL: enot.publicprocurement.be/enot-war/preViewNotice.do?noticeId=491396

145 Het akkoord van de Arizona-regering voorziet echter wel het legaliseren van gezichtsherkenning, zie regeringsverklaring, 04/02/2025, p. 145. URL: www.lachambre.be/flwb/pdf/56/0020/56K0020001.pdf

146 Rosamunde van Brakel. 2021. 'How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium'. *Surveillance & Society*, vol. 19, no. 2, pp. 228-240. URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779

147 COC, 2019. Rapport sur l'utilisation de la reconnaissance faciale l'aéroport national de Zaventem. *Organe de contrôle de l'information policière*. DIO19005. URL: www.organedecontrôle.be/files/DIO19005_

Later werd het gebruik van het AI-systeem voor gezichtsherkenning van Clearview in vraag gesteld. Clearview staat erom bekend om enorme hoeveelheden foto's van openbare gegevensbronnen zoals sociale netwerken te plukken. In augustus 2021 schreef een nieuwssite dat de Federale Politie opzoeken had verricht met Clearview.¹⁴⁸ De politie ontkende eerst het gebruik van Clearview, maar een onderzoek van het COC toonde het tegendeel aan. Er werd toen bekendgemaakt dat de pilootvergunning voor Clearview tijdens een evenement van Europol werd bekomen.¹⁴⁹

Deze ontwikkelingen in videobewaking geven aanleiding tot ernstige bezorgdheid. Ze tonen aan dat het gebruik van technologie door de federale politie niet transparant is, wat betekent dat de kans groter is dat mogelijke onwettigheden onopgemerkt blijven. Maar niet alleen dat, want de Federale Politie heeft zelfs gelogen tegen de toezichthoudende autoriteiten toen hun gebruik van videobewakingsystemen aan het licht kwam.

Gezien de voorbeelden van videobewakingssoftware nu al in gebruik bij de Belgische politie, suggereert het vooruitzicht van de integratie van gedrags-, gezichts- en nummerplaatherkenningssoftware binnen i-Police een erg dystopisch panopticum. Het is essentieel om zo'n ongebreidelde uitbreiding van videobewaking een halt toe te roepen. De *Ligue des droits humains (LDH)* en verschillende andere verenigingen steunen deze mening. Ze voeren actief campagne om gezichtsherkenning te verbieden met de hashtag #ProtectMyFace.



Figuur 10. Campagne #ProtectMyFace.

Teken de petitie om het gebruik van gezichtsherkenningssoftware te verbieden in openbare ruimtes in Brussel.

Contr%C3%B4le_LPABRUNAT_Reconnaissance_Faciale_Publique_F.PDF

148 Ryan Mac, Caroline Haskins and Antonio Pequeño IV. 'Clearview AI Offered Free Facial Recognition Trials To Police All Around The World'. *BuzzFeed News*. 25/08/2021. URL: www.buzzfeednews.com/article/ryan-mac/clearview-ai-international-search-table

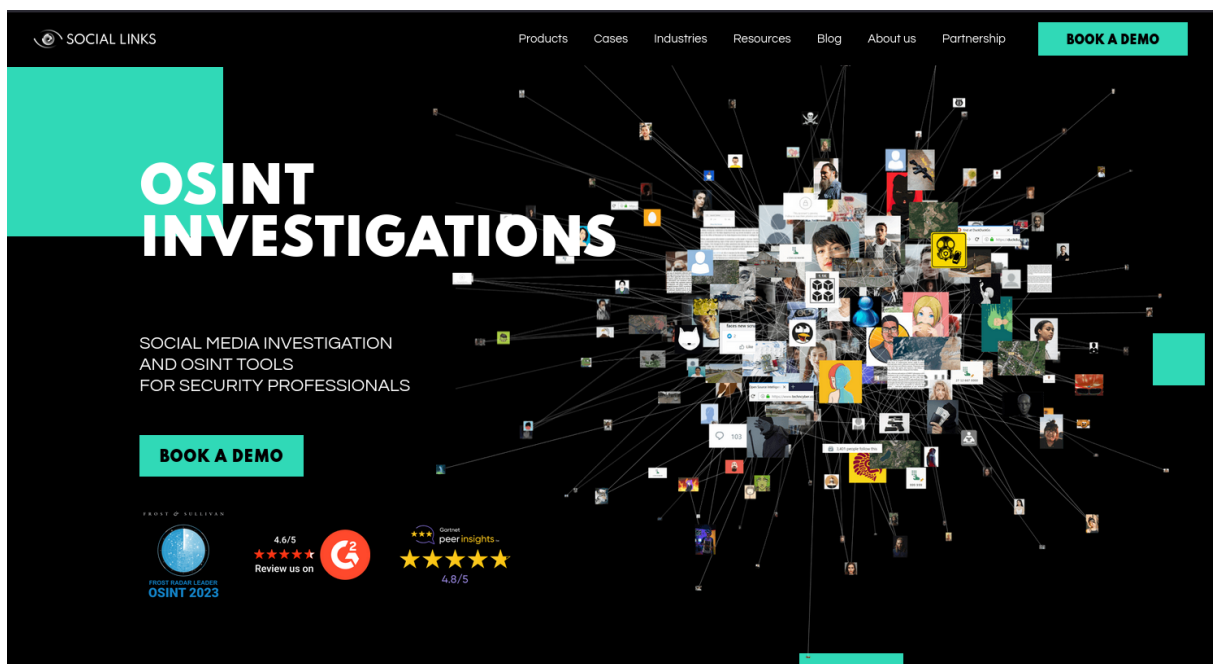
149 COC, 2022. 'Rapport relatif à l'utilisation de l'application Clearview AI par la police intégrée'. *Organe de contrôle de l'information policière*. DIO21006. URL: www.organedeconrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf

3. OPEN-SOURCE INTELLIGENCE (OSINT), ALGORITMISCHE ANALYSE EN ONDERAANNEMERS

Naast hun eigen gegevensbanken en videobewakingsbeelden, wil de politie ook externe gegevensbronnen integreren in i-Police. Die wens is al meermaals geuit door lokale politiediensten, de Federale Politie en criminologen die zich bezighouden met de ontwikkeling van technieken van *'predictive' policing*. De aanbesteding van i-Police noemt zo als mogelijke bronnen:

- “gegevens van derden zijn die gegevens die gevat en beheerd worden door derde partijen (externe bronnen). Onder deze categorie vallen zowel die informatie die voor de politie onmiddellijk beschikbaar is (bijvoorbeeld informatie uit het rijksregister, kruispuntbank voor ondernemingen, dienst inschrijving voertuigen,...), als informatie die op wettelijke basis kan opgevraagd worden bij derden (bijvoorbeeld mast data van telecom operatoren);
- open data is data die vrij toegankelijk is voor iedereen en die onmiddellijk kan gebruikt worden. Onder deze categorie vallen (vrij beschikbare) informatie van sociale media, informatie uit de pers”.¹⁵⁰

Een open-source intelligence (osint) eenheid werd in april 2023 opgericht in Brussel. Op het moment van de oprichting waren er bijna tien medewerkers, met een verwachte verdubbeling tegen 2024. De eenheid maakt gebruik van tools van het Duitse bedrijf Maltego Technologies¹⁵¹ en van Social Links,¹⁵² dat in Rusland is opgericht alvorens naar West-Europa en de VS te verhuizen na de Russische inval van Oekraïne in 2022.



Figuur 11. Landingspagina van de website van het Russische bedrijf Social Links met een sociale grafiek, 27/10/2023.

150 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*. pp. 43-44.

151 Maltego Technologies. URL: www.maltego.com

152 Social Links company. URL: sociallinks.io

Als deel van i-Police bereidt de osint-afdeling van de Federale Positie de implementatie van het IntSight-platform voor onderzoek en massale gegevensanalyse voor. Dat platform wordt door TA9 geproduceerd, een Israëlisch technologiebedrijf.¹⁵³ TA9 maakt deel uit van de Rayzone-groep, geleid door Yohai Bar-Zakai,¹⁵⁴ die voordien adjunctdirecteur van Unit 8200 was.¹⁵⁵

Unit 8200 is “het korps van de Israëlische inlichtingendienst van de defensietroepen, verantwoordelijk voor clandestiene operaties, verzameling van *signals intelligence*, *ontcijfering van codes*, *contraspionage*, *cyberoorlogvoering*, *militaire inlichtingen en bewaking*”.¹⁵⁶ Unit 8200 is verantwoordelijk voor de ontwikkeling van ‘Gospel’, een AI-systeem dat gebruikt wordt om bombardementsdoelwitten in Gaza te bepalen voor de Israëlische luchtmacht aan een veel hoger tempo dan manueel gegenereerde doelen.¹⁵⁷ ‘Gospel’ zou hebben bijgedragen aan de intensieve bombardementen in Gaza en de moord op Palestijnen in de recentste escalatie van Israëlisch geweld en vernieling.¹⁵⁸

Het is moeilijk exact te bepalen welke andere bedrijven en software geïntegreerd zullen worden in de osint-oplossingen van i-Police. Het is duidelijk dat Sopra Steria de belangrijkste aannemer voor i-Police is, met ondersteuning van het consultancybedrijf KMPG. Volgens een persbericht zullen zij samenwerken met een divers gamma aan onderaannemers, waaronder bedrijven zoals Microsoft, het Canadese bedrijf NicheRMS365,¹⁵⁹ en de Israëlische bedrijven Interionet¹⁶⁰ en TA9/Rayzone.¹⁶¹ Een hooggeplaatste beleidsadviseur verantwoordelijk voor de ICT-strategie van de Belgische politie verzekerde ons ervan dat alle externe entiteiten de nodige aanpassingen moeten doorvoeren om ervoor te zorgen dat hun software compatibel is met het Belgisch wettelijk kader.¹⁶²

Aan het hoofd van een andere onderaannemer van i-Police, Interionet, staat Yair Pecht, de voormalige CEO van de Israëlische cyberoffensiefspecialist NSO Group. NSO is het bedrijf achter de Pegasus-spyware, die gebruikt werd tegen verschillende journalisten, politici en politieke activisten. Informatie vergaard via Pegasus is verbonden aan ernstige gevolgen, waaronder de moord op dissidenten. Het controversiële verleden van NSO, getekend door deals met autoritaire regimes, botst op internationale kritiek. Dat heeft ervoor gezorgd dat verschillende

153 TA9 company. URL: www.t-a9.com

154 Rayzone Group. URL: rayzone.com

155 ‘A Bruxelles, la police fédérale construit sa nouvelle unité OSINT’. *Intelligence Online*. 02/05/2023. URL: www.intelligenceonline.fr/surveillance--interception/2023/05/02/a-bruxelles-la-police-federale-construit-sa-nouvelle-unite-osint,109949442-art

156 ‘Unit 8200’. *Wikipedia*. URL: wikipedia.org/wiki/Unit_8200

157 Geoff Brumfiel. ‘Israel is using an AI system to find targets in Gaza. Experts say it’s just the start.’ *NPR*. 14 December 2023. URL: www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st

158 Harry Davies, Bethan McKernan, Dan Sabbagh. ‘The Gospel’: how Israel uses AI to select bombing targets in Gaza.’ *The Guardian*. 1 December 2023. URL: www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

159 NicheRMS365 company. URL: nicherms.com/about-us

160 Interionet company. URL: www.interionet.com

161 Lars Bové and Jean-Paul Bombaerts. ‘La police entame une révolution digitale à 300 millions d’euros.’ *L’Echo*. 7 May 2022. URL: www.lecho.be/economie-politique/belgique/general/la-police-entame-une-revolution-digitale-a-300-millions-d-euros/10386480.html

162 Interview with a Senior Advisor R&D and ICT Strategy Belgian Federal Judicial Police, 16/06/2023.

dochterondernemingen werden ingericht, waaronder Interionet.¹⁶³

Ondanks deze inspanningen om weer in het reine te komen, blijft Interionet het doelwit van een boycot. De beweging *Boycott, Divestment and Sanctions (BDS)* zet zich in om internationale steun voor de onderdrukking van Palestijnen door Israël te stoppen en om druk te zetten op Israël om internationale wetten na te leven. De beweging spoort Belgen aan om zich uit te spreken tegen het contract tussen de Belgische Federale Politie en Interionet, omdat het bedrijf Palestijnen als proefpersonen voor de bewakingssoftware gebruikte, alvorens die wereldwijd op de markt werd gebracht.¹⁶⁴ Zulke praktijken zijn niet ongewoon, zo blijkt uit een recent boek van journalist Antony Loewenstein:

“Het militair-industrieel complex van Israël gebruikt de bezette Palestijnse gebieden als proeftuin voor wapens en bewakingstechnologie die ze vervolgens over de hele wereld exporteren naar despoten en democratieën.”¹⁶⁵



Figuur 12. Facebookpost van de BDS-beweging op 4 november 2022.

In de beschrijving staat: Palestijnen roepen op om druk te zetten om de Belgische politiecontracten met het Israëlische spionagebedrijf Interionet op te zeggen. Het bedrijf verbergt dat het gevestigd is in apartheid-Israël & dat haar gezichtsherkenningstechnologie getest werd op Palestijnen. #MilitaryEmbargo #BanSpyware #IsraelOutOfMyPhone

Begrijpen welke bedrijven exact onderaannemers zijn voor i-Police is moeilijk. Hoewel we verschillende aanvragen voor vrijheid van informatie hebben ingediend, zijn onze inspanningen om informatie te vergaren over de onderaannemers en hun software niet succesvol geweest. Toegang tot informatie werd geweigerd door te berusten op de nood voor commerciële geheimhouding of bezorgdheid

¹⁶³ Becky Peterson. 'The founders of a billion-dollar Israeli spyware startup accused of helping Saudi Arabia attack dissidents are funding a web of new companies that hack into smart speakers, routers, and other devices'. *Business Insider*. 9 May 2019. URL: [businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8](https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8)

¹⁶⁴ BDS Movement. 'Don't let the Belgian police use Israeli apartheid surveillance against Belgians!'. *Facebook*. URL: www.facebook.com/BDSNationalCommittee/photos/a.129952410382961/5947579748620169

¹⁶⁵ Antony Loewenstein. 2023. *The Palestine laboratory: How Israel Exports the Technology of Occupation Around the World*. Verso Books. URL: www.versobooks.com/en-gb/products/2684-the-palestine-laboratory

dat te veel details delen over de architectuur van het platform de veiligheid ervan in het gedrang kan brengen.

Julie Chanson, lid van het Federaal Parlement voor de partij Groen, wist geen andere resultaten te bekomen toen ze vroeg naar het project in april 2023:

“Onder de vorige regering werd de overheidsopdracht voor het nieuwe i-Police-platform aan de onderneming Sopra Steria gegund. [...] Er bestaan echter vermoedens dat een aantal onderaannemers van Sopra Steria geen onbezochelde reputatie heeft. Zo vernam ik dat een van die onderaannemers mogelijk een berucht Israëlisch bedrijf is dat nauwe banden onderhoudt met de voormalige NSO Group. [...] Ik maak me zorgen over de betrouwbaarheid van een zo strategisch platform als i-Police en de gegevensbescherming die dat noodzakelijkerwijs met zich meebrengt. Kunt u me de volledige lijst van de onderaannemers van Sopra Steria bezorgen?”¹⁶⁶

Het antwoord van minister van Binnenlandse Zaken Verlinden was ontwijkend en ze weigerde een lijst van de onderaannemers te verschaffen:

“De lijst van de onderaannemers kan op dit moment niet worden meegedeeld [...] met het oog op aspecten van geheimhouding en vertrouwelijkheid enerzijds, en veiligheidsaspecten van de i-Police oplossing anderzijds. In het kader van deze overheidsopdracht werden de vereiste controles uitgevoerd inzake het toegangsrecht en de uitsluitingsgronden [...]. Er was bijgevolg geen enkele wettelijke reden om de firma noch enige partner uit te sluiten van deelname in het kader van deze overheidsopdracht”.¹⁶⁷

In een rapport uit 2017 over big data, beveelt de Belgische autoriteit inzake gegevensbescherming aan dat het COC een specifieke opdracht krijgt om de gepastheid en effectiviteit van i-Police te evalueren.¹⁶⁸ Op de vraag wat zijn mening was over het feit dat het project i-Police met controversiële onderaannemers werkt, zei hij:

“Wij monitoren niet alle contracten. [...] Dat is de verantwoordelijkheid van het Ministerie van Binnenlandse Zaken en het Ministerie van Justitie. Op het einde van de dag zijn zij degenen die de contracten ondertekenen. Gezien onze beperkte capaciteit zijn we niet in staat om alles te controleren. We kunnen drie tot vijf proactieve onderzoeken per jaar uitvoeren, niet meer. [...]”

Je maakt je zorgen over Israëlische bedrijven, maar er is niet veel keuze. De Israëliërs zijn zeer efficiënt. Wanneer ik met de verantwoordelijken van de afdeling Criminele Opsporing praat, zeggen ze dat als je efficiënte software wil, er niet veel alternatieven zijn. In veel gevallen kunnen alleen de Israëliërs dit soort software leveren. [...]

[Gegevensbescherming] is altijd een probleem, niet alleen met de Israëliërs, maar ook met Microsoft! [...] Welke garanties hebben we dat gegevens niet naar de Verenigde Staten worden verzonden? De gekozen oplossing is om een contractuele

¹⁶⁶ Het antwoord van minister Verlinden op vraag 1775 door Julie Chanson, een lid van de Ecolo-Groen fractie in het Federaal Parlement. 12/04/2023. URL: <https://www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B108-1192-1775-2022202319320.xml>

¹⁶⁷ Ibid.

¹⁶⁸ CPVP. *Rapport Big Data*. 2017. p. 56. URL: www.autoriteprotectiondonnees.be/publications/rapport-big-data.pdf

verplichting op te leggen om de gegevens binnen de Europese Unie te houden. Maar zal de NSA die contracten respecteren? Niets is minder zeker, zoals we hebben gezien met de onthullingen van Snowden”.¹⁶⁹

In juni 2023 probeerde minister van Binnenlandse Zaken Verlinden desalniettemin om het Parlement gerust te stellen, door te stellen dat de Federale Politie met Europol samenwerkte om AI-gebaseerde methoden te evalueren en om de aansprakelijkheidsprincipes inzake kunstmatige intelligentie (ap4ai) toe te passen.^{170,171} De AP4AI-principes worden beschreven als “een universeel, empirisch gevalideerd kader voor AI voor rechtshandhaving en justitie. Hiermee kan legitiem en aanvaardbaar gebruik van AI door de interne veiligheidsgemeenschap fundamenteel worden beoordeeld en toegepast.”¹⁷² De principes omvatten:

- Universaliteit: Elk aspect van AI kan gemonitord en geëvalueerd worden.
- Verklaarbaarheid: Alle activiteiten, systemen en beslissingen met AI kunnen volledig verklaard worden aan het publiek en toezichthoudende instanties.
- Transparantie: Informatie om AI-gebruik te evalueren is eenvoudig en volledig toegankelijk.
- Onafhankelijkheid: Groepen die monitoren en handhaven zijn onafhankelijk van wetshandhavingsinstanties en AI-ontwikkelaars.
- Afdwingbaarheid: Het is mogelijk om wetshandhavingsinstanties te dwingen de benodigde informatie, systemen en individuen te verstrekken om hun gebruik van AI te beoordelen.
- Toewijding aan robuust bewijs: Wetshandhavingsinstanties zijn toegewijd aan het leveren van robuust bewijs om het gebruik van hun AI te beoordelen.
- Pluraliteit: Iedere groep die betrokken of geïmpacteerd is door AI-gebruik heeft een eigen stem.
- Uitvoerbaarheid en verhaal: Het is mogelijk om wetshandhavingsinstanties te dwingen om te voldoen aan alle verzoeken om hun AI-activiteiten te verbeteren.

Het is onduidelijk of we moeten lachen of wenen bij het zien van de kloof tussen deze principes en het huidige niveau van aansprakelijkheid dat de Belgische autoriteiten aan de dag leggen - zeker omdat deze programma's gebruik maken van algoritmes met afgeschermd code die beschermd wordt door intellectueel eigendom, waardoor het onmogelijk is om in te schatten hoe ze precies werken.

Zelfs wanneer de onderliggende code toegankelijk zou zijn en het mogelijk was om de methoden van de softwareontwikkelaars te bespreken, is het niet noodzakelijk mogelijk te begrijpen hoe ze werken. Meer en meer algoritmes zijn gebouwd met complexe methoden van machine learning. Modellen van machine learning worden vaak wel een ‘zwarte doos’ genoemd. Dat betekent dat een model werkt als een ondoorzichtig systeem waarvan de interne werking onduidelijk is, zowel voor

169 Tweede interview met Frank Schuermans (COC), 11/10/2023.

170 Accountability Principles for Artificial Intelligence. URL: ap4ai.eu

171 Minister Verlinden's answer to question 1911 by Daniel Seneseal, a socialist member of the Federal Parliament. 26/06/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B114-1192-1911-2022202320533.xml

172 The AP4AI Principles. URL: ap4ai.eu/about/principles

onderzoekers als gebruikers.¹⁷³ Het ‘probleem van de zwarte doos’ kan ervoor zorgen dat software bias en vooroordelen in machtsstructuren in stand houdt, zonder duidelijke oorsprong van of oplossing voor het probleem.

Verder bevatten zulke systemen met afgesloten code vaak ‘achterpoortjes’, waardoor ontwikkelaars vanop afstand toegang hebben. Die praktijken komen erg vaak voor bij Israëlische leveranciers. De Federale Politie heeft dit recent door schade en schande ondervonden. Volgens vertegenwoordigers van de politievakbond waarmee we hebben gesproken, moest de Federale Politie dringend van telefoon-tapleverancier veranderen, nadat ze ontdekten dat zij niet de enigen waren die de verdachten afluisterden. Wie zich afvroeg “wie de kijkers bekijkt”, heeft hiermee een antwoord.

4. HET PROGRAMMA I-POLICE: STAAT VAN VOORUITGANG

In augustus 2023 rapporteerde de minister van Binnenlandse Zaken aan het Federaal Parlement over de vooruitgang die geboekt was bij het project i-Police.¹⁷⁴ Het project begon met de implementering van een proces om gegevens internationaal uit te wisselen: op het moment van de verklaring van de minister werd de integratie van het Europese Schengeninformatiesysteem (SIS) gefinaliseerd en zouden Europol en Interpol in 2024 volgen.

Een tweede project maakte ook deel uit van de initiële uitrol van i-Police. Dat was een project over gegevensverwerking van de gegevensbanken van het islp en de ANG voor *information-led policing (ILP)*, wat centraal staat in de initiatieven van i-Police. In de aanbesteding lezen we:

“Het doel van ILP bestaat erin om gegevens (ruwe data) te verzamelen of te raadplegen, deze om te zetten in nieuwe inzichten en op basis van deze inzichten de werking van de 3 andere domeinen aan te sturen. De ruwe data die door ilp verwerkt worden, kunnen afkomstig zijn uit verschillende kanalen:

- gegevens afkomstig uit de operationele werking van de politie;
- gegevens afkomstig van partners van de politie of gegevens die door derde partijen aan de politie worden overgemaakt (externe gegevensbronnen);
- gegevens die publiek toegankelijk zijn en door de politie opgepikt worden.

Deze gegevens worden dan door ilp omgezet tot ‘Intelligence’ of anders genoemd ‘inzichten’. Deze inzichten dienen tijdig, accuraat, waardevol en actiegericht te zijn en zijn bedoeld om de werking aan te sturen. Afhankelijk van het soort aansturing spreken we over operationele, tactische of strategische intelligence”.¹⁷⁵

173 Lou Blouin, ‘AI’s mysterious ‘black box’ problem, explained’. *University of Michigan-Dearborn*. 6 March 2023. URL: umdearborn.edu/news/ais-mysterious-black-box-problem-explained

174 Antwoord van minister Verlinden op vraag 1964 van Daniel Seneseal, lid van de socialistische partij in het Federaal Parlement. 31/08/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B117-1192-1964-2022202320932.xml

175 GPI. 2020. *i-Police Selectiedossier. Bijlage H – Omschrijving van de opdracht*. p. 24.

Een pilootfase van het ilp-project werd eind 2023 gelanceerd. Dat vond plaats in de provincie Luik met zowel de lokale als Federale Politie. Het doel van de pilootfase was om aandachtspunten en verbeterpunten vast te stellen alvorens verder te werken in 2024.¹⁷⁶

Recente berichten in België tonen echter dat de ontwikkeling en implementatie van het systeem met problemen overladen waren. Een zulk bericht in *De Tijd* vermeldde een vernietigende audit van het Britse consultancybedrijf Deloitte. Volgens de krant was de conclusie van die audit dat de digitale transformatie bij de politie niet gestroomlijnd is, wat voor een gefragmenteerde aanpak zorgde. Ook concludeerde de audit dat er onvoldoende interne controle bestaat over de manier waarop politiemedewerkers de gegevensbank gebruiken en onderhouden. Dit kan tot misbruik leiden.¹⁷⁷ De auteurs van de audit spraken in het Federaal Parlement en zeiden:

“Wat betreft normen en wetgeving, constateerden we dat er niet echt een geformaliseerde manier van informatiebeheer over het operationele gebruik van gegevens, beveiliging en privacy bestond. We constateerden ook dat er geen echte strategie voor informatiebeveiliging bestond en geen actieplan voor de implementatie ervan. [...]

We constateerden dat de interne managementcontrole beperkt en ontoereikend is als het gaat om informatiebeheer. Het is daarom belangrijk om managementcontroleprocessen in te voeren, omdat het hier gaat om strikt vertrouwelijke gegevens.”¹⁷⁸

Een ander bericht in *Le Soir* waarschuwde dat de Federale Politie niet meer in staat is om haar facturen te betalen en dat het totale bedrag aan openstaande schulden oploopt tot verschillende tientallen miljoenen euro's. De krant voegt daaraan toe dat: “Sommige consultants, met name in de It-sector, worden niet meer betaald en beginnen erop aan te dringen dat ze naar behoren worden gehonoreerd”.¹⁷⁹ Volgens een vakbondsvertegenwoordiger waarmee we hebben gesproken, wordt i-Police momenteel sterk herzien om de stabiliteit van fundamentele IT-operaties van de politie te waarborgen en om de initiële wensen sterk in te perken.

Dit alles roept vragen op over de rol van privébedrijven die consultancydiensten aanbieden aan de blijkbaar failliete Federale Politie. De Federale Politie vroeg Sopra Steria/KPMG om i-Police te ontwikkelen, maar bestelde dan later bij Deloitte een audit van het proces, wat tot de conclusie leidt dat er een gebrek aan interne strategie bestaat. Het staat te bezien of andere privébedrijven verder voordeel zullen halen uit dit proces. Ongetwijfeld zijn er velen die mee een nieuwe strategie zouden willen opmaken.

176 Antwoord van minister Verlinden op vraag 1964 van Daniel Seneseal, lid van de socialistische partij in het Federaal Parlement. 31/08/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrv&language=fr&cfm=qrv&xml.cfm?legislat=55&dossierID=55-B117-1192-1964-2022202320932.xml

177 Stéphanie Romans. 'Audit kraakt digitale transformatie van politie'. *De Tijd*. 31/05/2023. URL: tijd.be/politiek-economie/belgie/federaal/audit-kraakt-digitale-transformatie-van-politie/10471186.html

178 Hoorzitting in het Federaal Parlement van inspecteurs van Deloitte na hun audit van de IT-afdeling van de Federale Politie. Belgische Kamer van Volksvertegenwoordigers. Doc 55 3516/001. URL: www.lachambre.be/media/index.html?language=fr&sid=55U4143#video

179 Xavier Counasse. 'La police fédérale ne peut plus payer ses factures'. *Le Soir*. 16/08/2023. URL: lesoir.be/531380/article/2023-08-16/la-police-federale-ne-peut-plus-payer-ses-factures

Het is onduidelijk welke vertelling van de feiten vertrouwd kan worden. Moeten we de woorden van de politie geloven als ze zegt dat ze hoogtechnologische systemen gebruikt om alle gegevens te verwerken en miraculeus de criminelen aan te duiden? Of moeten we de conclusies van Deloitte dat de politie slecht georganiseerd is en gebruik maakt van gedateerde software geloven?

In een interview zei de voorzitter van het COC, Frank Schuermans, het volgende over i-Police:

“De politie is lang niet zo efficiënt als mensen denken. [...] i-Police is pure praatjes, voorlopig toch nog. De situatie met de CCTV-bewakingscamera's laat geen ruimte voor andere interpretaties. We kondigen aan dat we overal ANPR-camera's gaan plaatsen, dat er 10.000 nieuwe camera's komen, maar we kunnen de 1.500 ANPR-camera's die er al zijn niet aansluiten of er een logsysteem op installeren. Het is allemaal maar schijn! Er gaapt een enorme kloof tussen de communicatie en de situatie in het veld. Het typische voorbeeld is de AMS (ANPR Managed Services), waar we het aantal camera's dat moet worden aangesloten niet kunnen bijhouden vanwege enorme technische problemen. Het is pure onzin.”¹⁸⁰

Het is geruststellend om te weten dat het niveau van technologische verfijning bij de politie niet overeen lijkt te komen met de vermeende capaciteiten. Desondanks moet de ontwikkeling van i-Police van nabij worden opgevolgd, aangezien het heel snel kan gaan wanneer het gaat over het gebruik van technologie bij de politie. Het zal ook belangrijk zijn om te garanderen dat, als i-Police wordt stopgezet, de meer ingrijpende delen niet eenvoudigweg onder een nieuwe naam weer gebruikt worden.

180 Tweede interview met Frank Schuermans (COC), 11/10/2023.

Automatisering van justitie in België: kleine stappen, grote problemen

In juridische omgevingen over de hele wereld worden algoritmen steeds vaker gebruikt om te anticiperen op beslissingen in toekomstige zaken en om rechterlijke uitkomsten te voorspellen door enorme hoeveelheden gegevens te verwerken (wetgeving, rechtspraak en rechtsleer).¹⁸¹ Verwacht wordt dat 'voorspellende' rechtspraak tal van functies zal hebben, zoals individuen inzicht geven in hun kansen op succes in juridische procedures en rechters helpen bij het nemen van beslissingen.

De implementatie van geautomatiseerde besluitvormingssystemen en AI in de gerechtelijke sector in België wordt aanzienlijk gehinderd door een gebrek aan toegang tot de gegevens die nodig zijn om dergelijke tools te trainen. De aanhoudende afhankelijkheid van analoge communicatiepraktijken binnen het Belgische rechtssysteem maakt een snelle implementatie van AI onwaarschijnlijk.

Burgerlijke rechtbanken hebben echter geëxperimenteerd met AI-gestuurd juridisch advies,¹⁸² universiteitsonderzoekers verkennen de ontwikkeling van AI-methoden die zijn aangepast aan het Belgische recht,¹⁸³ en recente wetgeving verplicht de oprichting van een centraal register voor rechterlijke beslissingen, waarmee AI-software kan worden getraind.¹⁸⁴ Dit alles geeft aanleiding tot bezorgdheid over de automatisering van aspecten van de rechtsgang en de uitbreiding ervan naar strafrechtbanken, en uiteindelijk de mogelijkheid van door algoritmen gestuurde rechterlijke beslissingen die individuen uit de rechtszaal kunnen verwijderen, wat de transparantie en betwistbaarheid in gevaar kan brengen.¹⁸⁵

Een rapport dat in december 2024 werd gepubliceerd door het Belgische Rekenhof geeft een uitgebreide analyse van de digitale strategie binnen het Belgische rechtssysteem.¹⁸⁶ Het constateert aanzienlijke tekortkomingen in de aanpak van digitale transformatie. Een belangrijk punt van kritiek is dat het ministerie van Justitie, ondanks het feit dat het maar liefst 140 miljoen euro specifiek heeft uitgetrokken voor digitalisering in 2023, geen eenduidige en samenhangende strategie heeft kunnen ontwikkelen. Het rapport wijst ook op de risico's van consultancyprojecten, zoals budgetbeheer, belangenconflicten en commerciële invloed.

De ontwikkeling van 'voorspellende' rechtspraak in het rechtssysteem gaat niet zo snel als die van de politie. Het lijkt echter wel een aantal gelijkaardige valkuilen te vertonen.

¹⁸¹ Matthias Van Der Haegen. 2023. 'Quantitative Legal Prediction: The Future of Dispute Resolution?' in De Bruyne & Vanleenhove (eds.). *Artificial Intelligence and the Law*. Second Revised Edition. Chapter 4. pp. 83-110.

¹⁸² Alain de Fooz. 'Legal Insights: Les avocats peuvent accéder à l'intelligence artificielle !' *Solutions Magazine*. 07/03/2018. URL: solutions-magazine.com/legal-insights-avocats-intelligence-artificielle

¹⁸³ Gregory Lewkowicz. 'Cross-jurisdictional AI Methods for Civil Law Court Decisions'. *LinkedIn*. June 2023. URL: [linkedin.com/posts/gregory-lewkowicz_intelligenceartificielle-droitcivil-activitey-7066291630386880512-GQHn](https://www.linkedin.com/posts/gregory-lewkowicz_intelligenceartificielle-droitcivil-activitey-7066291630386880512-GQHn)

¹⁸⁴ Loi du 16 octobre 2022 visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et modifiant la procédure d'assises relative à la récusation des jurés. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-10-24&numac=2022033790

¹⁸⁵ Rémy Farge & Emmanuelle Hardy. 2020. 'Justice : prédire la place de l'IA'. *La chronique des droits humains*. No. 203. URL: www.liguedh.be/wp-content/uploads/2023/07/2-Justice.pdf

¹⁸⁶ Cour des comptes. 2024. *Pilotage de la transformation numérique de la justice par l'État fédéral*. URL: www.ccrek.be/fr/publication/pilotage-de-la-transformation-numerique-de-la-justice-par

Conclusie: *Garbage in, garbage out*

De belangrijkste inzichten van dit rapport worden hieronder kort uiteengezet. De bevindingen worden vervolgens besproken met beleidsaanbevelingen voor een passende aanpak van AI en geautomatiseerde besluitvorming in politie en strafrecht. Dit omvat een aanbeveling voor een algeheel verbod op *'predictive' policing*, evenals verplichtingen op het gebied van transparantie, verantwoording en eerlijkheid.

1. SAMENVATTING

I. DE **LOKALE POLITIEKORPSEN** IN BELGIË BESCHIKKEN OVER EEN AANZIENLIJKE AUTONOMIE, WAT RESULTEERT IN VERSCHILLENDE *'PREDICTIVE'* POLICING INITIATIEVEN IN VERSCHILLENDE GEBIEDEN.

Een gebrek aan transparantie maakt het onmogelijk om een volledig beeld te krijgen van de eigenlijke werking van deze systemen. Toch is het duidelijk dat veel politiediensten gebruik maken van basis 'hotspot' geografische systemen. Enkele politiediensten hebben trots beweerd dat ze *'predictive policing'*-methoden toepassen: Westkust, Zennevallei en Antwerpen. De politie van Antwerpen, die een voortrekkersrol speelt in de automatisering van de lokale politie, heeft met name haar eigen mobiele applicatie FOCUS ontwikkeld. Dit moet agenten op straat onmiddellijk toegang geven tot een brede waaier van gegevensbronnen. De applicatie is sindsdien gedistribueerd naar andere korpsen in het hele land, voordat het werd geselecteerd als de fundamentele interface voor het federale i-Police project.

II. SYSTEMEN VOOR *'PREDICTIVE'* POLICING STEUNEN OP **POLITIEDATABANKEN**.

De Belgische politiedatabanken - die talrijk zijn - worden echter slecht onderhouden en voldoen vaak niet aan de wet. Politiedatabanken hebben al ernstige gevolgen voor individuen. Fouten en onterechte classificaties kunnen leiden tot ongerechtvaardigde huiszoekingen, verscherpte veiligheidscontroles op luchthavens en kan beroepsactiviteiten in het gedrang brengen. Verkeerde informatie leidt vaak tot beschadiging van iemands reputatie en broodwinning.

Bovendien zijn de aanpak van sekswerk en zogenaamde 'stadsbendes', samen met het anti-radicaliseringsbeleid, onevenredig gericht op gemarginaliseerde groepen en versterken ze bestaande structurele ongelijkheden. Zonder serieuze tegenmaatregelen zal de automatisering van de politie deze problemen alleen maar verergeren. Het ontbreken van rechten voor mensen om direct toegang te krijgen tot hun gegevens en legitieme mogelijkheden om in beroep te gaan, evenals het ontbreken van enig ander beschermend kader, betekent dat mensen en groepen die beïnvloed worden deze maatregelen niet kunnen aanvechten of verhaal kunnen halen.

III. **i-POLICE** IS EEN PROGRAMMA ONTWIKKELD DOOR DE FEDERALE POLITIE WAT EEN GRONDIGE HERZIENING VAN HAAR VEROUDERDE IT-INFRASTRUCTUUR INHOUDT.

Dit project van € 300 miljoen is bedoeld om automatisch een reeks gegevenstypen te analyseren en met elkaar te vergelijken: lokale, federale en internationale politiedatabases, maar ook camerabeelden en externe bronnen. Het is de bedoeling dat de gegevens en analyses daarvan op grote schaal beschikbaar worden gesteld aan agenten op straat en in politiebureaus.

1. Het i-Police-programma roept verschillende legitieme bezwaren op, in het bijzonder wat betreft de centralisatie van grote hoeveelheden gegevens in één enkele **data lake** en het gebruik van niet-transparante algoritmes.

Het 'data lake' leidt tot bezorgdheid over het mogelijke wegvallen van het onderscheid tussen 'gevalideerde' en 'niet-gevalideerde' informatie. In de computerwetenschap geeft het 'garbage in, garbage out'-principe aan dat gebrekkige invoergegevens geen betrouwbare uitvoer kunnen opleveren. Dit is een groot bezwaar bij het *data lake van i-Police*.

2. i-Police is van plan om videobewakingsbeelden te integreren.

Dit geeft aanleiding tot bezorgdheden, aangezien de Belgische politie herhaaldelijk de wet heeft overtreden op het gebied van videobewaking. Of het nu gaat om het gebruik van gezichtsherkenningstechnologie op de luchthaven van Brussel of het gebruik van Clearview AI-software voor het opsporen van criminelen, de Belgische politie lijkt gefixeerd op de mogelijkheden die nieuwe technologische ontwikkelingen bieden in plaats van zich te houden aan de minimale wettelijke vereisten. Gezien het plan van de regering om gezichtsherkenning te legaliseren en ANPR-camera's in het hele land te implementeren, is er reden om ongerust te zijn (en actie te ondernemen).

3. Het i-Police-programma is van plan om externe bronnen te gebruiken en te analyseren, een praktijk die bekend staat als open-source intelligence (OSINT). Er is onduidelijkheid over welke bedrijven deelnemen aan het project en welke software wordt gebruikt. De belangrijkste opdrachtgever voor i-Police is Sopra Steria, met ondersteuning van consultancybedrijf KPMG. De analyse van de gegevens zal afhankelijk zijn van geheime algoritmen die worden geleverd door particuliere en overzeese onderaannemers, met twijfelachtige ethische praktijken zijn.

4. Ondanks belangrijke vooruitgang in de afgelopen jaren is België gestuit op **obstacles** met het 'i-Police'-initiatief.

Een externe audit wees uit dat de digitale transformatie van de politie versnipperd is, met een gebrek aan interne controle-, beveiligings- en privacymaatregelen. Dit is vooral zorgwekkend gezien de grote hoeveelheden vertrouwelijke informatie die hiermee gepaard gaan. Bovendien kampt de federale politie met financiële problemen, met schulden die oplopen tot tientallen miljoenen euro. Het i-Police-project zal daarom waarschijnlijk worden herzien, waarbij de nadruk zal liggen op het waarborgen van de stabiliteit van de kernactiviteiten van de IT-politie.

2. DISCUSSIE

Digitalisering en automatisering bij politie en justitie in België verlopen via verschillende paden voor ordehandhaving en gerechtelijke procedures. Bij de politie wordt meer gebruik gemaakt van technologie dan bij justitie. Beide settings geven echter aanleiding tot bezorgdheid over mogelijke inbreuken op grondrechten en versterkte discriminatie en criminalisering. Daarom is voortdurende waakzaamheid en vooruitziendheid ten aanzien van digitalisering van het grootste belang.

Eerst en vooral is bekend dat ‘voorspellende’ AI-systemen zich onevenredig richten op en discrimineren tegen gemarginaliseerde groepen en bestaande structurele ongelijkheden versterken. Gegevens die worden ingevoerd op basis van ras, religie, sociaaleconomische status, migratiestatus en nationaliteit worden vaak bepalende factoren in de oneerlijke buitensporige controle, bewaking en criminalisering van bepaalde gemeenschappen.¹⁸⁷

Deze problemen worden nog versterkt door een gebrek aan transparantie en verantwoordingsplicht en door het ontbreken van effectieve rechtsmiddelen. Voorspellende AI-systemen opereren achter technologische en commerciële barrières, waardoor beslissingen aan het toezicht worden onttrokken. Getroffen individuen tasten in het duister, zonder duidelijke en effectieve middelen om de “black boxes” te openen en deze ontransparante beslissingen aan te vechten.¹⁸⁸

Bovendien schenden ‘voorspellende’ systemen kernbeginselen van het recht, zoals het vermoeden van onschuld, het recht op privacy, vrijheid en een eerlijk proces, de vrijheid van vergadering en vereniging en gelijke behandeling voor de wet. Individen, groepen en locaties worden voortijdig bestempeld als potentiële bedreigingen, wat leidt tot preventieve strafmaatregelen, zoals ongerechtvaardigde vrijheidsberoving. Dit holt het essentiële principe uit dat individuen als onschuldig zijn totdat het tegendeel is bewezen en vormt een ernstig risico op gerechtelijke dwalingen.¹⁸⁹

Ondertussen zijn mensenrechtenbeoordelingen of elementaire kosten-batenanalyses nergens te vinden bij het testen van Belgische ‘voorspellende’ systemen. De afwezigheid van evaluaties vooraf op basis van het potentieel van het systeem om schade te berokkenen, doet twijfel ontstaan over de efficiëntie, proportionaliteit, noodzakelijkheid en lange termijn gevolgen van deze maatregelen. Het moet absoluut noodzakelijk zijn om de gevolgen van ‘predictive policing’ te begrijpen voordat we het blindelings omarmen.

¹⁸⁷ Ibid.

¹⁸⁸ Debailleul, Corentin, Jérémy Grosman and Aline Wavreille. 2022. « Repolitiser l’usage des algorithmes ». in *État des droits humains en Belgique – Rapport 2021*. Brussels: Ligue des droits humains. URL: www.liguedh.be/wp-content/uploads/2022/01/Classeur7.pdf

¹⁸⁹ Fair Trials. 2021. *Automating Injustice: The Use of Artificial Intelligence and Automated Decision-Making in Criminal Justice in Europe*. URL: www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf

Op de vraag of ‘*predictive policing*’ in België zou moeten worden toegestaan, antwoordde Frank Schuermans van het COC:

“Dat is een heel moeilijke vraag. Dat is in de eerst en vooral een vraag voor de wetgever en voor het parlement [...]. Ik ben in dit stadium erg terughoudend om ja te zeggen op die vraag. Niet zozeer vanwege het principe dat het niet mogelijk zou moeten zijn, maar vanwege de dagelijkse ervaring die we hebben; vanuit ons dagelijkse werk zien we dat er een enorm probleem is met de nauwkeurigheid van politiegegevens. Zelfs nu, zonder big data. En net omdat dit de basis zou vormen van alle profileringssystemen...”.¹⁹⁰

Op dit moment zijn er dringende en lopende discussies tussen het maatschappelijk middenveld, beleidsmakers en academici over de regulering van AI, ook in het politiewerk, om de kans op schade zo klein mogelijk te maken. In België heeft Thomas Marquenie, academisch onderzoeker aan de KU Leuven, een reeks richtlijnen voorgesteld voor het reguleren van AI. Hij benadrukt:

- de noodzaak om te voldoen aan de wetgeving inzake gegevensbescherming, met name door systematisch gebruik te maken van Data Protection Impact Assessments (DPIA);
- de noodzaak om profilering te beperken, alsook het gebruik van gevoelige gegevens begrenzen
- het belang van steeds ‘menselijke controle’ te hebben om verantwoordelijkheidsplicht en aansprakelijkheid te handhaven;
- de behoefte aan meer publieke transparantie: overheden moeten burgers informeren en informatie delen over de instrumenten die ze gebruiken en de gegevens die ze verwerken;
- - dat het gebruik van AI beperkt moet blijven tot afgebakende doelen, profielen en situaties.¹⁹¹

Uiteraard moet het gebruik van AI ook altijd een wettelijke basis hebben en moet de politie in overleg treden met het Toezichtsorgaan (COC) voordat ze nieuwe systemen of hulpmiddelen implementeert. De voorstellen van Marquenie lijken niet meer dan redelijk. Aanvullingen op zijn voorstellen zouden kunnen zijn: gevalideerde politiedossiers, strenge dataminimalisatie praktijken en regelmatige audits kunnen. Dit als minimumvereisten voor de ontwikkeling van elke ‘datagestuurde oplossing’.

Om volledig rekening te houden met de schade die het gevolg is van datagestuurde politieoptreden in België, gaan dergelijke regelgevingsvoorstellen echter niet ver genoeg. Dit onderzoeksrapport heeft structurele problemen van racisme, islamofobie en classisme bij de politiewerking aan het licht gebracht. Deze problemen zijn systemisch en kunnen niet opgelost worden door de regulering van politiealgoritmen alleen.

¹⁹⁰ Interview with Frank Schuermans (COC), 17/02/2023.

¹⁹¹ Thomas Marquenie. 2022. ‘Het gebruik van AI-toepassingen binnen het politiewezen: voordelen, risico’s en best practices’. Staten Generaal over Artificiële Intelligentie. *Centre for IT & IP Law (CiTiP)*. 17 June 2022. URL: vaia.be/files/cursusmateriaal/presentaties/220617-3-Thomas-Marquenie.pdf

Het is een misvatting om te geloven dat de Belgische politie de wettelijke kaders voor het reguleren van AI naar behoren zal respecteren. Er zijn talloze voorbeelden van ordehandhavers die de bestaande vereisten voor het gebruik van gegevens en algoritmen door de politie niet naleven. COC-rapporten over gezichtsherkenning op de luchthaven van Brussel, over Clearview AI en over de ANG-databank bewijzen bijvoorbeeld dat de federale politie de wet dagelijks aan haar laars lapt. Dit wijst op structurele problemen die niet onmiddellijk kunnen worden opgelost.

Bovendien bestaat er ernstige bezorgdheid over de nauwkeurigheid van politiegegevens. Deze context bedreigt alle hoop op een correct gebruik van *'predictive' policing* tools in België. In een dergelijke omgeving kan men alleen maar de gegrondheid van investeringen in *'predictive' policing* tools in vraag stellen.

Daarnaast is *'predictive policing'* gebaseerd op de aanname dat bepaalde locaties of personen inherent vatbaar zijn voor criminele activiteiten. Deze aannames zijn gebaseerd op criminologische theorieën die empirische onderbouwing missen en de complexe aard van criminaliteitsoorzaken simplificeren.

Het lijkt dan ook terecht om zich in België te verzetten tegen de ontwikkeling van *'predictive' policing* tools. Zoals een recente thesis over i-Police concludeert:

“Bestaande oplossingen om de schade te beperken zijn hierboven al genoemd. Maar laten we onszelf niet voor de gek houden: deze oplossingen dienen uiteindelijk als reddingsboeien wanneer voorkomen moet worden dat het schip zinkt. Het gebruik van *'predictive' policing* is onzin [...]. Erger nog dan onzin, het is in veel opzichten een gevaar dat niet onderschat mag worden vanwege de onterecht neutrale uitstraling die aan de technologieën gegeven wordt. De tijd, energie en het geld die in deze tools worden geïnvesteerd, hadden beter kunnen worden besteed aan onderwijs [...] of het aanpakken van ongelijkheid, wat duurzame manieren zijn om criminaliteit aan te pakken. Sommige mensen zullen me een utopist noemen, maar waar is de utopie in het beweren dat je misdaad kunt voorspellen?”¹⁹²

Een verbod op *'predictive' policing* staat lijnrecht tegenover de aanpak van de Lokale Politie Vaste Commissie (VCLP) de koepelorganisatie van de lokale politiekorpsen. In haar visiedocument Horizon 2025 stelt de commissie:

“We zijn ondanks alle ondersteunende ontwikkelingen binnen informatiegestuurde politiezorg (i-Police, Focus, ANPR,...) nog maar aan de vooravond van deze evolutie. De toekomstige mogelijkheden zijn oneindig met als summum de evolutie naar een *"predictive policing"* op basis van *"big data"* en *"datamining"*. Dagelijks botsen we tegen de grenzen van privacy en mensenrechten. Het privacy debat moet dringend worden gevoerd met als uitgangspunten de inzet van informatie en technologie voor een betere leefbaarheid en veiligheid van de burger en het streven naar een uniform gemeenschappelijk gedragen beleid”.¹⁹³

¹⁹² Jérémie Vervoort, 2021. *I-Police ou l'art de prédire la discrimination*. Master's Thesis. Bruxelles: Université libre de Bruxelles.

¹⁹³ VCLP, 2019. *Horizon 2025*. Vaste Commissie van de Lokale Politie. p. 13. URL: www.politie.be/5806/sites/5806/files/downloads/HORIZON%202025_NL.pdf

In het kader van deze prangende bezorgdheden is het absoluut noodzakelijk dat België het gebruik van *'predictive' policing* en geautomatiseerde besluitvormings-systemen in politie- en strafrechtomgevingen verbiedt. Door deze systemen te verbieden, kan België een belangrijke stap zetten naar een meer rechtvaardige en democratische samenleving. Het is een gelegenheid om opnieuw te bevestigen dat we de grondrechten willen handhaven, gelijkheid willen bevorderen en de beginselen van rechtvaardigheid en verantwoordingsplicht willen handhaven.

Samengevat is *'predictive' policing*, zoals het nu bestaat in België, verre van verantwoordelijk, effectief of ethisch. Het is van het grootste belang dat we de invoering ervan aanvechten, met een vastberaden engagement om onze rechten en vrijheid te beschermen. Het is essentieel dat we onze stem verheffen tegen *'predictive policing'*. Het verbieden van *'predictive' policing* en geautomatiseerde besluitvorming in het strafrecht is een stap in de richting van een toekomst waarin rechtvaardigheid en gelijkheid niet in het gedrang komen in naam van technologische innovatie. Het is een bevestiging dat de rechten en het welzijn van de mensen op de eerste plaats komen en dat we fel gekant zijn tegen elke technologie die deze principes ondermijnt.

Acroniemen en afkortingen

ADM	<i>Automatic or algorithmic decision making</i>
AI	<i>Artificial intelligence</i>
ANG	<i>Algemene nationale gegevensbank (Banque nationale générale)</i>
ANPR	<i>Automatic number plate recognition</i>
CERD	<i>United Nations Committee on the Elimination of Racial Discrimination</i>
COC	<i>Controleorgaan op de politionele informatie (Organe de contrôle de l'information policière)</i>
DIV	<i>Dienst voor inschrijvingen van voertuigen (Direction pour l'immatriculation des véhicules)</i>
DPA	<i>Data protection authority</i>
DPIA	<i>Data protection impact assessment</i>
DPO	<i>Data protection officer</i>
DRI	<i>Directorate of Police Information and ICT Resources</i>
EHJ	<i>Europese Hof van Justitie</i>
FEEDIS	<i>Feeding information system (gebruikt door de Federale Politie)</i>
FRT	<i>Facial recognition technology</i>
GAFAM	<i>Google, Apple, Facebook, Amazon, Microsoft</i>
GDPR	<i>General Data Protection Regulation</i>
GPI	<i>Geïntegreerde politie (Police intégrée)</i>
ILP	<i>Intelligence-led policing</i>
ISLP	<i>Integrated system for local police</i>
LDH	<i>Ligue des droits humains</i>
LEZ	<i>Low Emission Zone</i>
NACE	<i>Nomenclature statistique des activités économiques dans la Communauté européenne (Statistische naamgeving van de economische activiteiten in de Europese Gemeenschap)</i>
OSINT	<i>Open-source intelligence</i>
QLP	<i>Quantitative Legal Prediction</i>
SICAD	<i>Service d'information et de communication de l'arrondissement (Informatie- en CommunicatieDienst van het Arrondissement)</i>
ULB	<i>Université libre de Bruxelles</i>
VCA	<i>Video content analysis</i>
VCLP	<i>Vaste Commissie van de Lokale Politie (Commission Permanente de la Police Locale)</i>
VUB	<i>Vrije Universiteit Brussel</i>

