WE SENSE TROUBLE

AUTOMATED DISCRIMINATION AND MASS SURVEILLANCE IN PREDICTIVE POLICING IN THE NETHERLANDS

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in 2020
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: EUR 35/2971/2020
Original language: English

amnesty.org

Cover illustration: **A drawing of a miniature road where police officers are picking up tiny cars and are inspecting them closely. The passengers in the car are selected for additional checks based on the colour of their skin.**
© Veerlesillustraties.

AMNESTY INTERNATIONAL

CONTENTS

EXECUTIVE SUMMARY

> **"Technology is not neutral or objective. It is fundamentally shaped by the racial, ethnic, gender and other inequalities prevalent in society, and typically makes these inequalities worse. It is resulting in discrimination and unequal treatment in all areas of life, from education and employment to healthcare and criminal justice."**
>
> Human Rights Office of the High Commissioner, Emerging digital technologies entrench racial inequality, UN expert warns, 15 July 2020.

Around the world, police forces are experimenting with data and algorithms with the aim of anticipating and preventing crime. Law enforcement agencies in many countries are deploying investigative tools that they allege can 'predict' crime. These tools consist of data and algorithmic models to assess the risk that a crime will be committed by a certain person or at a certain location. The use of these methods by the police is known as *predictive policing*. Based on the risk scores, the police take measures aimed at preventing or detecting the predicted crime by directing policing efforts towards 'high-risk' persons or locations. Across the EU, predictive policing systems are being developed at a tremendous rate, while regulation that would address the risks of predictive policing tools is still lagging far behind. One of the countries at the forefront of predictive policing in actual practice is the Netherlands. The Dutch police have set up various predictive policing projects which they refer to as 'living labs'. In these projects, the Dutch police experiment with data and algorithms. This report contains the findings of an investigation that Amnesty International conducted on one of these 'living labs': the Sensing project in the city of Roermond.

Chapter 1 of this report, "Human rights and the trend of predicting crimes", describes predictive policing as a trend. At the level of the European Union and the United Nations, we are seeing an attitude shift regarding predictive policing. After funding the development of predictive policing systems with millions of euros over a period of several years, the European Commission has acknowledged serious human rights concerns and warned against discrimination, prejudices and biases of algorithmic models and the societal harm resulting from the use of predictive policing systems. The UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, also warned that emerging digital technologies driven by big data are entrenching racial inequality, discrimination and intolerance. Despite this broad acknowledgement of the serious human rights risks of predictive policing projects, there is still insufficient regulation and weak oversight and accountability mechanisms. It is therefore alarming to see that the development of such systems in EU member states is moving forward at a tremendous rate. This Chapter explains the ways in which the application of predictive policing puts human rights at risk.

Chapter 2 of this report, "Legal framework", covers the human rights norms that are established under international and European law. This Chapter explains the right to privacy, the right to data protection and the right to non-discrimination.

Chapter 3, "The Sensing project in more detail", takes a closer look at exactly how the project was envisioned, designed and structured, how it has been implemented in actual practice, and what factors are involved. The Sensing project

focuses on the prevention and detection of 'mobile banditry', a term that is nowadays used by the Dutch police to describe property crime, such as pickpocketing and shoplifting, that the police allege are predominantly committed by people with Eastern European nationalities. The Dutch police associates 'mobile banditry' in Roermond with people with Roma ethnicity. In the Sensing project, the police systematically collect the data of all people driving in and around Roermond. Through cameras and other sensors, the police collect information about vehicles and movement patterns. The police then process such data in an algorithmic risk model to calculate the risk scores of vehicles driving in the city. The risk score is supposed to notify the police of the likelihood of the driver and passengers coming to Roermond with the intention to pickpocket or shoplift in the shopping centre. Some of the indicators it uses to make this assessment are also designed to establish whether a person is of Eastern European origin. Data on all cars are being collected, analysed and stored in the context of criminal law enforcement. Once the predictive policing system has assigned a high risk score to a car, i.e. 'created a hit', the police will try to intercept the car and perform a stop and identification check on all passengers, in the hope that this will prevent crime. The deployment of the Sensing project in Roermond has transformed the city into a living lab where every person travelling by car is a 'guinea pig', subjected to mass surveillance and other human rights violations.

Chapter 4, "Human guinea pigs under mass surveillance", discusses the privacy and data protection implications of the Sensing project.

Section 4.1, "Human rights still apply in living labs", explains that regardless of what they are called – experiments, try-outs, living labs and pilots – all police projects and operations must respect human rights. The Sensing project is portrayed by the police as a 'living lab', when in fact none of the research subjects (the people in Roermond) have consented to the experiment. The police processes personal data and data relating to people's private lives in the Sensing project. The surveillance of the predictive policing system using cameras and sensors interferes with privacy and data protection rights. To be lawful, these interferences would need to be justified under the conditions set out under international human rights law as outlined in Chapter 2. The interference must pursue a legitimate aim, be in accordance with the law, and be necessary in a democratic society. In the next four sections, the Sensing project is evaluated according to these criteria.

Section 4.2, "Mass surveillance in Roermond", describes that the Sensing project entails indiscriminate mass surveillance because it includes widespread monitoring, collection, storage and analysis of personal data without any individualised reasonable suspicion of criminal wrongdoing. Mass surveillance can never be a proportionate interference in the rights to privacy and freedom of expression. The project is therefore a violation of the right to privacy and must be put to an end immediately. The Sensing project places many people under mass surveillance and specifically targets people with Roma ethnicity, a marginalised group that has been the victim of systematic discrimination throughout Europe.

Section 4.3, "Flawed design of the Sensing project", identifies serious flaws in the design of the research, record-keeping, evaluation and databases of the Sensing project. The predictive policing system works with such generic profiles (e.g. a German car with multiple passengers on its way to the shopping centre) that the system creates many false positives. Moreover, vast numbers of people end up in additional police databases and their data is processed and stored. Also, the police are unable to demonstrate the effectiveness of the Sensing project and have admitted that the design of the project does not allow them to adequately measure its effectiveness in the prevention of pickpocketing and shoplifting. In practice, most risk scores are not analysed by the police. This lack of an adequate evaluation in the design prevents the police from challenging their assumptions regarding the profile of pickpockets and shoplifters and increases the risk of confirmation bias. The police interventions as a result of hits, such as stop and checks, are poorly registered and evaluated in the context of the Sensing project. This lack of record-keeping obstructs the assessment of proportionality which is necessary when human rights are affected. It also obstructs procedures for remedy and redress for those subjected to preventive checks. The design of the databases also violates data protection principles. The accuracy of the data is not checked and large quantities of irrelevant and inaccurate data is being stored for too long.

Section 4.4, "Overall lack of legality for predictive policing projects in the Netherlands", takes a step back and looks at the overall legality of predictive policing projects that make use of sensors, such as the Sensing project. The police base the data collection of such projects on the general tasks attributed to the police under Article 3 of the Dutch Police Act (DPA). This provision was not designed to foresee the use of predictive policing technologies, such as the Sensing project, nor to authorise them. Art. 3 DPA is not specific and does not include technical measures. It also does not offer any indication as to the circumstances under which the police may collect the data. Moreover, the law does not indicate the scope of discretion granted to the police to collect data on this scale, nor does it clarify the manner of exercise of that discretion, and it fails to ensure sufficient independent oversight as a safeguard against arbitrary interferences. The use of predictive policing systems that make use of sensors in the public space are not in accordance with the law and therefore violate privacy rights.

Section 4.5, "Misuse of the Road Traffic Act to follow up predictive policing hits", details how the police abuse their powers under the Road Traffic Act to follow up hits from the predictive policing system. In the Netherlands, the police rely on Article 160 of the Road Traffic Act for 'stops and checks' of cars. While this provision only provides powers to

the police to monitor compliance with road traffic rules, it is common police practice to request a stopped driver to submit to an extensive search. Most people who are stopped are unaware that the car search is not legally authorised, nor that they may refuse a search. In the Sensing project, the police abuse their power to stop cars in order to search cars for people who fulfil their target profile of 'mobile bandits'. Art. 160 of the Road Traffic Act lacks safeguards against abuse and leaves broad discretion to police officers, thus creating a clear risk of arbitrary and discriminatory use of powers. The breadth of the power makes it difficult, if not impossible, for those affected to show that any stops and checks, and subsequent searches, are outside the law.

Chapter 5, "Input = output: discrimination by design", demonstrates how the Sensing project is discriminatory from design to execution.

Section 5.1, "Bias by design", explains that the police present the predictive policing system as a neutral system, guided by objective criminal data statistics, while in reality the Sensing project embodies human choices and biased data, which results in amplifying and entrenching bias in policing. The Sensing project illustrates a number of ways in which discrimination may arise in predictive policing. In the Sensing project, bias is apparent in the choice to limit the focus of the project to 'mobile banditry', defined here as pickpocketing and shoplifting committed specifically by individuals of Eastern European nationality. The use of the concept of 'mobile banditry' inevitably leads to a predominant focus on particular groups of people based on their nationality and ethnicity, while at the same time overlooking people from other ethnic and/or national backgrounds. The definition of 'mobile banditry' results in direct discrimination on the basis of nationality and indirect discrimination on the basis of ethnic origin. On top of this, the police link nationality and ethnic origin to criminal behaviour in their reports and media messaging. Such linking amounts to direct discrimination and ethnic profiling.

Section 5.2, "Automated ethnic profiling", reveals that the Sensing project identified vehicles with Eastern European licence plates in an attempt to single out Roma as suspected pickpockets and shoplifters. The target profile is biased towards designating higher risk scores for individuals with an Eastern European nationality and/or Roma ethnicity, resulting in this group being more likely to be subjected to measures, such as storage of their data in police databases.

In Section 5.3, "Lack of transparency and accountability", the use of Art. 160 of the Road Traffic Act for crime prevention is discussed. This use brings a high risk of discriminatory use of powers in the stops and checks. The wide margin of discretion offered by this provision and its lack of safeguards enable the police to consider the passengers' presumed nationality or ethnicity in deciding if and how to follow up on a hit. Sufficiently circumscribed powers and adequate legal safeguards, in particular stop forms, would protect people against such abuses of powers.

Lastly, a list of recommendations is provided for Dutch law enforcement authorities, the Dutch legislature, and the Dutch Data Protection Authority. Key highlights from this list are featured below.

This report analyses the design and deployment of the Sensing project based on information from the media, publicly available documents and an interview with two senior police officers, the Programme Manager for the Sensing project and the Programme Director for Digitisation and Cybercrime. During the period that Amnesty International conducted this research, changes were made in data collection and processing in the Sensing project, but the main human rights concerns remain.

The human rights abuses that were identified in the Sensing project may be found in other predictive policing projects as well, since the projects are often designed in a similar fashion and include some form of mass surveillance. The recommendations below should, therefore, be addressed not only with regard to the Sensing project but with regard to all other predictive policing projects in the Netherlands, both by the national and regional police and by other law enforcement agencies.

KEY RECOMMENDATIONS

TO THE DUTCH LAW ENFORCEMENT AUTHORITIES:

1) Halt the Sensing project and comparable 'experimental' predictive policing projects that, through their design, application or effects, violate human rights, such as the right to privacy, the right to data protection, the right to non-discrimination and the principle of legality.

2) Halt and refrain from any and all policing operations that rely on mass surveillance, which is never a proportionate response that can justify limitations or restrictions on the right to privacy. Delete all data that was collected and inferred in the course of these operations, as it was unlawfully collected.

3) Stop the use of stereotypes in policing operations that violate the right to non-discrimination. The police must refrain from the use of ethnicity, nationality or proxies thereof in crime profiles; end the use of predictive policing against stereotypes of crime, which target specific communities; and refrain from using profiles and profile rules

in risk models that are based on protected grounds, such as race, ethnicity, colour, nationality, social origin or political affiliation.

TO THE DUTCH LEGISLATURE:

1) Explicitly prohibit the use of algorithmic systems which do not have appropriate safeguards to protect the rights and freedoms of individuals whose data is processed by these systems in the context of policing and criminal law enforcement. This includes a legal basis that meets the criteria of specificity, foreseeability and accessibility and which is announced in advance.
2) Implement a mandatory and binding human rights impact assessment requirement applicable to the public sector, including to law enforcement authorities, which must be carried out in the design, execution and evaluation phases of algorithmic systems and automated decision-making.
3) Create an independent supervisory authority that advises on, monitors and enforces human rights obligations and responsibilities in algorithmic systems and automated decision-making. The supervisory authority should have access to the training data, data categories and algorithms to examine the system and its outcomes in terms of respecting, promoting and fulfilling human rights. The supervisory authority must have capacity and expertise on all relevant human rights aspects, such as data protection compliance, data science, algorithmic systems and automated decision-making in order to effectively keep up with the introduction and ongoing development of algorithmic systems and automated decision-making in society.

TO THE DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS):

1) Investigate the Sensing project and enforce the data protection framework on the data processing operations relating to the Sensing project, taking into account the authority to impose administrative fines under Art. 35(1)(c) of the Dutch Police Data Act (DPDA), and other appropriate measures.
2) Investigate other 'experimental' predictive policing projects similar to the Sensing project. Enforce the data protection framework on the data processing operations relating to those projects, taking into account the authority to impose administrative fines under Art. 35(1)(c) DPDA, and other appropriate measures.

GLOSSARY

TERM	DEFINITION
ALGORITHM	A set of mathematical instructions or rules that calculate an answer to a problem or question. In predictive policing, algorithms calculate the risk posed by a certain place or person.
AUTOMATED NUMBER PLATE RECOGNITION (ANPR)	ANPR is a technology used in cameras in order to scan and read number plates of passing vehicles. The police use this technology to compare the number plates read by an ANPR camera with reference files which contain number plates of vehicles that are of interest to the police.
BIAS	Supporting or opposing a particular person or thing in an unfair way, because personal predetermined opinions influence the judgement. In an algorithmic model, bias may lead to systematic errors that create unfair outcomes.
HIT	A risk score of a place or person above a certain agreed threshold, which is regarded as 'high risk' by the data processor.
NO HIT	A risk score of a place or person below a certain agreed threshold, which is not regarded as 'high risk' by the data processor.
PERSONAL DATA	Any information relating to an identified or identifiable individual. This can be a name, location data, IP address etc.
POSITIVE HIT	When a hit is followed up by a stop and check and the stopped individuals meet the target profile of the predictive policing system.
PREDICTIVE POLICING	The application of analytical techniques across large datasets in an attempt to enable early identification of potential crime problems.

ABBREVIATIONS

ANPR	Automatic Number Plate Recognition
CCPR	International Covenant on Civil and Political Rights
CERD	Committee on the Elimination of Racial Discrimination
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DCCP	Dutch Code of Criminal Procedure
DPA	Dutch Police Act (*Politiewet*)
DPDA	Dutch Police Data Act (*Wet politiegegevens*)
LED	Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data ("Law Enforcement Directive")
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination
RTIC	Real Time Intelligence Centre of the Dutch police in Maastricht
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration on Human Rights
UN	United Nations

METHODOLOGY

The research for this report started in September 2019 and was completed in August 2020.

First, Amnesty International analysed media articles, academic literature, information released by the authorities based on freedom of information access (FOIA) requests submitted to the Dutch police and the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), and information released by the municipality of Roermond. The results of these FOIA requests were then analysed. A significant amount of information was found in documents that the Dutch police published online in August 2019 after a FOIA request.[1] In particular, an internal police report on 'mobile banditry' in Roermond provided information on the concept as deployed by the Dutch police.[2] In September 2019, Amnesty International requested information from the Dutch Data Protection Authority with the aim of obtaining the Data Protection Impact Assessments (DPIAs) carried out by the Dutch police in the context of the Sensing project and other predictive policing projects. The Dutch Data Protection Authority replied that they had no information relating to the DPIAs of the Sensing project.

Second, in an interview with the Programme Director for Digitisation and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020, Amnesty International verified the findings of this desk research and obtained additional information about the Sensing project. Audio recordings of this interview have been stored with Amnesty International.

Next, Amnesty International shared the findings presented in Section 1.2 of this report with the police and gave them the opportunity to respond and to provide comments and clarifications. These clarifications have been taken into account in the final version of this report.

Amnesty did not investigate individual cases of people affected by the Sensing project. Due to the lack of transparency on the risk model and the absence of systematic registration and evaluation of its findings, it was not possible to identify individuals who were affected by the Sensing project. This lack of transparency and adequate registration and evaluation in itself is problematic, as will be discussed in this report.

Lastly, Amnesty International conducted research on international human rights standards and European case law. Amnesty International also analysed Dutch case law to examine the jurisprudence that has developed around the scope and interpretation of the legal grounds on which the police base the data processing operations and preventive measures within the Sensing project. The legal framework that is applied in this report is included in Chapter 2.

[1] Dutch National Police, (2019) Programma Mobiel Banditisme – Proeftuin Roermond, 30 August 2019, https://www.politie.nl/wob/korpsstaf/2019-programma-mobiel-banditisme-%E2%80%93-proeftuin-roermond.html.
[2] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, n.d., https://www.politie.nl/binaries/content/assets/politie/wob/00-landelijk/programma-mobiel-banditisme-%E2%80%93-proeftuin-roermond/002---eindversie-mobiele-bendes-aan-het-roer_def.pdf.

1. HUMAN RIGHTS AND THE TREND OF PREDICTING CRIMES

In the 2002 science-fiction Hollywood film *Minority Report*, a special police unit arrests suspected criminals before they commit crimes based on the precognitive visions of three people with special powers who can see into the future.[3] Perceived back then as a far-away and fictional future, recent disturbing trends in policing indicate that "pre-crime" prediction methods are increasingly the reality. Law enforcement agencies in many countries are deploying investigative tools that they allege can 'predict' crime.[4] These methods are known as *predictive policing*.[5] Predictive policing systems are computer programs that use data and algorithmic models to assess the risk that a crime will be committed. Predictive policing systems calculate risk scores that allegedly reflect the likelihood that a person or group is or will be a victim or perpetrator (person-based predictive policing), or that a specific location will be a future crime scene (place-based predictive policing). Based on these computer-generated risk scores, the police take measures seeking to prevent or detect the predicted crime by directing policing efforts towards 'high-risk' locations, individuals or groups.[6] The Netherlands is one of the European countries at the forefront of these developments.[7]

The Dutch police increasingly deploy predictive policing techniques. One disturbing example of the use of predictive policing in the Netherlands is the Sensing project in the city of Roermond.[8] The Sensing project was launched in January 2019 and is still in place today.[9] In the Sensing project, the Dutch police collect data on vehicles driving in and around Roermond by using cameras. The collected data is analysed by an algorithm and allocated a risk score that is supposed to predict whether the driver and passengers of a car are potential pickpockets or shoplifters of Eastern European origin.

---

[3] https://www.imdb.com/title/tt0181689/.
[4] Jansen F., Data Driven Policing in the Context of Europe, Data Justice Lab, 7 May 2018, https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf; Oswald M., Grace J., Urwin S. and Barnes G., Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and Experimental Proportionality, SSRN Electronic Journal, https://doi.org/10.2139/ssrn.3029345; Perry Walter L., McInnis Brian, Price Carter C., Smith Susan C. and Hollywood John S., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.
[5] Babuta Alexander and Oswald Marion, Data Analytics and Algorithmic Bias in Policing, 16 September 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf; Garland David, The culture of control. Crime and social order in contemporary society; Chicago: University of Chicago Press, 2002, https://doi.org/10.1093/acprof:oso/9780199258024.001.0001; and Schuilenburg Marc, Predictive policing: de opkomst van een gedachtenpolitie? Ars Aequi, December 2016, https://marcschuilenburg.nl/_downloads/PredictivePolicing.pdf.
[6] Babuta and Oswald, Data analytics and Algorithmic Bias in Policing; Garland, The culture of control. Crime and social order in contemporary society; and Schuilenburg, Predictive policing: de opkomst van een gedachtenpolitie?
[7] In 2018, Amnesty International published a report on a predictive identification programme in the United Kingdom, the 'London Gang Matrix'. See: Amnesty International, Trapped in the Matrix. Secrecy, stigma, and bias in the Met's Gangs Database, May 2018, https://www.amnesty.org.uk/scrap-gangs-matrix.
[8] It should be noted that the police do not consider this particular project an example of predictive policing. They argue that they focus on observations of actual behaviour and available information [as stated in an interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020]. In Amnesty International's view, the modus operandi of the police in the Sensing project clearly falls within the generally accepted description of predictive policing, as explained in this report.
[9] In an interview in November 2019, the police explained that the software for the project was in place in January 2019. The police then started testing their algorithmic risk model. See: Prins Vera, Sensoren, risicoscores en mensenrechten, 21 June 2020, https://www.uu.nl/onderzoek/montaigne-centrum-voor-rechtsstaat-en-rechtspleging/onderzoek/montaigne-scripties, p. 11.

Over the past year, Amnesty International investigated the design and deployment of this predictive policing project and analysed it against the applicable human rights framework. The analysis finds that the Sensing project includes unlawful mass surveillance, is discriminatory from start to finish, and is extremely poorly designed, which results in an assault on human rights. Through the predictive policing tools that are used in the project, the Dutch police violate the right to privacy, the right to data protection and the right to non-discrimination. We also found that the human rights violations relating to the Sensing project are likely to occur in other predictive policing projects. This report describes the use of predictive policing tools in the Sensing project, sets out the human rights violations that result from the project, and provides recommendations to address these violations.

At the level of the European Union and the United Nations, we are seeing an attitude shift regarding predictive policing. After funding the development of predictive policing systems with millions of euros over a period of several years,[10] the European Commission has acknowledged serious human rights concerns and warned against discrimination, prejudices and biases of algorithmic models and the societal harm resulting from the use of predictive policing systems.[11] Margrethe Vestager, the EU Commissioner for Competition, explained: "Immigrants and people belonging to certain ethnic groups might be targeted by predictive policing techniques that direct all the attention of law enforcement to them."[12] Tendayi Achiume, UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, also warned that emerging digital technologies driven by big data are entrenching racial inequality, discrimination and intolerance:

> **"Technology is not neutral or objective. It is fundamentally shaped by the racial, ethnic, gender and other inequalities prevalent in society, and typically makes these inequalities worse. It is resulting in discrimination and unequal treatment in all areas of life, from education and employment to healthcare and criminal justice."**
>
> United Nations Human Rights Office of the High Commissioner, 15 July 2020.[13]

Despite this broad acknowledgement of the serious human rights risks of predictive policing projects, there is still insufficient regulation and weak oversight and accountability mechanisms. It is therefore alarming to see that the development of such systems in EU member states is moving forward at a tremendous rate.[14]

The application of predictive policing puts human rights at risk in the following ways:

- Personal data is collected or re-used without people being aware, as the police processes this information in secretive risk models that violate the right to privacy and data protection laws.
- Criteria for the inclusion of individuals in police databases and risk models are often broadly defined and lack transparency, violating the principle of legal certainty.
- The police may now take preventive measures based on the outcome of a risk model suggesting that someone is likely to have committed a crime or is planning to do so, instead of basing the decision to take preventive measures on information that connects a person to actual unlawful conduct. Subjecting someone to preventive measures (e.g. subjecting suspected individuals to additional surveillance or preventive checks) without a

[10] See: https://www.euractiv.com/section/digital/opinion/the-eu-is-funding-dystopian-artificial-intelligence-projects/.
[11] Stolton Samuel, Vestager warns against predictive policing in Artificial Intelligence, 30 June 2020, https://www.euractiv.com/section/digital/news/vestager-warns-against-predictive-policing-in-artificial-intelligence/.
[12] Ibid.
[13] United Nations Human Rights Office of the High Commissioner, Emerging digital technologies entrench racial inequality, UN expert warns, 15 July 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26101.
[14] See https://algorithmwatch.org/en/automating-society-introduction/.

reasonable suspicion of unlawful conduct is in **violation of international fair trial standards, in particular the presumption of innocence**.[15]

- People targeted by predictive policing models and subsequently submitted to preventive measures often **cannot seek effective remedy and redress** for human rights violations due to a lack of transparency in the process and the opaque nature of the algorithmic models.[16]
- Systems are designed and deployed without scientific underpinning or possibilities to measure efficacy, making it **impossible to balance the policing interest against the interests of individuals for the protections of their rights and freedoms.**
- Design and development of predictive policing systems are often touted as 'objective' and 'neutral', but prejudices and stereotypes that exist in society shape the models and algorithms and can lead to discriminatory results, with higher risk scores for certain social groups, in **violation of the right to non-discrimination**.[17]

PREDICTIVE POLICING TRENDS IN THE EU AND IN THE NETHERLANDS

Predictive policing fits within a wider trend in which governments increasingly adopt more measures that they think will exclude or reduce future risks and dangers.[18] Such measures can be employed in the pre-crime phase, even before a suspect or specific crime is identified, and also later in the criminal justice chain, for example when determining probation terms. Data and algorithms play a key role in this trend. The general assumption underlying the use of predictive policing is that these systems are beneficial for the police because crime fighting becomes more effective and efficient,[19] which will ultimately result in a safer society.[20] The use of predictive policing, however, has a range of likely adverse impacts on people's lives and their enjoyment of human rights and freedoms.

The Sensing project is not the only predictive policing project in the Netherlands. Another well-known example and the project with the largest geographical scale, is the Crime Anticipation System (*Criminaliteits Anticipatie Systeem*, often referenced as CAS), developed and tested in a pilot project in four police districts in 2014. The Crime Anticipation System allegedly predicts where and when crimes such as street robbery and burglary take place. Although the evaluation of the pilot project found no evidence that the system was effective, it was rolled out nationwide in 2017.[21] Another example is the Top400 programme deployed by the municipality of Amsterdam in partnership with the police, which calculates the risk that children and young adults will become crime suspects. Children and young adults who are listed in the top 400 entries in the ranking of risk scores are subjected to a special regime under which they may receive 'extra attention' from the authorities, including the police, municipal employees, the public prosecutor's office, and child protection services. Once added to this list of potential youth offenders, an individual's name is removed after two years, provided that they have not been a suspect of a crime during that time.[22]

---

[15] Jansen, Data Driven Policing in the Context of Europe; Lum Kristian and William Isaac, To predict and serve?, Royal Statistical Society, 2016, https://doi.org/10.1111/j.1740-9713.2016.00960.x; Bouma Kaya, 'Niet alles wat mogelijk is moet je willen', De Groene Amsterdammer, 15 June 2016, https://www.groene.nl/artikel/niet-alles-wat-mogelijk-is-moet-je-willen; Brayne Sarah, Big Data Surveillance: The Case of Policing, American Sociological Review, August 2017, https://doi.org/10.1177%2F0003122417725865; Brayne Sarah, Rosenblat Alex and Boyd Danah, Predictive Policing, Data & Civil Rights, October 25, 2015, http://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf; and Perry Walter L., McInnis Brian, Price Carter C., Smith Susan C. and Hollywood John S., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations.

[16] Amnesty International, Trapped in the Matrix.

[17] Van de Beld Jolanda, Bergstra Aldert, Huisman Eline, Kootstra Anouk and Van der Pol Linda, Smileys scoren, platlullen en downgraden, De Groene Amsterdammer, 13 March 2019, https://www.groene.nl/artikel/smileys-scoren-platlullen-en-downgraden; and Lum Kristian and William Isaac, To predict and serve?; Richardson Rashida, Schultz M. Jason and Crawford Kate, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, New York University Law Review, 2019, https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf.

[18] Garland, The culture of control. Crime and social order in contemporary society; and Control Alt Delete, Pre-crime aka predictive policing aka bijvoorbaat #verdacht, 13 February 2019, https://controlealtdelete.nl/blog/pre-crime-aka-predictive-policing-aka-bijvoorbaat-verdacht.

[19] This claim is disputed by scientists that research predictive policing systems. See e.g.: Gstrein, Oskar Josef and Bunnik, Anno and Zwitter, Andrej, Ethical, Legal and Social Challenges of Predictive Policing, 30 August 2019). Católica Law Review, Direito Penal, 2019, Volume 3 - N 3, pp. 77-98.

[20] Mali Bas, Carla Bronkhorst-Giesen and Mariëlle den Hengst, Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot, Dutch National Police, February 2017, https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF.

[21] Drenth Anthonie and Van Steden Ronald, Ervaringen van straatagenten met het Criminaliteits Anticipatie Systeem, June 2017, Tijdschrift voor de Dutch National Police, https://research.vu.nl/ws/portalfiles/portal/43772428/DrenthvanSteden2017_ErvaringenvanstraatagentenmetCAS.pdf; Dutch National Police, Criminaliteits Anticipatie Systeem verder uitgerold bij de Nationale Politie.
Das and Schuilenburg explain how in CAS, the legal mechanisms available are insufficiently transparent and precise to provide effective protection against 'dirty data', in: Abhijit Das and Marc Schuilenburg, 'Garbage in, garbage out'. Over predictive policing en vuile data, Beleid en Maatschappij (47) 3, 2020, https://tijdschriften.boombestuurskunde.nl/tijdschrift/benm/2020/3/BenM_1389-0069_2020_047_003_002.

[22] Municipality of Amsterdam, Top400, n.d., https://www.amsterdam.nl/wonen-leefomgeving/veiligheid/top400.

A political debate on the use of algorithmic models and big data predictions by the government is ongoing, although a comprehensive policy and legal framework for regulation and oversight is yet to be introduced.[23] Meanwhile, the police are running several experimental predictive policing projects under the premise that the existing legal framework sufficiently regulates their use of algorithmic models and big data predictions. With some input from academia and others in an advisory capacity, the police have defined ethical standards to address the challenges and strike a balance between the interests at stake. These standards are non-enforceable and lack effective redress mechanisms for the individuals who are subjected to the predictive policing system.[24]

[23] See e.g.: Motie van de leden Verhoeven en van der Molen over toezicht op het gebruik van algoritmes door de overheid, 26643-610, 29 May 2019; Motie van de leden Middendorp en Drost over voorwaarden voor het ontwikkelen van een richtlijn voor het gebruik van algoritmes door overheden, 35200-VII-14, 20 June 2019; Motie van de leden Verhoeven en Van der Molen over een meldplicht voor ingrijpende algoritmes, 26643-632, 10 September 2019; Motie van het lid Klaver c.s. over onderzoeken hoe het gebruik van risicoprofielen bijdraagt aan etnisch profileren, 30950-206, 1 July 2020.

[24] Amnesty International, Position paper Amnesty International t.b.v. rapport Cie. Digitale Toekomst, 9 April 2020, https://www.amnesty.nl/content/uploads/2020/04/Position-paper-Amnesty-Internatonal-cie-digitale-toekomst-voor-website.pdf?x52822.

2. LEGAL FRAMEWORK

The design and deployment of the Sensing project is assessed in light of the human rights and data protection frameworks at the level of the European Union and the Council of Europe. The analysis is based on human rights protections enshrined in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union, and the attendant case law of the European Court on Human Rights and the Court of Justice of the European Union. As regards the data protection framework, this report relies on the Council of Europe's Data Protection Convention and Recommendation No. R. (87) 15 regulating the use of personal data in the police sector, as well as EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, known as the Law Enforcement Directive.[25] For international readers, this report references the international human rights standards as laid down by the human rights bodies at the level of the United Nations, as well as their opinions and guidelines.

2.1 THE RIGHT TO PRIVACY

The right to private life is enshrined in Article 12 of the Universal Declaration on Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (CCPR), Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union (CFREU).[26] The right to private life is a broad term, which is not susceptible to an exhaustive definition.[27] The right to private life protects a right to identity and personal development, and the right to establish and develop relations with other people and the outside world.[28] There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'.[29] Limitations on the right to privacy are governed by strict criteria (see below).

Certain types of data are qualified as 'data relating to the private life', and the processing of such data falls under the scope of the privacy provisions that are laid down in Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union (CFREU). Amongst others, the European Court on Human Rights (ECtHR) has qualified personal data and data on movements in the public space as 'data relating to the private life'.[30] The ECtHR has held that the systematic collection and storing of data constitutes an interference with a person's private life, even if such data had been collected in a public space or concerned only the person's professional or public activities.[31] For example, collection of a person's movements through a GPS device attached to a person's car, and storage of such data, was found to constitute an interference with private life.[32] The

[25] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981. The Convention was modernised in 2018. See Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data; Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987; Directive (EU) Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[26] Art. 7 CFREU has at least the same meaning and scope as Art. 8 ECHR. EU law may provide more extensive protection. See Art. 52 (3) CFREU.
[27] ECtHR 25 December 2001, no. 44787/98 (P.G. and J.H. v. United Kingdom), para. 56.
[28] ECtHR 22 February 1994, Series A no. 280-B (Burghartz v. Switzerland), para. 28.
[29] ECtHR 25 December 2001, no. 44787/98 (P.G. and J.H. v. United Kingdom), para. 56.
[30] For personal data, see: ECtHR 16 November 2004, no. 29865/96 (Ünal Tekeli v. Turkey), para. 42. For data on movements in the public space, see: ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 52; and data on movements by train or air in surveillance databases: ECtHR 4 May 2000, no. 30194/09 (Shimovolos v. Russia), para. 66.
[31] ECtHR 21 June 2011, no. 30194/09 (Shimovolos v. Russia), para. 64-66.
[32] ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 51-53.

ECtHR has also recognised certain categories of sensitive data that automatically fall within the scope of the right to privacy, such as data relating to criminal offences, data revealing ethnic origin, and data relating to health.[33]

Regarding the monitoring of public spaces with sensors, the ECtHR explains:

> **"A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene […] is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."**
>
> ECtHR 25 December 2001, no. 44787/98 (P.G. and J.H. v. the United Kingdom), para. 57.

When data relating to private life are stored by authorities in the context of criminal law enforcement, there is an interference with privacy.[34] To determine the interference with privacy, it is irrelevant whether information was collected by intrusive or covert methods,[35] whether it included sensitive data,[36] was publicly available,[37] or was subsequently used[38] or consulted by a third party, and whether the person has in any way been inconvenienced as a result of the information being stored.[39] This list of circumstances do, however, add to the seriousness of the interference and should be taken into account in assessing of the justification for the interference with the right to privacy.

The ECtHR has also concluded that stopping and searching a person in public can be an interference with the right to privacy.[40] *Gillan and Quinton v. the United Kingdom* concerned stop and search powers that were used by the police authorities to search for goods that could be used in connection with terrorism-related offences. The ECtHR considered that the use of coercive powers to require an individual to submit anywhere and anytime to a detailed search of their person, clothing and personal belongings amounted to a clear interference with the right to privacy.[41] It was irrelevant in that context whether the authorities discovered any private documents during the search. The public nature of the search also did not render Art. 8 ECHR inapplicable: in the view of the ECtHR, the public nature may compound the seriousness of the interference due to experienced humiliation and embarrassment.[42]

This ruling and the analysis of the right to privacy indicate that predictive policing systems that rely upon sensor data in public spaces or in other ways collect personal information constitute an interference with the right to privacy. The following section analyses grounds for justification of the interference with privacy in order to determine whether predictive policing is lawful or not.

---

[33] ECtHR 4 May 2000, no. 28341/95 (Rotaru v. Romania), para. 43-46; ECtHR 17 March 2010, no. 5335/06 (B.B. v. France), para. 56; ECtHR 13 November 2012, no. 24029/07 (M.M. v. United Kingdom), para. 188; ECtHR 29 April 2014, no. 52019/07 (L.H. v. Latvia), para. 56; ECtHR 23 February 2016, no. 40378/06 (Y.Y. v. Russia), para. 38 and 57; ECtHR 26 January 2017, no. 42788/06 (Surikov v. Ukraine), para. 75; ECtHR 6 June 2013, no. 1585/09 (Avilkina v. Russia); ECtHR 15 April 2014, no. 50073/07 (Radu v. Republic of Moldavia); ECtHR 29 April 2014, no. 52019/07 (L.H. v. Latvia). See for an overview of 'data relating to the private life': Forder C.J., Vonk M.J., Sanderink D.G.J, Gysels C., Klaassen M.A.K., Smet S., Koning M. and Hagens M, Sdu Commentaar Europees Verdrag voor de Rechten van de Mens. Art. 8 – Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, 4 June 2019, https://opmaat-sdu-nl.proxy.library.uu.nl/book/SDU_SDU_COMMENTAAR_c_EVRM_N10008_8/c_EVRM_N10008_8.

[34] ECtHR 16 February 2000, no. 27798/95 (Amann v. Switzerland), para. 65-67; ECtHR 7 July 2015, no. 28005/12 (M.N. and others v. San Marino), para. 53.

[35] ECtHR 4 May 2000, no. 28341/95 (Rotaru v. Romania), para. 43-44.

[36] ECtHR 6 June 2006, no. 62332/00 (Segerstedt-Wiberg and others v. Sweden), para. 71-72.

[37] ECtHR 25 December 2001, no. 44787/98 (P.G. and J.H. v. the United Kingdom), para. 57.

[38] ECtHR 16 February 2000, no. 27798/95 (Amann v. Switzerland), para. 69-70.

[39] ECtHR 6 June 2006, no. 62332/00 (Segerstedt-Wiberg and others v. Sweden), para. 68.

[40] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 61-65.

[41] Ibid. para. 64.

[42] Ibid. para. 63.

2.2 JUSTIFICATION CRITERIA

The right to privacy is not absolute, but any government interference must adhere to a strict set of criteria provided in international standards. An interference with the right to privacy must pursue a legitimate aim, be in accordance with the law, and be necessary in a democratic society, as provided under Art. 8(2) ECHR. These criteria are cumulative, meaning that all three criteria must be fulfilled in order for the interference with the right to privacy to be justified.[43] Each criterion is explained in detail in the context of predictive policing in the following paragraphs.

First, the legitimate aim should be pursuant to the interests mentioned in Art. 8(2) ECHR, namely that of "national security, public safety or the economic well-being of a country, the prevention of disorder or crime, the protection of health or morals, and the protection of rights and freedoms of other persons."[44] For measures relating to predictive policing, authorities may rely upon the legitimate aim of "the prevention of disorder or crime". The ECtHR accepts the prevention of disorder or crime as a legitimate aim without extensive examination.[45]

Secondly, the measure must be in accordance with the law.[46] This requires first that the measure has some basis in domestic law. It also refers to the quality of the law that provides the legal grounds for interference.[47]

The law should be accessible to the persons concerned (accessibility) and have foreseeable effects (foreseeability).[48] The foreseeability requirement entails that the law must be formulated with sufficient precision to enable a person to regulate their conduct.[49] The law must be sufficiently clear in its terms to give people an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to the measures that interfere with privacy rights.[50] The law must therefore indicate the scope of discretion granted to the competent authorities and the manner of its exercise to protect against arbitrary interference by public authorities.[51]

In the context of interferences with the right to privacy, the ECtHR has emphasised that, as technology becomes more sophisticated, it is important that laws are sufficiently precise and that they contain adequate safeguards.[52] The ECtHR has held that the protection of personal data is of fundamental importance to a person's enjoyment of their right to privacy.[53] The ECtHR therefore finds that "the need for safeguards against arbitrary interferences is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data is used for police purposes".[54] The ECtHR considers that monitoring technologies have progressed in a way which is hardly conceivable for the average citizen, referring to the technological possibilities of automated and systemic data collection.[55] The development of surveillance methods resulting in masses of data collected must be accompanied by a simultaneous development of legal safeguards securing respect for human rights.[56] The need for data protection safeguards is thus all the greater when personal data is processed automatically and through new technologies, in particular when data is used for police purposes.[57]

Objective and impartial oversight is a key safeguard in criminal law enforcement when the authorities engage in measures that interfere with human rights. In *Sanoma Uitgevers B.V. v. the Netherlands*, the ECtHR emphasised the importance of a guarantee of review by a judge or another independent and impartial decision-making body.[58] This case concerned police demands for photographs taken by journalists, which constitutes interference with the freedom to

[43] ECtHR 30 July 1998, no. 27671/95 (Valenzuela Contreras v. Spain), para. 46.
[44] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) [1950] Art. 8, para 2.
[45] ECtHR 4 December 2008, no. 30562/04 and 30566/04 (S. and Marper v. United Kingdom), para. 100; ECtHR 7 July 2015, no. 28005/12 (M.N. and others v. San Marino), para. 75; See also CJEU 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd and Kärlrntner Landesregierung v. Michael Seitlinger, Christof Tschohl e.a.), p. 43.
[46] ECtHR 18 October 2016, no. 61838/10 (Vukota-Bojić v. Switzerland), para. 66.
[47] ECtHR 30 July 1998, no. 27671/95 (Valenzuela Contreras v. Spain), para. 46.
[48] ECtHR 30 July 1998, no. 27671/95 (Valenzuela Contreras v. Spain), para. 46. See also ECtHR, no. 27798/95 (Amann v. Switzerland) para. 50; ECtHR 25 March 1998 (Kopp v. Switzerland) para. 55; ECtHR 10 February 2009, no. 25198/02 (Iordachi and Others v. Moldova), para. 50; ECtHR 2 August 1984, no. 8691/79 (Malone v. the United Kingdom) para. 66.
[49] ECtHR 2 August 1984, no. 8691/79 (Malone v. the United Kingdom) para. 66.
[50] ECtHR 2 August 1984, no. 8691/79 (Malone v. United Kingdom), para. 67; ECtHR 26 March 1987, no. 9248/81 (Leander v. Sweden), para. 51; ECtHR 24 April 1990, no. 11105/84 (Huvig v. France), p. 29; ECtHR 4 May 2000, no. 28341/95 (Rotaru v. Romania), p. 55; ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 62; ECtHR 18 May 2010, no. 26839/05 (Kennedy v. the United Kingdom), para. 159.
[51] ECtHR 4 December 2008, no. 30562/04 (S. and Marper v. United Kingdom), para 95.
[52] ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 61.
[53] ECtHR 17 December 2009, no. 16428/05 (Gardel v. France), para. 62; ECtHR 13 November 2011, no. 24029/07 (M.M. v. United Kingdom), para. 195.
[54] Ibid. para. 195.
[55] ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 61.
[56] ECtHR 12 January 2016, no. 37138/14 (Szabó and Vissy v. Hungary), para. 66-68; ECtHR 18 October 2016, no. 61838/10 (Vukota-Bojić v. Switzerland), para. 67.
[57] ECtHR 17 March 2010, no. 16428/05 (Gardel v. France), para. 62.
[58] ECtHR 14 September 2010, no. 38224/03 (Sanoma Uitgevers B.V. v. the Netherlands), para. 90.

receive and impart information under Art. 10 ECHR.[59] The ECtHR held that a review of the interference should be carried out by a body separate from the executive and other interested parties and should be carried out at the very least prior to the access and use of obtained materials.[60] The decision taken should be governed by clear criteria.[61] This case is important in the light of criminal law enforcement, because the ECtHR held that the Dutch public prosecutor is a party that defends the interests of criminal law enforcement, and can therefore not be seen as sufficiently objective and impartial to make the necessary assessment of various competing interests, including the protection of human rights.[62] Moreover, the ECtHR did not consider the involvement of the public prosecutor in the Sanoma case to be an adequate safeguard because of the absence of a specific legal basis for the involvement of the prosecutor as well as clear criteria for the public prosecutor's proportionality decision.[63]

In the context of preventive measures, such as stops and searches, there is very limited jurisprudence from the ECtHR on the required legal safeguards – in particular where there is no reasonable suspicion against the individual being stopped. From the cases that have been addressed, the ECtHR has set out the following requirements against abuse. Firstly, the legal basis for preventive checks should only allow for preventive checks when they are necessary, which in turn can only be the case if the checks are actually effective in contributing to the defined objective of preventing and detecting crime. Checks that are unlikely to contribute to the objective would violate the principle of necessity and therefore also the human rights affected by the check. Furthermore, the proportionality of a preventive check should be assessed.[64] Secondly, the power given to the police should be limited geographically and/or temporally: the police may carry out preventive checks as far as necessary and proportionate in a specific area, for a given period of time.[65] Thirdly, the discretion of police officers to carry out preventive checks should be restricted. The category of people that may be subjected to preventive checks should be limited.[66] The ECtHR has stressed that a wide discretion creates a risk of arbitrariness and a risk of discriminatory use of powers.[67] In addition, affected people should be able to challenge a check to determine if the check was lawful or an abuse of power.[68] The powers of the police to carry out preventive checks must be sufficiently circumscribed and subjected to adequate legal safeguards against abuse. If such powers are insufficiently circumscribed and not subjected to adequate legal safeguards, they are not in accordance with the law and in violation of Art. 8 ECHR.[69]

Thirdly, for the interference to be necessary in a democratic society, the interference must correspond to a "pressing social need" that is proportionate to the legitimate aim pursued. The interest of the State, which has to indicate a pressing social need, must be balanced against the seriousness of the interference with people's right to respect for their private life.[70] In order to determine whether measures were "necessary in a democratic society", the ECtHR considers whether, in light of the case as a whole, the reasons adduced to justify the measures were relevant and sufficient, and whether the measures were proportionate to the legitimate aims pursued. The ECtHR leaves a 'margin of appreciation' to the competent national authorities in striking a fair balance between the competing interests. The scope of this margin of appreciation depends on factors such as the nature and seriousness of the interests at stake and the seriousness of the interference.[71]

It should be stated clearly that Amnesty International believes that indiscriminate mass surveillance will never fulfil the requirements of necessity and proportionality. Several factors demonstrate a disproportionate interference: the indiscriminate collection of personal data from persons who are not convicted of offences,[72] the storage of such data irrespective of the nature or gravity of the offence of which the person is suspected or the age of the offender, and the lack of independent review of the justification for data retention according to defined criteria, including factors such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and other special circumstances.[73] Furthermore, the Council of Europe explains in a practical guide to the use of personal data in law enforcement that "the high potential of severe interference with the right to privacy has to be balanced with the

[59] Ibid. para. 1-29.
[60] ECtHR 14 September 2010, no. 38224/03 (Sanoma Uitgevers B.V. v. the Netherlands), para. 90-91.
[61] Ibid. para. 92.
[62] Ibid. para. 93.
[63] Ibid. para. 92 and 96.
[64] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 80.
[65] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 80; ECtHR 15 May 2012, no. 49458/06 (Colon v. the Netherlands), p. 83.
[66] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 83-84.
[67] Ibid. para. 85.
[68] Ibid. para. 81 and 86.
[69] Ibid. para. 80-87.
[70] ECtHR 26 March 1987, no. 9248/81 (Leander v. Sweden) para. 58-59; ECtHR 4 December 2008, no. 30566/04 (S. and Marper v. the United Kingdom), para. 125.
[71] Ibid. para. 125.
[72] ECtHR 4 December 2008, no. 30566/04 (S. and Marper v. the United Kingdom), para. 125.
[73] Ibid. para. 119.

seriousness of the offence to be prevented or investigated and the cost-effectiveness, the use of resources and the efficiency of investigations".[74]

In summary, interference with the right to privacy conducted under predictive policing programmes that rely on mass surveillance would only be considered justified (and lawful) if it is conducted for the purpose of crime prevention, within the international and domestic legal safeguards, and must be necessary and proportionate to the legitimate aim pursued. Mass surveillance can never meet the criteria of necessity and proportionality.

2.3 THE RIGHT TO DATA PROTECTION

In the design and deployment of predictive policing programmes, the police frequently process personal data. Personal data is defined as "any information relating to an identified or identifiable individual". The identified or identifiable individual is the 'data subject'.[75] Predictive policing programmes often use personal data, especially in person-based predictive policing. Personal data is collected, stored, processed through algorithmic models, and used for operational and/or analytical purposes.

People have the right to data protection: data must be processed lawfully. The ECtHR has recognised the fundamental importance of data protection for the effective exercise of the right to privacy.[76] Within the Council of Europe, data protection norms have been laid down in the Data Protection Convention.[77] In addition, the Council of Europe issued a specific recommendation regulating the use of personal data in the police sector (Recommendation No. R (87) 15).[78] Within the EU, Article 8 CFREU enshrines a specific right to the protection of personal data. EU law also provides for a specific regime for the processing of personal data by the police for the purpose of the prevention of criminal offences, in Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, known as the Law Enforcement Directive (LED).[79]

The right to data protection requires a legitimate basis of processing, pursuant to Art. 8(2) CFREU. Data may only be processed if the purpose is explicit, specified, and legitimate under the law.[80] **Data processing must also be proportionate.** The principle of proportionality is to be respected at all stages of the processing, including at the stage of deciding whether or not to carry out data processing at all.[81] The right to data protection includes the principle of data minimisation, which requires data to be relevant for the purpose of the processing.[82] Safeguards are also required to guarantee that personal data kept in databases are accurate.[83] In the storage of data for example, a distinction must be made between categories of subjects and categories of data reliability. Personal data based on facts should for instance be distinguished from personal data based on personal assessments, or in the case of predictive policing, data based on mere algorithmic predictions.[84]

---

[74] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Practical guide on the use of personal data in the police sector, T-PPD (018)01, Strasbourg, 15 February 2018, para. 8.
[75] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18 May 2018, Art. 2 (A); Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Art. 3 (1). The ECtHR refers to this definition as well. See e.g. ECtHR 4 December 2008, no. 30562/04 and 30566/04 (S. and Marper v. United Kingdom), para. 41.
[76] ECtHR 17 December 2009, no. 16428/05 (Gardel v. France), para. 62; ECtHR 13 November 2011, no. 24029/07 (M.M. v. United Kingdom), para. 195.
[77] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981. The Convention was modernised in 2018. See Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.
[78] Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987.
[79] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Art. 2.
[80] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Art. 5 (4) (b); Directive 2016/680, Art. 4 (1) (b).
[81] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Article 5 (1); Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, para. 40.
[82] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Art. 5 (4) (c); Directive 2016/680, Art. 4 (1) (c). The ECtHR also requires e.g. that data is relevant and not excessive in relation to the purposes. ECtHR 17 March 2010, no. 16428/05 (Gardel v. France), para. 62; ECtHR 6 June 2016, no. 37138/14 (Szabó and Vissy v. Hungary), para. 73.
[83] Directive 2016/680, Art. 4 (1) (d). The ECtHR also requires procedural safeguards to prevent inaccurate data being processed. See ECtHR 18 February 2009, no. 22427/04 (Cemalettin Canli v. Turkey), para. 42.
[84] Directive 2016/680, Art. 7 (1).

Art. 27 LED requires the police to carry out a Data Protection Impact Assessment (DPIA) in the event that a type of processing is likely to result in a high risk to the rights and freedoms of people. The DPIA obligation has existed since 6 May 2018, when the revised European regulatory framework on data protection took effect.[85] A DPIA must contain at least a general description of the envisaged data processing, an assessment of the risks to the rights and freedoms of the data subjects, the measures envisaged to address those risks, and safeguards, security measures and mechanisms to ensure the protection of personal data.[86] In 2017, the European Data Protection Board (EDPB), the EU body in charge of the supervision of most of the EU data protection framework,[87] published guidelines on the factors contributing to a high risk to people's rights in data processing.[88] These factors include:

- Evaluation or scoring, including profiling and predicting;
- Systematic monitoring, including the systematic monitoring of a publicly accessible area;
- Processing of sensitive data or data of a highly personal nature, including personal data relating to criminal convictions or offences and location data;
- Data processed on a large scale;[89]
- Matching or combining datasets;[90]
- Innovative use or application of new technological or organisational solutions. As an example, the guidelines mention the use of a camera system to monitor driving behaviour on highways and consequently using intelligent video analysis to single out cars and automatically recognise licence plates.

When the data processing includes the use of new technologies and poses a high risk, the police are obligated to consult with the data protection authority of that member state as specified in Art. 28(1)(b) LED. State actions that affect human rights must not only have a sufficiently clear and precise legal basis, which fulfils the principles of foreseeability, necessity and proportionality, they must also be carried out in accordance with procedures established in law. Not carrying out a DPIA and not consulting with the national data protection authority therefore constitutes a violation of the principle of legality.

In a Recommendation on the human rights impacts of algorithmic systems, the CoE holds that States should not only address the data protection impact of algorithmic systems, but all human rights risks, by carrying out a *human rights* impact assessment.[91] Amongst others, States should ensure that computational experimentation that is likely to trigger significant human rights impacts is conducted only after a human rights impact assessment.[92] The free, specific, informed and unambiguous consent of participating individuals should be sought in advance, with an accessible means of withdrawing consent, and experimentation designed to produce deceptive or exploitative effects should be explicitly prohibited.[93]

In the design, development, ongoing deployment and procurement of algorithmic systems, States should carefully assess what human rights may be affected as a result of the quality of the data that are being put into and extracted from the algorithmic system. This recommendation relates not only to data protection norms, but also to the right to non-discrimination (discussed below): the CoE states that data "often contain bias and may stand in as a proxy for classifiers such as gender, race, religion, political opinion or social origin".[94]

States should carefully assess the provenance and possible shortcomings of the dataset, the possibility of its inappropriate or decontextualised use, the negative externalities resulting from these shortcomings and inappropriate

---

[85] Directive (EU) 2016/680, Directive (EU) 2016/680, Art. 64; Art. 27, (1). This obligation is implemented in Dutch law: see the Police Data Act (*Wet politiegegevens*), Art. 4c (1). Because Art. 27 is suitable for direct application, this obligation existed from the applicability date of the LED and is not dependent on transposition in Dutch national law for its legal effect on the police.
[86] Directive 2016/680, Article 27 (2).
[87] The EDPB consists of the head of one supervisory authority of each EU member state and of the European Data Protection Supervisor, or their respective representatives; Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Art. 68-76 and Art. 94. With the coming into force of the EU General Data Protection Regulation (GDPR), the European Data Protection Board (EDPB) was established, which has inherited the work of the Article 29 Working Party. The EDPB consists of the head of one supervisory authority of each EU member state and of the European Data Protection Supervisor, or their respective representatives.
[88] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017.
[89] Relevant factors are the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration of the data processing and the geographical extent of the processing.
[90] This includes, for example, merging datasets originating from two or more data processing operations performed for different purposes, in a way that exceeds the reasonable expectations of the data subject.
[91] Recommendation CM/REC(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Minister's Deputies, para. 5.2.
[92] Ibid. para. 3.1.
[93] Ibid. para. 3.1.
[94] Ibid. para. 2.2.

uses as well as the environments within which the dataset will be or could possibly be used.[95] In addition, algorithmic systems should be regularly tested, evaluated, reported and audited against state-of-the-art standards related to completeness, relevance, privacy, data protection, other human rights, unjustified discriminatory impacts and security breaches before, during and after production and deployment – in particular where automated systems are tested in live environments and produce real-time effects.[96]

With regard to bias and discriminatory outputs, States should ensure that the functioning of the algorithmic systems that they implement is tested and evaluated with due regard to the fact that outputs vary according to the specific context in which they are deployed and the size and nature of the dataset that was used in the system. States should be aware of the risks of testing samples or outputs being re-used in contexts other than those for which the system was originally developed, including when used for the development of other algorithmic systems. This should not be permitted without new testing and an evaluation of the appropriateness of such uses.[97]

2.4 THE RIGHT TO NON-DISCRIMINATION

In international human rights law, discrimination is defined as any distinction, exclusion, restriction or preference which is based on any grounds such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.[98] Discrimination is prohibited under various human rights treaties, including Art. 7 of the Universal Declaration on Human Rights (UDHR), Art. 26 of the International Covenant on Civil and Political Rights (CCPR), Art. 14 of the European Convention on Human Rights (ECHR) and Art. 21 of the Charter of Fundamental Rights of the European Union (CFREU).[99] The purpose of non-discrimination laws is to allow all people an equal and fair prospect to access the opportunities within a society.[100] People who are in similar situations should be treated similarly and should not be treated less favourably because they possess a particular characteristic, unless there is a reasonable and objective justification for doing so.[101] This means that not all unequal treatment constitutes discrimination: unequal treatment may be justified. In order for unequal treatment to be justified, the criteria for that differentiation must be reasonable and objective and have a legitimate purpose.[102] For example, unequal treatment cannot be justified based on negative views or aversion to a particular group.[103]

The prohibition of racial discrimination is a fundamental tenet of international law. The prohibition of racial discrimination is considered a *'Jus cogens'*, or peremptory norm of international law, which means it is binding on all States and cannot be derogated from, nor opted out of by a State.[104] A key treaty as regards racial discrimination is the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD). The ICERD obliges States to take measures to eliminate racial discrimination, which is defined as any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life.[105] The ICERD does not provide a definition of 'race' or 'ethnicity', and does not distinguish between the two concepts.[106] The ICERD is monitored by the Committee on the Elimination of Racial Discrimination (CERD), which has formulated norms to prevent discrimination by police authorities in a number of recommendations. The CERD has emphasised the need to combat discrimination of certain groups

[95] Ibid. para. 2.2.
[96] Ibid. para. 3.3.
[97] Recommendation CM/REC(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Minister's Deputies, para. 3.4.
[98] UN Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination, 10 November 1989, para. 7. For the protected grounds under European law, see European Union Agency for Fundamental Rights and Council of Europe, Handbook on European non-discrimination law, 2018, p. 155-227.
[99] Article 14 ECHR can only be invoked in connection with one of the substantive treaty rights of the ECHR. Since 2000, the ECHR also contains an independent prohibition of discrimination in Article 1 of Protocol No. 12 to the ECHR. This Article potentially has a broader material scope of application but is further interpreted in the same manner as Article 14 ECHR. See e.g. ECtHR 22 December 2009, nos. 27996/06 and 34836/06 (Sejdić and Finci v. Bosnia and Herzegovina), para. 55-56.
[100] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European non-discrimination law, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf, p. 42-43.
[101] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European non-discrimination law, 2018, p. 42-43.
[102] UN Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination, 10 November 1989, para. 13.
[103] ECtHR 20 June 2017, no. 67667/09, (Bayev and others v. Russia), para. 68.
[104] Vienna Convention on the Law of Treaties 1969, Article 53.
[105] International Convention on the Elimination of All Forms of Racial Discrimination, Art. 1 (1).
[106] The ECtHR and the CJEU refer to the definition of racial discrimination by the ICERD and hold ethnicity and race to be related concepts. ECtHR 22 December 2009, no. 27996/06 and 34836/06 (Sejdić and Finci v. Bosnia and Herzegovina), para. 43. See similarly CJEU 16 July 2015 (CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia), para. 46 and 73.

which are particularly exposed to exclusion, marginalisation, and non-integration in society. The CERD explicitly refers to non-citizens and Roma in its determination to combat discrimination:

> **"Combat all forms of discrimination in the administration and functioning of the criminal justice system which may be suffered, in all countries of the world, by persons belonging to racial or ethnic groups, in particular non-citizens – including immigrants, refugees, asylum-seekers and stateless persons – Roma/Gypsies, indigenous peoples, displaced populations, persons discriminated against because of their descent, as well as other vulnerable groups which are particularly exposed to exclusion, marginalisation and non-integration in society"**
>
> Committee on the Elimination of Racial Discrimination, General Recommendation 31 on the prevention of racial discrimination in the administration and functioning of the criminal justice system, 65th session, 2005, para. 29.

In the context of policing, one form of racial discrimination is 'ethnic profiling'. Amnesty International defines ethnic profiling as the use, without objective and reasonable justification, of personal characteristics such as colour, religion, nationality and/or ethnic origin in police control, surveillance or investigation activities.[107] In other words, ethnic profiling takes place if – in the absence of a suspect description – personal attributes such as presumed race, colour, descent, nationality or ethnic origin etc. are taken into account in law-enforcement decision-making.

The CERD is currently working on an internationally accepted definition. Amnesty has recommended that the CERD clarify in the definition that ethnic profiling includes the use of personal attributes (such as presumed race, colour, descent, nationality or ethnic origin) not only as stand-alone decisive factors, but also in combination with other factors. Amnesty also stresses that the definition of ethnic profiling encompasses its various manifestations. Ethnic profiling is not limited to situations of open discrimination, nor does it require any intention to discriminate. On the level of the individual officer, ethnic profiling may be the result of clearly discriminatory attitudes or of unconscious bias. At an institutional level, there may be policies or approaches that are explicitly discriminatory or encouraging ethnic profiling, while ethnic profiling practices may also be the result of seemingly neutral policies which impose criteria that disproportionately affect certain groups in actual practice.[108]

Under all circumstances, ethnic profiling violates the principle of non-discrimination. It is ineffective and has harmful consequences.[109] It leads to the criminalisation of certain categories of persons, reinforcing stereotypical associations between crime and ethnic origin. Ethnic profiling contributes to the stigmatisation of groups, which has a negative impact on the mindset and well-being of the people affected.[110] They often have fewer social and economic opportunities as a

[108] Amnesty International, Observations to the United Nations Committee on the Elimination of Racial Discrimination Draft General Recommendation No. 36 on Preventing and Combating Racial Discrimination, June 2019, https://www.amnesty.org/download/Documents/IOR4006242019ENGLISH.pdf
[109] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken; Open Society Institute, Ethnic Profiling in the European Union: Pervasive Ineffective, and Discriminatory, 2009, https://www.justiceinitiative.org/publications/ethnic-profiling-european-union-pervasive-ineffective-and-discriminatory.
[110] Bradford Ben, Jackson Jonathan and Stanko Elizabeth A., Contact and confidence: revisiting the impact of public encounters with the police, Policing and Society, March 2009, https://doi.org/10.1080/10439460802457594; Geller Amanda, Fagan Jeffrey, Tyler Tom and Link Bruce G., Aggressive Policing and the Mental Health of Young Urban Men, American Journal of Public Health, December 2014, https://dx.doi.org/10.2105%2FAJPH.2014.302046; Miller Joel, Davis Robert C., Henderson Nicole J., Markovic John, Ortiz Christopher W., Public Opinions of the Police. The Influence of Friends, Family, and News Media, May 2004, https://www.ncjrs.gov/pdffiles1/nij/grants/205619.pdf; Tyler Tom R., Fagan Jeffrey and Geller Amanda, Street Stops and Police Legitimacy: Teachable Moments in Young Urban Men's Legal Socialization, Journal of Empirical Legal Studies, 28 October 2014, https://doi.org/10.1111/jels.12055.

result.[111] These practices are not effective in preventing crime. In general, personal characteristics are not considered to be helpful operational criteria to combat crime. Criteria based on ethnicity, for example, are simultaneously over-inclusive (individuals with a certain characteristic are included in analysis, even if they are not involved in or associated with criminal conduct) and under-inclusive (individuals who are involved in criminal conduct, but do not have the same specific characteristic, are neglected by the system). Using such criteria risks creating a self-fulfilling prophecy, where a minority group targeted by the predictive policing system appears more frequently with high risk scores, and related crime committed by individuals from this specific group is reported in higher numbers as a result.[112] Moreover, ethnic profiling can hamper the effectiveness of the police. Feelings of injustice, humiliation and loss of trust in the police and other authorities can lead to a reduced willingness on the part of profiled individuals and groups to cooperate with the police or to report crimes.[113] In a recent draft recommendation, the CERD held that law enforcement agencies should commit to collecting disaggregated data on relevant law enforcement practices such as identity checks, traffic stops or boarder searches. This should include information on the ethnic origin of members of the public targeted, as well as the details and outcome of the encounter. The anonymised statistics should be made public and discussed with local police and communities.[114] Such data should be collected in accordance with human rights and should not be misused.[115]

A distinction is made between direct and indirect discrimination. In cases of direct discrimination, the unequal treatment is directly based on protected grounds. In cases of indirect discrimination, the unequal treatment is based on seemingly neutral grounds, but it disproportionately affects people with a certain protected characteristic. Both direct and indirect discrimination are prohibited under human rights law.[116] Direct discrimination may for example be found when police action is taken based on the protected characteristics of certain people. In *Lingurar v. Romania*, the ECtHR found the discriminatory nature of police measures proven by the police's statements in a policy document that linked ethnic origin to criminal behaviour.[117]

Indirect discrimination may be found when a measure results in a disproportionate number of people with a certain protected characteristic being disadvantaged. In such cases, a presumption of indirect discrimination arises. The burden of proof then shifts to the State, who must show that the difference in treatment is not discriminatory.[118] An example of indirect discrimination is found in the case *Biao v. Denmark.* In this case, the ECtHR explained that a measure which distinguishes between nationalities leads to indirect discrimination based on ethnicity when it can reasonably be assumed that people with a certain ethnic origin will generally be disadvantaged by the measure.[119] Where a difference in treatment is based on race or ethnicity, the notion of objective and reasonable justification must be interpreted as strictly as possible.[120]

States must not only refrain from discriminatory measures, but they also have a *positive obligation* to prevent the perpetuation of past discriminatory practices disguised in allegedly neutral tests.[121] The ECtHR explained this in *Horváth and Kiss v. Hungary*, a case concerning the placement of two young men at a 'special' school, created for children with mental disabilities. They argued that the diagnostic system for children in Hungary was flawed and discriminatory towards children of Roma ethnicity.[122] The ECtHR noted that the misplacement of Roma children in special schools had a long history across Europe.[123] In light of the recognised bias in past placement procedures, the Court considered that

[111] Open Society Justice Initiative, Reducing Profiling in the European Union: A Handbook of Good Practices, 6 March 2013, https://www.justiceinitiative.org/publications/reducing-ethnic-profiling-european-union-handbook-good-practices.
[112] Delsol Rebekah, Effectiveness, in: Stop and Search, Palgrave Macmillan London, 2015, https://doi.org/10.1057/9781137336101_5; European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide; Harcourt 2007; Open Society Justice Initiative 2007; Tiratelli et al 2018; Weisburg et al 2019.
[113] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p. 35-59; European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide; Open Society Justice Initiative, Reducing Profiling in the European Union. A Handbook of Good Practices; Tyler Tom R., Fagan Jeffrey and Geller Amanda, Street Stops and Police Legitimacy: Teachable Moments in Young Urban Men's Legal Socialization.
[114] CERD Draft General Recommendation No. 36, Preventing and Combating Racial Profiling: A call for contribution by 30 June 2019, CERD/C/GC/36, 14 May 2019.
[115] Ibid. p. 31.
[116] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European non-discrimination law, p. 42.
[117] ECtHR 16 April 2019, no. 48474/14 (Lingurar v. Romania), para. 74. See for similar reasoning CJEU 10 July 2008 C-54/07 (Centrum voor Gelijkheid van kansen en voor Racismebestrijding v. Firma Feryn NV), para 2; CJEU 23 April 2020, C-507/18 (Associazione Avvocatura per i diritti LGBTI), para. 39-46.
[118] ECtHR 13 November 2007, no. 57325/00 (D.H. and others v. Czech Republic), para. 185-189; CJEU 13 July 1989, C-171/88 (Ingrid Rinner-Kühn v. FWW Spezial-Gebäudereinigung GmbH & Co. KG); CJEU 7 February 1991, C-184/89 (Helga Nimz t. Freie and Hansestadt Hamburg); CJEU 27 June 1990, C-33/89 (Maria Kowalska v. Freie en Hansestadt Hamburg); CJEU 24 February 1994, C-343/92 (M.A. De Weerd, née Roks and others v. Bestuur van de Bedrijfsvereniging voor de Gezondheid, Geestelijke en Maatschappelijke Belangen and others).
[119] ECtHR 24 May 2016, no. 38590/10 (Biao v. Denmark), para. 111-113.
[120] ECtHR 24 May 2016, no. 38590/10 (Biao v. Denmark), para. 114; ECtHR 22 December 2009, no. 27996/06 and 34836/06 (Sejdić and Finci v. Bosnia and Herzegovina), para. 44.
[121] ECtHR 29 January 2013, no. 11146/11 (Horváth and Kiss v. Hungary), para. 116, 119 and 127.
[122] Ibid. para. 80 and 114. Reports showed that 20% of children with Roma ethnicity were assigned to special classes, compared with only 2% of other children.
[123] Ibid. para. 115.

Hungary had specific positive obligations to avoid the perpetuation of past discrimination or discriminatory practices embedded in allegedly neutral tests.[124] The ECtHR recalled its considerations in the case *Alajos Kiss v. Hungary*:

> **"If a restriction on fundamental rights applies to a particularly vulnerable group in society, who have suffered considerable discrimination in the past (…) then the State's margin of appreciation is substantially narrower and it must have very weighty reasons for the restrictions in question."**
>
> ECtHR, 20 May 2010, no. 38832/06 (Alajos Kiss v. Hungary), para. 42-44.

In *Horváth and Kiss v. Hungary*, Hungary had to demonstrate that the tests and their application were fair and objective.[125] The ECtHR emphasised that the State had to have made good faith efforts to achieve non-discriminatory testing. Various factors in the case lead the ECtHR to conclude that the tests did not provide the necessary safeguards against misdiagnosis that would follow from the positive obligations incumbent on the State in a situation where there was a history of discrimination against a certain ethnic group.[126] At the very least, there was a danger that the tests were culturally biased.[127] The schooling arrangements were not attended by adequate safeguards that would ensure that the State took into account the special needs of children with Roma ethnicity, as members of a disadvantaged class.[128] The ECtHR held that the tests could not be considered to serve as sufficient justification for the placement of children with Roma ethnicity in special schools and concluded that the practice was in violation of Article 14 ECHR.[129]

Finally, it is worth noting that there is a special provision under EU law that prohibits any discrimination on grounds of nationality (Art. 18 TFEU). With respect to data processing, the CJEU particularly held that the fight against crime cannot justify the systematic processing of personal data exclusively of EU citizens who are not nationals of the member state concerned. The CJEU stresses that the fight against crime should focus on the prosecution of crimes and offences, regardless of the nationality of perpetrators.[130]

[124] Ibid. para. 116.
[125] ECtHR 29 January 2013, no. 11146/11 (Horváth and Kiss v. Hungary), para. 117.
[126] Ibid. para. 119-123.
[127] Ibid. para. 121.
[128] Ibid. para. 127.
[129] Ibid. para. 123-129.
[130] CJEU 16 December 2008, C-524/06 (Heinz Huber v. Germany), para. 77.

3. THE SENSING PROJECT IN MORE DETAIL

Roermond is a small city with approximately 42,000 inhabitants, located in the province of Limburg in the south-eastern region of the Netherlands. Roermond is at the German border and only 20 kilometres from Belgium. Its number-one attraction, with 8 million visitors per year, is a privately-owned outlet shopping centre that houses designer brand shops.[131] The Dutch police run a predictive policing project in Roermond that centres around 'predicting' likely perpetrators of pickpocketing and shoplifting in this shopping centre. In an internal study, the Roermond police set out the scope and characteristics of pickpocketing and shoplifting in the city.[132] The Roermond police register between 310 and 449 suspects of pickpocketing or shoplifting in the shopping centre per year.[133] In the internal study, the police detail the nationality of suspects. The numbers show that more than half (around 60%) of those suspects are individuals of Dutch nationality, and that around 22% of the total number of suspects are individuals with an Eastern European nationality.[134]

However, the internal study conducted by the police, as well as the Sensing project in general, focused on 'mobile banditry', a concept generally used by the police for various economic crimes committed by foreign groups of so-called 'bandits'.[135] The police claim that most of the time, 'mobile banditry' is committed by persons coming to the Netherlands from Eastern European countries.[136] The police explicitly exclude crimes committed by people with a Dutch nationality from the definition of 'mobile banditry'.[137] In the media, the Dutch police point to Eastern European groups of 'mobile bandits' when addressing pickpocketing and shoplifting in Roermond.[138] As a consequence, the Dutch police convey the impression that the majority of pickpocketing and shoplifting in Roermond is committed by individuals with Eastern European nationalities.[139] In reality, the numbers point to between 36 and 90 suspects per year that hold a passport issued by an Eastern European country.[140]

The police do not clarify which nationalities are defined as 'Eastern European'. When speaking of 'mobile banditry' in general, the police refer to people from Poland, Bulgaria, Romania, and Lithuania. In the internal study, the police also

[131] Volkskrant, Waarom een steenrijke sjeik (en 8 miljoen anderen) shoppen in de outlet van Roermond, https://www.volkskrant.nl/nieuws-achtergrond/waarom-een-steenrijke-sjeik-en-8-miljoen-anderen-shoppen-in-de-outlet-van-roermond~b02d30d4/.
[132] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond.
[133] See the Annex to this report.
[134] See the Annex to this report.
[135] Dutch National Police, Mobiel banditisme, n.d., https://www.politie.nl/themas/mobiel-banditisme.html. See for example a report on bike theft: Kuppens Jos, Wolsink Joey, Van Esseveldt Juno and Ferwerda Henk, Fietsdiefstal in Nederland. Van fenomeen naar aanpak, Bureau Beke 2020, https://centrumfietsdiefstal.nl/fileadmin/CentrumFietsdiefstal-bestanden/Onderzoek/Download_Bekereeks_Fietsdiefstal_in_Nederland.pdf, p. 66.
[136] Dutch National Police, Mobiel banditisme, n.d.
[137] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, p. 17-18.
[138] In the interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020, it became clear that 'mobile bandits' are associated with multiple property crimes by the Dutch police, including burglary. The Sensing project, however, is focused on pickpocketing and shoplifting.
[139] Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan, 13 June 2019, https://www.rathenau.nl/nl/digitale-samenleving/dankzij-deze-sensoren-kunnen-rondreizende-bandieten-minder-hun-gang-gaan; NOS, De politie wil zakkenrollers en plofkrakers vangen met data, NOS, 17 September 2018, https://nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.html.
[140] See the Annex to this report.

refer to people with a nationality from Bosnia and Herzegovina or Serbia.[141] The police claim that pickpockets and shoplifters with Eastern European nationalities work in groups and systematically commit economic crimes: "In the municipality of Roermond, there is a feeling that crime that can be attributed to 'mobile banditry' has increased in recent years. Historically, since the early 2000s, the Dutch police have been confronted with itinerant Eastern European bandits committing various types of property crimes. Although the phenomenon of 'mobile banditry' has existed for centuries, in recent years great concern has arisen about the increase in the number of gangs from Eastern and Central Europe."[142]

In addition to the emphasis on nationality, the police associates 'mobile banditry' with the Roma ethnicity in the internal study on 'mobile banditry' Roermond. This is peculiar, since there is no national police data on the ethnicity of suspects in the Netherlands – because such data is not recorded by the police (see Section 5.3 about the issues of not recording this data).[143]

In order to prevent the type of pickpocketing and shoplifting that falls under the police's definition of 'mobile banditry' in Roermond, the Sensing Unit of the Dutch police developed a predictive policing system. The system was announced on the police website in July 2018 and became operational in 2019.[144] For this project, the city of Roermond has been designated as a 'living lab' (*proeftuin*) by the Dutch National Police.[145] The predictive policing system makes use of police records and data collected through new and existing sensors installed in public spaces. These sensors include Automated Number Plate Recognition (ANPR) cameras, as well as cameras that are able to detect a vehicle's brand, model, year of manufacture, and colour.[146] The collected data is then analysed using big data analytics and algorithms. The Sensing project collects and processes data for two purposes in two separate data processing operations:

- The Sensing project has an **operational objective**: the police use the data with the aim of preventing and detecting potential crimes. For this objective, the data is processed to follow up high-risk scores, known as 'hits'.[147] When a hit is generated, the police decide if and how to intervene. The police also process the data to maintain a reference file with the number plates of cars of that fulfil the criteria of the Sensing project, which aims to combat 'mobile banditry'.[148]
- The Sensing project also has a **learning objective**: the police use the data to learn more about data-driven policing. For the learning objective, data is processed for the purpose of exploring the security issue of 'mobile banditry', developing the target profile of 'mobile bandits', checking the algorithm used, developing the hit lists (lists of 'high-risk' vehicles), and building upon and improving their information position by creating what they call "white lists" (lists of low-risk vehicles) and understanding more about movement patterns.[149] For this purpose, all data that are collected by the sensors, including the data on 'no-hits', is processed and analysed to train crime-predicting algorithms in a broader sense.[150]

In order to predict if an individual is a relevant target for the predictive policing system (i.e. a potential suspect of pickpocketing or shoplifting that fulfils the criteria of 'mobile banditry'), the police have developed a target profile that is tweaked as the project evolves. As explained above, the internal study of 'mobile banditry' in Roermond shows that the police assume that most, if not all, 'mobile bandits' have an Eastern European nationality. The police state that "pickpocketing is an important part of Eastern European 'mobile banditry', especially perpetrated by Romanian and

---

[141] Dutch National Police, Mobiel banditisme, n.d.; Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, p. 37, 47, 69 and 88. In the absence of national data on race and the recording of ethnicity data of criminal suspects in the Netherlands, data from the city of Roermond is the only available information that reveals the personal characteristics of pickpockets and shoplifters.

[142] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, n.d., p. 9. Original text: "*In de gemeente Roermond heerst het gevoel dat criminaliteit die toegewezen kan worden aan mobiel banditisme de laatste jaren is toegenomen. Historisch gezien wordt de Nederlandse politie vanaf het begin van de jaren 2000 geconfronteerd met rondtrekkende Oost-Europese bendes die verschillende typen van vermogensdelicten plegen. Hoewel het fenomeen mobiel banditisme al eeuwenlang bestaat, is in de afgelopen jaren grote bezorgdheid gerezen over de toename van het aantal bendes uit Oost- en Centraal Europa.*"

[143] Ibid. p. 44, 64, 66-67 and 87.

[144] Dutch National Police, Zakkenrollers herkennen dankzij data-koppeling, 11 July 2018, https://www.politie.nl/nieuws/2018/juli/11/00-zakkenrollers-herkennen-dankzij-data-koppeling.html.

[145] Ibid.

[146] Interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 34-36. Confirmed in Amnesty International's interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.

[147] Usually the police use the term 'hit' when they were actually able to confirm a suspicion of criminal activity (e.g. they stopped a person and this person indeed carried stolen goods). In the Sensing project, the police use the term 'hit' for a risk score above a certain threshold. When the police consider a hit 'confirmed', they speak of a 'positive hit'.

[148] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.

[149] Dutch National Police, Nota rechtmatigheid OPTR en GPV Versie 1.3. Confirmed in interviews with the police in November 2019 and January 2020, in: Prins Vera, Sensoren, risicoscores en mensenrechten, p. 48-49.

[150] Dutch National Police, Nota rechtmatigheid OPTR en GPV Versie 1.3. The police added that they use this data to check the algorithm used. Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.

Bulgarian groups".[151] The police argue that shoplifting by 'mobile bandits' in Roermond specifically is committed mostly by people with Romanian nationality.[152] For the Sensing project, the police have translated a target profile of pickpockets and shoplifters that fulfil the criteria of 'mobile banditry' into a set of criteria in an algorithm. These criteria consist of simple profile rules that can be matched with information from police databases and the aforementioned sensors that collect data in and around the city of Roermond.[153] The police is secretive about the data collected, the sensors that are deployed, the details regarding the criteria used, or the values attached to each criterion to calculate the risk scores for individuals. What is known about the Sensing project is a result of combined information from academic articles, news articles and interviews with police officers. Due to the experimental nature of the project, parameters may be changing.[154] This investigation reveals that the Sensing project is likely to use at least the following criteria:

- *Target travels by car.* The Sensing project focuses on suspected pickpockets and shoplifters travelling by car. The sensors used thus far in the project detect cars, not persons travelling by other modes of transport.
- *Target is accompanied by passengers (other targets) in the car.* The police consider multiple individuals in one car as an indication of a group of targets.[155] The police are experimenting with sensors that can recognise the number of people in a car. At the time of writing, they are experimenting with millimetre-wave sensors that detect human beings by scanning the cars with extremely high frequency radar scanners.[156] The police are not sure whether this profile rule is useful, because the majority of visitors to the shopping centre arrive in a car with multiple passengers.[157]
- *Car takes a specific route.* The police can retrace the route of the car from the ANPR cameras. The police predict suspicious routes using such data. A car travelling from Germany and headed towards the shopping centre is regarded suspicious.[158]
- *Car may have a Romanian or German licence plate.* The police can retrace the origin of a licence plate from the ANPR cameras. In September 2018, the police stated that a Romanian licence plate would generate points in the risk model.[159] Later, in November 2019, the police claimed that pickpockets and shoplifters with an Eastern European nationality rarely drive a car with an Eastern European licence plate and that they mostly drive in cars with a German licence plate.[160] In August 2020, the police stated that they are considering deactivating this profile rule.[161]
- *Car may be a white rental car from Germany, three to five years old.* The police consider that the vehicle may be small in size, and therefore focus on smaller models.[162]
- *Car might be stolen, associated with previous criminality, or displaying false licence plates.* The police can retrace this information by linking the licence plate number (detected by the ANPR camera) to existing police databases.[163]

These criteria are fed into an algorithm, which calculates an overall risk score of the input from the sensors based on weights attached to each criterion. When a high-risk score is produced, then the car, the driver, and the passengers qualify as 'suspicious' and generate a *hit* in the predictive policing system, leading to the notification of and response by the police.[164]

Data processing for the operational objectives of the Sensing project does not stop with the generation of a 'hit' by the sensors and algorithm. The hits are automatically sent to the patrol officers, who have the choice to accept the call or

[151] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, n.d., p. 44 and 96.
[152] Ibid. p. 68-69.
[153] NOS, De politie wil zakkenrollers en plofkrakers vangen met data, 17 September 2018.
[154] Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.
[155] Andringa, De politie wil zakkenrollers en plofkrakers vangen met data; and Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.
[156] Interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 36. Confirmed in Amnesty International's interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.
[157] Interview with the police, August 2020.
[158] Andringa, De politie wil zakkenrollers en plofkrakers vangen met data; and Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.
[159] Andringa, De politie wil zakkenrollers en plofkrakers vangen met data.
[160] Interview with the police in November 2019, in: Prins, Sensoren, risicoscores en mensenrechten, p. 37.
[161] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.
[162] Interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 37.
[163] Ibid. p. 37-38.
[164] Andringa, De politie wil zakkenrollers en plofkrakers vangen met data; Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan; Dutch National Police, Projectplan Smart City Security Concept. Landelijk Project Operationele Proeftuinen Programma Sensing; Dutch National Police, Visualisatie proeftuinen met Tue.

not. In this decision-making process, the officers are supported by information about the characteristics of the hit, including the location of the car and information on whether the hit was established because the car meets multiple criteria but has not been registered in police databases in the context of 'mobile banditry' before, or whether it has been registered in this context before.[165]

When the patrolling officers take the call, the control room of the Real Time Intelligence Centre (RTIC) of the Dutch police in Maastricht (the capital city of the province of Limburg) registers the hit in the operational police databases. A connection between the car and the crimes connected with 'mobile banditry' has then been established in the police operational databases.

Patrol officers enjoy broad discretion when it comes to these calls: they can determine whether they will respond to a call, if they will intervene, how they will intervene, and whether they will check the identities of the driver and passengers and record those in connection with the call relating to 'mobile banditry'.[166] In practice, when the officers do respond, they will perform a final visual check to see if they think it is worthwhile to stop a car with these specific passengers in the context of the prevention of 'mobile banditry'. This depends on whether the passengers meet their subjective predetermined conceptions of what a 'mobile bandit' looks like.

A popular preventive measure is car interception.[167] Under the Dutch Road Traffic Act (*Wegenverkeerswet*), the police can stop any car as long as they check the driver's compliance with any rule that is laid down in the Road Traffic Act. By asking the driver for their driver's licence or car registration papers, the police officer has ticked this box and the inspection is considered lawful,[168] regardless of the fact that the car has been intercepted in the context of the prevention and detection of pickpocketing and shoplifting by individuals with Eastern European nationalities – which has no connection to road traffic safety. The police thus abuse the broad powers they are given under the Road Traffic Act as a pretext to target people of certain nationalities/ethnicities on the assumption that those people may commit shoplifting or pickpocketing crimes in the future (see Section 4.5 for more on this).

The data collected in the Sensing project is stored in three types of police databases. First there is a specific database relating to the operational objective. Data related to hits is stored for one year in this database and data related to no-hits is immediately deleted.[169] Secondly, if the hit is followed up by the patrol officers, data is stored in the regular operational police databases, to which the regular retention periods apply. Under Dutch law, such data must be deleted when it is no longer necessary for the performance of the daily police task, with a maximum retention period of 5 years.[170] Thirdly, the Sensing project stores data in a separate database for the purpose of pursuing the learning objective; all collected data – thus all location data and movement patterns of all individuals travelling by car in and around Roermond – is stored for one month.[171]

[165] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.
[166] Confirmed in interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.
[167] Confirmed in interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.
[168] Road Traffic Act (*Wegenverkeerswet*) 1994, Art. 160; Supreme Court of the Netherlands, 1 November 2016, ECLI:NL:HR:2016:2454.
[169] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020. See also interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 46-47.
[170] Police Data Act (*Wet politiegegevens*), Art. 8(6).
[171] Data in this learning objective database is not anonymized or pseudonymized. Only when the data is being re-used for scientific unrelated purposes the data will be pseudonymized. Interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 48-49. Confirmed in Amnesty International's interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020.

4. HUMAN GUINEA PIGS UNDER MASS SURVEILLANCE

4.1 HUMAN RIGHTS STILL APPLY IN LIVING LABS

The police describe the Sensing project as a 'living lab' (*proeftuin*), where they can experiment with data and algorithmic methods in pursuit of both learning and operational objectives. The use of the term 'living lab' by the police in reference to predictive policing programmes suggests that these programmes take place in an isolated area, outside the 'real world', where the police may freely tinker with data and algorithmic methods in an environment in which all study subjects have consented to the surveillance. This is not the case in Roermond. This 'living lab' is set up in a real urban space in the city of Roermond, without the people knowing they are taking part in an experiment. In the Sensing project, everyone present – the 40,000 residents of Roermond, the thousands of people from the larger province of Limburg that commute to Roermond on a daily basis, the people who visit the city, and the people who are merely passing through – are the living guinea pigs for law enforcement's learning objectives.[172] European and international human rights standards do not provide exceptions to the applicability of human rights, nor do they allow for specifically lenient interpretation of the justification conditions for interference with human rights in cases where police authorities are experimenting with new technologies and investigation methods. As a matter of fact, human right law dictates quite the contrary. There must be more stringent scrutiny of human rights when the police resort to technologically advanced and new investigative methods that have the potential to interfere with human rights.[173] The Council of Europe recommends human rights impact assessments before carrying out experiments with algorithms, and holds that the free, specific, informed and unambiguous consent of participating individuals should be sought in advance.[174] Human rights apply everywhere – including in so-called living labs.

The collected data, consisting of ANPR data, the model and colour of the vehicles and the movement patterns, can be traced back to individuals via ANPR and therefore constitute personal data, which falls under the scope of the right to data protection. The data collected in the Sensing project also qualifies as data related to private life under Art. 8(1) ECHR, which falls under the scope of the right to respect for private and family life, home and correspondence.[175] Data on movements and personal data collected by the police in the context of criminal law enforcement all have an implication for the right to privacy. The collection of data in the Sensing project constitutes an interference with the right to privacy,[176] as does the systematic analysis, storage and use of data in police databases.[177] The preventive measure of stopping and checking cars that relate to a hit that was produced by the predictive policing system equals the stopping

[172] Volkskrant, Waarom een steenrijke sjeik (en 8 miljoen anderen) shoppen in de outlet van Roermond, https://www.volkskrant.nl/nieuws-achtergrond/waarom-een-steenrijke-sjeik-en-8-miljoen-anderen-shoppen-in-de-outlet-van-roermond~b02d30d4/.
[173] ECtHR 6 June 2016, no. 37138/14 (Szabó and Vissy/Hungary), para. 68.
[174] Recommendation CM/REC(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems, Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Minister's Deputies, para. 3.1.
[175] Art. 8(1) ECHR reads: "Everyone has the right to respect for his private and family life, his home and his correspondence."
[176] ECtHR 28 October 1994, no. 14310/88 (Murray v. United Kingdom); ECtHR 25 September 2001, no. 44787/98 (P.G. and J.H. v. United Kingdom), para. 59-60; ECtHR 7 July 2015, no. 28005/12 (M.N. and others v. San Marino), para. 54.
[177] ECtHR 6 June 2006, no. 62332/00 (Segerstedt-Wiberg and others v. Sweden), para. 72.

and checking cars of people without a reasonable suspicion of a crime. This is similar in nature to stopping and searching persons in public, which the ECtHR has qualified as an interference with the right to privacy.[178] The search of personal belongings also interferes with the right to privacy.[179] The preventive measures used to follow up the hits of the system therefore also interfere with the right to privacy.

State interference in the right to privacy must strictly adhere to the criteria and safeguards that have been described under international human rights law, outlined in Section 2.2 of this report. Such interference must meet the criteria of legality, necessity and proportionality. The principle of legality requires that interference pursues a legitimate aim, has a sufficient basis in the law and is carried out in accordance with proceedings established in or through law. The prevention of disorder or crime is regarded a legitimate aim under Art. 8 (2) ECHR. This section assesses whether the predictive policing project meets the two other legality criteria to justify its interference with the right to privacy.

4.2 MASS SURVEILLANCE IN ROERMOND

The Sensing project relies on surveillance for data collection. Surveillance is the monitoring of a person's communications, behaviour or physiological characteristics. This includes monitoring of location data and movement patterns, as well as biometric data such as can be collected with certain types of millimetre-wave sensors. Mass surveillance involves surveillance that is not targeted at an individual or an identifiable and distinguishable group or specific location, and not based on reasonable suspicion.[180]

INDISCRIMINATE MASS SURVEILLANCE: A NO-GO IN HUMAN RIGHTS-COMPLIANT POLICING

Surveillance refers to all activities by or on behalf of a state that monitor, intercept, collect, select, retain, analyse, share or otherwise use communications or location data of all sorts. Surveillance constitutes interference in a range of human rights, including the rights to privacy and freedom of expression. Targeted surveillance may be justifiable, but only when it occurs based on reasonable suspicion, takes place in accordance with the law, is strictly necessary to meet a legitimate aim (such as protecting national security or combatting serious crime), and is conducted in a manner that is proportionate to that aim and non-discriminatory.

Indiscriminate mass surveillance is the widespread and bulk monitoring, interception, collection, storage, analysis or other use of communication or location data that is not targeted at an individual or an identifiable and distinguishable group or location and is not based on reasonable suspicion. Amnesty International believes that indiscriminate mass surveillance is never a proportionate interference in the rights to privacy and freedom of expression. Mass surveillance involves the indiscriminate collection of personal data of persons who have not been convicted of an offence and the storage of such data, irrespective of any concrete suspicion, the nature of the offence or the characteristics (such as the age) of the person, or any other special circumstances. Such blanket and indiscriminate use of powers fails to strike a fair balance between public interests and the private interests of persons in enjoying their human rights. Indiscriminate mass surveillance therefore constitutes a disproportionate interference with the right to respect for private life, and it cannot be regarded as necessary in a democratic society.[181]

The Sensing project includes indiscriminate mass surveillance because it monitors behaviour by tracking movement which is not targeted at a very specific location (an entire city), nor at specific individuals or groups, and it is not based on reasonable suspicion; the data of all people travelling by car is collected and analysed. The Sensing project amounts to mass surveillance because the general public travelling through Roermond by car are not suspected of any crime, but the police nevertheless collect and analyse their data in the context of criminal law enforcement. In order to allegedly prevent pickpocketing and shoplifting, the police collect and analyse data from all people travelling by car in and through Roermond – without indication whatsoever if any of them intending to commit a criminal offence. Travelling by car in and through Roermond is not a criminal act, nor an affirmative step towards the commission of a crime. The police do not have a reasonable suspicion to target any of these people. The police presume that the data of vehicles in Roermond

[178] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 61-65.
[179] Ibid. para. 63.
[180] Surveillance en mensenrechten, Amnesty International, n.d., https://www.amnesty.nl/encyclopedie/surveillance-en-mensenrechten.
[181] ECtHR 4 December 2008, no. 30566/04 (S. and Marper v. the United Kingdom), para. 119-125.

are relevant to prevent and detect pickpockets and shoplifters, based on the assumption that criminals travel in cars and drive towards the shopping centre. However, this behaviour does not differ from the normal behaviour of any individual: many people travel in cars in and around Roermond. As a result, the collected data relate to people who have no proven connection with pickpocketing or shoplifting in Roermond, yet their data is are being processed in connection with prevention of these crimes. The people travelling in and through Roermond have the right to be able to move around the city without being under surveillance by the police and without having their data stored in police databases and analysed for months with predictive algorithms in the context of crimes to which they have no connection whatsoever. The interests of these thousands of people outweigh the alleged interest of the police to predict a limited number of minor offences a year, and data collection on a massive scale for such a limited purpose is an egregious and unacceptable use of state surveillance power. When taking measures to achieve a legitimate aim, the police must adopt the least intrusive means available to them. The police fail to demonstrate what other means they have attempted in order to address the problem of pickpocketing and shoplifting. The data processing in the Sensing project can therefore not be considered necessary and proportionate, and thus violates the right to privacy.

4.3 FLAWED DESIGN OF THE SENSING PROJECT

Besides the flagrant violation of human rights through mass surveillance, the Sensing project represents an unsettling trend in the design and roll-out of predictive policing systems: the fundamental design of the research, record-keeping, evaluation and database for the project is flawed.

Personal data processing in the context of policing and criminal law enforcement has to be justified by, amongst other aspects, its effectiveness in contributing to investigations (see Sections 2.1-2.3).[182] When contacted by Amnesty International, the police were unable to demonstrate the effectiveness of the Sensing project and admitted that the design of the project does not allow them to adequately measure its effectiveness in the prevention of pickpocketing and shoplifting.[183] It is therefore unclear whether the measures have any effect on the crime rates in Roermond.[184] This is problematic, because only measures that are effective can potentially justify interferences with human rights. What is more, the Sensing project works with profile rules that are so generic, for example a German rental car with multiple passengers en route to the shopping centre, that the number of false positives that are produced by the system render its use ineffective, and leads to unjustified interference with human rights.

Another design issue that will result in human right violations is the feedback loop that is being created by this project. The system can create hits for cars that have no prior presence in police databases but are still being flagged, simply because the car takes a certain route, is of a certain brand, model and colour, and transports multiple passengers (see Chapter 3). When a patrol officer decides to follow up such a hit, information is entered in the regular operational police databases that makes a connection between on the one hand personal data relating to the car owner and potentially to the driver and passengers, and on the other hand the crimes associated with 'mobile banditry'. If this hit was a false positive – meaning that the people that were stopped and checked were not actual positives, i.e. individuals with Eastern European nationalities on their way to commit property crimes in the shopping centre – the car is still associated with 'mobile banditry' in the operational police databases. Next time this car drives in or around Roermond, the risk score that is attributed by the predictive policing system will be higher, because now the car also meets the profile rule of being associated with mobile banditry in the past.

For the results of the Sensing project, the police do not keep detailed records.[185] While the police aim to keep track of the interventions, such as stops and checks for evaluation purposes, this is seriously hampered for two reasons. First, many hits are not followed up because there are simply no police officers available to respond. Second, when there are police officers available, they have discretion in deciding whether or not to follow up a hit.[186] As a consequence, most risk scores are not evaluated. In particular the no-hits data of the predictive policing system seem to be left out of the evaluation, preventing the police from addressing possible false negatives. This lack of record-keeping and adequate evaluation design prevents the police from correcting their assumptions regarding the profile of pickpockets and shoplifters and increases the risk of confirmation bias. The overall design of the project is therefore inadequate to give trustworthy intelligence about the operational methods of pickpockets and shoplifters in Roermond. The lack of a proper mechanism for evaluation is all the more worrying since the Sensing project is a pilot study, from which the police aim

[182] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Practical guide on the use of personal data in the police sector, T-PPD (018)01, Strasbourg, 15 February 2018, para. 8.
[183] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020. See also interviews with the police in November 2019 and January 2020, in Prins, Sensoren, risicoscores en mensenrechten. P. 41-42.
[184] See also ECtHR 17 December 2009, no. 1642805 (Gardel v. France), para. 57-71.
[185] Under international human rights law, there is an obligation of detailed record-keeping. See Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Surveillance and Human Rights (A/HRC/41/35), para 50(d).
[186] Interview with the Programme Director for Digitization and Cybercrime and the Programme Manager of the Sensing project of the Dutch police in August 2020. See also interviews with the police in November 2019 and January 2020, in: Prins, Sensoren, risicoscores en mensenrechten, p. 41-42.

to learn in order to improve future data-driven policing. Pilot projects that have a learning objective should be accompanied by a state-of-the-art evaluation framework in order to justify any interferences with human rights.

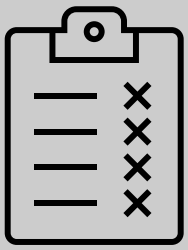
In addition to the lack of systematic record-keeping, the evaluation framework of the project is inadequate due to the poor evaluation criteria that the police formulated. Most interventions within the Sensing project are not evaluated at all, and when the police do evaluate an intervention, they set the criteria for 'success' at a low and unreliable bar. When the police evaluate the effectiveness of a 'stop and check' following a hit from the predictive policing system, they assume that a car which takes a route out of Roermond after a 'stop and check' or even after a simple drive-by by the police indicates that potential pickpockets or shoplifters were deterred from committing a crime.[187] This assessment approach is flawed by design, specifically because it does not prove any intent to commit a criminal offence nor that such an offence was deterred. The people in the vehicle may simply have been passing through Roermond with no intention of stopping in the first place. The lack of a robust evaluation framework makes it nearly impossible to demonstrate the effectiveness of the Sensing project in the prevention of pickpocketing and shoplifting, which obstructs the proportionality assessment that is necessary under human rights law. Equally worrying is that the absence of information about the stops and checks frustrates the possibility of remedy and redress for people who want to challenge the illegal infringement on their right to privacy.

What is more, the police also violate a number of data protection standards (see Section 2.3) in the design and maintenance of the databases that are used for this project.[188] First, in the database relating to the learning objective of the Sensing project, the police fail to distinguish between categories of individuals (e.g. a category for previously convicted persons for crimes associated with 'mobile banditry' on the one hand, and a category for random passers-by on the other hand) and categories of data reliability (e.g. the distinction between positive positives and false positives, as explained above). All data is stored for one month. The police only distinguish between hits and no-hits, without verifying the accuracy of this grouping.[189] The police store this combined data in an uncategorised state: no differentiation is made between categories of individuals, nor categories of data. Consequently, different data categories are stored together and the time limits on data retention are not based on the need to retain specific data, but rather on an unsubstantiated one-size-fits-all decision.[190] Moreover, irrelevant and inaccurate data may be stored due to the large amount of uncategorised and unevaluated data. If a police officer follows up a hit, data relating to the car and potentially to the passengers is stored in police databases without it being clear that the data originates from an algorithmic prediction, and that the presumed connection between the car and 'mobile banditry' might be completely inaccurate.[191] The Sensing project lacks safeguards to guarantee that personal data kept by the police in databases is accurate, which violates data protection standards.[192]

The above indicates that even in a situation where predictive policing projects are conducted without mass surveillance, the Dutch police has a long way to go when it comes to respecting human rights in its experimental living labs and pilot projects. Human rights violations have been engrained in the design of the current project. This alarming observation calls for stringent oversight in all phases of predictive policing projects, including the design phase, and a rigorously different approach in the thinking about experiments and pilots executed by the police.

[187] NOS, De politie wil zakkenrollers en plofkrakers vangen met data; Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.

[189] Dutch National Police, Nota rechtmatigheid OPTR en GPV Versie 1.3.
[190] Directive 2016/680, Art. 7 (1).
[191] Ibid.
[192] Ibid. Art. 4 (1)(d). The ECtHR also requires procedural safeguards to prevent inaccurate data from being processed. See ECtHR 18 February 2009, no. 22427/04 (Cemalettin Canli v. Turkey), para. 42. Das and Schuilenburg explain how the current legal framework in the Netherlands fails to provide mechanisms that keep out false or unlawfully obtained data, in: Abhijit Das and Marc Schuilenburg, 'Garbage in, garbage out'. Over predictive policing en vuile data.



OBVIOUS HUMAN RIGHTS VIOLATIONS OVERLOOKED DUE TO DISRESPECT FOR DATA PROTECTION REQUIREMENTS

European data protection laws mandate several safeguards, which – had they been followed – may have allowed the authorities to identify and mitigate some of the human rights challenges posed by the Sensing project before it was deployed. Our research uncovered that the police did not carry out a Data Protection Impact Assessment (DPIA) prior to processing the data, nor did police consult with the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*). Given the high risk of the Sensing project, the police had the obligation to do both prior to the data processing operations. The European Data Protection Board (EDPB) has published guidelines suggesting a number of factors that imply a high risk to data protection (see Section 2.3). Data processing within the Sensing project should be considered of high risk given the following characteristics:

- Individuals are being profiled and scored;
- The predictive policing system makes use of sensors that result in systematic monitoring of publicly accessible areas;
- The project includes the processing of data of a highly personal nature, such as location data, movement patterns;
- The data is processed on a large scale: every car is monitored in a large area in and around the city of Roermond,[193] resulting in a high number of individuals and a large volume of data being processed. The police have been processing the data since the start of 2019 and have not indicated an end date for the project;
- The system uses reference lists which point to the combination of data from multiple databases;
- The project makes innovative use of technological solutions. While the use of Automated Number Plate Recognition (ANPR) may not be seen as a new technological solution by the Dutch police, the use thereof in the Sensing project is an innovative one that poses a major risk to the rights and freedoms of the people affected. In the guidelines, the EDPB highlights a number of examples of data processing that present a high risk, including "the use of a camera system to monitor driving behaviour" and consequently using "an intelligent video analysis system to single out cars and automatically recognise licence plates".[194] This is exactly how the police use ANPR in the Sensing project.

It is likely that a DPIA and a consultation with the DPS would have revealed the adverse impacts on human rights that are discussed in this report. If the police had not violated these data protection safeguards, the DPIA and consultation with the DPS would have given them insights into the human rights risks presented in this report, which would have resulted in a different project design with better human rights protections. The failure to follow the mandatory proceedings presents a violation of the principle of legality**.**

4.4 OVERALL LACK OF LEGALITY FOR PREDICTIVE POLICING PROJECTS IN THE NETHERLANDS

Sections 4.2 and 4.3 revealed that the Sensing project puts the people of Roermond and its visitors under mass surveillance and that the design of the project unlawfully infringes on human rights. But what if the police were to scrap the mass surveillance aspects by finding a way to narrow the scope of surveillance, and the project were accompanied by a better design for research, record-keeping, evaluation and database management? Would the Sensing project then be in line with human rights? The short answer is no, because any interference with the right to privacy must not only be necessary and proportionate, it must also pursue a legitimate aim and be in accordance with the law (see Section

[193] The municipality of Roermond covers 71 km2.
[194] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, p. 10.

2.2). Predictive policing with sensor networks is not in accordance with the law because the Dutch police lack the authority to use systems like this. Such use therefore does not fulfil the principle of legality.

At this moment, the police use sensors to collect data on people on the basis of Art. 3 of the Dutch Police Act (DPA) (*'Politiewet'*). In Dutch legal doctrine, Art. 3 DPA is regarded as providing the legal basis for data collection by the police when the collection amounts to at most "a minor infringement on the fundamental rights and freedoms of a person" ("*niet meer dan geringe inbreuk op de grondrechten*").[195] The provision states the following:

> **Article 3 of the Police Act**
>
> The police have the task, subordinate to the competent authority and in accordance with the applicable rules of law, of ensuring effective law enforcement and rendering assistance to those who need it.[196]

The infringement that is caused by predictive policing systems that make use of sensors is not minor in nature, nor does it resemble the surveillance of, for example, a patrolling police car. This latter type of surveillance might be based on Art. 3 DPA, a legal provision with a low level of precision. In contrast, policing systems that make use of sensors are characterised by factors that require a high level of precision in the law, because they involve the automated processing of personal data for police purposes and the use of technologically advanced investigation methods. While Art. 3 DPA is accessible to the persons concerned, thus meeting the criterion of accessibility, the provision does not legitimise the collection of ANPR data, movement patterns, details of the model and colour of a car and the storage of those data for one month in relation to individuals, including individuals that have no connection to any criminal offence(s). These effects are not foreseeable when studying the general task description of the police, because the provision lacks the specification of technical measures, and does not offer any indication as to the circumstances under which the police may collect data for predictive policing with the help of sensors.[197] Also, Art. 3 DPA does not indicate the scope of discretion granted to the police to collect data, nor does it clarify the manner of exercise of that discretion. [198] The provision does not provide any details as to the nature of the offences that may give rise to the interference with the right to privacy.[199]

The need for safeguards against arbitrary interferences, such as independent oversight, is all the greater in such cases.[200] The police argue that their data collection and processing within the context of living labs takes place under the authority of the Public Prosecutor's Office (*Openbaar Ministerie*).[201] The police request authorisation by the public prosecutor (*Officier van Justitie*) for data collection and processing.[202] The role given to the public prosecutor in the Sensing project is thus similar to the role given to the public prosecutor in the case of *Sanoma Uitgevers B.V. v. the Netherlands*, discussed in Section 2.2, which the ECtHR held did not meet the standards for an independent and impartial body. Nor does it meet the standards for adequate oversight in terms of substance when there are no clear and precise criteria for the assessment that has to be carried out by the public prosecutor prior to giving authorisation.[203] The prosecutor's approval of the sensors and the data retention period is therefore not an adequate safeguard against arbitrary interferences.

Our analysis of the legal basis of predictive policing projects with sensors reveals that the data processing does not meet the criterion of being based on a sufficient legal basis which is compliant with human rights law. The data collection for these projects thus fails to meet the criteria of Art. 8(2) ECHR, and thus violates the right to privacy.

---

[195] Supreme Court of the Netherlands, 19 December 1995, ECLI:NL:HR:1995:ZD0328 (Zwolsman); In the context of predictive policing, Section 141 of the Dutch Code of Criminal Procedure is also referenced. This article instructs the police on the task of investigating crime. This article is instructive and cannot be regarded as providing legal grounds for the collection of personal data in the context of criminal law enforcement. The article will therefore be left out of our analysis.

[196] Translation of: "*Artikel 3 Politiewet. De politie heeft tot taak, in ondergeschiktheid aan het bevoegd gezag, en in overeenstemming met de geldende rechtsregels, te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.*" Translation accessed at https://www.government.nl/binaries/government/documents/leaflets/2009/01/01/policing-in-the-netherlands/policing-in-the-netherlands.pdf.

[197] ECtHR 30 July 1998, no. 27671/95 (Valenzuela Contreras v. Spain), para. 46. See also ECtHR, no. 27798/95 (Amann v. Switzerland) para. 50; ECtHR 25 March 1998 (Kopp v. Switzerland) para. 55; ECtHR 10 February 2009, no. 25198/02 (Iordachi and others v. Moldova), para. 50; ECtHR 2 August 1984, no. 8691/79 (Malone v. the United Kingdom) para. 66.

[198] ECtHR 2 August 1984, no. 8691/79 (Malone v. United Kingdom), para. 67; ECtHR 26 March 1987, no. 9248/81 (Leander v. Sweden), para. 51; ECtHR 24 April 1990, no. 11105/84 (Huvig v. France), p. 29; ECtHR 4 May 2000, no. 28341/95 (Rotaru v. Romania), p. 55; ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 62; ECtHR 4 December 2008, no. 30562/04 (S. and Marper v. United Kingdom), para. 95.

[199] ECtHR 18 May 2010, no. 26839/05 (Kennedy v. the United Kingdom), para. 159.

[200] ECtHR 17 December 2009, no. 16428/05 (Gardel v. France), para. 62; ECtHR 13 November 2011, no. 24029/07 (M.M. v. United Kingdom), para. 195; ECtHR 2 September 2010, no. 35623/05 (Uzun v. Germany), para. 61; ECtHR 12 January 2016, no. 37138/14 (Szabó and Vissy v. Hungary), para. 66-68; ECtHR 18 October 2016, no. 61838/10 (Vukota-Bojić v. Switzerland), para. 67; ECtHR 17 March 2010, no. 16428/05 (Gardel v. France), para. 62.

[201] Interview Police August 2020.

[202] Dutch National Police, Nota rechtmatigheid OPTR en GPV Versie 1.3.

[203] ECtHR 14 September 2010, no. 38224/03 (Sanoma Uitgevers B.V. v. the Netherlands), para. 90-100.

4.5 MISUSE OF THE ROAD TRAFFIC ACT TO FOLLOW UP PREDICTIVE POLICING HITS

In the Sensing project, when the police decide to follow up on a hit in the predictive policing system, they intercept the car and check if the driver and passengers have Eastern European nationalities and could therefore be anticipated to commit the crimes of pickpocketing and shoplifting.

The police rely on Art. 160 of the Road Traffic Act for these 'stops and checks'. The police usually ask the driver and the passengers for their identification papers.[204] Pursuant to the Road Traffic Act, the police are authorised to observe and take into account the contents of the car when these are visible from the outside.[205] The Road Traffic Act does not authorise a search of the car.[206] Despite the lack of legal authority to search a car during the stop and check procedure, it is common for the police to request the driver to open up the trunk, the dashboard locker, luggage and other contents inside the car.[207] This request is not a police order, which someone is legally bound to follow, but a question that may be refused without legal consequences. Most people who are subjected to stops and checks are unaware that the car search is not legally authorised under the Road Traffic Act. Similarly, to the majority of people, the difference between a police request and a police order will not be clear. Consequently, drivers consent to the search of their cars because they are unaware that they are cooperating voluntarily, waiving their right to object to the search at a later moment.[208]

Stopping and checking cars of people without a reasonable suspicion of a crime is similar in nature to stopping and searching persons in public, which the ECtHR has qualified as an interference with the right to privacy.[209] The search of personal belongings also interferes with the right to privacy.[210] Art. 160 Road Traffic Act authorises the stop and check of persons anywhere and anytime, without notice and without a real choice as to whether or not to submit to the procedure. The follow-ups in the Sensing project that consist of stops and checks based on risk scores produced by the predictive policing system therefore interfere with the right to privacy. Also, a person can feel obliged to submit to a search of their car, which is considered a personal possession.

The reliance on Art. 160 Road Traffic Act for predictive policing follow-ups aimed at preventing crime is problematic, as this provision provides the police with powers for a different objective: to monitor compliance with road traffic rules. The criminal offences targeted by the Sensing project have no connection to the road traffic safety rules. Pickpocketing and shoplifting are not punishable under the Road Traffic Act, but under the Criminal Code. The use of the Road Traffic Act for crime prevention presents a serious misuse of powers. This misuse of powers is common practice in the Netherlands; the Dutch police frequently use the Road Traffic Act for crime objectives, referring to this procedure as 'dynamic traffic controls'.[211]

Furthermore, Art. 160 Road Traffic Act also lacks a number of safeguards against abuse that the ECtHR set out for preventive checks in *Gillan and Quinton v. United Kingdom*. First, Art. 160 does not require that preventive checks be a necessary measure, and there is no requirement that the proportionality of a preventive check is assessed.[212] Second,

[204] Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, January 2015, https://www.misdaadjournalist.nl/wp-content/uploads/2015/12/Blauwe-Boekje.pdf, p. 27-33.
[205] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p, 62-64; Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, p. 27-33.
[206] A car search can be executed under the Dutch Code of Criminal Procedure (DCCP) when the driver or passengers are either caught red-handed during the execution of a criminal offence or when, prior to the search, the police had a reasonable suspicion that the driver and/or passengers of the car were engaged in criminal conduct (Art. 96B DCCP). The police can also search vehicles on the grounds of several other powers, such as the Opium Act and the Weapons and Ammunition Act, which requires a somewhat lower threshold for reasonable suspicion. However, the police stick to the search powers offered by criminal enforcement law, and only deviate to special laws such as the Opium Act and the Weapons and Ammunition Act "when absolutely necessary". See Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, p. 36.
[207] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p, 62-64, https://www.nrc.nl/nieuws/2016/02/19/adam-wil-boevenfuik-houden-1590511-a659443; Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, p. 27-33.
[208] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p, 62-64; Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, p. 27-33.
[209] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 61-65.
[210] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 63.
[211] Supreme Court of the Netherlands, 1 November 2016, ECLI:NL:HR:2016:2454. The Dutch Supreme Court (*Hoge Raad*) ruled that in general the police may use Article 160 of the Road Traffic Act for the purpose of investigating crimes, provided that the inspection is carried out by an authorised officer and has also been carried out to check compliance with road traffic rules. The lower Court of Appeal explained, however, that this provision cannot be used in discriminatory projects that submit people with Eastern European nationalities to preventive stops and checks by singling out their cars by number plates from Eastern European countries, when there is no objective reason to stop the car, other than matching the nationality profile. The Sensing project also relies on nationality and uses the number plates as a proxy for this characteristic. Court of Appeal of 's-Hertogenbosch, 17 June 2020, ECLI:NL:GHSHE:2020:2007.
[212] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 80.

the power given to the police is not limited geographically or temporally: the police may carry out preventive checks at any time in any area, in this case the entire city of Roermond, and there is no time limit given for the Sensing project.[213]

Thirdly, police officers are given broad discretion to carry out preventive checks; there are hardly any restrictions at all. Under the Road Traffic Act, it is not necessary to demonstrate the existence of any reasonable suspicion of a crime or offence, or even a traffic safety issue. The only requirement is that the police officer also checks compliance with road traffic rules, which may merely consist of asking for a driver's licence and car registration papers during a stop and check. As a consequence, a very wide-ranging category of people may be stopped and checked: essentially anyone driving a car through Roermond.[214]

The ECtHR has stressed that such broad discretion creates a clear risk of arbitrariness. The risk of discriminatory use of powers is a very real consideration.[215] In addition, the breadth of the power makes it difficult for individuals to show that a check is outside the law or that it constitutes an abuse of power.[216] The powers of the police to stop and check cars are therefore insufficiently circumscribed and not subjected to adequate legal safeguards against abuse. Accordingly, such powers are not in accordance with the law and are in violation of Art. 8 ECHR.[217]

[213] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 80; ECtHR 15 May 2012, no. 49458/06 (Colon v. the Netherlands), p. 83.
[214] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 83-84.
[215] Ibid. para. 85.
[216] Ibid. para. 81 and 86.
[217] Ibid. para. 80-87.

5. INPUT = OUTPUT: DISCRIMINATION BY DESIGN

The Sensing project is presented by the police as a neutral system that overrides the reliance of police officers on their gut feeling.[218] This chapter takes a close look at whether the rights to equality and non-discrimination are protected in the Sensing project in its various stages: the design of the Sensing project (Section 5.1), the effects of the actual data processing with the predictive policing system on the rights of the people targeted by the system (Section 5.2), and the legitimacy of the police interventions that follow up a hit in the Sensing project (Section 5.3).

DISCRIMINATION AGAINST ROMA BY THE DUTCH POLICE

Several studies have revealed that personal characteristics, such as colour, religion, nationality and/or ethnic origin, are used by the Dutch police in decisions on preventive measures, such as stops under the Road Traffic Act.[219] In 2016 the scientific research group of the Police Academy concluded, for example, that people belonging to a different ethnic group are stopped and checked more frequently by police officers without there being any justification for doing so. [220] Dutch news media have also been reporting discriminatory and racist attitudes amongst policemen.[221] In 2020, five policemen in Limburg, the province in which the city of Roermond is located, were fired after using derogatory language to describe people with Eastern European nationalities.[222] These racist attitudes are cultivated by the use of profiles in general policing and predictive policing that directly and indirectly include nationality and ethnicity and link those characteristics to predicted future criminal conduct. This has to stop.

[218] Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.
[219] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken; Çankaya Sinan, De controle van marsmannetjes en ander schorriemorrie. Het beslissingsproces tijdens proactief politiewerk, 25 December 2012; European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide, 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf.
[220] Landman W. and Kleijer-Kool L., Boeven vangen. Een onderzoek naar proactief politieoptreden, Politie & Wetenschap, Twynstra Gudde, 2016, https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2016/boeven-vangen-279/.
[221] Haenen Marcel, Politie Rotterdam onderzoekt racisme in appgroep agenten, NRC, 30 June 2020, https://www.nrc.nl/nieuws/2020/06/30/racistische-apps-bij-politie-rdam-a4004619.
[222] Haenen Marcel, Vijf Limburgse agenten wegens ernstig plichtsverzuim ontslagen, NRC, 10 June 2010, https://www.nrc.nl/nieuws/2020/06/10/vijf-limburgse-agenten-wegens-ernstig-plichtsverzuim-ontslagen-a4002328.

5.1 BIAS BY DESIGN

The Sensing project is not designed to combat all forms of pickpocketing and shoplifting. Rather, the project is designed to combat pickpocketing and shoplifting as far as these crimes fall under the police's definition of 'mobile banditry'.[223] The concept of 'mobile banditry' is used by the police for various economic crimes committed by foreign groups.[224] Pickpocketing and shoplifting that cannot be defined as 'mobile banditry' falls outside the scope of the Sensing project. The majority of people suspected of pickpocketing and shoplifting do not fulfil the criteria of 'mobile banditry'. The numbers show that more than half (around 60%) of those suspects are individuals of Dutch nationality, and that around 22% of the total number of suspects are individuals with an Eastern European nationality.[225] As explained below, the choice of the police to focus on 'mobile banditry' creates a biased design, as the concept of a 'mobile bandit' is biased towards people with Eastern European nationalities and/or Roma ethnicity.

First, the police explicitly exclude a number of nationalities from the definition of 'mobile banditry' and therefore from the design of the Sensing project. As the numbers released by the police indicate (see the Annex to this report), the majority of suspects of pickpocketing and shoplifting in Roermond have a Dutch nationality. Between 2010 and 2014, a total of 1,854 persons were suspected of pickpocketing or shoplifting in Roermond.[226] Of those suspects, 1,106 persons were of Dutch nationality.[227] In these five years, only 313 persons fulfilled the criteria of mobile banditry.[228] Crimes committed by individuals who have Dutch nationality, were born in the Netherlands or are registered as residents in the Netherlands are nevertheless explicitly excluded from the definition of 'mobile banditry', so these individuals fall outside the scope of the Sensing project.[229] The police also observed a relatively high number of Belgian and German suspects of pickpocketing and shoplifting in Roermond, but these people are excluded from the input data on 'mobile banditry', since the police presume that they do not belong to a network of 'mobile bandits'.[230]

The police link the profile of a 'mobile bandit' to people with Eastern European nationalities, as the police claim that most 'mobile bandits' have an Eastern European nationality.[231] As addressed in Chapter 3, the police do not clarify which nationalities are defined as 'Eastern European'. When speaking of 'mobile banditry' in general, the police refer to people from Poland, Bulgaria, Romania, and Lithuania. In an interview about the Sensing project, the police argue that an analysis of the crime reports "remarkably often point to people from Bulgaria, Poland and Romania".[232] In the internal study on 'mobile banditry' in Roermond, the police also refer to people with a nationality from Bosnia and Herzegovina or Serbia.[233] The police claim that pickpockets and shoplifters with Eastern European nationalities work in groups and systematically commit economic crimes.[234]

Further, the Roermond police connect 'mobile banditry' to Roma ethnicity.[235] The police stress that Romanian and Bulgarian criminal networks include "many gypsies (especially Roma) who are involved in things such as scams".[236] There is no national police data on the ethnicity of suspects in the Netherlands, because such data is not recorded by the police. Instead, the police's report on 'mobile banditry' in Roermond refers to a study where the Bulgarian and Romanian police argue that, based on their experience, 90% of pickpocketing is committed by Roma groups.[237] These

[223] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond.
[224] Dutch National Police, Mobiel banditisme.
[225] See the Annex to this report, table 1 and 2.
[226] 1,740 suspects of shoplifting and 114 suspects of pickpocketing. See the Annex to this report, table 1 and 2.
[227] 1042 suspects of shoplifting and 64 suspects of pickpocketing were of Dutch nationality. See the Annex to this report, table 1 and 2.
[228] 293 suspects of shoplifting and 20 suspects of pickpocketing fulfilled the criteria of mobile banditry. See the Annex tot his report, table 1 and 2.
[229] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, p. 17-18.
[230] Ibid. p. 68-69.
[231] NOS, De politie wil zakkenrollers en plofkrakers vangen met data; Dutch National Police, Mobiel banditisme; Van Teeffelen Kristel, Met camera's en sensors is een winkeldief straks op grote afstand te herkennen, Trouw, 17 September 2018, https://www.trouw.nl/nieuws/met-camera-s-en-sensors-is-een-winkeldief-straks-op-grote-afstand-te-herkennen~bcdee79e.
[232] Rathenau Instituut, Dankzij deze sensoren kunnen rondreizende bandieten minder hun gang gaan.
233 Dutch National Police, Mobiel banditisme, n.d.; Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, p. 37, 47, 69 and 88. In the absence of national data on race and the recording of ethnicity data of criminal suspects in the Netherlands, data from the city of Roermond is the only available information that reveals the personal characteristics of pickpockets and shoplifters.
[234] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, p. 9. Original text: "*In de gemeente Roermond heerst het gevoel dat criminaliteit die toegewezen kan worden aan mobiel banditisme de laatste jaren is toegenomen. Historisch gezien wordt de Nederlandse politie vanaf het begin van de jaren 2000 geconfronteerd met rondtrekkende Oost-Europese bendes die verschillende typen van vermogensdelicten plegen. Hoewel het fenomeen mobiel banditisme al eeuwenlang bestaat, is in de afgelopen jaren grote bezorgdheid gerezen over de toename van het aantal bendes uit Oost- en Centraal Europa.*"
[235] Ibid.
[236] Ibid. p. 64 and 67: "*Vooral Roemeense en Bulgaarse criminele netwerken, waaronder veel zigeuners (vooral Roma) [houden] zich onder meer met oplichting bezig.*"
[237] Ibid. p. 44 and 60.

references in the police report are being used to argue that the experiences of Bulgarian and Romanian police are relevant in the context of Roermond in the Netherlands, and that criminal behaviour can be attributed to ethnicity.

For example, the report describes that the Bulgarian police claim that in at least 90% of the pickpocketing cases in Bulgaria the perpetrator is a woman of Roma ethnicity. Subsequently, the Dutch police conclude that they arrested more female than male pickpockets during a specific period in the Roermond.[238] The report fails to take into account not only the differences between these countries and the Netherlands, but also the subjectivity of the experiences of the Bulgarian and Romanian police, as well as the decades of discriminatory police practices against individuals of Roma ethnicity in these countries.[239] The report includes various negative and generalised assumptions about people with Roma ethnicity and Eastern European nationalities, for example that "Romanian and Bulgarian children learn early on that pickpocketing is an accepted form of work" and that in certain Roma clans "daughters would be trained as pickpockets from birth".[240] Statements like these made by the police reinforce existing stereotypes and lead to stigmatisation of Roma, a particularly marginalised group that has historically been the target of systematic discrimination in Europe.[241]

The use of the concept of 'mobile banditry' inevitably leads to a predominant focus on particular groups of people on the grounds of their nationality and ethnicity, while at the same time overlooking people from other ethnic and/or national backgrounds. [242] Despite the fact that most suspects of pickpocketing and shoplifting do not meet the criteria of 'mobile banditry', the Dutch police have attributed the high rates of pickpocketing and shoplifting in Roermond to this ethnically charged concept. The definition of 'mobile banditry' results in direct discrimination on the basis of nationality. Because Roma people will more often have a nationality from an Eastern European country than from the Netherlands, Germany or Belgium, the design of the project is also based on indirect discrimination on the basis of ethnic origin.[243] On top of this, the police link nationality and ethnic origin to anticipated criminal behaviour in reports and media messaging. Such links provide a fertile environment for discrimination and encourage the targeting of certain nationalities and ethnicities for ethnic profiling.[244]

The police statements about the alleged over-representation of Eastern European nationals and Roma in crime statistics on 'mobile banditry' seem to be put forward as a justification for ethnic profiling with the predictive policing system in the Sensing project.[245] These statements are misleading, since the police have excluded certain nationalities from the definition. In addition, the statements regarding nationality are based on police records which are in themselves a reflection of police priorities and bias. Criminological research concludes that prejudices and stereotypes play a role in police officers' enforcement decisions, both in Europe in general as well as in the Netherlands specifically.[246] As a result, police records may be biased and do not always reflect an objective depiction of actual crime rates. Even more worrying is that the Roermond police's report on 'mobile banditry' relies on information depicting the subjective experiences of Bulgarian and Romanian police officers in their home countries. This information has no bearing on anticipated criminal conduct in the Netherlands and the use thereof is highly problematic, considering the established track record of discrimination against Roma in those countries.[247] In any case, differential treatment based on alleged over-representation of certain groups is not in line with the international human rights framework. Generalisations about

[238] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond p. 87-88.
[239] ECtHR 16 April 2019, no. 48474/14 (Lingurar v. Romania); Amnesty, Bulgaria 2019, n.d., https://www.amnesty.org/en/countries/europe-and-central-asia/bulgaria/report-bulgaria/; Amnesty, Romania 2019, n.d., https://www.amnesty.org/en/countries/europe-and-central-asia/romania/report-romania/.
[240] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, p. 46 and 87.
[241] Committee on the Elimination of Racial Discrimination, General recommendation XXXI on the prevention of racial discrimination in the administration and functioning of the criminal justice system, sixty-fifth session, 2005, p. 29; See the Amnesty archive: Amnesty International, Discrimination. Discrimination against Roma, n.d. https://www.amnesty.eu/news/category/press-releases/discrimination-press-releases/roma-press-releases.
[242] The Public Prosecutor also applies special guidelines for prosecution of individuals that are suspected of 'mobile banditry'. 'Mobile banditry' is a priority in prosecution. Having no permanent residence in the Netherlands plays a decisive role in the decision to apply the guidelines. Art. 140 and 311 of the Dutch Criminal Code; Guidelines for criminal procedure mobile banditry (*Richtlijn voor strafvordering mobiel banditisme*) (2019R010).
[243] See for similar reasoning ECtHR 24 May 2016, no. 38590/10 (Biao v. Denmark), para. 111-113.
[244] ECtHR 16 April 2019, no. 48474/14 (Lingurar v. Romania), para. 74-78.
[245] See Section 1.2.
[246] Çankaya Sinan, De controle van marsmannetjes en ander schorriemorrie. Het beslissingsproces tijdens proactief politiewerk; Mijatović Dunja, Ethnic profiling: a persisting practice in Europe, Commissioner for Human Rights, Strasbourg, 9 May 2019, https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe; Weijters G., Van der Laan A.M. and Kessels R.J., De overeenstemming tussen zelfgerapporteerde jeugdcriminaliteit en bij de politie bekende jeugdige verdachten, Wetenschappelijk Onderzoek- en Documentatiecentrum, Cahier 2016-3, 2016, https://www.wodc.nl/onderzoeksdatabase/kwalitatief-onderzoek-naar-de-hedendaagse-jeugdcriminaliteit-en-het-dark-number-jeugdcriminaliteit-deel-ii.aspx; Couchman Hannah, Policing by machine. Predictive policing and the threat to our rights, Liberty, January 2019, https://www.libertyhumanrights.org.uk/issue/policing-by-machine.
[247] Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, p. 44, 46, 66 and 87.

particular ethnic groups based on higher offending rates cannot serve as a justification for unequal treatment of individuals based on their race, ethnic origin or skin colour.[248]

It can therefore be concluded that discrimination and ethnic profiling are embedded in the design principles of this Sensing project, which is focused on the concept of 'mobile banditry' as described above.

5.2 AUTOMATED ETHNIC PROFILING

The previous section (Section 5.1) explained how the Sensing project is by design based on a biased understanding of a particular crime phenomenon due to the use of an ethnically charged concept of 'mobile banditry'. Subsequently, the way in which the risk model is constructed and deployed is inevitably discriminatory as well.

First, in the risk model, licence plates from certain countries result in higher risk scores and therefore arouse suspicion in order to accommodate police efforts to find people with Eastern European nationalities. The police stated publicly that a Romanian licence plate will generate points in the risk model (see Chapter 3 for an overview of all publicly known criteria).[249] In August 2020, the police indicated that the profile rule relating to the issuing country of the licence plate was not operational at that moment, because the criterion turned out to be too generic. When licence plates from certain countries yield points in an algorithmic model, there is unequal treatment on the basis of nationality, since the licence plate is commonly linked to the nationality of the driver of the car. In doing so, the police process data that stand proxy for ethnicity and link this data to crime predictions.

LONG-STANDING POLICIES THAT DUTCH POLICE USE TO TARGET EASTERN EUROPEANS IN CAR CONTROLS

The Sensing project is preceded by other police projects that use licence plates to target persons with Eastern European nationalities for preventive stops and checks in the Netherlands. The most controversial is a project called *Moelander,* which instructs the police to select cars for preventive stops and checks when the car has a licence plate from a Central or Eastern European country. The Supreme Court of the Netherlands (*Hoge Raad*) established that this project led to an indirect distinction based on nationality or ethnic origin of the passengers, which amounts to unequal treatment on the grounds of nationality.[250] The Court clarified that such measures may only be justified under specific circumstances, for example when the measures are necessary and proportionate to combat cross-border criminal offences and/or crimes in which the perpetrators cross national borders.[251] When the Court of Appeal applied the Supreme Court's reasoning in 2020, it concluded that:

"by making an indirect distinction, in the context of the 'Project Moelander', on the basis of the nationality or ethnic origin of the passengers of a vehicle, where there was no justification for doing so, the most fundamental principles of the legal order, the principles of equality and non-discrimination, have been breached. The way in which the 'Project Moelander' was conducted therefore constitutes a serious infringement of those principles, for which accountability exists. The defendant has been harmed in those fundamental interests which has resulted in a disadvantage for the defendant in this case, namely that he has not been treated equally in relation to cars that do not originate from Central and Eastern Europe."[252]

Second, considering the biased design of the Sensing project, there is a high risk of discriminatory use of the broad discretionary powers offered to the police in following up hits. Because of their wide margin of discretion, the police may consider the passengers' presumed nationality or ethnicity in deciding how to follow up once the car and its passengers

[248] ECtHR 20 June 2017, no. 67667/09 (Bayev and others v. Russia).
[249] NOS, De politie wil zakkenrollers en plofkrakers vangen met data.
[250] Supreme Court of the Netherlands, 9 October 2018, ECLI:NL:HR:2018:1872.
[251] Ibid. para. 2.5.2.
[252] Court of Appeal of 's-Hertogenbosch, 17 June 2020, ECLI:NL:GHSHE:2020:2007. Unofficial translation of: "*door in het kader van het "Project Moelander" indirect onderscheid te maken naar nationaliteit of afkomst van de inzittenden van een voertuig, terwijl hier geen gerechtvaardigde grond voor was, er in aanzienlijke mate inbreuk is gemaakt op een van de meest fundamentele beginselen van de rechtsorde, zoals het gelijkheidsbeginsel en het non-discriminatiebeginsel. Door de wijze van handelen in het kader van het "Project Moelander" is derhalve een ernstige inbreuk op voormelde beginselen gemaakt, welke inbreuk verwijtbaar is. Hierbij is de verdachte in deze fundamentele belangen geschaad en door het verzuim is voor de verdachte in dit geval nadeel veroorzaakt, namelijk dat hij niet gelijk is behandeld ten opzichte van auto's die niet afkomstig zijn uit Midden- en Oost-Europa.*"

are in their sight. The police's use of Art. 160 of the Road Traffic Act, as described in Section 4.5, may lead to people being subjected to an extensive method of control.[253] Sufficiently circumscribed powers and adequate legal safeguards would protect people against such abuse of powers. However, they are clearly lacking in this case.[254]

The outcome of the data processing in the predictive policing system is that people who are presumed to have an Eastern European nationality and/or Roma ethnicity are treated unequally: they will receive higher risk scores, are more likely to have their data stored in police databases, are more likely to have their stored data processed in the context of other and unrelated criminal law investigations and predictive policing projects, will be subject to police surveillance and interventions relating to the Sensing project (see Sections 4.2 and 4.5), and are potentially subject to more future data-driven police interventions unrelated to the Sensing project because of their presence in police databases resulting from the risk profile used in the Sensing project. Due to the poor reporting in the Sensing project (see Section 4.3), it is impossible to research the extent to which ethnic profiling takes place within the interventions.

Chapter 4 concluded that the processing of personal data within the predictive policing system in the Sensing project amounts to a violation of the right to private life and the right to protection of personal data, including the processing of data on 'hits' based on the risk profile. Given the unequal treatment described above and the lack of a justification for doing so, data collection and processing by the police using the predictive policing system, and the possible follow-up police interventions, such as 'stops and checks', also amount to direct discrimination under Art. 14 ECHR and Art. 21 CFREU, which is prohibited.[255]

All of the above qualifies as racial discrimination under the international human rights framework. [256] In addition, the discriminatory nature of the Sensing project can also be concluded from two other human rights standards. First, by deploying the Sensing project, the Netherlands did not fulfil its positive obligation to refrain from discriminatory practices disguised in allegedly neutral tests and to actively eliminate these practices.[257] Both in the design phase and the execution phase of the Sensing project, the police assert that they are using a neutral test, while in fact deploying a risk profile based on the discriminatory concept of 'mobile banditry'. The police response to these kinds of hits from the system cannot be considered equivalent to a follow-up after a neutral assessment of all the circumstances, because the risk profile is designed to single out people with Roma ethnicity and Eastern European nationalities. Second, differential treatment on the grounds of nationality amounts to direct discrimination between EU citizens and is in violation of Art. 18 TFEU. For the operational objective of the Sensing project, the Dutch police systematically process personal data exclusively of EU citizens that are not from the Netherlands in order to fight 'mobile banditry'. The CJEU has specifically ruled that the fight against crime cannot justify the systematic processing of personal data exclusively of EU citizens who are not nationals of the member state concerned.[258]

5.3 LACK OF TRANSPARENCY AND ACCOUNTABILITY

The algorithmic model of the Sensing project and its risk scores are opaque (see Chapter 3) and the police are unlikely to indicate which criteria led them to carry out a preventive check. For a targeted person, it will be difficult to prove that an intervention was discriminatory. He or she might not even be aware that the stop and check was carried out on the basis of predictive policing tools.

In the case of the Sensing project, additional information on the stops and checks performed is not needed to demonstrate the unlawfulness and discriminatory nature of the Sensing project, as this is inherent in the design of the project. Systematic record-keeping on interventions is not a means to improve a project that should not take place at all, but the use of standardised 'stop forms' by the police would provide an extra check during policing projects and facilitate any person stopped to seek a remedy. The use of stop forms is recommended in *all police stops*, whether or not they are carried out in the context of a predictive policing project (see box below). As described Section 2.4, stop forms are recommended in general terms by the CERD. Amnesty International has also advocated this in the past.[259] In

[253] Dutch National Police, De Dynamische Verkeerscontrole. Het 'Blauwe' Boekje, p. 29.
[254] ECtHR 12 January 2010, no. 4158/05 (Gillan and Quinton v. United Kingdom), para. 80-87. It may be argued that a 'stop and search' of a person is more intrusive than a 'stop and check' of a car, and that the criteria that the ECtHR established in *Gillan and Quinton v. United Kingdom* do not unequivocally apply to the stops and checks as carried out in the Sensing project. Still, the similarities point to an equally high risk of discriminatory use of powers.
[255] ECtHR 16 April 2019, no. 48474/14 (Lingurar v. Romania), para. 74-78.
[256] International Convention on the Elimination of All Forms of Racial Discrimination, Art. 1 (1).
[257] ECtHR 29 January 2013, no. 11146/11 (Horváth and Kiss v. Hungary), para. 116 and 127.
[258] CJEU 16 December 2008, C-524/06 (Heinz Huber v. Germany), para. 77.
[259] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p. 47-49; Amnesty International, Stopformulieren essentieel voor eerlijke en effectieve politiecontroles, September 2015, https://www.amnesty.nl/content/uploads/2016/12/amnesty_international_memo_stopformulieren.pdf?x14032; Amnesty International, The Netherlands, Submission to the United Nations Human Rights Committee, 126th Session, 1-26 July 2019, https://www.amnesty.org/download/Documents/EUR3504392019ENGLISH.PDF, p. 23-24.

predictive policing, the use of stop forms would produce statistics on whether the police use a risk model that disproportionately subjects people with a certain protected characteristic to measures.[260] The forms would also provide statistics for the evaluation of the effectiveness of projects. However, in the Sensing project the police do not collect data about the ethnic origin of those targeted by the stops and checks. In fact, Dutch legislation prohibits the collection of information on ethnic origin, and exceptions to this rule are narrowly defined. The collection of this information in connection with the performance of law enforcement duties is not considered grounds for exception according to Dutch legislation. The Dutch authorities refuse to systematically collect data about preventive checks and advocate against the practice with the CERD.[261]

MANDATORY USE OF STOP FORMS TO MONITOR BIAS

On a stop form, a police officer provides various information, including their identity, the motive behind the stop and preventive check, and the outcome of the check. The form should also indicate relevant personal details about the stopped person, such as gender, age and ethnic origin. The police officer must provide a copy of the filled-out stop form to the person being stopped. Research shows that mandatory use of stop forms has multiple advantages.

STOP FORMS:

- √ encourage a police officer to carefully weigh their decision to carry out stops and preventive checks;
- √ provide information to the stopped person about the motive behind the stop and preventive check. This information can be used by the person being stopped to check if the police officer's decision was biased or not;
- √ contribute to the monitoring of discriminatory practices by the police and can be used for statistics on police practices for evaluation and review processes. For the public and the persons subjected to preventive checks, these statistics are necessary to substantiate complaints about police bias. The evaluation and review process can also help the police illustrate non-discriminatory police practices and refute accusations of biased practices;
- √ boost the effectiveness of police work. Pilot projects on the use of stop forms have led to discovery of more crime in multiple European countries. For example, in Spain the number of stops and preventive checks fell from 958 to 396 per month, while at the same time the percentage of detected crimes rose from 6 to 17 percent during the pilot period;[262]
- √ can also be used to assess if the use of a predictive policing system – even if the system uses seemingly neutral profiles and algorithms – leads to an increase or decrease of discriminatory police practices.

[260] ECtHR 13 November 2007, no. 57325/00 (D.H. and others v. Czech Republic), para. 185; CJEU 13 July 1989, C-171/88 (Ingrid Rinner-Kühn v. FWW Spezial-Gebäudereinigung GmbH & Co. KG); CJEU 7 February 1991, C-184/89 (Helga Nimz v. Freie and Hansestadt Hamburg); CJEU 27 June 1990, C-33/89 (Maria Kowalska v. Freie en Hansestadt Hamburg); CJEU 24 February 1994, C-343/92 (M.A. De Weerd, née Roks and others v. Bestuur van de Bedrijfsvereniging voor de Gezondheid, Geestelijke en Maatschappelijke Belangen and others).

[261] Comments of the Netherlands concerning Draft General Recommendation no. 36 on Preventing and Combating Racial Profiling, AVT19/BZ128883, n.d., https://www.ohchr.org/EN/HRBodies/CERD/Pages/GC36.aspx.

[262] Amnesty International, Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken, p. 47-49; Open Society Justice Initiative, Toolkit for the analysis of police identifications. A practical guide to the analysis of police stop data, 2020, https://www.justiceinitiative.org/uploads/e453fbec-f116-4c85-b7e4-771fdd4c5dff/toolkit-for-the-analysis-of-police-identifications-20200302.pdf.

RECOMMENDATIONS

TO THE DUTCH LAW ENFORCEMENT AUTHORITIES:

1) Halt the Sensing project and comparable 'experimental' predictive policing projects that, through their design, application or effects, violate human rights, such as the right to privacy, the right to data protection, the right to non-discrimination and the principle of legality.

2) Evaluate how many people have been impacted and in what way their rights have been affected by the Sensing project and similar 'experimental' predictive policing projects. This information should be made public and appropriate steps should be taken to allow for effective remedy and redress by affected individuals.

3) Halt and refrain from any and all policing operations that rely on mass surveillance, which is never a proportionate response that can justify limitations or restrictions on the right to privacy. Delete all data collected and inferred in the course of these operations, as it was unlawfully collected.

4) Stop the use of stereotypes in policing operations that violate the right to non-discrimination. The police must refrain from the use of ethnicity, nationality or proxies thereof in crime profiles; end the use of predictive policing against stereotypes of crime, which target specific communities; and refrain from using profiles and profile rules in risk models that are based on protected grounds, such as race, ethnicity, colour, nationality, social origin or political affiliation.

5) Evaluate the use of all risk models to assess whether the criteria used, including seemingly neutral factors, lead to discrimination against certain individuals, groups or communities. Assess if the decision to use risk models and the use thereof are free from direction bias and confirmation bias. Meaningfully consult with external experts, including non-discrimination experts and affected communities, in the design and evaluation of risk models.

6) Consult with human rights experts prior to and during the deployment of any project that includes risk models and new forms of surveillance, such as sensors, to ensure compliance with the Netherlands' national and international human rights obligations. Assess the quality of the training data, data categories and algorithms prior and during such projects in cooperation with experts.

7) Design and deploy a proper evaluation framework for predictive policing projects that measures compliance with human rights at various stages in the project.

8) Be transparent and accountable about the use of predictive policing systems and allow for public scrutiny. A key element in this regard is the introduction of forms to be used during vehicle stops. Dutch police should promote and enable oversight by the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

9) Prohibit the use of the Road Traffic Act as a pretext for stops serving objectives not covered by the Road Traffic Act.

TO THE DUTCH LEGISLATURE:

1) Explicitly prohibit the use of algorithmic systems which do not have appropriate safeguards to protect the rights and freedoms of individuals whose data is processed by these systems in the context of policing and criminal law enforcement. This includes a legal basis that meets the criteria of specificity, foreseeability and accessibility and which is announced in advance.

2) Implement a mandatory and binding human rights impact assessment requirement applicable to the public sector, including to law enforcement authorities, which must be carried out in the design, execution and evaluation phases of algorithmic systems and automated decision-making.

3) Create an independent supervisory authority that advises on, monitors and enforces human rights obligations and responsibilities in algorithmic systems and automated decision-making. The supervisory authority should have access to the training data, data categories and algorithms to examine the system and its outcomes in terms of respecting, promoting and fulfilling human rights. The supervisory authority must have capacity and expertise on all relevant human rights aspects, such as data protection compliance, data science, algorithmic systems and automated decision-making in order to effectively keep up with the introduction and ongoing development of algorithmic systems and automated decision-making in society.

4) Initiate a parliamentary review of Art. 160 of the Road Traffic Act, restricting the possibility of stops under the Act to individualised cases reasonably justifying a stop for the purpose of enforcing road and traffic security regulations.

TO THE DUTCH DATA PROTECTION AUTHORITY (AUTORITEIT PERSOONSGEGEVENS):

1) Investigate the Sensing project and enforce the data protection framework on the data processing operations relating to the Sensing project, taking into account the authority to impose administrative fines under Art. 35(1)(c) of the Dutch Police Data Act (DPDA), and other appropriate measures.

2) Investigate other 'experimental' predictive policing projects similar to the Sensing project. Enforce the data protection framework on the data processing operations relating to those projects, taking into account the authority to impose administrative fines under Art. 35(1)(c) DPDA, and other appropriate measures.

3) Enforce the data protection framework, taking into account the authority to issue incremental penalty payments under Art. 35(1)(b) DPDA, in the situation where the police do not immediately halt the Sensing project and comparable 'experimental' predictive policing projects that through their design, application or effects violate human rights, such as the right to privacy, the right to data protection, the right to non-discrimination and the principle of legality.

4) Investigate to what extent unlawfully collected data relating to the Sensing project and comparable 'experimental' predictive policing projects have been stored in operational police databases, and if they have been processed by the police in the context of other police operations. Enforce the data protection framework on the data processing operations that rely on unlawfully collected data, taking into account the various tools provided in Art. 35 DPDA.

5) Investigate the use of ethnicity, nationality and proxies thereof by the police to consider whether they violate non-discrimination rights and enforce the data protection framework on the data processing operations associated with the unlawful use of ethnicity, nationality and proxies thereof, taking into account the various tools provided in Art. 35 DPDA.

6) Promote human rights, including the right to non-discrimination, in the data processing operations of the police.

ANNEX: POLICE FIGURES

The following tables are derived from: Police Unit Limburg, Mobiele bendes aan het Roer. Een exploratief onderzoek naar aard, omvang en aanpak naar mobiel banditisme in de gemeente Roermond, Dutch National Police, n.d., available on https://www.politie.nl/wob/korpsstaf/2019-programma-mobiel-banditisme-%E2%80%93-proeftuin-roermond.html, p. 37, 69, 47 and 88.

Table 1: Numbers of reported shoplifting incidents and numbers of shoplifting suspects arrested in Roermond

From top to bottom: number of reports, number of reports resolved, total number of suspects, suspects with Dutch nationality, suspects with a non-Dutch nationality, and suspects who fulfil the criteria of 'mobile banditry'.

Winkeldiefstal	2010	2011	2012	2013	2014	Totaal
Aantal opgenomen aangiften	466	396	354	338	406	1.960
Aantal opgehelderde aangiften	338	295	256	240	279	1.408
Totaal aantal verdachten (totaal aantal)	430	351	309	298	352	1740
Verdachten met Nederlandse nationaliteit	295	223	186	172	166	1.042
Verdachten met niet-Nederlandse nationaliteit	135	129	123	126	186	699
Verdachte criteria mobiel banditisme	33	58	60	62	80	293

Table 2: Number of reported pickpocketing incidents and numbers of pickpocketing suspects arrested in Roermond

From top to bottom: number of reports, number of reports resolved, total number of suspects, suspects with Dutch nationality, suspects with a non-Dutch nationality, and suspects who fulfil the criteria of 'mobile banditry'.

Zakkenrollerij	2010	2011	2012	2013	2014	Totaal
Aangiften opgenomen	192	299	281	324	425	1.521
Aangiften opgehelderd	14	14	12	8	28	76
Verdachten	19	26	18	12	39	114
Verdachte met Nederlandse nationaliteit	13	24	11	7	9	64
Verdachten met niet-Nederlandse nationaliteit	6	2	7	5	30	50
Verdachte criteria mobiel banditisme	3	2	2	3	10	20

Table 3: Nationalities of shoplifting suspects arrested in Roermond who fulfil the criteria of 'mobile banditry'

From top to bottom: Romanian, Belgium, Polish, German, Lithuanian, other.

In this table, the police excludes suspects with Dutch nationality. Only the suspects who fulfil the criteria of 'mobile banditry' are included.

Nationaliteiten winkeldieven	2010	2011	2012	2013	2014	totaal	
						abs.	%
Roemeense	9	12	23	18	40	102	*33*
Belgische	2	12	11	10	6	41	*13*
Poolse	4	3	6	9	11	33	*11*
Duitse	7	7	5	7	7	33	*11*
Litouwse	3	1	3	4	5	16	*6*
Overigen	8	24	13	20	14	79	*26*
TOTAAL	**33**	**59**	**61**	**68**	**83**	**304**	***100***

Table 4: Nationalities of pickpocketing suspects arrested in Roermond who fulfil the criteria of 'mobile banditry'

From top to bottom: Bulgarian, citizen of Bosnia-Herzegovina, citizen of Serbia, unknown, Romanian, Polish, Somali.

In this table, the police excludes suspects with Dutch nationality. Only the suspects who fulfil the criteria of 'mobile banditry' are included.

Nationaliteit	2010	2011	2012	2013	2014	totaal
BULGAARSE	0	0	0	2	8	**10**
BURGER VAN BOSNIE-HERZEGOVINA	0	0	0	0	1	**1**
BURGER VAN SERVIE	1	0	0	0	0	**1**
ONBEKEND	1	0	0	0	0	**1**
ROEMEENSE	1	2	1	1	0	**5**
POOLSE	0	0	1	0	0	**1**
SOMALISCHE	0	0	0	0	1	**1**
TOTAAL	**3**	**3**	**2**	**3**	**10**	**20**

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

WE SENSE TROUBLE

AUTOMATED DISCRIMINATION AND MASS SURVEILLANCE IN PREDICTIVE POLICING IN THE NETHERLANDS

Police worldwide are experimenting with data and algorithms in the hope of the ability to 'predict' crime. The large-scale data processing within these predictive policing projects bring high risks to human rights. In this report, Amnesty International uncovers human rights violations committed by the Dutch police through the design and use of a predictive policing system in the Netherlands: the 'Sensing project' in the city of Roermond. This project has transformed this city into a "living lab" where every person travelling by car is a "guinea pig", subjected to indiscriminate mass surveillance for the data-driven aspirations of the Dutch police. The project is also discriminatory from front to back as it targets people with Eastern European nationalities and Roma ethnicity. The report explains how the Sensing project violates the right to privacy, neglects multiple data protection standards and results in discrimination based on nationality and ethnicity.

Amnesty International calls upon the Dutch police to halt the Sensing project and comparable 'experimental' predictive policing projects, to refrain from policing operations that rely on indiscriminate mass surveillance, to take steps to allow for appropriate remedy and redress of affected individuals, to stop the use of stereotypes in policing operations that violate the principle of non-discrimination, and, which is never a proportionate response that can justify limitations or restrictions on human rights.