

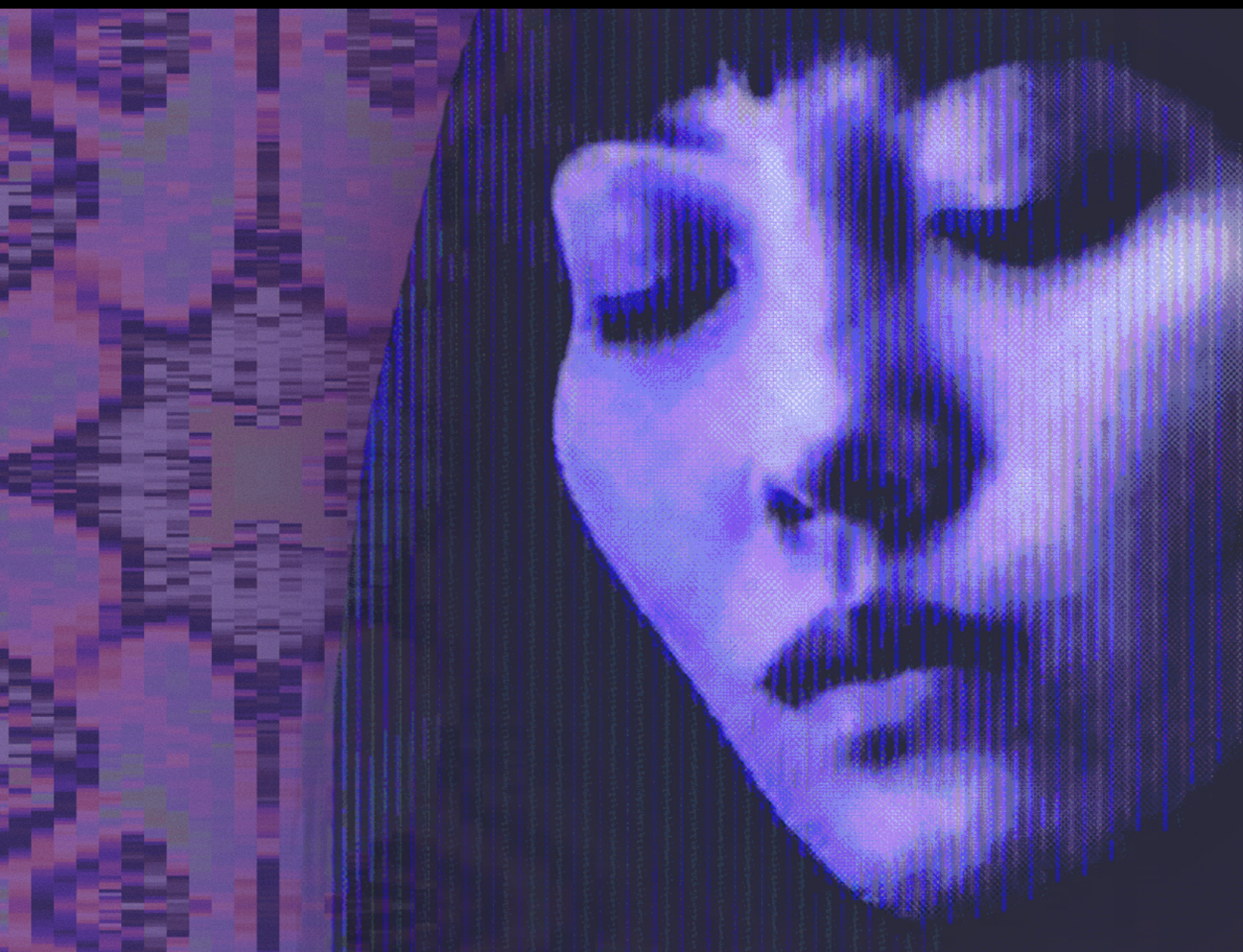


REPORT

AUTOMATED DISCRIMINATION

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

October 2026



ABOUT ORG

Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online.

ABOUT THIS POLICY PAPER

Paper written by Fabio Chiusi, with contributions from Sara Alsherif, Jim Killock and Wendy Grossman.

Published in October 2026

Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. Space4, 113-115 Fonthill Road, London N4 3HH.

Published under a Creative Commons Attribution Sharealike licence (CC BY-SA 4.0).



ABOUT THE AUTHOR

Fabio Chiusi is a journalist, researcher, writer, and adjunct professor whose work focuses on the intersection of digital technology, artificial intelligence, and society. Concerning AI and immigration systems, he worked as project lead for “Automation on the Move” at AlgorithmWatch, where he investigated the deployment of automated decision-making (ADM) systems and AI in migration and border surveillance. His research examined how these technologies affect people on the move, advocating for transparency and the protection of human rights in the face of increasingly automated border control systems.

Also for AlgorithmWatch, he authored their “Automating Society Report 2020”. His academic work includes a Fellowship at the Nexa Center for Internet & Society in Turin and working as an Assistant Researcher on the “Journalism AI” project at the London School of Economics’ Polis think tank. He is an Adjunct Professor at the Vita-Salute San Raffaele University in Milan, where he teaches a course on artificial intelligence in journalism.

Chiusi has written extensively for major Italian and international publications, exploring topics such as online disinformation, the regulation of digital political campaigns, and digital rights. He previously worked as a consultant and assistant researcher in data and politics for the NGO Tactical Tech, contributing to reports on the influence of data-driven practices on digital campaigning in Italy. During the XVIII legislature, he was responsible for digital policies for the Quaestor of the Italian Chamber of Deputies.

Chiusi is the author of several essays and books on media, democracy, and digital technologies. His publications include *Critica della democrazia digitale* (2014), *Io non sono qui. Black Mirror. Visioni e inquietudini da un futuro presente* (2018), and *L'uomo che vuole risolvere il futuro. Critica ideologica di Elon Musk* (2023). His most recent book, *La fortezza automatica. Se l'IA decide chi può varcare i confini* (2025), offers an analysis of the technocratic ideology that seeks to entrust human mobility to advanced technological devices.

CONTENTS

FOREWORD.....	6
BELL RIBEIRO-ADDY MP.....	7
PETE WISHART MP.....	9
SIÂN BERRY MP.....	11
DR CLAUDIA ARADAU.....	13
EXECUTIVE SUMMARY.....	17
INTRODUCTION.....	19
AI AND TECHNOLOGY POLICY.....	22
WHAT WE KNOW ABOUT AI IN IMMIGRATION.....	24
USES OF AI IN THE UK IMMIGRATION SYSTEM.....	25
SUMMARISATION OF ASYLUM INTERVIEWS AND COUNTRY POLICY INFORMATION.....	25
PRIORITISATION AND ASSESSMENT OF IMMIGRATION CASES.....	28
AUTOMATING THE CASE MANAGEMENT INFRASTRUCTURE.....	30
AGE ESTIMATION FOR PEOPLE SEEKING ASYLUM.....	33
MOBILE PHONE DATA EXTRACTION IN THE CONTEXT OF THE ASYLUM PROCEDURE.....	35
SHAM MARRIAGES TRIAGE TOOL.....	37
USES OF AI IN BORDER SURVEILLANCE.....	38
AUTOMATED BORDER CROSSINGS WITH AI-BASED FACE RECOGNITION.....	38
LIVE FACE RECOGNITION TO DEPORT MIGRANTS.....	41
ARTIFICIAL INTELLIGENCE TO “STOP THE BOATS”.....	42
AI-POWERED DRONES PATROLLING THE CHANNEL.....	44
AUTOMATED RISK ASSESSMENT OF THREATS AT THE BORDER.....	47

AI WON'T FIX THE IMMIGRATION SYSTEM. CAN WE FIX AI IN THE IMMIGRATION SYSTEM?..... 52

A. AUTOMATING THE HOSTILE ENVIRONMENT IS NOT THE SOLUTION.....53

 INNOVATION WITHOUT BORDERS..... 54

 AUTOMATING IN THE DARK..... 58

 AUTOMATED RACISM IS STILL RACISM.....61

BEYOND SECURITISATION: RECLAIMING HUMANITY.....62

 FROM TECHNOLOGICAL DEPENDENCY TO DIGITAL SOVEREIGNTY.....63

 APPLY EXISTING SAFEGUARDS..... 66

 INTRODUCE MECHANISMS TO PROTECT MIGRANTS FROM AI HARM.....70

 STOP NORMALISING THE AUTOMATED HOSTILE ENVIRONMENT.....74

CONCLUSION AND RECOMMENDATIONS.....81

1. REJECT SECURITISATION AND TECHNO-SOLUTIONISM IN IMMIGRATION POLICY, AND PUT PEOPLE FIRST..... 81

2. RECOGNISE THE EXISTENCE OF REGULATORY GAPS AND FILL THEM.....82

3. ENHANCE STRUCTURAL TRANSPARENCY IN THE PUBLIC INTEREST.....83

4. CURB OUTSIZED CORPORATE INFLUENCE AND REGAIN DIGITAL SOVEREIGNTY.84

5. AVOID REVERSE SOLUTIONISM, AND STRIVE FOR HUMANITY IN THE BROADER IMMIGRATION SYSTEM.....86

REFERENCES.....88

FOREWORD

BELL RIBEIRO-ADDY MP

People seeking safety are not a risk to be scored, a data point to be calculated, or a backlog to be managed. They are people who have fled persecution. Some may have been tortured, displaced by war, threatened, or forced from their homes. Decisions made by the UK government can determine whether they are sheltered, are reunited with their families, or sent back into danger.

That is why this report matters. It exposes how quickly artificial intelligence is spreading through the UK's immigration and border system, and it asks questions that the government has too often avoided. We know the names of the companies that build these systems. We know far less about what they do. The Home Office has not explained how it will ensure there is accountability when they fail or justified why some of the most vulnerable people, with the least power, should bear the greatest risks.

In my work as an MP, I have questioned the Home Office about its use of AI to summarise asylum interviews and information about people's countries of origin. Ministers insist that these AI tools are used to support decisions, rather than replacing human judgement. However, a summary does not need to be the source of a decision to influence it profoundly. A summary can place some factors ahead of others. A country summary can ignore information or rely on out-of-date guidance. Where someone's physical safety depends on the details of their account, the use of AI in the claim process cannot be shrugged off as a mere administrative efficiency.

Speed is not the same as efficiency, and it is certainly not justice. The Home Office's own trial evidence showed that some AI-generated summaries were rejected because they were inaccurate or had missed crucial information, and that some of their own staff were not confident in the AI system's results. That should have been a warning, rather than an invitation to press ahead.

We need full transparency about the way these tools work. The Home Office must publish the equality and data protection assessments it has made, explain how staff are inducted and trained to use these tools, and allow independent validation of how well they perform. At present, asylum seekers are not even told when AI has been used to summarise their cases. The Home Office should not be using AI

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

in decisions this fundamental to people's lives until it can show the tools are accurate, that proper safeguards are in place, and that it can explain clearly how they are used.

In spite of questions and requests, the Home Office has been reluctant to publish the documents that would explain how AI is used in asylum processing, what the problems are and how they are being addressed. That is a source of real frustration. It is also hard to understand if the Home Office genuinely believes its policies are effective and justifiable.

There are many alternative and potentially effective means of addressing the administrative failures of the asylum system, including employing more staff, and giving them training and support. These are not about technology, but fairness. Likewise, proposals such as safe routes for asylum applicants, and changes to ensure that applicants' lives are not placed on indefinite hold while their claims are processed, could improve their situation and reduce costs to the taxpayer. Yet for political reasons, successive Home Secretaries have preferred to prioritise hostility and control over humanity and compassion.

This is not an isolated concern. I have raised concerns with the use of algorithms in the immigration system for many years, because opacity shields those in power from scrutiny while the people being judged, including migrants and refugees, suffer the consequences. I have also drawn attention to the bias built into facial recognition technology and its potential to worsen stop and search and other discriminatory policing. As this report highlights, the Home Office continues to promote similar technologies, such as age estimation, despite widespread evidence that they are deeply flawed. I share the authors' concern about the influence of Big Tech in shaping AI, promoting its use and ultimately shaping government policy. Technology should serve democracy, not undermine it.

Too often, AI is sold as a policy solution rather than a tool. We are asked to believe that automation and surveillance are inevitable and that the results, because they emerge from digital systems, are somehow neutral and accurate. Very little of this is true. If we build technologies based on policies of suspicion and hostility, we get systems that deliver harms and discrimination more quickly. That is not efficient or fair. This report is a timely reminder that there is a much better and more humane way of managing our immigration and asylum systems, if we are prepared to break with the Home Office's toxic record of failure.

PETE WISHART MP

The asylum system deals with people at some of the most difficult points in their lives. For someone who has fled persecution, war or violence, the decision made about their asylum claim can have consequences that are quite literally a matter of life and death.

That is why we need to be very careful about how artificial intelligence is introduced into the asylum system.

There is nothing inherently wrong with using new technology to help officials with their work. If it can reduce unnecessary administration and give caseworkers more time to consider individual cases properly, then it may have a useful role to play.

But we should never lose sight of what these decisions are about.

An asylum claim is about an individual's experiences and whether they can safely return to the country they have fled. The consequences of getting that decision wrong can be devastating.

AI systems can make mistakes. They can produce inaccurate information, leave out important details or present something that is wrong with a confidence that makes it appear reliable. In an asylum case, they can have ruinous consequences.

There are serious concerns about the use of AI by the Home Office in the asylum system, including the reliability of AI generated case summaries, the possibility of hallucinations and the lack of transparency around how these systems are being used. These concerns deserve proper scrutiny.

If an AI system leaves an important part of an asylum interview out of a summary, that information may not receive the attention it deserves. If it produces incorrect or incomplete information about conditions in someone's home country, it could affect how their claim is understood.

There is also an important question of accountability. If an asylum seeker believes that an AI system has made a mistake, they need to be able to know that the technology was used and have the chance to challenge its output.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

I have previously raised concerns about the use of technology in assessing the age of people arriving in the UK, particularly where there is a risk that children could be wrongly treated as adults.

We should be careful not to assume that making the system faster necessarily makes it better. The asylum system needs to make good decisions as well as timely ones. A quicker wrong decision is not an improvement.

If AI is to be used, there must be proper safeguards. There should be transparency about where it is being used, independent scrutiny of whether it works, proper consideration of bias and errors, and a clear way for mistakes to be identified and challenged.

Most importantly, responsibility must remain with people.

Technology can assist those making asylum decisions, but it cannot take responsibility for what happens to the person whose case is being considered.

And human oversight must mean more than having a human being somewhere at the end of the process. Caseworkers must be able to check the original evidence, question what the technology produces and disregard it when it is wrong.

We should welcome technology where it genuinely improves the system. But we should never use AI simply because it is available or because it promises to save time.

When someone's future depends on getting a decision right, human rights, fairness and accuracy must come first.

SIÂN BERRY MP

The asylum system deals with people who have fled war, persecution and violence, and whose future depends on whether this system treats them with fairness.

In reality, however, the lives of those in dire need of help are used for political point scoring, in efforts to prove that the Government of the day is 'tough' on immigration.

This point scoring becomes incredibly damaging when it drives the Government's technology choices. If ministers demand migrants be treated as numbers and threats to be assessed, then there will be a big tech solution. That is the promise of many Artificial Intelligence vendors selling border technologies.

Systems that summarise interviews, assign risk scores, estimate age, scan faces or sift through people's health records may appear efficient, but they also create errors, reproduce bias, and make it harder for people to understand how and why decisions have been made about their asylum status. Worse still, challenging these decisions, even when someone's life may be in danger, becomes much harder.

This report is an important and timely account of how the UK is rapidly deploying these systems, without sufficient parliamentary scrutiny and external oversight. As the report shows, for parliament, the questions to ask are, who has power over these systems, in whose interest are they operating, and what happens when they go wrong?

I know from my work as a Member of the London Assembly how quickly these systems develop from exceptional use to something routinely deployed. Use of Live Facial Recognition by the Metropolitan Police has expanded throughout the country without scrutiny in parliament or a legal framework. We should learn from that experience. Technologies that can silently and secretly identify, track and categorise people cannot be left to private companies, with vague promises that it will be used responsibly.

As MP for Brighton Pavilion, I am frequently confronted with the human cost of the asylum and migration systems. Constituents and their families come to me

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

for help dealing with extremely difficult and hostile processes, or to understand the poor decisions the Home Office routinely makes.

Many people seeking asylum have their applications rejected, but are eventually recognised as needing our protection, often after very long delays. The Home Office's response is to automate summaries with AI and speed processes up, and with new legislation, it seeks to prevent people seeking asylum from using the courts to challenge these errors.

We should not accept the false choice between control and compassion. A fair asylum system means providing safe routes, accurate first decisions, keeping families together, providing the right to work, and proper support so that applicants can build a life in our communities. It means addressing the conditions that make people vulnerable to exploitation, rather than treating them as a problem to be managed through AI surveillance systems.

This is also a question of civil liberties. These technologies are applied to everyone. Duties that place employers, public servants and landlords in the position of immigration officers. The use of biometric checks, digital ID and data sharing are normalised, creating a more suspicious and less free society for all of us.

There is a better way. Artificial Intelligence systems must be subject to clear laws founded in human rights and fairness, with decisions subject to scrutiny and challenge. Human beings need to make decisions about people, and not rely on opaque calculations. The people who are most affected must have a real voice in the way these systems are designed and used. And public bodies must not hand over democratic control of the way that technologies are designed and deployed to a handful of corporations with dubious human rights records.

This report offers a route out of the automated hostile environment. We should take it, not by rejecting technology and innovation, but by ensuring technology serves humanity, justice and democracy.

Siân Berry MP

Green Party MP for Brighton Pavilion

DR CLAUDIA ARADAU

The promise of Artificial Intelligence (AI) to solve everything, from health crises and climate change to security threats and border control, continues unabated despite AI technologies' many failures, errors, and unreliability. The Open Rights Group report, *Automated Discrimination: Unpacking the digital hostile environment*, sheds light on what the uncritical belief in AI as the 'great fixer' of border security and immigration policy means for people, planet and politics. AI has become a sort of magic lubricant of all areas of governance. However, AI is rarely explained publicly in relation to the specific technologies deployed across various areas of governance, whether probability calculations of risk, image recognition or text summarisation. Each of these does something different. Probability calculations have long been used to classify, order and rank people and problems. Who and what should be tackled first? Which resources should be prioritised? Image recognition adds a new dimension to probability calculations, as it requires a threshold to make a Yes/No decision. What is the threshold beyond which an object counts as a car, a passer-by as a suspect, or an individual on a move as the person on an outdated watchlist? Text processing technologies such as summaries produced by what is now known as GenAI do something different again. They are pre-trained on large volumes of text and therefore reconstruct text according to the most common understandings in the data they were trained on.

These three technologies illustrate many of the problems with their use in immigration governance and border security. Probability calculations embed assumptions about what and who should be prioritised and depend on data accuracy. Yes/No decisions efface the decision of where to draw the threshold and obscure ambiguity and uncertainty. A tiny tweak of a threshold can make the difference between suspicion and innocence. Summaries based on what is most common in training data can erase or misconstrue details vital to an asylum seeker's case. The more data is produced, the less reliable it becomes. The more data is shared across different systems and institutions, the more difficult it is to trace its provenance and retrieve its context.

Automated Discrimination offers insights into the different kinds of systems and AI used in the UK's immigration system and border security. By moving away

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

from the overly general moniker of AI, it shows how systems as diverse as case summarisation, live facial recognition, age assessment or automated risk assessment have real, impactful and disproportionate consequences upon the most vulnerable people in our societies. These systems do not just amplify existing social biases in the data, but produce hostility as both an intended and unintended consequence. Making these systems legible is an increasingly difficult endeavour, as opacity and secrecy pervade their use across private and public actors.

There are many questions that need to be asked about these systems and what they do: who develops the systems, who acquires them, how is their impact assessed, what are their long-term consequences, how do they transform relations between individuals and public authorities, and between private and public actors; who is accountable for their use and impact? Furthermore, the turn to AI as a universal problem-solver for public authorities raises the question of what this AI fixation means for democracy, democratic participation and accountability. In other words, what we can ask and answer about these systems tells us as much about the state of democracy today as it tells us about these systems themselves.

AI technologies promise a lot: control, efficiency, speed, and cost-cutting. The report rightly cautions against uncritically accepting these techno-solutionist promises. This is not to say that looking for solutions is misguided or unacceptable. Yet, solutions are implemented on the basis of insufficiently deliberated – and often misdiagnosed – problems. What is the problem that AI systems seem to try to fix? Calls for more AI in immigration and border governance try to revert to a sovereign imaginary of a world inhabited only by sovereign states whose actions are not bound by democratic norms but increasingly justified only in the name of security. The AI systems do not promise more democracy, better livelihoods, or more just decisions.

Drawing inspiration from the report, I highlight three ways in which democracy is marginalised and made vulnerable not only by AI systems, but by the authorities' use of them. First, the proliferation of AI technologies has amplified both state and commercial secrecy. Secrecy is often taken for granted in the context of national security. It is also accepted as commercially valuable trade secrets. Yet, in a democracy, the boundaries of secrecy always need to be negotiated, as extensive secrecy undermines the possibilities of democratic

participation, contestation and public deliberation. As AI systems infuse more and more practices of governance, what are the limits of secrecy, where are its boundaries? What happens to democratic accountability when both private and public actors claim secrecy in the name of security and refuse to justify their actions? The 'near-total secrecy' that civil society organisations and researchers find when trying to access information about these technologies should concern us all.

Secondly, the implementation of AI systems across immigration and border infrastructures seems increasingly without limits. Even when the Home Office conducted its own 'Evaluation of AI trials in the asylum decision making process' in 2025, concerns about inaccuracies and quality of decision-making were ignored or downplayed. More than an AI fix, it is AI without limits that undermines democratic processes of deliberation and contestation. Deliberation and contestation force public authorities to pay attention to social and political demands. As political philosopher Pierre Rosanvallon put it, "democracy can flourish only if it acknowledges the risks of dysfunctionality and equips itself with institutions capable of subjecting its own inner workings to constructive evaluation".¹

Finally, despite failures, errors, and inadequacies, more AI technologies are introduced in the name of security. It often takes public scandals and the persistent work of civil society organisations to draw attention to how public actors ignore or dismiss the democratic imperative to justify their actions under the mantle of protecting the 'people'. The people are invoked here as a unitary, homogeneous entity, obscuring the need to negotiate disagreement, multiplicity and complexity within a people. Democracies need to negotiate relations between majorities and minorities without succumbing either to the tyranny of a majority or a minority.

An AI fixation that intensifies secrecy, refuses disclosure and access to information and ignores civil society concerns undermines democratic participation, negotiation and contestation. When secrecy, discretion and security become limitless, it is democracy that becomes limited, marginalised and weakened. Limitless secrecy also reinforces the impression of a 'deep state' that works beyond public reach and accountability, thus feeding conspiratorial and anti-democratic discourses.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

If AI is not a fix for immigration policy in the UK, fixating on AI without limits carries serious risks for democracy. This does not mean that the use of certain AI technologies cannot have good outcomes, or that some AI systems might even appear less 'hostile' than public authorities themselves. What the AI fixation in border and migration governance brings to light is how democracy is deferred in the name of security, limited in the name of secrecy, and held back in the name of efficiency.

Claudia Aradau, Professor of International Politics,
King's College London

EXECUTIVE SUMMARY

The United Kingdom is betting on artificial intelligence to ‘fix’ immigration. Driven by a techno-solutionist ideology that reduces the complex human phenomenon of migration to a technical problem awaiting a technical fix, successive governments, including the current Labour administration, have committed to embedding AI across the immigration system and at the nation’s borders. Based on desk and literature research, expert interviews, and analysis of Home Office documents obtained through freedom of information (FOI) requests, this paper argues that this is no longer rhetoric: AI is being woven into crucial parts of the immigration machinery, and is poised to shape all of it.

We document a rapidly expanding catalogue of deployments. Within the immigration system, AI is being trialled or used to estimate the age of people seeking asylum, summarise asylum interviews and country policy information, prioritise and assess cases through the opaque Identify and Prioritise Immigration Cases (IPIC) tool, sift through irregular entrants’ mobile phones, and automatically flag potential “sham” marriages with a red or green light. At the border, live facial recognition, AI-powered drones and satellites, and foreign-built autonomous surveillance towers are marshalled to “stop the boats”, while obscure programmes such as Cerberus promise to pre-empt unknown threats, marking a decisive shift from reactive to ‘predictive’, proactive enforcement.

This automated fortress raises grave and converging concerns. The systems rely on technologies renowned for bias, disproportionately harming the most vulnerable people on the move, and therefore encoding discrimination into the infrastructure of border control. They operate in near-total secrecy: officials routinely invoke ‘national security’ to stonewall FOI requests, redact disclosures. In at least one instance, the authorities have pressured a researcher to withdraw published findings. Much of this technological arsenal is not British but supplied by US, Israeli, and other foreign defence and security giants, producing technological dependency, and techno-political lock-in, that reality sits awkwardly with the Government’s stated ambition to be an “AI maker”, not an “AI taker”. All of this unfolds within a regulatory vacuum that ministers have shown no intention of filling, having instead promised the world’s most “unfettered”

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

environment for AI experimentation, even as the Government seeks to “modernise” the European Convention on Human Rights in ways that threaten the right to asylum itself.

AI will not fix the immigration system. But the deeper problem is the ideology that frames migration as a permanent emergency to be solved by algorithms, criminalising migrants and normalising an “automated Hostile Environment”. This paper therefore sets out five recommendations:

1. Reject AI techno-solutionism and put people ahead of their data-driven reduction;
2. Recognise and fill regulatory gaps, banning undemocratic uses such as mass live surveillance of public spaces and strictly regulating high-risk applications before deployment;
3. Enhance structural transparency in the public interest, with stronger FOI laws, a narrower definition of national security and a robust public register of government AI tools;
4. Curb outsized corporate influence and reclaim digital sovereignty; and
5. Avoid ‘reverse solutionism’ by situating the critique of AI within a wider contestation of prejudicial, ideologically driven anti-immigration politics. Only then can AI become a tool of humanitarian assistance rather than one of blind, automated discrimination.

INTRODUCTION

The United Kingdom is fully committing to artificial intelligence to “fix” immigration. Driven by a flawed ideology that reduces complex social phenomena to technological problems in search of a technological solution,² the current Labour administration is rushing towards the integration of AI into a vast array of government activity, including in both the immigration system and border security.

While consistent with the vision laid out by previous Tory administrations, the Labour government has pushed this ‘techno-solutionist’ posture to the extreme, defining AI as the key driver of a ‘national renewal’,³ in which productivity, efficiency, liberty, and security will finally be optimised and reconciled. Given AI’s transformational nature, “we need to run towards it”, then-prime minister Keir Starmer said,⁴ vowing to make the UK an “AI superpower”.⁵ For Starmer’s Minister for AI and Digital Government, Kaniska Narayan, this meant⁶ moving even faster than the US state – evoking Silicon Valley’s signature “move fast and break things” approach – to ultimately become “the world’s best adoption nation” for AI.

This is by no means mere rhetoric. Based on a combination of desk and literature research, expert interviews, and analysis of Home Office documents disclosed as a result of freedom of information (FOI) requests, this paper argues that artificial intelligence is already in place for crucial pieces of the immigration system puzzle, and will most likely affect all of it in the foreseeable future.

As we will detail in the first chapter, AI is being trialled or deployed to estimate the age of people seeking asylum, summarise asylum interviews and immigration policies, inform decisions on which asylum requests to prioritise or grant, sift through mobile phones belonging to irregular entrants searching for hints of “assisting illegal immigration”, and evaluate – with an automated green or red light – the likelihood that a marriage is a sham to circumvent immigration restrictions.

The Government makes it explicit that this all amounts to a call for total cybernetic control⁷ of any migrant deemed to be a threat. For example, Home Secretary Shabana Mahmood vowed⁸ to finally “achieve” Jeremy Bentham’s

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

Panopticon – meaning, in her own words, that “the eyes of the state can be on you at all times”. Under her watch, live face recognition has been trialled⁹ to help immigration authorities at the Anglesey, Wales Port of Holyhead to identify and locate those in breach of a Deportation Order. This signals a broader shift from reactive to proactive immigration enforcement, underpinned by predictive analytics and data-driven algorithmic risk assessments, as in the major but still obscure ‘Cerberus’ project,¹⁰ which promises to defend the UK from unknown threats.

Securing the nation’s borders through AI is consequential. This piecemeal construction of an automated fortress that aims to be capable of securing the protection of British citizens from the “invading” Others – which, as detailed in chapter 2, is the ultimate goal of techno-solutionist immigration policies and tools. This is the stated justification for using autonomous border surveillance towers produced by US giant Anduril to patrol the Channel, together with AI-powered drones and satellites, to “stop the boats”.¹¹ AI doesn’t get distracted, doesn’t need coffee breaks, doesn’t sleep, and is always watching.

AI does not (willingly) leak unwanted information to the press or the public. And, judging from the FOI replies we assess throughout this report, the Home Office is very protective of the secrecy of its “intelligent” arsenal to safeguard border security. While national security does require a certain degree of opacity, the extensive redactions in the (few) documents the Home Office disclosed and, even more, the silence with which public officials repeatedly greeted specific questions about AI-based systems for immigration scream the need for additional transparency in the public interest.

As we document below, the direction taken by the Home Office, is very different. In the material we were able to access, officials went so far as to use vaguely threatening language to appeal to a journalist’s “conscience”, trying to convince him to remove certain information from published research¹² on Anduril towers on the grounds of alleged – but unproven – inaccuracies. Officials even accused the journalist of unnecessarily endangering the lives of those attempting to cross the Channel.

Among the many issues raised by the material we consulted and the experts we spoke to, some stand out as particularly acute and urgent. For one, it’s troubling that many AI-based technologies deployed in the UK immigration system and used to patrol UK borders are not UK-made, but rather made in the US, Israel, and

other foreign countries. In the current unpredictable and rapidly shifting geopolitical context, technological dependence risks locking this country into unwanted or otherwise problematic choices.

It also might not be the smartest idea to build an infrastructure of pervasive, smart control for certain individuals but not others in a broader context of eroding democracy and human rights. This is exacerbated by the fact that the system in progress relies on biased technologies that notoriously disproportionately affect people on the move,¹³ especially the most vulnerable such as refugees and people seeking asylum. Government promises to only apply automated technologies ethically and responsibly, including at the border, conflict with their own idea of “modernising” the European Convention on Human Rights by adding limitations¹⁴ – which ultimately means erasing the right to asylum as we know it.

Experts do agree that the current regulatory framework – which does not include specific norms for AI in migration – is inadequate, given current technological developments.¹⁵ However, UK governments across the political spectrum have not aimed to fill that gap: instead, they have consistently promised free rein for AI experimentation. The 2021 ‘National AI Strategy’, published during the Boris Johnson’s administration, was meant to “signal to the world our intention to build the most unfettered, unregulated business environment in the world”.¹⁶

While AI can help streamline procedures and produce much-needed efficiency gains compared to obsolete and faulty legacy systems, the ideological assumptions driving its rushed adoption worry civil society activists and academics, who have repeatedly warned over the last two decades that “techno-solutionism” is a recipe for disaster.

Reducing people on the move and migrants with legal status to data points is all the more dangerous when coupled with constant and incorrect criminalisation of migrants. The normalisation of anti-immigrant sentiments increasingly results in discrimination and abuse against people seeking asylum. As multiple civil society organisations have noted, this amounts to automating the ‘Hostile Environment’ first envisioned for ‘illegal migrants’ by then-prime minister Theresa May in 2012.¹⁷

Protecting the rights of all, and thus the foundations of democracy, has never been and is not now the point for AI in immigration. That urgently needs to change. This paper provides a set of policy recommendations to help challenge this

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

untenable status quo, demanding effective transparency and democratic checks and balances to open up the immigration AI black box.

In the never-ending quest to 're-balance' security and liberty, which has tilted heavily toward security since 9/11 and the 'War on Terror', it is time for liberty to reclaim its place, especially as a growing nexus of nationalism, racism, and technocracy threatens the foundation of the international order.

The UK frames itself as a technology "adoption nation", a term coined by the Government to signal AI's rapid integration into an all-encompassing array of administrative functions. However, the term obscures a dark side made of bias, discrimination, entrenched privilege, and locked-in surveillance technologies that provide the infrastructure for authoritarian repression, as demonstrated in the AI-informed mass deportations and abuse seen from the Trump administration. It is high time to shine some light on its opaque surface.

AI AND TECHNOLOGY POLICY

While the UK appears uncritical in its assumptions about the potential of AI as a technology, academia and technologists note some fundamentals that need to be spelled out up front in any discussion of AI. We go into greater depth regarding these in our separate paper, "AI and the Public Sector".¹⁸ The key points to note are:

- AI is not intelligent. It is a pattern matching technology.
- AI is subject to biases and errors absorbed via gaps in the data it is trained on.
- Correlation is not causation. Therefore, AI's judgements can replicate patterns of discrimination within society at large.
- Human complexity, variety, and change do not readily fit with statistical monitoring and prediction of the kind provided by AI. AI may be understood as 'reductive' (trying to produce a mechanical model of reality) while policy needs to be 'holistic' (understanding the world as complex, unpredictable, and subject to constant change).

As we discuss below, the approach to using AI at the borders is predominantly ideological and rooted in national security thinking. While national security is a necessary part of what governments do, it is problematic when applied to civilian

situations such as handling migrants. Reductive thinking is common in national security situations, and errors, even deaths, can be tolerated when national security is at stake. Applying this logic to someone's asylum application or right to cross a border is unacceptable.

When government deals with complex policy issues such as migration and borders, datafication, reductionism, and AI all lead in the wrong direction and risk veiling the actual solutions and measures that governments should take to provide stability. Indeed, government itself recognises the risk of simplistic and counter-productive policy making. The Government Office for Science, for example, encourages systemic policy analysis through its Systems Thinking toolkit, which asks civil servants to understand the interrelations between policy landscapes to deliver effective interventions.

It is incredibly worrying, then, to see cutbacks to foreign aid budgets, weak responses to genocide and the displacement of peoples, and attempts to slow action on climate change. Warnings of climate-related increase of displaced people and resource wars have persisted for several decades. It makes no sense to endanger our own climate targets by fuelling the exponential growth of domestic AI data centres.

While these policy interactions are beyond the scope of this document, we detail the ideology that results from ignoring them: 'techno-solutionism' that seeks to manage this systemic failure by targeting its victims. Such an approach is neither moral nor sustainable. It is likely to generate further authoritarianism, followed by political collapse.

WHAT WE KNOW ABOUT AI IN IMMIGRATION

Artificial intelligence is rapidly becoming a core feature of public service delivery in the UK. From welfare to healthcare, from education to the justice system, pilots and deployments of AI tools have multiplied in recent years.

According to the Government, AI will generate minimum pupil attendance targets in schools,¹⁹ cut animal testing,²⁰ improve the quality of rape trial evidence,²¹ and prevent prisoners from being mistakenly released from jail.²² Policymakers themselves will soon be able to consult a suite of large language model (LLM) applications. Dubbed ‘Humphrey’, these chatbots will summarise and analyse proposed policies, and even provide “a parliamentary vibe check” predicting their popularity.²³

This is just the beginning. According to a former aide speaking to Politics Home in October 2025, prime minister Keir Starmer saw British society as a testing ground for the deployment of as much artificial intelligence as humanly possible: “He’s like, ‘Where it exists, why aren’t we using it everywhere?’”.²⁴

In its “2030 Digital Strategy” the Home Office envisions mass adoption of AI as one of the core “strategic shifts”, with the ambition to quickly become “the leading UK government department in the use of digital, data and technology” and thereby “transform our digital services with AI and more automation”.²⁵ Predictably, this wave of socio-technical dehumanising change is profoundly affecting the conception and operation of the immigration system and border security. Examples abound.

This chapter details what is publicly known about the use of AI in the immigration system and border security in the UK. A methodological note: given that – as we will show – most such use cases are deliberately shrouded in opacity, the list we provide can by no means be considered exhaustive or completely accurate. When freedom of information requests are considered a threat to national security, and officials fail to answer basic questions concerning the aims, capabilities, and even mere existence of AI-powered systems being tested and/or deployed against settled and irregular migrants there is no way to fill crucial knowledge gaps in the public interest.

What follows is our best effort to provide an evidence-based description of confirmed AI tools in the immigration system (*Uses of AI in the UK immigration system*) and for border security (*Uses of AI in border surveillance*). Wherever doubts remain, they will be promptly highlighted and discussed.

USES OF AI IN THE UK IMMIGRATION SYSTEM

Uses of artificial intelligence in the UK immigration system are promoted with the idea that AI will achieve “efficiency”, save time, and “assist” – rather than substitute for – human judgement, allowing officials to focus on more meaningful tasks such as complex asylum cases and “risky” subjects. The Government claims that the AI efficiency approach cannot be addressed without human checks, but includes little clarification or assessment of the actual “efficiency gains” these systems are meant to provide. In addition, the government’s framing of “human judgement” reduces human involvement to a narrow supervisory function, overlooking the broader human qualities that governance and decision-making should entail.

SUMMARISATION OF ASYLUM INTERVIEWS AND COUNTRY POLICY INFORMATION

In April 2025, the Home Office published its “Evaluation of AI trials in the asylum decision making process”²⁶. In it, the HO set out the results of pilots conducted between May and December 2024 for two novel AI-based systems: ACS, or Asylum Case Summarisation, a tool which uses artificial intelligence to summarise asylum interview transcripts; and APS, or Asylum Policy Search, defined as “an AI search assistant that finds and summarises country policy information”.

According to the evaluation, these tools are meant to work “as an aid for decision-makers to improve efficiency but do not, and cannot, replace any part of the decision-making process”. Both tools use large language models (LLMs). The campaign groups Foxglove and Open Rights Group have confirmed the non-profit newsroom Inkstick’s reporting that ACS is “based on San Francisco based OpenAI’s GPT-4”.²⁷ All LLMs are prone to errors, known to “hallucinate”, and produce distorted or flat-out false information.²⁸

Consistent with the techno-solutionist principles driving these pilots, the document frames key findings as efficiency gains. For example, the Home Office

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

says, “the ACS tool could save 23 minutes per case when reviewing interview transcripts”, whereas “decision-makers could save an average of 37 minutes per case when searching for country policy information using the APS tool”. This allegedly reduces the “cognitive load” on human decision-makers. Such a claim is difficult to sustain when the Home Office insists that these tools will not replace caseworkers reviewing the original text and information themselves, because then it would contradict the entire premise of their deployment.²⁹

Importantly, the results showed that the tools do not affect “decision quality” in either direction. This implies that using AI did not promote better decisions – only faster and more careless ones.

The time savings are also questionable. Some case workers involved in the pilots “highlighted minimal time-saving due to the summary not providing source references”. In addition, both ACS and APS are based on ChatGPT-4o, which in many cases cannot provide references or clearly evidence how particular outputs or summaries were generated.³⁰

The evaluation summary also found that “a small proportion of summaries produced (9%) were deemed to be inaccurate or had missing information”. Almost a quarter of interviewees (23%) lamented not being fully confident in the summary information.

The pilots also could not ensure that time savings claims translate into cost savings. As we are seeing elsewhere, the use of AI often creates additional work in the form of the need to check, verify, and correct its errors.

According to Context News, these systems have already been strongly criticised by rights advocates, who have framed the idea as “outsourcing life-and-death decisions to dehumanising technology”. The story cites Laura Smith, a legal director at the Joint Council for the Welfare of Immigrants: “Relying on AI to help decide who gets to stay here and who gets thrown back into danger is a deeply alarming move”.³¹

It is also likely unlawful, according to a legal opinion commissioned by Open Rights Group.³² The opinion provided a detailed assessment of the ACS and APS tools’ compliance with both the Principles contained in the UK AI Playbook³³ and the broader “domestic legal framework” (including the European Convention of Human Rights and UK public law).

The legal opinion found that both systems miss the mark on multiple foundational aspects. Some were technical. For example, the HO provided no quantitative assessment of the accuracy of APS's outputs, while AI-produced summaries could not be cross-referenced with the original source material, making them difficult for decision-makers to verify and raising serious concerns over the transparency and explainability of the resulting decisions.

Additional indicators of non-compliance included ethical and potentially unlawful issues, such as limited testing for bias, which the authors deemed "unacceptable," and the failure to register ACS and APS in the Algorithmic Transparency Recording Standard (ATRS) hub. The lawyers also noted procedural concerns, including the lack of public information about whether the Government considered analogue or non-AI solutions before implementing AI.

"Our conclusion", the authors write, "is that – on the basis of the information currently publicly available – the UK AI Playbook is not being followed or we have serious concerns that there is non-compliance due to the absence of publicly available information." Subsequently, in response to a parliamentary question from Carla Denyer, the Home Office confirmed that they did not follow the AI Playbook.³⁴

The Home Office's failure to inform asylum applicants when AI tools were used in their assessment, together with other missteps, likely crossed into illegality, the authors argue. They go on to detail "unlikely" compliance with Article 3 of the ECHR (because of missing safeguards against inaccurate information and automation bias), unmet requirements for Public Sector Equality Duty (lacking a published Equality Impact Assessment), and even the breach of data protection rules for ACS.

They also identified "significant risks" in terms of process irrationality and decisions made on the basis of inaccurate information. According to ORG, this assessment ultimately "opens the way to legal challenges by asylum applicants who believe that AI has been used in their assessments that determine whether or not they can be granted protection in the UK".³⁵

Nonetheless, in October 2025 the HO further explored the use of AI for the automated "interpretation, translation and transcription"³⁶ of speech in languages other than English in the context of border and immigration operations.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

Anecdotal evidence gathered by the Migrants' Rights Network suggests that this might already be happening. As the Network's January 2025 'AI Under Watch' reports: "People in the asylum system and refugees in our Network have spoken to us about instances where they believe AI has been used in the process of their asylum cases".³⁷

PRIORITISATION AND ASSESSMENT OF IMMIGRATION CASES

The Home Office adopted an algorithmic tool called 'Identify and Prioritise Immigration Cases' (IPIC). According to the Public Law Project's "Tracking Automated Government Register", IPIC is "used to assess the removability and level of harm posed by immigration offenders, automate the identification and prioritisation of cases, and to provide information on the length of time a barrier to removal has been in place".³⁸

In an in-depth Investigation of the system, Privacy International concluded that it "automatically identifies and recommends migrants for particular immigration decisions or enforcement action", including detention, denial of services, and the "conditions which individuals on immigration bail are subject to, and deportations".³⁹ The 2025 Migrants' Rights Network "AI Under Watch" report calls IPIC "a prominent, confirmed use of AI in the asylum system".⁴⁰ In response, the Home Office contested any characterisation of IPIC tool as an AI, and argued that IPIC is a "rules-based" system instead of an "AI" tool.⁴¹

The difference is significant. As Louise Amoore puts it in her 2024 article "The Deep Border",⁴² "where rules-based algorithms sought to capture the relationship of variables within a dataset – often with human domain specialists crafting the rules – deep learning seeks to generate the rules from features that are not pre-programmed in advance".

As a result, deep learning algorithms do more than produce logical outputs. They also reveal and reinforce societal power imbalances by identifying and generating patterns from datasets that contain hostile narratives about migration.

This turns the technology into a political instrument that both implements and shapes immigration and border procedures. In Amoore's words, these processes are now "written through the machine learning models that make the world in their own image – as clusters of attributes and feature spaces from which data examples can be drawn".

Freedom of information requests sent by Privacy International helped shed light on how IPIC actually works and, even though much is still unknown, the organisation was able to discover that “the algorithm is designed in ways that push caseworkers towards accepting its recommendations. For example, officials have to provide an explanation if they reject a recommendation whereas this is not the case if they accept it”.⁴³

Nationality – together with age – emerged as one of the “business categories” IPIC employs. This follows the design of a previous streaming algorithm, which also discriminated by nationality. This was deployed in 2015 to process visa applications and withdrawn five years later under the threat of litigation from the Joint Council for the Welfare of Immigrants and Foxglove.⁴⁴ This algorithm implemented what campaigners characterised as a “fast lane” for the “speedy boarding” of “white people” from certain countries, leading the Council to accuse the system of producing racist results. IPIC’s design, similarly, means that, “people with certain nationalities could be more likely to receive negative decisions against them (such as recommending detention or electronic monitoring via a worn device)”.

As the Public Law Project notes, while the specific “types of interventions that might be recommended by IPIC have not been disclosed”, the system “may be used to decide whether someone should be subject to GPS tagging”. This was confirmed in a 2023 Home Office reply to a FOI request by researcher Mia Leslie.⁴⁵

Touted as a more humane alternative to detention, since 2021 the heavily contested practice of GPS tagging has been applied to migrants released on immigration bail⁴⁶ with the involvement of companies such as Capita, G4S, Airbus Defence, Space Ltd, and Telefonica.⁴⁷ From July 2022 to December 2023, the Home Office held a pilot to expand the use of GPS ankle tags to tracking migrants arriving in the UK by “small boats”.⁴⁸ The pilot, labelled “appalling” and “draconian” by refugee charities,⁴⁹ was also found to be in violation of data protection laws by the Information Commissioner’s Office. In 2022, Privacy International also exposed a contract⁵⁰ between the Home Office and the British electronics manufacturer Buddi Limited⁵¹ for facial recognition-based smartwatches, a type of “non-fitted” devices to be used as an alternative to “fitted” ankle tags.

In all such technologies, AI does not drive the GPS tags themselves. However, AI may be involved in interpreting or acting on data, potentially including GPS

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

tracking information, that's been collected within the broader immigration enforcement process – further embedding the criminalisation of migrants into the system.⁵²

For example, the Home Office uses specific algorithmic tools to manage and review the tagging of migrants. Until the development of IPIC's "electronic monitoring module" is complete, the Home Office will continue to operate the Electronic Monitoring Review Tool (EMRT), an automated system that provides decision recommendations for individuals whose electronic monitoring condition is under review.⁵³ EMRT automatically generates "harm scores" to determine how long individuals should wear ankle tags before being allowed to transition to non-fitted devices. When Public Law Project researcher Mia Leslie inquired further in a FOI request, the Home Office refused disclosure.⁵⁴

To clarify further, in August 2025 Privacy International filed a complaint with the Information Commission's Office (ICO) about IPIC and EMRT,⁵⁵ arguing that both "appear to [be] being used in immigration enforcement operations to assist or even replace human decision-making in ways that could lead to life-changing outcomes for migrants, seemingly without sufficient safeguards to protect the right to privacy and meet data protection standards".⁵⁶ Also, according to the complaint, EMRT's "harm scores" essentially amount to "decisions made solely by automated processing".

Privacy International's conclusion is stark:

"This is yet another example of how the UK Home Office appears to believe it can make use of new technologies such as automated-decision making without having to uphold its obligations to protect the rights of migrants."

AUTOMATING THE CASE MANAGEMENT INFRASTRUCTURE

A key component of Home Office operations is the Atlas platform, the casework system for managing immigration and asylum applications that has recently replaced the legacy Case Information Database (CID). It digitises casework, notifying applicants via "email, text messages and physical letters (where necessary) sent automatically at specific milestones in the caseworking process".⁵⁷

The Home Office maintains that “greater automation removes the need for paper applications, meaning a speedier application journey”, all the while liberating casework officials “from repetitive administrative and manual tasks to focus on crucial case consideration and decision-making”.

However, it is difficult to precisely describe Atlas and its actual impact on immigration procedures on an evidence-based level. Kaelynn Narita, Research and Policy Manager at the grassroots organisation the3million, tried to provide an in-depth description of an earlier version of the system in her 2024 doctoral thesis, “The Digital Hostile Environment: Migration and Technology”, as Atlas “offers a case study on how technology is becoming the ‘back bone’ of the UK border system”.⁵⁸

Narita characterises Atlas as “fluid, everchanging to the new technological solutions developed”. She writes, “Atlas should not be considered a fixed entity that placidly transmits various data sources to the caseworkers at the Home Office. In the back end of Atlas, several automated tools are working to mediate the data to the caseworker, resulting in outcomes in migration governance.”

In other words, Atlas is a hub for managing cases for the Home Office – one that suffered from the “patchy, dysfunctional and heavily automated features” that, according to Narita, ultimately embody the “ethos of the Digital Hostile Environment”. For example, she cites reports that Atlas produced “76,000 mis-recorded” entries “or data errors”, some of which have actually “ruined people’s lives”.⁵⁹

As a constantly-evolving hub of automated functionalities, contracts reveal that Atlas is now about to be enhanced with artificial intelligence produced by “AI-first digital engineering and cloud transformation” company Mastek, a global provider of AI services.

Besides recently expanding its UK presence⁶⁰, Mastek has been working with the Home Office at least since 2018, including on immigration management. Even though the relationship has been rocky at times – Mastek actually sued the Home Office in December 2025, claiming it acted unlawfully when deciding who would receive a £138 million contract to run the IT system for processing immigration applications⁶¹ – it recently secured multiple contracts with the Home Office, including one that concerns the provision of AI services to enhance the Atlas platform.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

Precisely what kind of “AI services” is hard to say. The £85 million contract speaks cryptically about “Technical development & support for a suite of shared services that support the Atlas case working system”,⁶² while its press release⁶³ is riddled with marketing speak:

“The service aims to scale Atlas, making its common components scalable, resilient and highly available. A combination of high-end engineering techniques and AI-driven engineering accelerators will be applied across human and automated casework and the modernisation of the platform.”

It’s not clear what “AI-driven engineering accelerators” actually means in operational terms, even though the contract’s description speaks of “the provision of specialist software engineering teams” to work on “enhancements to Out of Country services”, the “development of Audit capabilities”, and on ensuring “ongoing live service and operational support for Border Force and Immigration Enforcement”.

Mastek expects the contract to play out over the coming few years to help the HO deliver “various complex” – but unspecified – policies through Atlas.

This level of opacity is nothing new to Narita: “With Atlas”, she told ORG in an interview, “it is really hard to even say how AI would be integrated into it”, given its complex, multi-layered, and mostly invisible operations. Even with her deep knowledge of the system, she couldn’t decipher what precisely the contract was about.

Atlas is listed as a “low” transparency system in the Public Law Project’s Tracking Automated Government Register.⁶⁴

A second contract between Mastek and the Home Office envisions the adoption of AI for “supporting, maintaining, and enhancing” the Biometrics Services Gateway (BSG) and National DNA Database (NDNAD) systems which will “enable Passports, Visa, Study and Asylum routes, DNA Search and Match Caseworking, and its enforcement operations” – all of which are increasingly tied to biometric recognition technologies.⁶⁵

Unrelated to immigration, Mastek also recently secured a third contract, for £15 million, with the Financial Conduct Authority to “provide specialised digital

engineering and service management expertise to scale and modernize processes” of the FCA’s Digital Delivery Hub.⁶⁶

Previously, the company supported the Home Office’s biometric application (2021-2024) and, according to Biometric Update,⁶⁷ was also one of the main suppliers of the Immigration Platform Technologies programme, “which began in 2013 and was originally expected to be completed in 2017”.

AI-based services advertised on Mastek’s website⁶⁸ include “AI and machine learning predictive analytics” and “AI-driven citizen services” to “speed up delivery, reduce risk, and improve service reliability for citizens”. The website also describes an AI-based suite to “accelerate data modernisation” featuring “predictive analytics, AI-powered Data Quality Checkers, anomaly detection models, and autonomous monitoring agents”. These might be relevant in the current context, with the Home Office transitioning from legacy systems towards a newer infrastructure prominently featuring artificial intelligence.

Words matter. In contrast to Mastek’s marketing claims, AI is inherently unreliable, making guesses rather than analysis or predictions, and in these cases is engaging in surveillance rather than mere ‘monitoring’.

AGE ESTIMATION FOR PEOPLE SEEKING ASYLUM

AI is being trialled to estimate the ages of people seeking asylum, possibly beginning with live cases at Western Jet Foil, a processing centre in Dover, in 2027.⁶⁹

On 28 May, the Home Office awarded a new contract for facial age estimation (FAE) to the Harlow-based company Akhter Computers Limited and the German company Cognitec Systems GmbH.⁷⁰ The three-year, £322,000 contract will support further testing and development of the technology before its planned rollout in mid-2027.

The Home Office guidance published on 29 May 2026⁷¹ acknowledges⁷² that FAE systems are imprecise at the critical 16-to-18-year-old boundary. Even the “top systems” have an “error margin of around 2.5 years here”, yet this is the age range for which the Home Office has chosen to deploy the technology.

An Inkstick investigation⁷³ obtained the names of seven companies involved in the trial. Three are American: Aware Inc., Paravision AI, and Trust Stamp. In an investigation, Inkstick found that until 2022 Trust Stamp provided a “migrant-

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

tracking app” to the controversial US government agency Immigration and Customs Enforcement (ICE), thanks to a contract for face recognition and GPS tracking technologies worth \$7,2 million annually⁷⁴. Predictably, the Home Office declined to reply when Inkstick asked whether it had completed a human rights impact assessment for the facial age estimation AI programme.

Human rights organisations have been extremely critical of the proposal, considering the technology inaccurate and intrinsically discriminatory.⁷⁵ They have highlighted substantial and well-founded concerns about bias in FAE, including its failures and discrimination, particularly in relation to women and people of colour.⁷⁶ The Home Office has itself noted that “FAE performance can vary depending on ethnicity” and skin tone.⁷⁷

The Home Office guidance referenced the work of the US National Institute of Standards and Technology (NIST) in measuring the accuracy of FAE algorithms, ignoring evidence from the NIST report that shows that FAE is most accurate when estimating the ages of Eastern European men, but even then consistently produces errors.⁷⁸ Its error rates were almost always higher for female faces.⁷⁹

Throughout the Home Office plan, well-documented research on changes to the faces of children seeking asylum is overlooked. These children often appear prematurely aged due to trauma,⁸⁰ violence, and prolonged travel, as well as malnutrition, dehydration, sleep deprivation, and exposure to salt water during dangerous sea crossings.⁸¹ As a result, their facial features may differ significantly from those of peers who have not experienced such hardships.

A recent report by the UK government’s independent immigration inspector found instances where both adults and children were wrongly identified. This is particularly concerning when children are denied their rights and protections.⁸²

Another report, from the Jesuit Refugee Service, indicates that children are being misidentified as adults and, in some cases, have been deported under the one-in-one-out policy.⁸³

“This isn’t a new topic: age assessment proposals have been around for years, but there aren’t really any proven, scientifically tested methods”, migration and technology expert Antonella Napolitano told ORG in an interview. “And yet now, also in the wake of age assessments due to social media bans and numerous companies offering these services, there’s a strong push to create and use these types of tools”.

Griff Ferris, an Advocacy and Campaigns Manager at the Joint Council for the Welfare of Immigrants, agreed with Napolitano's assessment in written comments sent to ORG: "Age assessments are a clear source of harm currently, with children often being wrongly classed as adults, and therefore put at significant risk by being housed with adults, and even deported." AI-based capabilities, however, won't help address this. On the contrary, "facial age estimation technology obviously lacks a coherent scientific basis, and in addition is deeply inaccurate and discriminatory".

Quoted in a Context News article, a Home Office spokesperson said that "this technology will not be used alone, but as part of a broad set of methods used by trained assessors". Experts are not convinced: "We don't actually know if it works", Anna Bacciarelli, a senior AI researcher at Human Rights Watch, told Context. Sile Reynolds, head of asylum advocacy at charity Freedom from Torture, added that, "The asylum system must not be the testing ground for what are currently deeply flawed AI tools operating with minimal transparency and safeguards."⁸⁴

MOBILE PHONE DATA EXTRACTION IN THE CONTEXT OF THE ASYLUM PROCEDURE

According to a 2022 high court ruling, the Home Office had an unlawful and secret "blanket policy to seize some 2,000 mobile phones from people arriving in the UK on "small boats"⁸⁵. Content could then be downloaded to an intelligence database called 'Project Sunshine'.

The court required independent authorisation and oversight, and yet at the beginning of January 2026, new powers contained in the Border Security Asylum and Immigration Act of 2025⁸⁶ came into force that allow immigration officers to continue extracting data from asylum seekers' mobile phones. The BBC reported that seizures began at the Manston migrant processing centre in Kent on 5 January 2026.⁸⁷

According to the bill's Equality Impact Assessment (EIA),⁸⁸ the new powers allow immigration officers "to search for, seize, retain and use information from electronic devices" when a device is found on an "illegal entrant" and there are "reasonable grounds" to suspect that it "may contain" information relating to "assisting unlawful immigration" or helping people seeking asylum to enter UK.

Natasha Tsangarides, associate director at the NGO Freedom from Torture, argues this is still a "profoundly inhumane" policy that treats "all refugees as a security

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

threat, regardless of evidence”, and warns that independent oversight is still lacking.⁸⁹

According to the factsheet issued alongside the bill,⁹⁰ the new powers granted to law enforcement – including phone search and seizures and “expanded data-sharing capabilities” – are explicitly inspired by “counter terrorism” measures. The EIA even admits that this measure could have a disproportionate, but justified, impact on people with disabilities.⁹¹

It is unclear what precise technology will be adopted to “copy and extract information from electronic devices” of irregular migrants, including whether it will be AI-enhanced.

However, according to Privacy International,⁹² the controversial Israeli surveillance company Cellebrite has for years been pitching its “digital intelligence” and mobile forensic tools to authorities interrogating people seeking asylum, and received payments of £133,000 from the Border Force and Immigration Enforcement.

Cellebrite, which has long worked with ICE in the US, is also heavily involved with UK law enforcement. PI has traced Cellebrite’s contracts with several local police forces (including in Leicestershire,⁹³ Lancashire,⁹⁴ South Wales⁹⁵ and Cumbria⁹⁶) for AI-powered tools such as Inseyets and Pathfinder.⁹⁷

Cellebrite’s website quotes a digital forensics manager for the South Wales Police, which also uses other Cellebrite tools such as Responder, Touch2, and Physical Analyzer:

“When you examine somebody’s phone, it’s almost like looking into their soul. You find things on a phone that the owners wouldn’t even discuss with their own family. You can find out a lot about a person by examining their phone.”⁹⁸

More generally, Cellebrite says it is “Ensuring Our Nation’s Security”,⁹⁹ helping protect “the national security of the United Kingdom”.¹⁰⁰

In 2021, Privacy International examined another £335,000 payment, made in 2018 to Sweden-based Micro Systemation. The company, whose motto is “turning data into justice,”¹⁰¹ boasts specific “border control solutions” that “have been implemented and are currently in use by multiple border authorities – with great success”. “Automated and AI-supported analysis solutions” are included.¹⁰² Case

studies detailed on the company's website include "2 UK police forces"¹⁰³ and "a UK Law Enforcement Agency."¹⁰⁴

Given the prominence of AI-based solutions in the field of analysing data that has been extracted from mobile phones, it is highly likely that AI is – or at least will be – used in exercising the enhanced powers to utilise extracted information from mobile phones of irregular migrants.

SHAM MARRIAGES TRIAGE TOOL

Introduced in 2015 by the Home Office as part of the "Hostile Environment", a triage tool to automate the detection of sham marriages adopted machine learning in 2019.¹⁰⁵ The Home Office's "Marriage and civil partnership referral and investigation scheme: statutory guidance for Home Office staff", last updated on 31 March 2025,¹⁰⁶ confirms this automated tool is still in use.

The automated system produces a green or red light ("the couple is flagged for further investigation at the decision-maker's discretion")¹⁰⁷ for cases where "either or both parties" are "from a country outside of the UK, Switzerland or the European economic area, or have insufficient settled status or lack a valid visa".¹⁰⁸ These are judged according to a number of risk factors – eight until 2020, six since – which the Home Office refuses to disclose.

While the secrecy makes it impossible to produce an exhaustive evaluation of the potential discrimination deriving from the system's use, the Guardian has reported that the tool "has been disproportionately selecting people of certain nationalities", primarily affecting people from Albania, Greece, Romania, and Bulgaria, according to an "internal Home Office evaluation".¹⁰⁹ The Guardian also noted that the Home Office itself included the tool in its list of current uses of "AI".

The Public Law Project concludes:

"There is no evidence, other than the outcomes of the triage tool itself, that the nationalities disproportionately affected are more likely to be involved in sham marriages".¹¹⁰

Chai Patel, legal policy director of the Joint Council for the Welfare of Immigrants, has told the Bureau of Investigative Journalism, "The Home Office data on past enforcement is likely to be biased because Home Office enforcement is biased against people of certain nationalities".¹¹¹

USES OF AI IN BORDER SURVEILLANCE

The UK is also building an automated fortress at its border. The vision, consistent with the techno-political practices increasingly put in place by the European Union,¹¹² the US, and many other countries from Africa to Asia to protect their borders,¹¹³ preaches “seamless”, “frictionless” border crossings for trustworthy individuals, while an array of “intelligent” surveillance technologies uses algorithmic guesses to decide who is “suspicious” or “risky” in the name of national security.

Artificial intelligence is allegedly the key to realising this utopia of total freedom (for those deemed safe) and total control (for those deemed suspicious), as it provides the tools governments allege will transform the border into an information space that can be completely known and dominated. The focus on this vision unfortunately ignores the inaccuracies and discrimination that follow from automation.

AUTOMATED BORDER CROSSINGS WITH AI-BASED FACE RECOGNITION

The travel industry has promoted the vision of a queue-free border for trusted travellers for two decades.¹¹⁴ By 2020, the Boris Johnson government was considering the use of AI to create “a highly digitised and automated border”.¹¹⁵ Face recognition gates had been deployed a decade earlier at airports such as Gatwick, Stansted, Birmingham, Manchester, Cardiff and Bristol.¹¹⁶ The idea was to better control the nation’s borders by injecting artificial intelligence into the main international crossing points, including ports such as Portsmouth and Dover.

Fast forward to October 2025, when a “contactless” system equipped with AI-based, biometric e-gates was trialled at Manchester airport so British citizens would no longer need to show their passports at immigration.¹¹⁷ According to Biometric Update, the intention was that the system would work in conjunction with the UK’s Electronic Travel Authorisation (ETA) scheme,¹¹⁸ which is also part of the Home Office’s ambition to create “a border that is fit for the 21st century” by automating “large swathes of the existing digital borders processes”.¹¹⁹ The automation would allow the Border Force to “use their specialised skills on protecting the border from those who seek to harm the UK”.

It is this vision that informed the Manchester trial. According to the Border Force director-general, Phil Douglas, quoted in the Times, “The trial demonstrated that processing times are faster because the physical passport scan has been removed.”¹²⁰ As a result, Douglas said, officials could focus exclusively on travellers “with high-harm activity”.¹²¹

Under this system, passengers only need to have their facial features scanned once at an AI-powered e-gate; if their data successfully matches against government databases, doors open automatically. Further checks are only necessary for passengers the system fails to recognise and those who are algorithmically flagged.¹²²

Modelled after facial biometric systems adopted in Dubai and Australia, Douglas has said the system will be connected to immigration systems to prevent ineligible travellers from boarding.¹²³

Meanwhile, this means that the security border time will be only dedicated to non EU and non British or Irish travellers, who are not eligible to use the e-gate. Which again means treating all non white populations, and travellers from poor global south countries, as the ‘potential risks’ or ‘harm’ in the context of the Border Force director-general statement .

In 2024, when the UK first revealed the idea of the ‘contactless border’, the Border Force director claimed that the goal was to create an “intelligent border” that used “much more frictionless facial recognition than we currently do”. ‘Frictionless’ here is industry jargon.

The year before, Douglas told the Airport Operators’ Association conference that biometric technology was making paper passports redundant: “I’d like to see a world of completely frictionless borders where you don’t really need a passport. The technology already exists to support that.” In a slogan: “In the future, you won’t need a passport – you’ll just need biometrics”.¹²⁴ Douglas seems to overlook the proven discriminatory record of biometric technologies, which pose disproportionate risks and harms¹²⁵ for African-American and Asian passengers and ultimately perpetuate racial bias.¹²⁶ Privacy and human rights implications should also be considered. As Birgit Schippers, a senior lecturer in politics at St Mary’s University College Belfast, puts it in the Irish Times: “When your face is your boarding pass you are holidaying with Big Brother”.¹²⁷

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

In the European context, technological solutions for similar AI-powered capabilities were and are researched in EU-funded projects for border security such as CarMen,¹²⁸ PopEye,¹²⁹ D4FLY,¹³⁰ and EINSTEIN.¹³¹ All feature the Home Office and the University of Reading among their participants, with PopEye also adding the UK-based company Intrepid Minds Ltd and the Defence Science and Technology Laboratory, signalling a clear interest in putting research outputs into operational use in the UK.

These projects are meant to further embed the same automation-based, 'frictionless' logic into border and immigration checks, promising abilities such as real-time biometric identification of passengers in vehicles moving up to 20 km/h under all weather conditions (CarMen), the identification of multiple travellers crossing the border either on foot or in a vehicle from up to 200 metres (PopEye), the generation of 3D face data from mugshots (D4FLY), and "advanced fraud detection" systems (Einstein).

Much is still unknown about these projects. Some are ongoing. Others have been completed but provided insufficient transparency about their outputs. One thing is clear: in the EU, as in the UK, AI and biometrics are seen as the future of human mobility, no matter the risks. Authorities will seek to introduce these technologies despite the potential lost human autonomy, structural discrimination, and systemic opacity that will undermine the rights of people on the move and especially those of migrants.¹³²

When compounded by the many additional uses of AI in the immigration system, these risks are poised to become actual harms. Ultimately the vision of 'seamless' border crossings facilitated by AI and increasingly sophisticated biometric recognition technologies is rooted in the capabilities of discriminatory machines. These operate by maximising data collection and minimising human intervention – ideally turning each crossing into a series of data points to be automatically and instantaneously evaluated by risk assessment algorithms in a fully automated and inhuman fashion.

The vision is to reduce people crossing borders to data points with risk scores. This cybernetic and techno-solutionist approach is held to be the only way to fully control and monitor, with a particular agenda to control migrants' mobility and movement.¹³³ Total knowledge requires total control, and AI falsely promises to finally fit the bill, turning the longstanding security industry fantasy¹³⁴ of

building an 'automated fortress' and invisible walls at the border to protect 'us' from 'them' into reality.¹³⁵

It is clear that artificial intelligence will reproduce, automate, and amplify the many forms of 'analogue' discrimination and bias suffered by migrants coming the UK from certain nationalities and ethnicities, violating their rights and dignity. Automated borders, sociologist Steffen Mau has written, work as "sorting machines" that simultaneously create mobility for the algorithmically 'deserving' and immobility for the 'undeserving'.¹³⁶ In a context in which widespread anti-immigration prejudices inform migration technologies, AI do this sorting by creating a veil of rationalisation to institutional racism.¹³⁷

LIVE FACE RECOGNITION TO DEPORT MIGRANTS

Multiple pilots are being conducted for the deployment of live facial recognition technology¹³⁸ at the Port of Holyhead in Anglesey, Wales, with the aim of identifying and locating people returning in breach of a deportation order.¹³⁹

A first trial took place from 10 to 29 November 2025.¹⁴⁰ Conducted by Immigration Enforcement, the Border Force, and "police partners", it screened some 7,500 faces over eight deployments, leading to one arrest. More importantly, it claimed no false alerts. The live facial recognition capability was provided by NEC's NeoFace V4 system, which was mounted on a total of 15 cameras.¹⁴¹

According to a Home Office spokesperson quoted in the Irish Sun, the trial "is a major step in stopping offenders from evading justice and sends a clear message: anyone trying to slip through will be stopped".¹⁴²

According to the Irish Times, a second trial was announced for the week commencing 23 February 2026.¹⁴³ The newspaper described how the system would work:

"Live facial recognition technology captures digital images as people move through a designated 'Zone of Recognition'. Facial features are then 'extracted and expressed as numerical values' (...). At Holyhead, images are compared against a watch list of individuals who have previously been issued deportation orders and are suspected of attempting to return to the UK."

The results were reported by the Irish Times. The scanning of thousands of passengers over the three days of the trial produced no matches, an outcome that

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

“raises fresh questions about the effectiveness and proportionality of the technology”.¹⁴⁴ Interestingly, over the same period the Home Office released a series of policy documents concerning the use of live face recognition for immigration enforcement – including the legal mandate,¹⁴⁵ the Equality Impact Assessment,¹⁴⁶ the Data Protection Impact Assessment template,¹⁴⁷ and the Standard Operating Procedures.¹⁴⁸ These provide some help in assessing how the technology is being conceptualised and deployed in Home Office operations.¹⁴⁹

According to a Press Association report, in April 2024 the Government’s independent anti-terror law adviser, Jonathan Hall KC, said he would recommend using “live AI facial recognition to screen migrants arriving in the UK for threats” at “migrant processing facilities in Kent” to allow border officers to screen those crossing in small boats against a database of terror suspects when presenting his annual report.¹⁵⁰ The article adds that in an interview with LBC Hall said that live facial recognition (LFR) should be deployed “at Western Jet Foil, so when people get off the boat, they can be screened” and checked against a “database of images of people who are suspicious, who are potential terrorists”. These recommendations were indeed included in Hall’s report, but were deemed “subject to wider review”.¹⁵¹

ARTIFICIAL INTELLIGENCE TO “STOP THE BOATS”

AI-powered surveillance towers are patrolling the Channel, looking for “small boats” approaching the UK, according to a seminal investigation written by the journalist and researcher Samuel Storey and published by the Migrants’ Rights Network. Supplied by US defence giant Anduril, the so-called “Sentry Towers” are “5.5 meters tall” and “fitted with radar as well as thermal and electro-optical imaging sensors which continuously scan the sea horizon”.¹⁵²

The towers’ electronic brain is ‘Lattice OS’, an AI-based operating system that translates all of the informational inputs provided by the sensors and the broader border surveillance assemblage into a real-time, digitised, and actionable picture of the border, all the while “algorithmically identifying, detecting, and tracking individuals or subjects considered to be of interest”.

Through what Politico and The Bureau of Investigative Journalism (TBIJ) have called “a massive PR operation”, Anduril has won “influential supporters and government contracts worth tens of millions”. As a result, “it has firmly

established itself as a central part of the UK's plans for security".¹⁵³ And yet, the existence and operation of these towers is shrouded in extreme opacity.

In fact, we don't know how many towers have already been deployed, how many are planned, or how long they are expected to remain operational. A three-year contract obtained by researcher Anna Christoforou through a FOI request indicated a £16 million payment by the Home Office, but this expired on June 2025.¹⁵⁴

In an interview with Open Rights Group, Samuel Storey revealed that he had personally verified that the tower placed in Dover was still operational after the contract term ended. While we have no certain knowledge that Anduril's contract(s) has been extended, Storey is adamant that, "These don't look like temporary installations at all."

Storey has painstakingly documented the existence of ten Anduril towers between Hastings and Margate,¹⁵⁵ but could obtain no confirmation about their number and location from the Home Office, despite multiple FOI requests – so many, in fact, that the Home Office took issue with Storey's work.

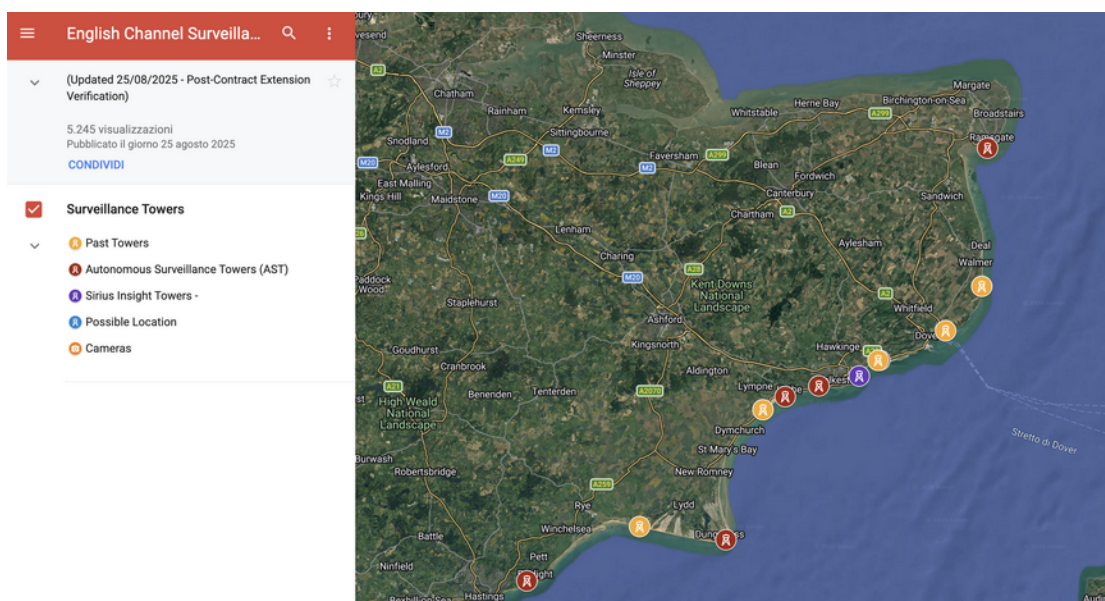


Figure 1: Map of English Channel Surveillance Towers by Samuel Storey, last updated on 25 August 2025

In an official reply, the Home Office strongly contested the accuracy – and even legitimacy – of Storey's work, appealing to Storey's "conscience" to ask him to "remove" details on the location and operational status of Anduril towers from his published investigations, claiming they were not only "factually" inaccurate but also "likely" to "promote active countermeasures" by criminals.¹⁵⁶

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

While officials provided no concrete evidence to substantiate their claims about Storey's reporting, they implied that public knowledge of the towers' locations and operations would put the lives of those attempting to cross the Channel at greater risk. "Migrants", the Home Office wrote, "may be placed in even greater jeopardy by making them less easy to detect by UK and French patrols engaged in safety of life at sea (Solas) operations". By contrast, civil society experts and academics have long maintained that it is pervasive "smart" surveillance that forces people who are seeking safety into utilising even more dangerous routes.

In a video essay,¹⁵⁷ Storey claims that in fact border surveillance technologies do not reduce migration, but relocate it. More fundamentally, these technologies are increasingly framed in the literature as tools for automated apartheid.¹⁵⁸ Storey agrees:

"These towers are far from neutral sentinels. They are active agents in an increasingly automated system of border apartheid designed to filter, categorise, and repel those deemed undesirable ... They do not render asylum safer, nor do AI algorithms make migration fairer. Instead, they entrench the logic of exclusion".

Lastly, Storey told ORG that UK-made technology for surveilling the Channel is almost non-existent. Only solutions by the Belgian maritime data analysis company Sirius Insight "were trialled in places where current Anduril towers now are". A 2023 CNN investigation found that the company touted its collaboration with the Home Office on its website for technology that "can provide instant autonomous alerts" on the targets it is tracking, including cameras capable of spotting "a very small vessel at 10 miles with just a couple of people in it." This content was quickly taken down after the CNN report aired.¹⁵⁹

AI-POWERED DRONES PATROLLING THE CHANNEL

Drones powered by artificial intelligence are also part of the UK's border surveillance arsenal to "stop the boats" or, as the former Starmer administration framed it, "smash the gangs".¹⁶⁰ While confirmations are predictably scarce, multiple investigations over the last few years have demonstrated that drones produced by foreign security giants such as Tekever (Portugal), Elbit Systems (Israel) and Anduril are implicated in patrolling the Channel.

After it was first reported by Wired,¹⁶¹ CNN's investigation confirmed that an "AI-trained" AR5 drone produced by Tekever "flies across large swathes of the UK side of the Channel", and that the company's contract with the Home Office was renewed for three years in February 2023.¹⁶² A Channel Crossings briefing also found previous contracts, including one "for fixed wing UAS managed service to enhance maritime awareness" that ran from November 2019 to the end of September 2022.¹⁶³ This could be the largest the researchers have found to date, as it's for an unspecified "£0-1 billion".¹⁶⁴

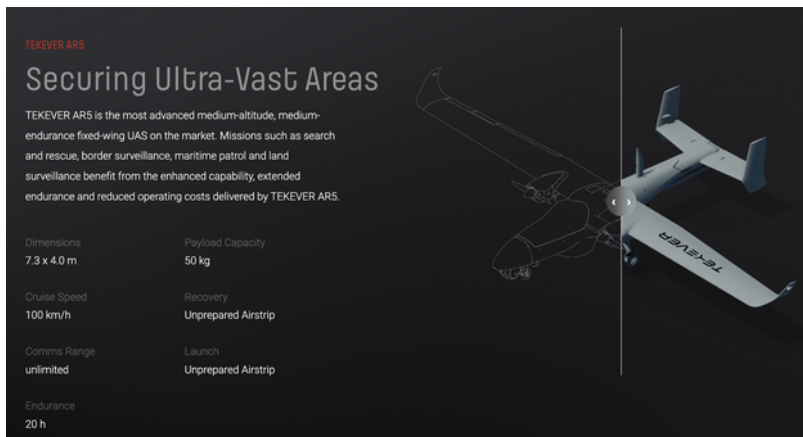


Figure 2: The AR5 drone as described on Tekever's website

And yet, among the several questions raised, the CNN investigation rightly asked, "Where was the tech?" on 14 December, 2022. That day, a small boat attempted to carry migrants across the Channel from France to the UK and capsized in freezing waters, resulting in the deaths of at least four people.¹⁶⁵ According to CNN, ADS-B data from Flightradar24 shows that the AR5 drone used by the Home Office was "capable of deploying a life raft", and "was operating in the Channel the day before the incident and in the hours after it, but not while the vessel was sinking". The conclusion is stark: "Despite all the surveillance equipment, people have still lost their lives attempting to cross the Channel".

According to company material, the AR5 drone has a flight endurance of 20 hours, a payload capacity of 50kg, a cruise speed of 100km/h and "unlimited" communications range.¹⁶⁶ According to the UK Defence Journal, "The specific payload package used to survey the Channel allows it to cover vast areas, detecting and recognising potentially illegal vessels, and then track and identify them, providing the authorities with real time and highly accurate intelligence".¹⁶⁷

Tekever and the UK Home Office previously collaborated on COMPASS2020, a €6 million EU-funded research project that aimed to further expand surveillance reach through the combined use and seamless coordination of manned and

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

unmanned assets.¹⁶⁸ Ending in 2021, it used AI to “automatically determine suspect and irregular behaviour”, reduce “operator workload”, and “advise on the best way of intervention”.

The so-called “system of systems”, comprising a “data fusion” engine and “anomaly detection, classification, risk & predictive analysis” in coordination with drone operations, was trialled in Portuguese waters, including in a Search and Rescue scenario derived from irregular immigration.¹⁶⁹ Results were deemed satisfactory at the time, but there is no public information to indicate an actual deployment of the system after the project ended.¹⁷⁰

Crucially, Tekever AR3 drones – among the ones deployed in the Channel to patrol “small boats” – are mentioned in COMPASS2020 material as being involved in demonstrations.¹⁷¹ Autonomously deployed and operated by existing offshore patrol vessels, the AR3 drones are said to be able to “augment the surveillance capabilities of the vessel tenfold”.

The use of two Anduril Ghost drones is also implicated by the CNN investigation into the December 2022 incident, but multiple FOI requests did not lead to official confirmation.

Lastly, a study by a team of leading UK universities found a £990,000 contract¹⁷² with the Israeli company Elbit Systems for “Drone Demonstration and Development Project for the UK Maritime and Coastguard Agency” (2020-2021).¹⁷³ The contract’s page on Tussell speaks of assessing “the potential use of Unmanned Aerial Vehicle (UAV) to augment current and future aerial surveillance capability by reducing, enhancing or replacing existing delivery methods”.¹⁷⁴

According to Computer Weekly, the surveillance assemblage described above is complemented by AI-powered satellites.¹⁷⁵

A £15 million plan to use spy satellites to track migrants crossing the Channel was finalised in November 2024.¹⁷⁶ Awarded to the Luton branch of satellite communications service provider Telespazio UK, it lasted until September 2025.

In April 2026, the Times further revealed¹⁷⁷ that drones equipped with military grade face recognition cameras were being trialled by Border Force in the Channel, with the aim of catching migrant smugglers on small boats.

Officials told The Times that the radar-enabled cameras are capable of identifying faces from half a mile away and will help the Border Force identify smugglers

even if they change clothes or appearance, as they regularly do to blend in with passengers and make it more difficult to prove who was steering the boat.

According to the Times, “The technology analyses various attributes of an individual, such as their height, their shape, unique facial features, their gait and creates a unique digital identity and applies notes to their skeleton. That person can then be identified regardless of what they are wearing or a change in facial hair.”¹⁷⁸ There is no available independent analysis of these claims at the time of writing.

AUTOMATED RISK ASSESSMENT OF THREATS AT THE BORDER

In February 2023, BAE Systems Digital Intelligence announced that it had secured a three-year £38 million contract “to develop advanced risk analytics services” for the Home Office to help it “identify national security risks at the UK border”.¹⁷⁹

Through an “advanced risk assessment programme” called ‘Cerberus’ the deal aimed to provide a “Digital Defence of UK Borders” that “will enable Border Force and related agencies to manage, in real time, the vast amounts of data relating to the 300 million passenger journeys and 385 million tonnes of freight that enter the UK every year”.

The idea is that the system will collate passport and visa data, records from criminal databases and watchlists, and “data collected from various private carriers including in the international freight and aviation sectors”¹⁸⁰ to automatically provide actionable insights aimed at preemptively computing “risks” before the border.¹⁸¹

Dominic Gallard, Director of Home Office Intelligence, argues that “technology sits at the heart of operations at the UK border”. Therefore, the partnership with BAE enables “a more data-driven approach”, one that “helps us keep the UK safe by identifying high threat movements of goods and people and interdicting them”.¹⁸²

It is unclear whether Cerberus already uses artificial intelligence. However, it is absolutely clear that it will.

A March 2022 tender for “Cerberus Product Development and Associated Services” lists a series of capabilities – “ingest, transform, enhance, match, risk assess border movements and then issue targets for intervention by front line officers” – that are “based around network analytics and ultimately machine learning”,¹⁸³

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

However, researchers who tried to look deeper into Cerberus's actual functioning have doubts.

Academics Gavin Sullivan and Dimitri Van Den Meerssche, for example, argued in a November 2024 paper in German Law Journal that “much of what Cerberus ultimately aims to do in terms of the UK Border Strategy’s “revolution” in AI-driven decision-making has yet to be realised in practice”. This means that “the ML-based targeting capabilities of the system are still at a very early stage of development”, especially as “its implementation at specific border ports to date has been plagued by organisational, legal, and technical issues”.¹⁸⁴

In an interview with ORG, the authors further explained that their judgment is based on conversations they had with Home Office officials in 2022-23, when they were still creating the infrastructure to enable the move from rule-based systems to AI.¹⁸⁵ Sullivan argued that while we do not know what progress has actually been made, “the way the system is thought of internally is that it is going to become an AI system”.

In other words, he added, “It is not just rhetoric”. While AI capabilities are not fully developed, “it is still useful to think of Cerberus as an AI system”, because, “if you look at the significant amount of time and money invested into it, it is clear that this isn’t just a minor prototype, but rather a large infrastructural shift towards data analytics-based targeting”.

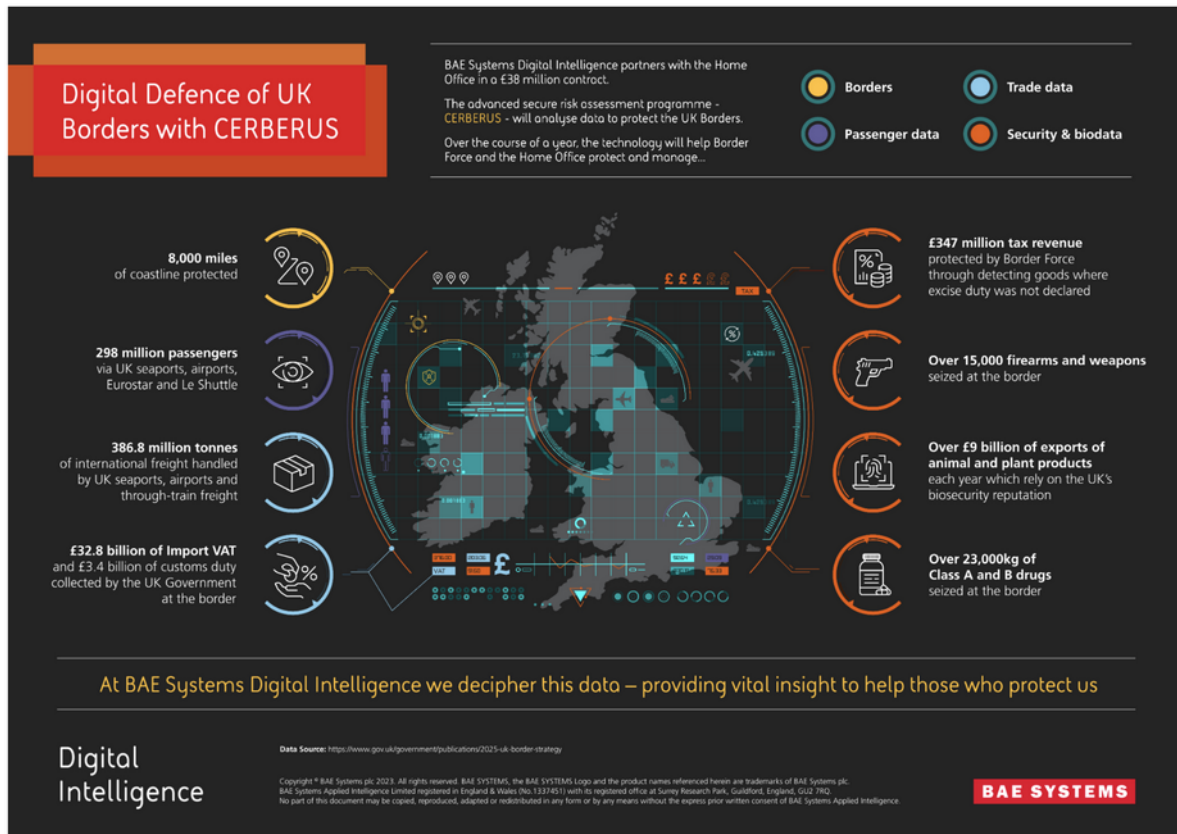


Figure 3: Infographic by Bae Systems detailing the company's vision for the "Digital Defence of UK Borders" with Cerberus

Sullivan's contention is indirectly confirmed by Adrian Peachey, BAE Systems Digital Intelligence's CTO for central government. In an October 2024 advertorial published in *The Sunday Times* pitching the virtues of border AI systems, including Cerberus, Peachey argued that "developments in AI" could – and of course should – "absolutely" allow us "to go beyond responding reactively to threats at the border".¹⁸⁶ The ideological shift is radical, as "AI could help position operational teams in areas where risks are most likely to emerge, enhancing our ability to respond proactively". The border thus becomes a perennial state of suspicion that only algorithms can fix.

Derya Ozkul, an Associate Professor of Sociology at the University of Warwick who has published important research documenting artificial intelligence in the immigration system all over Europe,¹⁸⁷ draws some crucial deductions from the distinctions and shifts we highlighted in regards to Cerberus. "I think it's important to distinguish between different types of AI", she told ORG in an email interview. "Rule-based systems do not fundamentally alter the logic of bureaucratic decision-making in immigration".

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

“By contrast”, she added, “systems like Cerberus, which was introduced under Sunak and which uses machine learning to predict future mobility, completely shift the logic of bureaucratic decision-making and its implications for our lives”.

Which leads us back to proactive intervention, as she went on to say:

“These systems operate on the premise that the unknown can be predicted by collecting and analysing large amounts of data on travellers’ characteristics and identifying new patterns. This introduces a fundamentally different way of thinking about risk: rather than responding to known pre-defined risks, states now aim to anticipate unknown risks through large-scale data analysis. Risk then becomes a dynamic prediction rather than a fixed category, inferred from patterns rather than rules. That means uncertainty about travellers’ future behaviour is managed through massive data accumulation, rather than reliance on pre-defined categories”.

What this shift actually implies in terms of Cerberus’s operational capabilities is however unknown. Travis Van Isacker, a senior researcher at the University of Bristol, fought a long FOI battle to obtain additional transparency on the system, but only obtained some limited disclosures, ultimately resulting in an unsuccessful complaint to the ICO. He told ORG:

“The Home Office has been extremely reluctant to provide transparency on how Cerberus functions, including the extent to which machine learning algorithms are involved in decision making trees.”

However, the complaint still provided some useful details. In particular, Van Isacker shared with ORG a “sensitive” document illustrating the Cerberus Business Case , and, while mostly redacted, it reveals “the Cerberus vision”:

“A unified, analytical system, powered by the best data and intelligence available, enabling threat agnostic and cross-modal targeting, allowing better deployment of resource to risk while facilitating the legitimate flow of border traffic”.¹⁸⁸

This overall strategy is perfectly consistent with what the travel industry has been pushing for the last 20 years, and also with the EU’s obsession with obtaining “seamless” border crossings thanks to automation. In fact, Van Den Meerssche argues in our interview that Cerberus and the forthcoming European

Travel Information and Authorisation System (ETIAS) share the same core vision: algorithm-enabled profiling with multiple, mostly unknown, indicators that together compose an individual risk profile, that is then refined in light of new data.¹⁸⁹

However, as Van Isacker highlighted in response to our questions, “how that data, including protected characteristics, is being used to target law enforcement interventions at the border is currently not known to the public”.

Nonetheless, according to the ‘National Infrastructure and Service Transformation Authority 2024-25 Report’, last updated in August 2025, “Cerberus has been rolled out to the first cohort of users”.¹⁹⁰

The ‘Cerberus Project Accounting Officer Assessment’ of 25 October 2024 reveals a total cost of £241m, “of which £126m is future expenditure from FY24/25 to 34/35.”¹⁹¹

AI WON'T FIX THE IMMIGRATION SYSTEM. CAN WE FIX AI IN THE IMMIGRATION SYSTEM?

In order to make sense of the rapidly growing catalogue of AI uses in the UK immigration system and at the nation's borders we have just illustrated, we need to better understand the broader ideological vision that informs it.

Digitising or digitalisation in immigration system isn't necessarily problematic.

However, these transformations become extremely problematic when driven by a vision that hails technology as a superhuman saviour capable of magically fixing all the socio-political issues implied by human mobility with the stroke of an algorithm.

Unfortunately, that is the predicament into which UK governments have put themselves and the British public over the last two decades. The claims of the security industry, which has long touted artificial intelligence as the fix to all bugs in the "operating system" of migration and mobility, have seduced Tory and Labour administrations alike. Intense lobbying and partnerships with AI giants — such as the ones recently signed with OpenAI,¹⁹² DeepMind,¹⁹³ and Starmer's favourite, Palantir,¹⁹⁴ complete the techno-solutionist picture we have drawn above.

Research from the Universities of York, Liverpool, Sheffield, and Nottingham published in April 2025 revealed that over the last decade the UK government has awarded some 213 contracts to private companies for managing border security.¹⁹⁵ Prominently included in the £5 billion spent is "high tech surveillance", raising the question: was this actually the best use of this money?

Many have doubts. Joe Turner, a professor at the University of York's Department of Politics and International Relations, one of the researchers, is among them. "The corporate profits we have identified come at the expense of investment in all UK communities and at the expense of the people forced to make dangerous journeys across the Channel", he said. "Rather than growing the border industry, government could focus on creating a sustainable system where people could reach the UK safely and apply for asylum on British soil."¹⁹⁶

But in order for the government to adopt such thinking, there will be a need for a different approach to the migration and asylum system, other than dealing with it as a security threat.

The sums the Government has invested in border control technologies appear to show that the immigration system in the UK has become a testing ground for these new technologies. Simultaneously, techno-solutionism helps explain why the UK lacks an adequate regulatory framework to address the many challenges brought by introducing AI into the immigration system, especially as it attaches itself to a politics of securitisation.

Crucially, developing an anti-solutionist and human rights based perspective allows us to imagine whether and how AI can be put to good humanitarian uses and articulate a set of policy demands and recommendations aimed at redirecting developments in migration management towards a future where such systems are based on a respect for fundamental rights, rather than increasingly automated abuse and discrimination.

A. AUTOMATING THE HOSTILE ENVIRONMENT IS NOT THE SOLUTION

Securitisation and the framing of the immigration system as a security threat are among the leading drivers for every UK government's belief in technological solutionism, and for the rapid and expanding use of AI in immigration system, in order to control, rather than to fix it. In general, technological solutionism is characterised by an unwavering faith in technology as the fix to society's bugs. It informs the staunchly "pro-innovation" policy posture assumed by multiple UK governments over the last few years, including the Labour administration that came to power in 2024.

There is an urgent need here to reclaim a humanitarian approach in the UK's immigration system. By treating migration as an emergency to be controlled rather than a human phenomenon to be managed, the UK has built an immigration regime where technological 'fixes' are deployed to surveil, screen, and exclude, not to safeguard rights or improve outcomes. Thus, for techno-solutionism to be rejected, and transparency and accountability be present, we must first reject the security paradigm and re-imagine migration policy. It should be a domain for rights, transparency, and inclusion, so that policy discussions can

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

move beyond a government or vendor-mediated, evidence-free, faith-based experience. Furthermore, if we want to give technology, and AI more specifically, a real chance at providing a positive contribution to migration and mobility management, then human right based approach and safeguarding, not opacity and assertion, must be the rule.

INNOVATION WITHOUT BORDERS

Techno-solutionism is everywhere in UK migration and technology policy. The experts we spoke with for this report agree that while there is a strong ideological continuity between Tory and Labour administrations, this vision came into sharper focus with the Starmer government.

Starmer and his cabinet manifested their techno-solutionist beliefs in multiple statements. Starmer has called AI “the greatest force for change in the world right now”,¹⁹⁷ a “game changer that has massive potential on productivity, and on driving our economy”,¹⁹⁸ and one that “will deliver a decade of national renewal”.¹⁹⁹ Placed at the helm of the Government’s ‘Plan for Change’, AI will “turbocharge growth and boost living standards”, including by revolutionising “the delivery of public services”.

This implies a hands-off approach to experimentation and deployment of AI across several government functions, including the immigration system. As Reuters has noted,²⁰⁰ Starmer has been keen on charting a “pro-growth and pro-innovation” course on regulation.²⁰¹ “We will go our own way on this”, he said referring to the UK’s departure from the EU in 2016, and “We will test and understand AI before we regulate it to make sure that when we do it, it’s proportionate and grounded.”

Again, this isn’t particularly new. A “pro-innovation” policy has been posited in detail across multiple official policy documents produced by previous administrations from both parties. It is found from the “10 year vision” to “Support the transition to an AI-enabled economy” through the “intention to build the most pro-innovation regulatory environment in the world” contained in the 2021 National AI Strategy published by the Boris Johnson administration,²⁰² to the 2023 Policy paper Rishi Sunak’s government aptly titled “A pro-innovation approach to AI regulation”.²⁰³ Throughout, the UK has departed from the comprehensive, risk-based approach to AI regulation the EU has taken with its AI Act, at least until Mario Draghi’s sirens began singing of “simplification”²⁰⁴ - that is, deregulation.

For example, the Sunak policy paper was informed by the idea of “regulating the use – not the technology”. “Our framework is context-specific”, it read. “We will not assign rules or risk levels to entire sectors or technologies. Instead, we will regulate based on the outcomes AI is likely to generate in particular applications”. This is at odds with the approach adopted by the European Union with the AI Act that is currently being implemented among Member States.

And yet, as shown by his strategic commitments and the plethora of pilots and deployments detailed in the previous chapter, Starmer has sought to turn this “pro-innovation” environment into one in which the rushed adoption of AI is not only practised, but explicitly theorised – and glorified. When Starmer claimed that “we need to run towards” AI,²⁰⁵ and his Minister for AI and Digital Government added that the UK should be moving “at a pace that’s way quicker than the United States” to become “the world’s best adoption nation”,²⁰⁶ it is clear that respect for the fundamental rights of migrants, if considered at all, is low on the list of government priorities, compared to the desire for data-driven efficiency gains .

This AI-first approach permeates the Home Office’s “2030 Digital Strategy”,²⁰⁷ which features mass AI adoption for all its activities as the first of the eight envisioned “strategic shifts”. The ambition is to “transform our digital services with AI and more automation”, thus becoming “the leading UK government department in the use of digital, data and technology”. However given that, according to the document, “AI and automation already sits at the centre of key Home Office missions”, what seems ultimately to matter is the newfound ability to “design and build new products and services faster and more reliably”.

Even though the public doesn’t seem to be on board the solutionist train,²⁰⁸ *faster, more* is the logic behind the UK’s AI-related policy documents. The 2025 “AI Opportunities Action Plan”,²⁰⁹ which touches on immigration only to highlight how talent in the AI sector can and should be attracted from all over the globe. Yet beneath the rhetoric of growth and technological revolution lies a persistent logic; that only ever-more sophisticated digital tools can provide the control and surveillance required to protect the nation from the supposed threat posed by migration.

The few existing safeguards are not specific to the use of AI in the immigration system, and mostly consist of generic principles that are only vaguely translated into actionable policies and practices. Some could be found in the 2025 “AI

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

Playbook for the UK Government”,²¹⁰ which features “10 common principles to guide the safe, responsible and effective” use of AI in government organisations. But these only broadly tackle the extremely complex issues AI raises at legal, ethical, and societal level: for example, “You use AI lawfully, ethically and responsibly” and “You have meaningful human control at the right stages”.

However, the Playbook does contain a valuable principle when it comes to implementing a regulatory framework for public uses of AI: the one that holds that “Fully automated decision making” and “high-risk or high-impact applications” which “could cause harm to someone’s health, safety, fundamental rights or the environment” are “not appropriate and (...) should be avoided in the public sector”.

However, as little regulation exists for the use of AI, when it comes to its use in the immigration system, the Home Office acts with near-total impunity and does not follow these principles at all. This disregard is not only the product of a general approach that treats AI “solutions” as tools for greater efficiency or progress, but is fundamentally rooted in a policy logic that persistently frames immigration as a security threat. It is this securitisation that enables the Home Office to sidestep regulatory standards and ethical safeguards that would otherwise apply, justifying exceptional measures and unchecked technological experimentation in the name of national security.

A striking example of that is the use of ACS and APS tools in asylum system, as both tools failed to comply with multiple principles established in the Playbook.²¹¹

Over the last few years, several policy documents have paved the way for “seamless” and “contactless” border crossings thanks to a “digital by default” approach and the extensive use of biometric technologies and algorithmic “pre-screenings”. These include the Johnson administration’s “2025 UK Border Strategy”²¹², and the “Delivering Border Security”²¹³ policy paper by the Border Security Command at Starmer’s Home Office.

Some more specific notions are included in the May 2025 “Restoring Control over the Immigration System”²¹⁴ white paper. Drawing on a cybernetic vision of mobility management, in which individuals are reduced to data points within a broader, fully knowable information space called the “border”, it promises to “bring down net migration” not just by moving to “digital evidence of immigration status”, but also by harnessing “the latest developments in artificial intelligence,

facial recognition and age assessment technologies to ensure that we gather the most accurate information available on each individual seeking to enter the UK.”²¹⁵

Put together with schemes like ETA²¹⁶ and eVisas,²¹⁷ AI becomes essential in this ideologically-driven quest to “know more about everyone coming to the UK”. This is a prerequisite to fully “dominat[ing]”²¹⁸ the border, and thus ultimately preventing each and every threat, even potential ones from unknown sources, from ever materialising. Only through mass data collection can the authorities know it all, and in this way grant the absolute, certain degree of “security and protection” that solutionist technologies promise to embody in immigration system.

The reality, however, is very different: what the technology is really ‘controlling’ is not immigration, but the political debate around it, by giving the illusion that the government is doing something about it, whether it’s working or not.

The government seems to have forgotten that digitisation and automation are not always the solution, or even just part of it, when it comes to efficiently and fairly delivering public services. In fact, historically these approaches have often been part of the problem. Examples go as far back as the early 2000s, and crucially include earlier systems that tried to implement a vision for digital borders based on biometrics and data-based, automated profiling.

The ‘e-Borders’ project was first. Based on fingerprints and iris scans, it aimed to track “over 99 per cent of foreign nationals outside the European Economic Area”, checking data collected at the border against “immigration and security watch lists”.²¹⁹ According to Christina Boswell and colleagues at the University of Edinburgh,²²⁰ however, the project only “created a form of political lock-in, whereby the project became impossible to abandon because of its political urgency, despite increasing awareness of its unfeasibility”.

Even its successor, the “Digital Services at the Border” programme of 2014, failed and was reset multiple times over the years. Indeed, it failed so often that in a 2021 report assessing the programme,²²¹ the Public Accounts Committee said, “The Home Office continues a miserable record of exorbitantly expensive digital programmes that fail to deliver for the taxpayer or for border security”. The report went on to denounce delays that had so far cost taxpayers £173 million, and said

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

the programme was being used “by only 300 border staff, against the 7,000 supposed to be using the system by June 2021”.

An additional £134m was wasted by Conservatives on “never-used IT systems for the failed Rwanda scheme”, which was repealed in the ‘Border Security, Asylum and Immigration Bill’ 2025.²²²

More recently, the electronic visa (eVisa) system adopted to transition to a fully digital immigration system also became mired in “frequent” technical errors, according to the ‘Exclusion by Design’ report,²²³ to which ORG contributed. The report found that errors caused “high levels of stress, fear and exhaustion” to migrants in the UK, with participants sharing “a deep fear of losing their rights” if they made mistakes.

Even the advanced capabilities under development in systems such as the ACS and Cerberus have had technical setbacks, as noted above. AI hype and reality rarely coincide.

AUTOMATING IN THE DARK

Where techno-solutionism fails most notably is in promoting and safeguarding democratic principles, but this failure in the UK immigration system is not accidental or incidental. It is a direct consequence of securitisation.

The persistent framing of migration as an existential security threat legitimises the adoption of the latest ‘intelligent’ technologies, and in portraying them as both indispensable and unavoidable to protect national security. This security logic combined with pervading techno-solutionism creates an infrastructure for the perpetuation and reinforcement of opacity, and enables the Home Office to normalise secrecy that weakens independent scrutiny, erodes checks and balances, and ultimately promotes the unchecked display of state violence and abuse against migrants and refugees.

Unsurprisingly, innumerable studies and investigations have documented that the “age of AI” is one of “black box”, inscrutable technological systems,²²⁴ often embedded in even more inscrutable socio-political webs of relationships, affecting institutions that are opaque by default, such as intelligence and law enforcement agencies and the military.

This security-driven ideological framework becomes gradually, but structurally, ingrained in the handling of actual deployments. In 2021, the above-cited PAC

report found that the Home Office had failed to “identify, acknowledge and be transparent about problems” in delivering tech programmes that are “crucial to national security objectives”. Meg Hill MP, chair of the audit committee, said, “It is incredible that the Home Office can have failed so badly, for so long, to deliver technology that is crucial to our national security objectives”.

Opacity is particularly problematic when AI systems are deployed against vulnerable and marginalised communities and individuals, which is often the case with immigration, because of the intensity of harms that result. The fact that the Home Office has refused multiple times to disclose basic details concerning AI-based tools and surveillance assemblages is therefore to be expected, but remains just as problematic.

The logic displayed by the Home Office in reply to freedom of information requests sent by researchers Anna Christoforou, Samuel Storey, and Travis Van Isacker concerning the Anduril towers patrolling the Channel and the Cerberus risk assessment tool stretches the notion of “national security” to deny transparency and frustrate democratic oversight, making any evidence-based scrutiny of the institution’s operations effectively impossible.

In reply to Van Isacker’s complaint to the ICO, the Home Office argued that, “The public interest lies in the prevention and detection of crime”.²²⁵ Any information request, however benign, is constructed as a potential threat to border enforcement. That excuse legitimises the refusal to disclose even basic details of AI-powered surveillance.

The more detailed the request, the more Government argues that answering it can threaten the security of the nation. As previously shown, according to the Home Office none of Storey’s investigations into Anduril towers should have been published. Despite the prominence of these objects in the landscape, evidence of their purpose should be removed altogether from public view, as the risk of countermeasures – by either criminals or those taking irregular routes to UK shores – is “great” when their “location and operational status” is revealed.

The Home Office’s response to genuine inquiries about these tools may help to portray AI as life-saving, but it does not provide any evidence to support this position. Independent observers in journalism, academia or civil society should be given access to the information they need to assess whether automated tools actually perform a humanitarian function, or merely realise the form of panoptic

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

control that the Home Secretary Shabana Mahmood wants to see deployed against irregular migrants. Rather than ensuring safety, the adoption of these tools is to allow authorities to check and even foresee migrants' every move, so that they can be promptly identified, tracked, detained, and reported.

This fundamental and structural lack of transparency even affects institutional efforts at providing actual transparency. Take the public register of government AI and automated tools²²⁶ built as a result²²⁷ of the public outcry about the biases found in the visa streaming algorithm that was halted in 2020 and in the sham marriages tool described above. While the register is "mandatory for all departments", months after its launch the Guardian lamented that "not a single Whitehall department" had entered a single AI system.²²⁸

The former Secretary of state for Science and technology Peter Kyle even admitted that the public sector "hasn't taken seriously enough the need to be transparent in the way that the government uses algorithms".

As of April 2026, the register contains 131 records. The CARS(V) system, described as "a semi-automated workflow routing solution which identifies the likely complexity of visitor visa applications based on applicant's declared attributes", is the only record concerning uses of automation by the Home Office.

A register of "government automation" tools is also independently maintained by the Public Law Project. Called "The Tracking Automated Government Register",²²⁹ it includes 55 automated tools at the time of writing. But opacity affects that, too. Of the 55, 38 are in fact classified as "low transparency", while only one as "high transparency". Almost all entries concerning immigration are classed as "low transparency".

As public interest becomes separated from public knowledge,²³⁰ and as the logic of security is used to justify ever greater opacity, fundamental rights start looking like enemies too. Techno-solutionism preaches "seamless" technological fixes that must operate instantly and autonomously to maximise their benefits. This can only be possible when human rights protections when the protections for the human rights of vulnerable individuals like migrants and people seeking safety, which require careful human judgement, are sidelined in the name of national security. While it is abundantly clear that analogue solutions may be inefficient and subject to the whims of bureaucrats and border authorities, portraying

automation and AI as tools that can objectively distinguish between deserving and undeserving applicants also produces biased, unfair results.

AUTOMATED RACISM IS STILL RACISM

The danger is that such security driven techno-solutionist ideological framework will lead to rejecting the human rights architecture. This is already becoming apparent in the gradual normalisation of illegal pushbacks at EU borders,²³¹ and, even more so, in the AI-informed mass deportations brutally enforced by Trump's Immigration and Customs Enforcement (ICE). To many, including in the EU and the UK, it is time to "modernise" what it means to be human, starting with the rights protected by the European Convention on Human Rights.

In December 2025, the Guardian reported that Starmer urged European leaders to "urgently curb joint human rights laws so that member states can take tougher action to protect their borders".²³² This rhetoric, echoing the security framing, reduces the right to asylum to a loophole, that becomes mere leverage exploited inappropriately by "unwanted" individuals to avoid deportation, justifying further erosion of protections in the name of national security and border control.²³³ And within hours European ministries backed the plan of the PM's call.²³⁴ Months later, we would hear the shameful chants in the European Parliament 'Send Them Back', in a very grim moment after the vote on the Return Regulation.²³⁵

Starmer intended this hardened stance on asylum rights to counter the rise of the far right, both in the UK and across the continent. And yet, recent political science literature discredits the idea that imitating and/or accommodating far right ideas lead to their demise,²³⁶ and, to the contrary, finds that it has the opposite effect of further normalising and even augmenting their allure.²³⁷ Especially in the context of steep and rapid erosion of democratic rights and rising anti-immigration sentiments all over the globe, this approach will only further embolden populists and extremists.

The techno-solutionist infrastructure of identification, tracking, prediction, and surveillance we have described in this the report is not politically neutral. It is fundamentally shaped by, and serves to reinforce, the security framing of migration. Unless this securitisation is challenged, the risk remains that such infrastructure could easily enable anti-democratic forces and abuse with the means to enact explicitly racist, xenophobia, Islamophobic, and authoritarian

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

policies of repression. One only needs to look at Trump's US²³⁸ to understand what this actually means for those caught on the wrong side of the algorithm.²³⁹

BEYOND SECURITISATION: RECLAIMING HUMANITY

For all the above reasons, it is imperative and urgent to sketch a systemic alternative, not only to techno-solutionism itself, but to the deeper logic that powers it, the persistent securitisation of migration, treating migrants as a threat. Techno-solutionism translates the politics of threat into systems of automated suspicion, risk scoring, and exclusion.

It is imperative, as securitisation and techno-solutionism undermine human rights and the rule of law. And it is urgent, because the transition of immigration enforcement and border security to AI-based systems is in progress, which means that it still can be challenged.

Many experts in the field of technology and migration agree: it is time to provide an anti-techno-solutionist alternative to the current, untenable status quo.²⁴⁰

In the UK, this means reclaiming humanity in migration policy, which demands more than technical fixes. It requires a fundamental rejection of the logic that frames migration as a problem of security and control. The alternative must be rooted in human rights and the recognition of migration as a social and human phenomenon, not a perpetual emergency crisis.

In this final section, we sketch some essential elements for such an alternative.

Where techno-solutionism preaches devotion to and dependency on Big Tech corporations, our view calls for humanism, holism, and digital autonomy.

Whenever the current policy landscape justifies regulatory gaps in the name of vague AI-based utopias of abundance, rejuvenation, and security, our approach calls to enshrine into primary laws specific, enforceable safeguards and oversight mechanisms – and urges the strict application of those that already exist.

We require understanding that the reductionist logic of AI technologies is not a representation of truth and never neutral but a calculation, a guess, or an estimate that often falls short, in a system designed from the outset to treat people as threats.

Instead of presenting techno-solutionist immigration AI as inevitable, as if it were a law of nature or a rising sun, in our view AI should only be adopted when proven to be beneficial to people on the move and society at large. Whenever this evidence is lacking, adoption should be paused, or – depending on the severity of the risks involved – banned.

Technologies also need to represent value for money; they objectively deliver what they claim.

Techno-solutionist immigration AI automates the Hostile Environment. It is the product of decades of policy that has treated migrants as risks to be managed, rather than as people to be protected. It embeds its discriminatory assumptions into immigration enforcement operations through decisions that are increasingly (and ideally) solely automated: humans can only insert friction, undermining the efficiency gains promised by ‘frictionless’ automation. In our view, on the contrary, artificial intelligence should serve humanitarian purposes, focusing on preserving the dignity and rights of each and every human being, whatever their immigration status.

This fundamentally implies rejecting the normalisation of mass surveillance tools, rather than using them to nurture the discriminatory fantasies enjoyed by those who believe that immigrants can only turn the UK into an “isle of strangers”.²⁴¹

Lastly, techno-solutionism thrives in darkness, shrouding immigration technologies in opacity and protecting them from public scrutiny. A responsible approach to the use of AI in the immigration system relies instead on serving the public interest by creating more effective mechanisms for transparency concerning these systems’ deployment, technical features, objectives, assessment methods, and mitigation measures. True accountability requires dismantling the exceptionalism that ‘security’ claims have given the Home Office and border authorities.

FROM TECHNOLOGICAL DEPENDENCY TO DIGITAL SOVEREIGNTY

In June 2025, while sharing the stage at London Tech Week with NVIDIA chief executive Jensen Huang, then-prime minister Keir Starmer proclaimed that the UK will become “an AI maker not an AI taker”.²⁴²

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

This motto includes a clear commitment to build the preconditions for digital sovereignty. It would funnel millions of pounds into training AI professionals; incentivise government departments to “buy British” tech²⁴³ to better navigate the geopolitical instability brought about by wars and tariffs over 2026; and launch a ‘Sovereign AI Unit’²⁴⁴ in April 2026 with a rather paltry £500 million fund²⁴⁵ to “maximise the UK’s stake in frontier AI” and “build the UK’s AI capabilities and support high-growth AI companies in the UK”.²⁴⁶

And yet, the catalogue of AI uses we list above is populated by foreign tech companies. The autonomous surveillance towers deployed to monitor “small boats” crossing the Channel are made by US-based defence giant Anduril. The drones complementing their operations come from the Portuguese and Israeli companies Tekever and Elbit Systems. The algorithm powering face recognition experiments for immigration enforcement at UK ports is produced by Tokyo-based multinational NEC. And both the ACS and APS summarisation tools deployed within the asylum procedure employ ChatGPT-4, produced by San Francisco-based OpenAI.

Meanwhile, the extremely controversial²⁴⁷ data analysis powerhouse Palantir is rapidly becoming the AI-based operative system for essential public services, from healthcare to defence, with obvious implications for an increasingly data, automation, and interoperability-based immigration system such as that of the UK.

Successive governments have justified vast investments in surveillance and automation, often relying on foreign vendors, on the basis that only the most advanced technological solutions can secure the border and manage the risks posed by migration.

Much still has yet to be done to transform the UK into an immigration “AI maker”. Even so, the country’s digital stack for public services is already deeply intertwined with foreign technologies at both infrastructure and applications level.²⁴⁸ Why?

In an interview with ORG, political science researcher Paolo Gerbaudo, at Complutense University in Madrid, said he believes the main argument is technological superiority. However, Gerbaudo, who co-authored a 2024 collective proposal by the Democratic and Ecological Digital Sovereignty Coalition on

“Reclaiming Digital Sovereignty”,²⁴⁹ is not convinced that foreign companies necessarily provide better AI solutions.

“There is an element of marketing illusion”, he told ORG. “In reality, the argument about the technological superiority of these companies is often exaggerated, and the real paradigm shift lies in usability and user experience, particularly on the commercialisation side. In other words, their value does not reside solely in computational sophistication, but in their usability and accessibility.”

Therefore, Gerbaudo said, “This implies that it is by no means impossible for a state to acquire that kind of technology: data centres, computing power, qualified personnel, etc., are not beyond the capabilities of states – even if they must adapt to higher latency or somewhat lower technical specifications, which may not be essential for most services.”

In fact, developing sovereign technological solutions has a lot of upsides. Firstly, digital sovereignty is technological independence, which means the ability to counter vendor lock-in. This is especially important in the context of the digitalisation of UK public services, which, as already noted, has repeatedly been plagued by technical failures. No public administration would want to remain stuck with flawed proprietary systems just because it depends on them for its operations.

Further, the fact that many Big Tech providers increasingly and explicitly display and enact reactionary ideas adds a crucial element of independence from ideological lock-in.²⁵⁰

When implemented through in-house, open source technological solutions, digital sovereignty also means greater control over the discretionary power and political influence of private entities, resulting in more effective transparency and therefore better accountability for public choices.

Lastly, sovereign technologies – when coupled with the appropriate architectural constraints – can help constrain data extractivism.²⁵¹ Gerbaudo argues:

“From the point of view of sovereignty, the issue is the parasitic relationship with these companies: on the one hand, they allow you to extract value from data; but on the other, within this Faustian bargain, these companies extract training value from the use of public data.”

This is especially problematic for the immigration system:

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

“Blind trust in systems whose biases are baked into the data they ingest –and which are not self-aware but merely statistical parrots—combined with reduced human oversight of their outputs, creates a recipe for abuse, operational errors, and systemic failures, all the more consequential in a sensitive policy domain such as immigration.”

Open source solutions, run locally and produced either in-house or in partnership with British companies, should therefore become the norm for AI-based services for the immigration system. While British companies can be bought by foreign multinationals, their open source code cannot. Cross-border open source partnerships can also help de-risk relationships with foreign vendors.

As put in the “Reclaiming Sovereignty” paper, this approach amounts to 1) offering a “democratic, public-led digital stack”, 2) developing “strict mechanisms at every step to dismantle existing and prevent potential forms of state surveillance or misappropriation of collective solutions” by the government, and 3) crafting “a research agenda focused on digital developments that are not driven by the hype or pressures of technological solutionism but that have the potential to solve collective problems and enhance human capacities”.²⁵²

Nevertheless, we also recognise that sovereign technologies and open source tech do not automatically mean that governments respect human rights, or that authoritarian political agendas are automatically dismantled. Rather, they are a step towards democratic control, transparency, and accountability. They are a means of removing ourselves from a cycle of vendor-led policy making, where techno-solutionism, and reductionist data approaches are part of a sales pitch that, once purchased, delivers technical dependency and creates a ‘path dependency’ towards further inappropriate technological policy approaches.

APPLY EXISTING SAFEGUARDS

While specific primary legislation concerning the adoption of AI in the UK immigration system is lacking, a number of safeguards do already exist. The problem is to ensure their application.

As explained in Allen, Masters and Jackson’s Opinion on the use of AI tools in asylum practices,²⁵³ some are contained in the “domestic legal framework”. They go on to list the Equality Act 2010, the Human Rights Act 1998, data protection

rules, and “general public law principles”, but in the context of migration, these protections are frequently sidelined or diluted.

However, the February 2025 UK AI Playbook however introduced two sets of “principles” aimed at guiding – both speculatively and pragmatically – the deployment of AI for public services. While not specific to the immigration system, they certainly apply to use of artificial intelligence within it. Despite that, and as a result of the ‘national security concept’ in immigration, the Home Office treat regulatory standards as optional rather than binding.

According to the Opinion, a first set of principles concerns AI Ethics; a second illustrates “a detailed step-by-step procedure for decisions as to the deployment, use, risk assurance and review of AI systems”.

These set of principles have significant implications, and provide important coordinates for an independent and analytical assessment of AI systems for immigration.

Ethical deployment must respect, among other things, the principles of ‘Fairness, Equality & Non-discrimination’, ‘Human Dignity & Autonomy’, ‘Privacy & Data Governance’, ‘Transparency & Explainability’, ‘Accountability & Responsibility’, ‘Contestability’, and ‘Oversight & Redress’. Human rights must also always be respected.

The second set of procedural principles illustrate how these high-level notions should be translated into operational guidelines. These include:

Principle 1: You know what AI is and what its limitations are;

Principle 4: You have meaningful human control at the right stage;

Principle 6: You use the right tools for the job;

Principle 7: You are open and collaborative; and

Principle 10: (a) You use these principles alongside your organisation’s policies and (b) have the right assurance in place.

These principles are not respected in the uses of AI we catalogued. For example, the Opinion contains a detailed analysis of many ways in which the APS and ACS generative AI tools deployed within the asylum procedure fail to comply, “in significant respects” leading to “serious concerns”.

If, for example, inaccurate outputs are not assessed quantitatively, and we don’t even know what “accuracy” means in this context, how can Principle 1 be

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

respected? How can Principle 10's "right assurance" be in place when there is no ability to cross-reference the inputs summarised by the ChatGPT-based tools against the original source material? In that case, is there meaningful human control (Principle 4) of outputs?

Again, arguably not – an issue that can and should be examined well beyond the APS and ACS systems, especially considering the more permissive approach adopted in the Data (Use and Access) Act 2025 concerning "solely automated decision-making".²⁵⁴ This not only allows organisations and law enforcement agencies "to carry out solely automated decision-making in wider circumstances, as long as they implement measures to provide certain safeguards".²⁵⁵

It also crucially introduces an "Active Human Review exemption", which temporarily allows law enforcement to delay human review of automated decisions when immediate review would harm investigations or national security²⁵⁶ – provided that a meaningful human reassessment happens as soon as practicable. This way, human intervention becomes a "post-decision safeguard",²⁵⁷ raising a structural issue: the safeguard no longer prevents harm at the point of decision, but merely offers the possibility of later correction, this fundamentally weakening its protective function, especially in a policy domain where migrants are consistently treated as potential threats.

This facilitation of fully automated decisions introduces a "human-after-the-loop" model of safeguards – or a "liberalisation with safeguards".²⁵⁸ In the context of widespread and structural criminalisation of migrants, and denial of the benefit of doubt, this becomes immediately relevant to immigration-related decision-making. If irregular immigration is routinely seen as a threat to national security, it is easy to imagine that the human review exemption will impact AI-informed decisions for border control and management, where accountability is always deferred, often indefinitely, on security grounds.

Delayed human reassessment would also hardly escape the perils of automation bias, which leads humans to tend to confirm rather than question automated decisions. As put by Alexandra Harrington in her 2023 essay "Automation Nation: What Happens When Algorithms Decide Entry for Immigrants and Refugees?":²⁵⁹

"If automated systems are deciding immigration or refugee placements, with the priority being efficiency, it is highly likely that automation bias

will lead to officials rubber-stamping the decisions given to them by the system.”

That assumes we will know about any such deliberations. What happens to the transparency advocated in Principle 7 of the AI Playbook when there is no published Data Protection Assessment, no published Equality Impact Assessment, and asylum applicants are not even “told about the use of the ACS tool”? That failure, according to the Opinion, is likely unlawful.

Ultimately, one could legitimately question the scientific and evidence basis for assuming that generative AI tools are “the right tool for the job” (Principle 6) of better managing the asylum procedure. Or, with another example from our catalogue, to ask whether there are receipts to show that AI is “the right tool for the job” of assessing the age of asylum applicants, given that there seem to be none.

This last question should be posed for all uses of AI in the immigration system. In fact, as Pakistani border officer Ateeq Javed and academics at the Riphah Institute of Public Policy argue in a 2025 literature review,²⁶⁰ “research gaps” strongly limit our evidence base concerning the actual impact of AI in border control operations:

“Even with the growing literature on the issues, there are still major gaps in knowledge. The available empirical data that analyses the real success of AI, its accuracy, and its long-term effects on the migration policy are limited. The current literature does not commonly assess the practical usefulness and precision of AI in border operations and creates a significant gap in the knowledge of the practical results.”

On a similar note, but more specific to immigration AI in the UK, in a 2024 paper Indira Boutier, a lecturer at the Glasgow Caledonian University, wrote that, “There is limited publicly available data on the actual use and impact of AI in the UK’s asylum processes”. She adds, “Without robust data on outcomes, the risks of using such technologies may outweigh anticipated benefits.”²⁶¹

The AI Playbook itself identifies cases in which uses of artificial intelligence “are not appropriate” and should therefore “be avoided in the public sector”. These include, “but are not limited to”, “high-risk or high-impact applications”; when they can “cause harm to someone’s health, safety, fundamental rights or the

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

environment”; and, noticeably, “fully automated decision making”, in relation to which we should “be cautious about any use case involving significant decisions, such as those involving someone’s health or safety”.

Given that immigration-related decisions certainly qualify among these “significant” decisions, it is hard to square the rationale for relaxing wholly automated decision-making in the Data (Use and Access) Act 2025 with the much more cautious approach contextually detailed in the AI Playbook.

More fundamentally, what is the sanction for violating its principles? What, more precisely, is a “high-risk or high-impact application” of AI? And who is the enforcing authority?

When the EU sought to address these and other regulatory issues, it tried to come up with a comprehensive normative framework for AI. The result was the AI Act. While a bold attempt, its deficiencies include omitting protections for people on the move and a lack of oversight for policing and national security.²⁶² In principle, these deficiencies should be capable of being challenged at the EU Court of Justice under the EU’s Charter of Fundamental Rights. It is hard to justify wholesale exemptions. Nevertheless, in disputes between governments and courts, arguments have to be won politically, or we risk politics undermining courts and rights.

INTRODUCE MECHANISMS TO PROTECT MIGRANTS FROM AI HARM

There is an urgent need in the UK to introduce new and better safeguards to protect all of us, including migrants from AI harm, that arise directly from the persistent framing of migration as a national security threat. As the failings of the EU AI Act show, this is no easy feat. And yet, enshrining specific protections into law and, crucially, applying them once approved, is arguably the only way to prevent the predictable and inevitable deluge of harms that mass adoption of techno-solutionist immigration AI will cause.

Until recently, automation decision making (ADM) in public services mostly was simpler and rarer. However, these were still enough to cause massive and systemic disruptions to delivery. As Joe Tomlinson, a King’s College professor who co-authored a 2022 volume, “Experiments in Automating Immigration Systems”,²⁶³ put it in an online interview with ORG, even “Doing simple automation at the scale that large bureaucracies have to do is really, really hard”.

Tomlinson argues for a precautionary approach to the deployment of these technologies.

Often, bureaucracies find implementation simply too hard. Faulty voice recognition algorithms caused more than 7,000 students to be wrongly accused of cheating on the Test of English International Communication (TOEIC), a visa requirement, leading to their mistaken deportation. Notably, the Independent reported, most students were “not allowed to appeal the Home Office decision, nor were they able to obtain evidence against them”. This resulted in severe harms: “Some were detained by immigration officials”, others “lost their jobs, and were left homeless (...) despite being in the UK legally”.²⁶⁴

The sham marriage tool disproportionately flagged people of Bulgarian, Greek, Romanian, and Albanian nationality, while the (now abandoned) visa streaming algorithm created a “fast lane” that would have led to “speedy boarding for white people”.²⁶⁵ Importantly, researcher Kaelynn Narita argued in her 2024 doctoral thesis, both systems “perpetuate racialised outcomes and patterns of sociotechnical harms in the administrative technologies of the Home Office...with and without the direct input of nationality”.²⁶⁶

But this is potentially just the tip of the automated iceberg. Wrongful arrests caused by faulty biometric recognition matches are already well documented, both in the UK²⁶⁷ and elsewhere.²⁶⁸ As the Home Office itself has confirmed, generative AI systems structurally produce inaccurate information in a statistically significant number of cases in which APS and ACS were adopted; and pervasive, automated border surveillance assemblages could well help save lives, but also push irregular migration towards ever more dangerous routes, which continue to lead to deaths in the Channel.²⁶⁹

The experts ORG spoke with in producing this paper agree: the current regulatory framework is inadequate to withstand the onslaught of threats brought about by the many solutionist immigration AI technologies envisioned – and deployed – by the UK government.

Reasons are many, but a methodological one stands out: without effective transparency mechanisms in place, it is simply impossible to distinguish correlation from causation in pinpointing the source of harms to people on the move. In other words, It is hard, if not impossible to clearly establish whether harm was produced by AI, human decision-makers or both in a socio-technical

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

assemblage that combines procedures, practices, technologies, bureaucracies, and cultures.

“People are not being informed of the multiple uses of AI or automated decision-making systems used by the Home Office or generally in the UK Immigration system”, JCWI Advocacy and Campaigns Manager Griff Ferris in an email interview with ORG. “This means that it is virtually impossible to know if a decision or outcome that causes harm has been made or influenced by AI or ADM.”

This is true of current experiments as much as previous ones, signalling a structural issue that requires structural intervention. As Joe Tomlinson, a professor who investigated an earlier iteration of the sham marriage tool, told ORG: “it was so difficult to connect harms to the system. That doesn't mean they're necessarily not there”.

Opacity is a foundational issue, affecting all analyses of the use of AI in immigration. How can the public determine in an evidence-based manner whether Anduril towers deployed in the Channel actually contribute to saving lives or ending them, when their very existence is shrouded in secrecy and the results of their operations are forcefully kept out of the public record? How can the public judge whether automated risk assessments performed by Cerberus ultimately result in the automation of racial profiling when we cannot even know whether it is based on rules or machine learning algorithms?

It is clear that effective transparency mechanisms must be introduced if AI is to be properly and independently scrutinised. This new mechanisms must go beyond technical fixes and the mere removal of blanket exemptions for immigration AI from transparency and accountability standards. Creating them will require a new approach according to which the authorities cannot invoke national security on a whim and empty ‘the public interest’ of all meaning. There are multiple options:

- Drafting stronger, public-oriented freedom of information laws that do not allow the Home Office blanket impunity for missing disclosures in the public interest.
- Narrowing the definition of “national security” from its current arbitrary vagueness.
- Strictly enforcing algorithmic transparency standards.

- Including an obligation to enter all uses of AI systems within the immigration system, regardless of their level of risk, into a governmental transparency register.

Policy recommendations to remedy dangerous blanket national security exceptions were detailed in November 2025 by European Digital Rights (EDRi) Slovenian affiliate Danes je nov dan.²⁷⁰ While addressed to the Slovenian government, they can be usefully adapted to the UK context. These include adopting a clear protocol for AI use in national security, implementing stricter rules for high-risk AI systems, ensuring robust and transparent authorisation procedures, and establishing comprehensive public oversight and control mechanisms, including “an effective internal system for monitoring these systems and for their immediate suspension if any violation of fundamental rights is found”.

Crucially, according to Danes je nov dan this approach implies that

“The government must adopt a clear and strict framework that narrowly defines the use of AI for national security purposes. This will ensure a clear demarcation between activities that fall within the areas of prevention, detection or investigation of criminal offences and the area of national security, avoiding dangerous overlaps.”

Unfortunately, however, the UK’s National Security Strategy 2025²⁷¹ seems to go in the opposite direction, proposing “a hardening and a sharpening of our approach to national security across all areas of policy”, as “we will need to be more unapologetic and systematic in pursuit of our national interests.” As put by then-prime minister Keir Starmer in the Strategy’s foreword: “That is the animating idea of this entire strategy – a hardening and sharpening of our approach. It means viewing higher living standards as an essential national security goal. It means restoring security to our borders as a crucial test of fairness and social cohesion.”

Other recent legislative changes push towards the same “unapologetic and systematic” pursuit of opacity in the name of national security.

For example, the Border Security Bill, which received Royal Assent on 2 December 2025, established formalised cooperation arrangements between the Border Security Commander and intelligence agencies. While these are are not

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

recognised as “partner authorities”, they will need to provide support to border operations. According to written testimony by the Open Rights Group:

“This cooperation, particularly through data-sharing in clauses (...), means that investigative techniques initially designed for counterterrorism could be applied to immigration and gang-related crime.”²⁷²

These techniques can result in immigration enforcement actions that are even more “difficult to scrutinise or hold accountable”, and which can lead to policing bias and abuse – especially considering the expanded wealth of data available the bill grants to the authorities, including from mobile data extraction and electronic monitoring.²⁷³ As a result, “Individuals seeking asylum or protection may be treated as potential criminals rather than vulnerable people fleeing persecution”, violating the proportionality principle established under UK law and the European Convention on Human Rights.

For all these reasons, ORG’s testimony concludes, the clauses giving intelligence agencies these powers should be scrapped.

Given the extraordinary invasiveness of AI-based tools for immigration, ORG also proposed in a series of amendments to the Bill that:

“No artificial intelligence system may be trained using personal data that has been produced in the exercise of immigration control powers”.²⁷⁴

This is all the more important in the context of reduced data protection rules for immigrants.²⁷⁵

Instead of restricting their rights in the name of treating each and every individual on the move as a potential criminal,²⁷⁶ migrants should be given “Digital Sanctuary”, which means that:

“Migrants should enjoy the same human rights as everyone else, including digital rights protected by similar principles”.²⁷⁷

STOP NORMALISING THE AUTOMATED HOSTILE ENVIRONMENT

Not all the risks and harms of AI in the immigration system can be mitigated, and not all AI systems can be made ethical, responsible, or even acceptable through

an appropriate set of legal safeguards. Some AI technologies are radically incompatible with a well-functioning democratic society, and should instead be either paused until effective mitigation strategies can be put in place to ensure their beneficial use. Alternatively, they may need to be banned altogether if the benefits cannot be either justified by or squared with democratic principles and the full enjoyment of human rights by all individuals, with no discrimination based on legal status or the means of entry. Crucially, once these practices are normalised for migrants, they inevitably expand to erode rights and protections for the entire public.

No matter how strictly you regulate them, some AI technologies will inevitably normalise hostile environment policies, racism and discrimination, a process which can only be reinforced and turbocharged by increasing automation.

Take pilots of AI-based live facial recognition technologies for immigration enforcement described above. While a lot of what is actually happening at UK ports is still unknown, and “LFR for law enforcement purposes is not subject to dedicated primary legislation”,²⁷⁸ the government did produce an important set of contextual policy documents providing some specific guidelines concerning LFR’s adoption and oversight. These include the legal mandate,²⁷⁹ the Equality Impact Assessment,²⁸⁰ and the Standard Operating Procedures.²⁸¹

Some ideas developed there help shed light on how the technology should be used. According to the legal mandate, for example, in order to respect human rights LFR adoption should be “proportionate”, “clear and foreseeable to the public” – who should therefore be informed of its use.

Compliance with the Equality Act 2010 prohibits “discrimination on the basis of protected characteristics” – but even though police chief Alex Murray, the National Crime Agency’s director of threat leadership and the national lead for AI, admitted that “artificial intelligence used to boost crime fighting will contain bias”,²⁸² Immigration Enforcement is described in the mandate as “confident that the use of LFR will not lead to any discrimination/bias”²⁸³ through the application of safeguards.

A human is always supposed to be in the loop,²⁸⁴ while “robust governance and oversight” mechanisms are promised, including through the implementation of “a transparent and visible internal inspection, audit, and compliance enforcement regime.”

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

The documentation outlines plenty of other apparent safeguards. Consideration of any potential adverse impact.; deployment only after an established authorisation procedure; the best available technological solution.; and a focus on using LFR only for what is “strictly necessary for the law enforcement purpose”, as put by the EIA. What more could one want?

Yet Big Brother Watch,²⁸⁵ Statewatch,²⁸⁶ and other civil society organisations argue that the adoption of LFR for law enforcement uses should be stopped, including for immigration enforcement.

For one, safeguards are still enshrined in principles that may be subject to various and contradicting interpretations. In one of the most striking examples, LFR is advertised in the Equality Impact Assessment as “a precision tactic to locate people who are within **Immigration Enforcement’s** (IE) Population of Interest”.

Statewatch begs to differ. The UK charity explained in a submission to the Home Office consultation on a new legal framework for law enforcement uses of biometrics that individuals are “often not aware of being scanned”, “millions of custody images held in the Police National Database include large numbers of individuals who have never been charged with a crime”, and “evidence has shown that at present the technology is more than fallible and often leads to biased or discriminatory outcomes”.

When all these factors are compounded with LFR’s technical capabilities:

“The cumulative effect of the use of such technology equates to mass surveillance, through which individuals are automatically and unwittingly subject to suspicion”

This strikes a very different note to the government material. Here, LFR is not considered a “precision tactic”, but rather a dystopian dragnet that “effectively inverts the long-held principle of innocent until proven guilty”. Which is precisely what one would expect from a self-defined “hostile environment” that is being automated.

Officials might also be just as hostile to migrants as biased technologies, Statewatch reminds. In fact:

“There should not be an automatic presumption that individual police forces can provide or uphold the necessary safeguards and protections. Official reviews have found, and senior officials have admitted, that

police forces in England and Wales are in some cases institutionally sexist, racist and homophobic.”

Relying on neutral, objective biometric technologies would therefore arguably help address racial profiling. However, there is no such thing as neutral and objective biometric technologies.

At times, as in the case of the Essex police, officials promptly recognised the issue and immediately paused deployments when presented with evidence the police force itself had commissioned, that “cameras were significantly more likely to target black people than people of other ethnicities”.²⁸⁷

However, in general most police forces have continued to rely on biased biometric technology,²⁸⁸ despite a 2023 National Physical Laboratory report that argued that the bias displayed against women and people of colour becomes statistically insignificant when certain settings are implemented.²⁸⁹

This study’s methodology has been questioned by Peter Fussey and Daragh Murray at the University of Essex, who argued²⁹⁰ that a the sample of 28 individuals (those engaged by a Metropolitan Police Service officer over the course of ten LFR test deployments) is not big enough to draw significant conclusions. It could possibly find “differences in FR algorithm performance due to ethnicity” that “are not statistically significant” simply because “the total number of matches themselves are not statistically significant”.

But even if LFR technologies were to become perfectly accurate, the foundational threat they represent to liberal democracies would not disappear. Actually, they would possibly be even more dangerous.

“These technologies are bad when they get it wrong, and they’re even worse when they get it right”, Jasleen Chaggar, Senior Legal & Policy Officer at Big Brother Watch, told ORG in a video interview. “Because then you’re living in a society in which publicly accessible spaces are no longer capable of being anonymous. You can’t go about your daily life without having your identity checked. And the key to checking is your face, which is obviously something that’s very difficult to conceal,” Chaggar explained.

This is why having operational guidelines for LFR in place is a good development, does not go far enough. Chaggar told ORG:

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

“It’s so important that they have a policy in place. But I think from our view, we need primary legislation to put real safeguards around facial recognition technology. And that’s what the EU has done with the AI Act. They’ve prohibited it in most circumstances and then laid out exceptions and carve-outs rather than adopting the really permissive approach that you see in these policies.”

Within the UK, live facial recognition is not used in Scotland or Northern Ireland. England and Wales are therefore outliers.

The securitisation approach to borders always bleeds into broader society, and borders always arrive back in our everyday lives. Risks affect all of us, not just migrants, once these exceptional powers, technologies, and oversight gaps are justified for ‘border security,’ they become available for, and attractive to, other parts of government, threatening the rights and freedoms of all. For example, a 39-year-old Londoner was wrongly flagged by the Metropolitan Police’s face recognition cameras while travelling across London Bridge, and was subsequently threatened with arrest during a police stop that lasted more than 20 minutes, even though according to Big Brother Watch he produced “multiple identification documents showing that he had been falsely identified by the facial recognition technology”.²⁹¹ The case is subject to a legal challenge in the High Court, at the time of writing.

“While we’re waiting for a decision on that”, Chaggar continued, “I will say that the concern is that face recognition gets used not just on those suspected of having committed offences that make them not eligible to return to the UK, but that it will get used to manage the border irrespective of any suspicion of wrongdoing.”

This is already happening, after all, in another (failing) democracy.²⁹²

“We’re seeing that happen in the US, for example, where ICE agents are using facial recognition in their phones. With the mobile Fortify app²⁹³ they can literally just go up to people and scan their faces. And the way it works there is it’s linked to huge databases on the back end, like the immigration enforcement database. And so suddenly, you can literally scan someone’s face, and it becomes the key to unlock all their records.”

Once the environment is made hostile for people on the move, in order to target migrants and people seeking safety, it rapidly becomes hostile for everyone.

That is why Chaggar says policies and guidelines are good, but not optimal: “because they are not legally binding primary legislation, the concern is that they could change overnight”. The actions of the second Trump administration clearly shows that once the automated surveillance infrastructure is in place, it only takes someone with the power and the will to abuse it to turn a legitimate national security operation into an onslaught of racist mass deportations and violence.²⁹⁴

So on the one hand obtaining a law that severely restricts how the technology is used, requiring judicial authorisation for the deployment of LFR or limiting watch lists to a small number of serious offences would be a welcome development. On the other hand, no safeguard is good enough to avoid the normalisation of mass surveillance in democratic settings. The only effective safeguard is to reject the security framing itself, restore democratic control, and ensure that AI and automation serve humanitarian, not carceral purposes.

As Statewatch put it in its submission,

“The use of LFR is fundamentally incompatible with the protection of human rights and, as has been shown, is open to abuse and very often leads to unjust outcomes. The challenges posed by LFR make it clear that its use cannot be effectively regulated and must, therefore, be prohibited.”

This is not just a problem for migrants. The hostile environment, once automated, becomes a template for governance across society. The very technologies and rationales deployed at the border quickly find their way into domestic policing and public spaces, transforming everyone into a potential suspect.

At a time when democratic governments mull “modernising” human rights law to ease the efficient performance of mass deportations, and normalise anti-immigrant hatred across the political spectrum, opposing the routine adoption of inherently authoritarian technologies becomes imperative. No efficiency gain will ever protect our democracies once their core values have been emptied for the profit of so-called “innovators”.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

In the immigration sphere, only transparent, fully democratic adoption of artificial intelligence for humanitarian purposes – rather than for absolute, predictive control and discrimination – would be truly innovative.

AI-supported empathy and community, rather than AI-sanctioned detentions and deportations: that, to up-end tech-bro jargon, would indeed count as a “revolution”.

CONCLUSION AND RECOMMENDATIONS

1. REJECT SECURITISATION AND TECHNO-SOLUTIONISM IN IMMIGRATION POLICY, AND PUT PEOPLE FIRST

AI adoption by itself will not fix the immigration system, and no amount of hype or corporate PR will change that. The persistent framing of migration as a security threat is the root cause of unchecked AI adoption, regulatory loopholes, and the erosion of rights in the UK immigration system. Migration is a complex human phenomenon, not a constant state of emergency to be solved by the latest automated assemblage at all costs – including compromising human rights and democratic checks and balances for all people on the move, but especially migrants. Techno-solutionist promises should be rejected, especially when it comes to informing immigration and technology policies, as these concern vulnerable individuals and communities who are already disproportionately targeted. Biased automation will only add further discrimination to the mix. Instead of vowing to “modernise” human rights to put AI first, policy-makers should put people first.

This implies:

1. Ensuring digital sanctuary for migrants, refugees and people seeking asylum. There should be no “balancing” of human rights and ethical principles against security and the protection of the nation. This means that no human right can be even partly sacrificed to experiment with new technological solutions in migration management and border security. Migrants must instead enjoy the same human rights as everyone else. Begin with privacy: exemptions that allow the authorities to collect and process their personal data in violation of data protection law in the name of an arbitrarily defined notion of “national security” should be scrapped
2. Lead with the right policy goals, not the technological perceived solution.

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

3. Commit to the transparent use of systemic analysis of the whole policy area, rather than fixating on migration targets and numbers of successful asylum claims.
4. Stop the use of AI tools in asylum decision-making process. Migrants should not be expected to bear the brunt of the structural deficiencies of AI tools, especially given unproven and unsatisfactory mitigation strategies. Generative AI tools such as APS and ACS, deployed by the Home Office to summarise asylum interviews, are particularly problematic, given their systemic and mathematically inevitable tendency to insert fake information,²⁹⁵ or summarise incorrectly. The use of AI is particularly risky when combined with time-based processing targets and high staff turnover within the asylum assessment system.
5. Declare the use of AI and disclose the prompts to migrants when involved in making decisions about them. Craft an anti-tech-solutionist research agenda driven by humanitarian uses of AI rather than by corporate profits and efficiency gains.

2. RECOGNISE THE EXISTENCE OF REGULATORY GAPS AND FILL THEM

Aiming for the most “pro innovation” regulatory environment in the world is not enough to put people first. While evidence needs to be collected in order to properly regulate some uses of AI, others – for example, live mass surveillance of public spaces – are inevitably at odds with democratic principles, and should therefore be banned regardless of whether they function accurately and productively for law enforcement. The current policy landscape should be complemented with an overarching normative framework banning undemocratic uses of AI in migration, similar to the original intentions behind the EU’s AI Act. Applications that pose risks to human rights, democratic principles, and the environment, and so on should be strictly regulated before deployment.

This means:

1. All blanket exemptions for ‘security’ or ‘public order’ must be narrowed, time-limited, and subject to judicial review. Without this, the immigration sector will remain a testing ground for surveillance and state secrecy that inevitably expands to other domains.

2. Producing primary legislation with stringent safeguards for the use of live facial recognition and other biometric technologies for immigration enforcement. The law should first and foremost avoid the normalising of mass surveillance tools in democratic settings, for example by strictly limiting LFR uses to a small number of geographically contained and demonstrably severe/urgent threats to national security, while also ensuring it accurate in these contexts. If this turns out to be technically impossible, then the technology must be banned altogether no matter what its benefits.
3. Scrapping the provisions that allow the sharing of migrants' data with intelligence agencies. Migrants cannot be assumed to be criminals or terrorists, and should not be treated as 'guilty until algorithmically proven innocent'. Anti-terrorism methods, which are essentially inscrutable and opaque to the public, should not be adopted for immigration management, especially when embedded in black box AI systems.
4. Preventing the use of data collected during immigration controls for training AI systems. This prohibition is dictated by data protection requirements such as purpose limitation, proportionality, and data minimisation; by the impossibility of obtaining meaningful consent from migrants; and by risks such as function creep and the danger of reinforcing bias and discrimination.
5. Ensuring independent authorisation for mobile phone data extraction, for all the above reasons.

3. ENHANCE STRUCTURAL TRANSPARENCY IN THE PUBLIC INTEREST

The systemic secrecy that shrouds AI in the immigration system should be fundamentally challenged. Currently, transparency laws allow public officials to reject each and every freedom of information request on national security grounds. All it takes is portraying the requested disclosures as potentially helping criminals circumvent immigration enforcement. While some information can and should be withheld from public view in the name of national security, protecting the public's right to know should not be portrayed as opposed to it. On the contrary, better safeguarding liberty – as enshrined in fundamental and

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

democratic rights – actually means enhancing the nation's security, including when it comes to the adoption of AI in the immigration system. Consequently, foundational details concerning the aim, functioning, safeguards, results, and costs – of both pilots and actual deployments – of AI-based systems in migration should be readily disclosed to the public. Such disclosure should be proactive and mandatory – for example, in an enhanced public register of government AI tools – whenever there may be a significant impact on migrants rights. The norm of secrecy justified by security claims is incompatible with democratic accountability for all.

Steps that are instrumental towards effective transparency include:

1. Drafting better freedom of information laws to ensure the public's right to know does not stop where private contracts begin. Arbitrary “stonewalling” and delays should be taken into account. The Information Commissioner's Office should have strong enforcement powers including the ability to impose fines on authorities that consistently fail to meet statutory deadlines or deliberately obstruct requests.
2. Transparency must be restored by default, with the “national security” invoke only through clear evidence-based procedures, and always with sunset clauses. Any exemption should be subject to judicial oversight, and should be imposed on government secrecy concerning uses of AI in the immigration system.
3. Providing a clear definition of AI's role in national security, with a framework that clearly details its uses, oversight, and safeguards, so that immigration enforcement is not automatically conflated with anti-terrorism activities and prohibits intelligence agencies from arbitrarily applying structural opacity to migrants.

4. CURB OUTSIZED CORPORATE INFLUENCE AND REGAIN DIGITAL SOVEREIGNTY

The AI infrastructure that the UK is building is based on technological assemblages produced by powerful, mostly foreign, corporate giants, which in many cases aim not only for profit, but to promote their own ideology (such as “saving the West” from “invaders”) while blurring the line between military and

civilian applications. The resulting techno-political lock-in ties the hands of public officials to technologies of violence and apartheid. This fully contradicts the government's stated desire for the UK to be an "AI maker" rather than an "AI taker". The deployment of military-grade artificial intelligence and predictive technologies in border and immigration control, particularly when provided by technology firms implicated in abusive immigration raids and war crimes, intensifies human rights violations against migrants, perpetuates xenophobic narratives, and enables mass deportations through automated data aggregation. Storing and sharing migrants' data on these firms' cloud servers compromises their safety and privacy, especially when such servers are located in jurisdictions with regulations that are actively hostile toward migrants and marginalised groups. Asserting digital sovereignty should entail rejecting frameworks that treat migration, and ultimately all aspects of public life, as zones of permanent exception.

In order for democratic institutions to regain control over AI in the immigration system, the UK government should

1. Develop in-house, open source solutions that run locally to offer a democratic, public-led automated stack for the immigration system. Unlike the proprietary, opaque solutions developed by powerful foreign contractors, AI systems delivering immigration services in the UK should prioritise open standards. These can facilitate explainability, redress, and accountability while building internal skills, capacities, and resources that will enable technological independence for future solutions. Critically, developing in-house, open source technologies also reduces vendor dependence which is driving vendor-led policy making in policing and migration.
2. Use British contractors. While all corporate actors pursue their own goals, which include, but are not limited to, maximising profits, foreign providers of AI solutions are especially problematic. Over-reliance on powerful Big Tech corporations from foreign countries can lead to a form of dependence that is both ideological and technological, and should be avoided whenever possible. Buying British doesn't eliminate the possibility that contracted UK companies will be bought by foreign tech giants, nor does it eliminate fundamental incompatibility of infrastructures of mass surveillance with fundamental rights or democracy. However, especially when combined

UNPACKING THE DIGITAL HOSTILE ENVIRONMENT

with open source or code ownership, it provides the government with greater control over the requested technological outputs and long term development and ensures that the capabilities, skills, and economic value produced in the UK stay in the UK.

3. Mandate independent human rights due diligence and review procedures for all AI that is used in border surveillance and migration control.
4. Give both people on the move and UK civil society a louder voice in policy development. Especially in the current context of geopolitical rupture, it is essential to balance the interests of corporate actors – especially foreign contractors – with a truly multi-stakeholder approach to policy including AI deployment in the immigration system. This means giving much greater influence to civil society actors prominently featuring the voice, experiences, and needs of individuals on the move in the UK. This is most important in the policy development and testing phase. Consulting those most affected can both result in greater ideological pluralism and bring a stronger focus on prioritising human rights and humanitarian uses in deployments of artificial intelligence.

5. AVOID REVERSE SOLUTIONISM, AND STRIVE FOR HUMANITY IN THE BROADER IMMIGRATION SYSTEM

While crucial to understanding the UK immigration system, issues related to managing migration and human mobility should not be reduced to problems related to artificial intelligence. We should, in other words, avoid falling for the reverse solutionism trap, criticising the ideological precedence of technology over politics by contesting uses of technology rather than the broader techno-political assemblages they produce. As researcher Lucy Mayblin put it in an interview with Open Rights Group: “AI is not the key thing. The main thing is that bordering doesn’t work to stop irregular migration”; on the contrary, “it actually drives smuggling”. This means that in order to correctly and democratically deploy AI in migration, if and when it is actually useful, we need to subsume its critique within a larger contestation of prejudicial and ideologically-driven anti-immigration attitudes and policies. Only then can AI become a helpful tool of humanitarian assistance rather than an instrument of blind, automated discrimination. Therefore:

1. Do not undermine human rights in the name of efficiency. In both the UK and the EU, governments have vowed to “modernise” human rights law, in particular the European Convention of Human Rights, to better enforce and streamline immigration management. In an increasingly automated hostile environment, this can easily translate into AI-powered mass detentions and deportations within a regime that imposes pervasive control over every aspect of migrants’ lives – just like in Trump’s US. All attempts to “balance” human rights against techno-solutionist efficiency gains – assuming AI technologies provide any produced by AI technologies – should be decisively rejected, as should all attempts to amend asylum rights (for example, by making refugee status “temporary”²⁹⁶).
2. Strive for empathy, community, and inclusion rather than automated discrimination and exclusion. Immigrants have not and will not turn the UK into an “island of strangers”, and should not be presumed to be threats to the stability and security of the nation unless (algorithmically) proven otherwise.

Until these basic principles of human decency are encoded into governmental action – on all shades of the political spectrum – immigration AI is only poised to further dehumanise migrants and refugees. A fundamental change in the mindset of policy-makers is therefore required – not merely embrace whatever is presented as “innovation” by corporate actors, but to display the level of empathy, community, inclusion, understanding, and actual innovation necessary to deal humanely with people seeking asylum, migrants, refugees and individuals on the move more broadly, with or without technology. Ultimately, the challenge is not just technical or procedural, but structural: dismantling the security logic that makes exceptional measures the norm, and restoring a rights-based, democratic approach that protects everyone.

REFERENCES

- 1 Rosanvallon, P. (2008) *Counter-Democracy: Politics in an Age of Distrust*. Cambridge: Cambridge University Press. p. 88.
 - 2 Ajanovic Andelic, A. (2025) 'When technology is the problem, not the solution: Lessons from harmful consequences of techno-solutionism in digital surveillance', *European Digital Rights (EDRI)*, 7 May. Available at: <https://edri.org/our-work/when-technology-is-the-problem-not-the-solution-lessons-from-harmful-consequences-of-techno-solutionism-in-digital-surveillance/> (Accessed: 17 September 2026).
 - 3 Department for Science, Innovation and Technology and Prime Minister's Office, 10 Downing Street (2025) 'Prime Minister sets out blueprint to turbocharge AI', *GOV.UK*, 13 January. Available at: <https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai> (Accessed: 17 September 2026).
 - 4 Clarke, L. (2024) 'UK's Keir Starmer: Don't be scared of AI', *POLITICO*, 14 October. Available at: <https://www.politico.eu/article/britain-must-run-towards-ai-opportunities-says-keir-starmer/> (Accessed: 17 September 2026).
 - 5 MacAskill, A. and Sandle, P. (2025) 'Prime Minister Starmer plans to make Britain AI "superpower"', *Reuters*, 13 January. This is consistent with the vision displayed by the Boris Johnson government in the 2021 'National AI Strategy', and in particular with what Nadine Dorries, then Secretary of State for Digital, Culture, Media and Sport, labelled 'Our ten-year plan to make Britain a global AI superpower' (Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Business, Energy & Industrial Strategy and Department for Digital, Culture, Media & Sport (2021) *National AI Strategy*. GOV.UK, 22 September.). Sources: MacAskill, A. and Sandle, P. (2025) 'Prime Minister Starmer plans to make Britain AI "superpower"', *Reuters*, 13 January. Available at: <https://www.reuters.com/world/uk/uk-pm-starmer-outline-plan-make-britain-world-leader-ai-2025-01-12/> (Accessed: 17 September 2026). Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Business, Energy & Industrial Strategy and Department for Digital, Culture, Media & Sport (2021) *National AI Strategy*. GOV.UK, 22 September. Available at: <https://www.gov.uk/government/publications/national-ai-strategy> (Accessed: 17 September 2026).
 - 6 Crowther, Z. (2025) 'AI Minister Kanishka Narayan: "We want to go further and faster"', *PoliticsHome*, 21 October. Available at: <https://www.politicshome.com/news/article/ai-minister-kanishka-narayan-we-want-go-faster> (Accessed: 17 September 2026).
 - 7 For an investigation into the role of cybernetics in the conceptualisation and realisation of border surveillance assemblages, cfr. Iván Chaar-López (2024), 'The Cybernetic Border. Drones, Technology and Intrusion', Duke University Press, Sources: Chaar López, I. (2024) *The cybernetic border: Drones, technology, and intrusion*. Durham, NC: Duke University Press.
 - 8 Hymas, C. (2026) "'Minority Report policing' to catch criminals before they strike', *The Telegraph*, 18 January. Available at: <https://www.yahoo.com/news/articles/minority-report-policing-catch-criminals-192443803.html> (Accessed: 17 September 2026).
 - 9 Home Office (2026) *Live facial recognition deployment in November 2025*. GOV.UK, 9 January. Available at: <https://www.gov.uk/government/publications/live-facial-recognition-deployment-in-november-2025> (Accessed: 17 September 2026).
 - 10 Home Office (2024) *25 October 2024: Cerberus project Accounting Officer Assessment*. GOV.UK, 25 October. Available at: <https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/25-october-2024-cerberus-project-accounting-officer-assessment> (Accessed: 17 September 2026).
 - 11 Storey, S. (n.d.) 'The UK's AI borders: Anduril's autonomous surveillance towers', *Migrants' Rights Network*. Available at: <https://migrantsrights.org.uk/projects/hostile-office/the-digital-hostile-environment/ai-borders-anduril-autonomous-surveillance-towers/> (Accessed: 17 September 2026).
 - 12 Ibid.
 - 13 The term "people on the move" is commonly used as an umbrella expression encompassing all forms of human mobility—including migrants, refugees, asylum seekers and internally displaced persons—defined broadly as the movement of individuals within or across borders regardless of cause, duration, or legal status. Widely adopted in the literature and in policy documents by both the academia and civil society, it "enables us to take the humanity of people on the move as a starting point", rather than their legal status (Pijnenburg and Rijken, 2020, <https://tandfonline.com/doi/full/10.1080/1369801X.2020.1854107#d1e110>)
- Sources: Pijnenburg, A. and Rijken, C. (2021) 'Moving beyond "refugees" and "migrants": Reconceptualising the rights of people on the move', *Interventions*, 23(2), pp. 273–293. Available at: <https://www.tandfonline.com/doi/full/10.1080/1369801X.2020.1854107> (Accessed: 17 September 2026).
- 14 Crerar, P. and Syal, R. (2025) 'Starmer urges Europe's leaders to curb ECHR to halt rise of far right', *The Guardian*, 9 December. Available at: <https://www.theguardian.com/law/2025/dec/09/starmer-urges-europe-leaders-update-echr-halt-rise-far-right> (Accessed: 17 September 2026).
 - 15 Public Law Project (2023) *Public Law Project response to the AI White Paper consultation*. June. Available at: <https://publiclawproject.org.uk/content/uploads/2023/06/Public-Law-Project-AI-white-paper-consultation-response.pdf> (Accessed: 17 September 2026).
 - 16 Department for Digital, Culture, Media & Sport and Office for Artificial Intelligence (2021) *National AI Strategy*. GOV.UK, 22 September. Available at: <https://www.gov.uk/government/publications/national-ai-strategy> (Accessed: 17 September 2026).
 - 17 Privacy International (2024) 'Automating the hostile environment: Uncovering a secretive Home Office algorithm at the heart of immigration decision-making', 17 October. Available at: <https://privacyinternational.org/news-analysis/5452/automating-hostile-environment-uncovering-secretive-home-office-algorithm-heart> (Accessed: 17 September 2026). Open Rights Group (2026) *Automating the*

hostile environment: AI in the asylum decision making process. 14 January. Available at: <https://www.openrightsgroup.org/publications/automating-the-hostile-environment-ai-in-the-asylum-decision-making-process/> (Accessed: 17 September 2026).

- 18 Mackenzie-Gray Scott, R. (2026) *AI and the public sector: A human rights approach*. Open Rights Group, 3 September. Available at: <https://www.openrightsgroup.org/publications/ai-and-the-public-sector-a-human-rights-approach/> (Accessed: 17 September 2026).
- 19 Weale, S. (2025) 'All schools in England to be given AI-generated pupil attendance targets', *The Guardian*, 12 November. Available at: <https://www.theguardian.com/education/2025/nov/12/all-schools-in-england-to-be-given-ai-generated-pupil-attendance-targets> (Accessed: 17 September 2026).
- 20 Grierson, J. (2025) 'UK minister unveils plan to cut animal testing through greater use of AI', *The Guardian*, 11 November. Available at: <https://www.theguardian.com/science/2025/nov/11/uk-plan-to-cut-animal-testing-artificial-intelligence-ai-3d-bioprinting> (Accessed: 17 September 2026).
- 21 Woode, D. (2026) 'Police could use AI to improve quality of rape trial evidence', *The Times*, 4 January. Available at: <https://www.thetimes.com/uk/crime/article/ai-rape-convictions-investigations-avon-and-somerset-police-c3nx2b6gg> (Accessed: 17 September 2026).
- 22 Syal, R. (2025) 'AI chatbots could help stop prisoner release errors', *The Guardian*, 10 November. Available at: <https://www.theguardian.com/society/2025/nov/10/ai-chatbots-stop-prisoner-release-errors> (Accessed: 17 September 2026).
- 23 Elgot, J. and Booth, R. (2025) 'AI tool can give ministers 'vibe check' on whether MPs will like policies', *The Guardian*, 20 January. Available at: <https://www.theguardian.com/technology/2025/jan/20/ai-tool-can-give-ministers-vibe-check-on-whether-mps-will-like-policies> (Accessed: 17 September 2026).
- 24 Crowther, Z. (2025) 'AI Minister Kanishka Narayan: "We want to go further and faster"', *PoliticsHome*, 21 October. Available at: <https://www.politicshome.com/news/article/ai-minister-kanishka-narayan-we-want-go-faster> (Accessed: 17 September 2026).
- 25 GOV.UK (n.d.) *Home Office 2030 Digital Strategy (accessible)*. Available at: <https://www.gov.uk/government/publications/home-office-2030-digital-strategy/home-office-2030-digital-strategy> (Accessed: 17 September 2026).
- 26 GOV.UK (n.d.) *Evaluation of AI trials in the asylum decision making process*. Available at: <https://www.gov.uk/government/publications/evaluation-of-ai-trials-in-the-asylum-decision-making-process/evaluation-of-ai-trials-in-the-asylum-decision-making-process> (Accessed: 17 September 2026).
- 27 Inkstick (2025) 'American AI Arrives on Fortress Europe's Borders. At What Cost?', *Inkstick*, 3 December. Available at: <https://inkstickmedia.com/american-ai-arrives-on-fortress-europes-borders-at-what-cost/> (Accessed: 17 September 2026).
- 28 Banerjee, S., Agarwal, A. and Singla, S. (2024) 'LLMs will always hallucinate, and we need to live with this', *arXiv.org* [Preprint]. Available at: <https://arxiv.org/abs/2409.05746> (Accessed: 17 September 2026).
- 29 Home Office (2025) *Evaluation of AI trials in the asylum decision making process*. GOV.UK, 29 April. Available at: <https://www.gov.uk/government/publications/evaluation-of-ai-trials-in-the-asylum-decision-making-process/evaluation-of-ai-trials-in-the-asylum-decision-making-process> (Accessed: 17 September 2026).
- 30 Petrova, K. (2025) 'Study finds nearly two-thirds of AI-generated citations are fabricated or contain errors', *PsyPost*, 20 November. Available at: <https://www.psypost.org/study-finds-nearly-two-thirds-of-ai-generated-citations-are-fabricated-or-contain-errors/> (Accessed: 17 September 2026). Checker, R. (2026) 'ChatGPT Citations: Why AI-Generated References Are Wrong and How to Fix Them', *Reference Checker*, 19 July. Available at: <https://referencechecker.org/blog/chatgpt-citations-wrong-how-to-fix> (Accessed: 17 September 2026).
- 31 Taylor, L. (2025) 'AI will help make 'life-or-death' calls in rammed UK asylum system', *Context*, 9 May. Available at: <https://www.context.news/ai/ai-will-help-make-life-or-death-calls-in-rammed-uk-asylum-system> (Accessed: 17 September 2026).
- 32 Open Rights Group (n.d.) 'Legal Opinion: The use of Artificial Intelligence tools in asylum cases', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/publications/legal-opinion-the-use-of-artificial-intelligence-tools-in-asylum-cases/> (Accessed: 17 September 2026).
- 33 For an analysis and discussion of the UK AI Playbook's Principles, cfr. Chapter 2, section B.
- 34 UK Parliament (2026) 'Written question: 125725', *UK Parliament*, 10 April. Available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-04-10/125725/> (Accessed: 17 September 2026).
- 35 Open Rights Group (2026) 'Home Office use of AI in asylum cases likely to be unlawful, legal opinion finds', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/press-releases/home-office-use-of-ai-in-asylum-cases-likely-to-be-unlawful-legal-opinion-finds/> (Accessed: 17 September 2026).
- 36 Find a Tender (n.d.) 'Home Office - Auto-translation and transcription Request for Information - Find a Tender', *Find a Tender*. Available at: <https://www.find-tender.service.gov.uk/Notice/067065-2025> (Accessed: 17 September 2026).
- 37 Migrants' Rights Network (2025) *AI under watch*. Available at: <https://migrantsrights.org.uk/wp-content/uploads/2025/02/AI-under-watch-English.pdf> (Accessed: 17 September 2026).
- 38 Public Law Project (2023) 'Tracking Automated Government (TAG) Register'. Public Law Project, 9 February. Available at: <https://trackautomatedgovernment.shinyapps.io/register/> (Accessed: 17 September 2026).
- 39 Privacy International (2024) 'Automating the hostile environment: Uncovering a secretive Home Office algorithm at the heart of immigration decision-making', 17 October. Available at: <https://privacyinternational.org/news-analysis/5452/automating-hostile-environment-uncovering-secretive-home-office-algorithm-heart> (Accessed: 17 September 2026).

- 40 Migrants' Rights Network (2025) 'AI Under Watch - Migrants' Rights Network', *Migrants' Rights Network*, 30 January. Available at: <https://migrantsrights.org.uk/projects/hostile-office/the-digital-hostile-environment/ai-under-watch/> (Accessed: 17 September 2026).
- 41 Booth, R. (2024) 'AI' tool could influence Home Office immigration decisions, critics say', *The Guardian*, 11 November. Available at: <https://www.theguardian.com/uk-news/2024/nov/11/ai-tool-could-influence-home-office-immigration-decisions-critics-say> (Accessed: 17 September 2026).
- 42 Amoores, L. (2024) 'The deep border', *Political Geography*, 109, article 102547. Available at: <https://www.sciencedirect.com/science/article/pii/S0962629821002079> (Accessed: 17 September 2026).
- 43 WhatDoTheyKnow (2023) 'Web page', *WhatDoTheyKnow*. Available at: https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3 (Accessed: 17 September 2026).
- 44 McDonald, H. (2020) 'Home Office to scrap 'racist algorithm' for UK visa applicants', *The Guardian*, 4 August. Available at: <https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants> (Accessed: 17 September 2026).
- 45 In it, Leslie asks about "The plans to transition the functionality of the EMRT to IPIC", to which the HO replies: "The Home Office plan to transition the functionality, once the development of IPIC's electronic monitoring module has been completed, there will be a period of testing, training and user familiarisation. There will also be a period of dual running to ensure that IPIC delivers recommendations that match those expected. A decision will then be taken over when to move solely to using IPIC for providing recommendations for future case actions."
Sources: WhatDoTheyKnow (2023) 'Electronic monitoring review too', *WhatDoTheyKnow*. Available at: https://www.whatdotheyknow.com/request/electronic_monitoring_review_too (Accessed: 17 September 2026).
- 46 Privacy International (2024) 'GPS tagging of migrants UNLAWFUL, UK authority finds after PI complaint', *Privacy International*. Available at: <https://privacyinternational.org/news-analysis/5261/gps-tagging-migrants-unlawful-uk-authority-finds-after-pi-complaint> (Accessed: 17 September 2026).
- 47 Ozkul, D. (2023) *Automating immigration and asylum: The uses of new technologies in migration and asylum governance in Europe*. Oxford: Refugee Studies Centre, University of Oxford. Available at: https://www.hertie-school.org/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/Automating-immigration-and-asylum_Ozkul.pdf (Accessed: 17 September 2026).
- 48 Cockerell, I. (2022) "'Crazy invasive technology': UK faces legal challenge for GPS tagging of migrants", *Coda Story*, 18 August. Available at: <https://www.codastory.com/surveillance-and-control/surveillance-uk-migrants-gps-trackers/> (Accessed: 17 September 2026).
- 49 Bancroft, H. (2025) 'GPS tagging of asylum seekers is ineffective, government report finds', *The Independent*, 13 January. Available at: <https://www.independent.co.uk/news/uk/home-news/gps-tag-asylum-seeker-migrant-home-office-b2678445.html> (Accessed: 17 September 2026).
- 50 Ministry of Justice (2022.) 'Electronic Monitoring Non-Fitted Devices - Contracts Finder', *Contracts Finder*. Available at: <https://www.contractsfinder.service.gov.uk/notice/60bb8854-257a-4c11-b3e0-efc733a87512> (Accessed: 17 September 2026).
- 51 Privacy International (2022) 'Buddi Limited - Immigration Enforcement's favourite tracking buddy', *Privacy International*. Available at: <https://privacyinternational.org/long-read/4991/buddi-limited-immigration-enforcements-favourite-tracking-buddy> (Accessed: 17 September 2026).
- 52 As we'll detail in chapter 2, the Border Security, Asylum and Immigration Bill 2025 contains provisions that establish a formalised collaborative relationship between the Border Security Commander and intelligence agencies, such as the MI5 and GCHQ. According to a written evidence by the Open Rights Group, "This cooperation, particularly through data-sharing in clauses (27–33), means that investigative techniques initially designed for counterterrorism could be applied to immigration and gang-related crime". Data gleaned from electronic monitoring devices could therefore potentially become part of automated risk assessments and analyses by intelligence agencies that structurally conflate migrants with terrorist – an assumption that informs the whole technosolutionist approach long adopted by UK governments – in the absence of bespoke oversight.
- 53 Privacy International (2025) 'UK Justice and Home Affairs Committee publishes report on electronic monitoring', *Privacy International*. Available at: <https://privacyinternational.org/advocacy/5717/uk-justice-and-home-affairs-committee-publishes-report-electronic-monitoring> (Accessed: 17 September 2026).
- 54 WhatDoTheyKnow (2023) 'Electronic monitoring review too 2', *WhatDoTheyKnow*. Available at: https://www.whatdotheyknow.com/request/electronic_monitoring_review_too_2 (Accessed: 17 September 2026).
- 55 Privacy International (n.d.) 'Complaint against the UK's automated recommendation tools in immigration operations', *Privacy International*. Available at: <https://privacyinternational.org/legal-action/complaint-against-uks-automated-recommendation-tools-immigration-operations> (Accessed: 17 September 2026).
- 56 Privacy International (2025) 'PI alerts regulator about the use of algorithms by the UK Government and their impact on migrants', *Privacy International*, 15 August. Available at: <https://privacyinternational.org/long-read/5639/pi-alerts-regulator-about-use-algorithms-uk-government-and-their-impact-migrants> (Accessed: 17 September 2026).
- 57 HoDigital (2025) 'Transforming our caseworking system to improve outcomes for our users', *HoDigital*, 3 November. Available at: <https://hodigital.blog.gov.uk/2025/11/03/transforming-our-caseworking-system-to-improve-outcomes-for-our-users/> (Accessed: 17 September 2026).

- 58 Narita, Kaelynn (2024) *The Digital Hostile Environment: Migration and Technology*. Available at: <https://research.gold.ac.uk/id/eprint/38044/> (Accessed: 17 September 2026).
- 59 According to the Guardian, the issue concerned "merged identities" ("where two or more people have biographical and biometric details linked incorrectly"), resulting in "people unable to prove their rights to work, rent housing or access free NHS treatment". "Imagine waking up one day and it's your word against a computer system – and your future depends on it", said Andreea Dumitrache, of the campaign group the3million, describing how digital tools can enable Hostile Environment policies. SourceS: Dyer, H., Taylor, D. and Syal, R. (2024) 'Home Office immigration database errors hit more than 76,000 people', *The Guardian*, 14 March. Available at: <https://www.theguardian.com/uk-news/2024/mar/14/home-office-immigration-database-errors-hit-more-than-76000-people> (Accessed: 17 September 2026).
- 60 Wire, B. (2026) 'Mastek Expands Leeds Office, Strengthening AI-Led Innovation and Long-Term Commitment to the UK', *Yahoo! Finance*, 11 February. Available at: <https://finance.yahoo.com/news/mastek-expands-leeds-office-strengthening-131600726.html> (Accessed: 17 September 2026).
- 61 Burt, C. (2026) 'Mastek win £49M deal to support UK Home Office Biometrics delivery', *Biometric Update | Biometrics News, Companies and Explainers*, 2 March. Available at: <https://www.biometricupdate.com/202603/mastek-win-49m-deal-to-support-uk-home-office-biometrics-delivery> (Accessed: 17 September 2026).
- 62 Finder, C. (n.d.) 'Framework Engineering - Contracts Finder', *Contracts Finder*. Available at: <https://www.contractsfinder.service.gov.uk/notice/51ed93a2-33d0-42dc-aacb-cfc70525e49d> (Accessed: 17 September 2026).
- 63 Mastek (2026) 'Mastek secures £85m framework engineering contract with UK Home Office's Migration & Borders Technology Portfolio to scale the ATLAS platform', *Mastek*, 5 March. Available at: <https://www.mastek.com/pressreleases/mastek-85m-uk-home-office-atlas-engineering-contract/> (Accessed: 17 September 2026).
- 64 Public Law Project (2023) *Tracking Automated Government (TAG) Register*. 9 February. Available at: <https://trackautomatedgovernment.shinyapps.io/register/> (Accessed: 17 September 2026).
- 65 Mastek (2026) 'mastek-secures-49m-uk-home-office-biometrics-hades-2026', *Mastek*. Available at: <https://www.mastek.com/pressreleases/mastek-secures-49m-uk-home-office-biometrics-hades-2026/> (Accessed: 17 September 2026).
- 66 Mastek (2026) 'mastek-fca-digital-delivery-hub-contract', *Mastek*. Available at: <https://www.mastek.com/pressreleases/mastek-fca-digital-delivery-hub-contract/> (Accessed: 17 September 2026).
- 67 Biometric Update (2024) 'UK data watchdog to investigate country's troubled immigration IT systems', *Biometric Update | Biometrics News, Companies and Explainers*, 20 March. Available at: <https://www.biometricupdate.com/202403/uk-data-watchdog-to-investigate-countrys-troubled-immigration-it-systems> (Accessed: 17 September 2026).
- 68 Mastek (n.d.) 'Mastek', *Mastek*. Available at: <https://www.mastek.com/> (Accessed: 17 September 2026).
- 69 BBC News (2026) 'AI will be used to estimate age of asylum seekers from next year', *BBC News*. Available at: <https://www.bbc.co.uk/news/articles/ce3pe36qe7ro> (Accessed: 17 September 2026).
- 70 Home Office (2026) 'Facial Age Estimation Contract Award Notice - Contracts Finder', *Contracts Finder*. Available at: <https://www.contractsfinder.service.gov.uk/notice/ef4b35f6-c1e6-4be6-8c1c-b6c7dc1b142e> (Accessed: 17 September 2026).
- 71 GOV.UK (2026) 'Facial age estimation: Using AI to support initial age decisions (A guide) (accessible)', *GOV.UK*. Available at: <https://www.gov.uk/government/publications/facial-age-estimation/facial-age-estimation-using-ai-to-support-initial-age-decisions-a-guide-accessible> (Accessed: 17 September 2026).
- 72 GOV.UK (2026) 'Facial age estimation: Using AI to support initial age decisions (A guide) (accessible)', *GOV.UK*. Available at: <https://www.gov.uk/government/publications/facial-age-estimation/facial-age-estimation-using-ai-to-support-initial-age-decisions-a-guide-accessible#the-governments-plans-for-fae-in-the-asylum-system~:text=Accuracy%20is,here> (Accessed: 17 September 2026).
- 73 Inkstick (2025) 'American AI Arrives on Fortress Europe's Borders. At What Cost?', *Inkstick*, 3 December. Available at: <https://inkstickmedia.com/american-ai-arrives-on-fortress-europes-borders-at-what-cost/> (Accessed: 17 September 2026).
- 74 Haskins, C. (2022) 'ICE has a new \$7.2 million contract for facial recognition check-ins for migrants', *Business Insider*, 2 May. Available at: <https://www.businessinsider.com/ice-7-million-contract-trust-stamp-facial-recognition-location-tracking-2022-5> (Accessed: 17 September 2026).
- 75 McKinney, I. (2018) 'Customs and Border Protection's Biometric Data Snooping Goes Too Far', *Electronic Frontier Foundation*, 15 February. Available at: <https://www.eff.org/deeplinks/2018/02/customs-and-border-protections-biometric-data-snooping-goes-too-far> (Accessed: 17 September 2026).
- 76 Human Rights Watch (2025) 'UK Plans AI Experiment on Children Seeking Asylum', *Human Rights Watch*, 31 July. Available at: <https://www.hrw.org/news/2025/07/31/uk-plans-ai-experiment-on-children-seeking-asylum> (Accessed: 17 September 2026).
- 77 Home Office (2026) 'Facial age estimation: Using AI to support initial age decisions (A guide) (accessible)', *GOV.UK*. Available at: <https://www.gov.uk/government/publications/facial-age-estimation/facial-age-estimation-using-ai-to-support-initial-age-decisions-a-guide-accessible#~:text=older%2E,Can,system,%2E> (Accessed: 17 September 2026).
- 78 National Institute of Standards and Technology (2024) *NIST.IR.8525*. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf> (Accessed: 17 September 2026).
- 79 Boutin, C. (2024) 'NIST Reports First Results From Age Estimation Software Evaluation', *National Institute of Standards and Technology*, 30 May. Available at: <https://www.nist.gov/news-events/news/2024/05/nist->

- [reports-first-results-age-estimation-software-evaluation](#) (Accessed: 17 September 2026).
- 80 American Psychological Association (2020) 'Experiencing childhood trauma', *American Psychological Association*. Available at: <https://www.apa.org/news/press/releases/2020/08/experiencing-childhood-trauma> (Accessed: 17 September 2026).
 - 81 Independent Chief Inspector of Borders and Immigration (2025) *An inspection of the Home Office's use of age assessments (July 2024 – February 2025)*. Available at: https://assets.publishing.service.gov.uk/media/687f6f9dfdc190fb6b84685e/An_inspection_of_the_Home_Office_s_use_of_age_assessments_July_2024_February_2025_.pdf (Accessed: 17 September 2026).
 - 82 Independent Chief Inspector of Borders and Immigration (2025) *An inspection of the Home Office's use of age assessments (July 2024 – February 2025)*, GOV.UK, 22 July. Available at: <https://www.gov.uk/government/publications/an-inspection-of-the-home-offices-use-of-age-assessments-july-2024-february-2025> (Accessed: 17 September 2026).
 - 83 Jesuit Refugee Service UK and Humans for Rights Network (2026) *Age disputed children detained under the 'one-in-one-out' scheme: Briefing note*. May. Available at: <https://static1.squarespace.com/static/5a69d94949fc2bad10754433/t/6a16c8dc05cb23342faa809b/1779878108950/Briefing+on+age-disputed+minors.pdf> (Accessed: 17 September 2026).
 - 84 Taylor, L. (2025) 'UK use of AI age estimation tech on migrants fuels rights fears', *Context*, 17 October 2025. Available at: <https://www.context.news/ai/uk-use-of-ai-age-estimation-tech-on-migrants-fuels-rights-fears> (Accessed: 17 September 2026).
 - 85 Taylor, D. (2022) 'Home Office illegally seized phones of 2,000 asylum seekers, court rules', *The Guardian*, 25 March 2022. Available at: <https://www.theguardian.com/uk-news/2022/mar/25/home-office-illegally-seized-asylum-seekers-phones> (Accessed: 17 September 2026).
 - 86 Home Office (2025) 'Border Security, Asylum and Immigration Act 2025', GOV.UK, 30 January 2025. Available at: <https://www.gov.uk/government/collections/border-security-asylum-and-immigration-bill-2025> (Accessed: 17 September 2026).
 - 87 Jones, S. (2026) 'UK powers to seize phones from migrants without arrest come into force', *BBC News*. Available at: <https://www.bbc.com/news/articles/cm240jvnen0o> (Accessed: 17 September 2026).
 - 88 Home Office (2025) 'Border Security, Asylum and Immigration Act 2025: equality impact assessment', GOV.UK, 3 December 2025. Available at: <https://www.gov.uk/government/publications/border-security-asylum-and-immigration-act-2025-equality-impact-assessment> (Accessed: 17 September 2026).
 - 89 Syal, R. (2026) 'UK's plans to seize asylum seekers' phones condemned by campaigners', *The Guardian*, 4 January 2026. Available at: <https://www.theguardian.com/uk-news/2026/jan/04/uk-plans-seize-asylum-seekers-phones-condemned-campaigners> (Accessed: 17 September 2026).
 - 90 Home Office (2025) 'Border Security, Asylum and Immigration Bill 2025: factsheets', GOV.UK, 30 January 2025. Available at: <https://www.gov.uk/government/publications/border-security-asylum-and-immigration-bill-2025-factsheets> (Accessed: 17 September 2026).
 - 91 Home Office (2025) 'Border Security, Asylum and Immigration Bill 2025: equality impact assessment (accessible version)', GOV.UK, 2 December 2025. Available at: <https://www.gov.uk/government/publications/border-security-asylum-and-immigration-bill-2025-equality-impact-assessment/border-security-asylum-and-immigration-bill-2025-equality-impact-assessment-accessible-version> (Accessed: 17 September 2026).
 - 92 Privacy International (n.d.) *UK migration surveillance regime*. Available at: https://privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf (Accessed: 17 September 2026).
 - 93 Police and Crime Commissioner for Leicestershire (2025) 'Digital Forensics Software Renewal for Cellebrite Software - Find a Tender', *Find a Tender*. Available at: <https://www.find-tender.service.gov.uk/Notice/009640-2025> (Accessed: 17 September 2026).
 - 94 Privacy International (n.d.) 'Are UK police accessing your cloud apps?', *Privacy International*. Available at: <https://privacyinternational.org/report/3551/are-uk-police-accessing-your-cloud-apps> (Accessed: 17 September 2026).
 - 95 Cooper, V. (2021) 'How South Wales Police manage the rapid pace of digital transformation to keep citizens safe', *Cellebrite*, 29 June. Available at: <https://cellebrite.com/en/how-south-wales-police-manage-the-rapid-pace-of-digital-transformation-to-keep-citizens-safe/> (Accessed: 17 September 2026).
 - 96 Cellebrite (2025) 'Cumbria Constabulary's commitment to excellence in digital forensics and investigations', *Cellebrite*, 18 August. Available at: <https://cellebrite.com/en/cumbria-constabulary-s-commitment-to-excellence-in-digital-forensics-and-investigations/> (Accessed: 17 September 2026).
 - 97 Cellebrite (2025) 'The AI advantage: Managing investigations with confidence', *Cellebrite*, 4 November. Available at: <https://cellebrite.com/en/the-ai-advantage-managing-investigations-with-confidence/> (Accessed: 17 September 2026).
 - 98 Cooper, V. (2021) 'How South Wales Police manage the rapid pace of digital transformation to keep citizens safe', *Cellebrite*, 29 June. Available at: <https://cellebrite.com/en/how-south-wales-police-manage-the-rapid-pace-of-digital-transformation-to-keep-citizens-safe/> (Accessed: 17 September 2026).
 - 99 Cellebrite (2023) 'Ensuring our nation's security', *Cellebrite*, 16 June. Available at: <https://cellebrite.com/en/uk-defence/> (Accessed: 17 September 2026).
 - 100 Cooper, V. (2021) 'How South Wales Police manage the rapid pace of digital transformation to keep citizens safe', *Cellebrite*, 29 June. Available at: <https://cellebrite.com/en/how-south-wales-police-manage-the-rapid-pace-of-digital-transformation-to-keep-citizens-safe/> (Accessed: 17 September 2026).

- 101 MSAB (2026) 'MSAB – Trusted Partner in Digital Forensics | XAMN & XRY', MSAB, 27 January 2026. Available at: <https://www.msab.com/> (Accessed: 17 September 2026).
- 102 MSAB (2021) 'Border control software - Mobile forensic & data recovery software - MSAB', MSAB, 15 September 2021. Available at: <https://www.msab.com/industries/border-control/> (Accessed: 17 September 2026).
- 103 MSAB (2022) 'CASE STUDY: Two UK Police Forces - MSAB', MSAB, 15 March 2022. Available at: <https://www.msab.com/case-studies/case-study-two-uk-police-forces/> (Accessed: 17 September 2026).
- 104 MSAB (2022) 'CASE STUDY: UK Law Enforcement Agency - MSAB', MSAB, 15 March. Available at: <https://www.msab.com/case-studies/case-study-uk-law-enforcement-agency/> (Accessed: 17 September 2026).
- 105 Milliken, A. (2021) 'Home Office algorithm to detect sham marriages may contain built-in discrimination', *TBIJ*, 19 April. Available at: <https://www.thebureauinvestigates.com/stories/2021-04-19/home-office-algorithm-sham-marriages> (Accessed: 17 September 2026).
- 106 GOV.UK (n.d.) 'Marriage and civil partnership referral and investigation scheme: statutory guidance for Home Office staff (accessible version)', GOV.UK. Available at: <https://www.gov.uk/government/publications/marriage-and-civil-partnership-referral-and-investigation-scheme/marriage-and-civil-partnership-referral-and-investigation-scheme-statutory-guidance-for-home-office-staff-accessible-version> (Accessed: 17 September 2026).
- 107 Public Law Project (2023) *Tracking Automated Government (TAG) Register*. 9 February. Available at: <https://trackautomatedgovernment.shinyapps.io/register/> (Accessed: 17 September 2026).
- 108 Milliken, A. (2021) 'Home Office algorithm to detect sham marriages may contain built-in discrimination', *TBIJ*, 19 April. Available at: <https://www.thebureauinvestigates.com/stories/2021-04-19/home-office-algorithm-sham-marriages> (Accessed: 17 September 2026).
- 109 Stacey, K. (2023) 'UK officials use AI to decide on issues from benefits to marriage licences', *The Guardian*, 23 October. Available at: <https://www.theguardian.com/technology/2023/oct/23/uk-officials-use-ai-to-decide-on-issues-from-benefits-to-marriage-licences> (Accessed: 17 September 2026).
- 110 Ade (2023) 'Legal action launched over sham marriage screening algorithm', *Public Law Project*, 17 February. Available at: <https://publiclawproject.org.uk/latest/legal-action-launched-over-sham-marriage-screening-algorithm/> (Accessed: 17 September 2026).
- 111 Milliken, A. (2021) 'Home Office algorithm to detect sham marriages may contain built-in discrimination', *TBIJ*, 19 April. Available at: <https://www.thebureauinvestigates.com/stories/2021-04-19/home-office-algorithm-sham-marriages/> (Accessed: 17 September 2026).
- 112 AlgorithmWatch (n.d.) 'The Automated Fortress Europe: No Place for Human Rights', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/automated-fortress-europe/> (Accessed: 17 September 2026).
- 113 Chiusi, F. (2025) *La fortezza automatica: Se l'IA decide chi può varcare i confini*. Turin: Bollati Boringhieri.
- 114 Hasbrouck, E. (2009) 'Congress, investors won't let "Trusted Traveler" die', *Papers, Please!*, 1 October. Available at: <https://papersplease.org/wp/2009/10/01/congress-investors-wont-let-trusted-traveler-die/> (Accessed: 17 September 2026).
- 115 Cotterill, T. (2020) 'AI being considered by UK government to control nation's borders', *The News (Portsmouth)*, 28 October. Available at: <https://www.portsmouth.co.uk/news/defence/ai-being-considered-by-uk-government-to-control-nations-borders-3018006> (Accessed: 17 September 2026).
- 116 Wired-Gov (2009) 'High tech border control success | Home Office', *Wired-Gov*. Available at: <https://www.wired-gov.net/wg/wg-news-1.nsf/0/AF404FCE93F76715802576770038A726?OpenDocument> (Accessed: 17 September 2026).
- 117 Clatworthy, B. (2025) 'No passports please! Airport trial of facial recognition a success', *The Times*, 10 November. Available at: <https://www.thetimes.com/uk/politics/article/uk-airport-border-trials-contactless-no-passports-g7mt5g8z5> (Accessed: 17 September 2026).
- 118 Biometric Update (2025) 'UK completes passport-free border trial with biometric e-gates', *Biometrics News, Companies and Explainers*, 12 November. Available at: <https://www.biometricupdate.com/202511/uk-completes-passport-free-border-trial-with-biometric-e-gates> (Accessed: 17 September 2026).
- 119 Handley, E. (2023) 'Implementing digital borders in the UK: Lessons from the rest of the world', *Open Access Government*, 5 April. Available at: <https://www.openaccessgovernment.org/implementing-digital-borders-uk-lessons-ai/156666/> (Accessed: 17 September 2026).
- 120 India, T.T.O. (n.d.) 'How UK is using technology to reduce immigration queues at airports across the country', *The Times of India*. Available at: <https://timesofindia.indiatimes.com/technology/tech-news/how-uk-is-using-technology-to-reduce-immigration-queues-at-airports-across-the-country/articleshow/125302804.cms> (Accessed: 17 September 2026).
- 121 World, C.S. (2023) 'The border must continually evolve: How Border Force is tackling new threats', *Civil Service World*, 25 May. Available at: <https://www.civilserviceworld.com/in-depth/article/border-force-small-boats-migration-phil-douglas> (Accessed: 17 September 2026).
- 122 Already in 2023, Douglas told the Times of India: "We will introduce a "universal permission to travel" requirement, which will require everyone (except British and Irish citizens) to seek authorisation before travelling, and give us 100% coverage on who is coming to the border". This knowledge, produced well before the border and distributed across government databases, is what allegedly allows border officials to just focus on passengers algorithmically deemed to be risky, for example by systems such as Cerberus (detailed later in the chapter). The digitisation of immigration status (problematised in an ORG report) and the creation of the Electronic Travel Authorisation scheme are both integral to the realisation of this vision for "seamless" border crossings. Sources: Ozkul, D. & Godin, M. (2025). *Exclusion by Design: Digital Identification and the Hostile Environment for Migrants*. In collaboration with Nazek Ramadan and Anne Stoltenberg (Migrant Voice)

- and Sara Alsherif (Open Rights Group). <https://doi.org/10.31273/9781911675211> ; TOI Tech Desk (2025) 'How UK is using technology to reduce immigration queues at airports across the country', *The Times of India*. Available at: <https://timesofindia.indiatimes.com/technology/tech-news/how-uk-is-using-technology-to-reduce-immigration-queues-at-airports-across-the-country/articleshow/125302804.cms> (Accessed: 17 September 2026).
- 123 Biometric Update (2024) 'UK officials plan face biometrics trial for passport-free border checks', *Biometric Update | Biometrics News, Companies and Explainers*, 2 January. Available at: <https://www.biometricupdate.com/202401/uk-officials-plan-face-biometrics-trial-for-passport-free-border-checks> (Accessed: 17 September 2026).
 - 124 Topham, G. (2023) 'March of the robots: how biometric tech could kill off paper passports', *The Guardian*, 3 February. Available at: <https://www.theguardian.com/politics/2023/feb/03/biometric-technology-paper-passports-redundant> (Accessed: 17 September 2026).
 - 125 In the USA, going as far as preventing Black applicants to file asylum claims altogether. Source: Bosque, M.D. (2023) 'Facial recognition bias frustrates Black asylum applicants to US, advocates say', *The Guardian*, 8 February. Available at: <https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias> (Accessed: 17 September 2026).
 - 126 According to Joy Buolamwini, the founder of the Algorithmic Justice League and a prominent researcher in the field of biometric recognition, face recognition solutions deployed at airports suffer from racial bias. "The National Institute of Standards and Technology released research showing that not just dark African-American faces, but also Asian faces were up to 100 times more likely to be failed by these systems than the faces of white individuals", she claimed in a WGBH article. "There are also studies that show age bias and gender bias as well." Source: GBH (2023) 'Facial recognition software in airports raises privacy and racial bias concerns', *GBH*, 16 June. Available at: <https://www.wgbh.org/news/national/2023-06-16/facial-recognition-software-in-airports-raises-privacy-and-racial-bias-concerns> (Accessed: 17 September 2026).
 - 127 Schippers, B. (2019) 'When your face is your boarding pass you are holidaying with Big Brother', *The Irish Times*, 8 July. Available at: <https://www.irishtimes.com/opinion/when-your-face-is-your-boarding-pass-you-are-holidaying-with-big-brother-1.3949353> (Accessed: 17 September 2026).
 - 128 AlgorithmWatch (n.d.) 'CarMen, biometric solutions for fully automated, continuous border controls', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/aotm-db/carmen-biometric-solutions-for-fully-automated-continuous-border-controls/> (Accessed: 17 September 2026).
 - 129 AlgorithmWatch (n.d.) 'PopEye, unobtrusive on-the-move biometric technologies to maximize travellers' experience', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/aotm-db/popeye-unobtrusive-on-the-move-biometric-technologies-to-maximize-travellers-experience/> (Accessed: 17 September 2026).
 - 130 AlgorithmWatch (n.d.) 'D4FLY, new technologies for on the fly identity verification at border crossings', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/aotm-db/d4fly-new-technologies-for-on-the-fly-identity-verification-at-border-crossings/> (Accessed: 17 September 2026).
 - 131 AlgorithmWatch (n.d.) 'EINSTEIN, a suite of interoperable solutions for "phygital" identity checks', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/aotm-db/einstein-a-suite-of-interoperable-solutions-for-phygital-identity-checks/> (Accessed: 17 September 2026).
 - 132 AlgorithmWatch (n.d.) 'The Seamless Surveillance Machine: Europe's Biometric Border Vision', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/seamless-surveillance-machine-europes-biometric-border-vision/> (Accessed: 17 September 2026).
 - 133 Chaar López, I. (2024) *The cybernetic border: Drones, technology, and intrusion*. Durham, NC: Duke University Press.
 - 134 Bourne, M., Johnson, H. and Lisle, D. (2015) 'Laboratizing the border: The production, translation and anticipation of security technologies', *Security Dialogue*, 46(4), pp. 307–325. Available at: <https://journals.sagepub.com/doi/full/10.1177/0967010615578399> (Accessed: 17 September 2026).
 - 135 Fabio Chiusi (2025), *La fortezza automatica*. Se l'IA decide chi può varcare i confini, Bollati Boringhieri. The idea is that AI promises to once and for all fulfil the authorities' desire and alleged need of omniscience to radically eliminate insecurity from our societies, making threats to national security at the border effectively impossible. Threats to the nation in the context of immigration are therefore always portrayed as a lack of information. This is why the 'Restoring control over the immigration system' white paper, for example, claims that "We will also continue to harness the latest developments in artificial intelligence, facial recognition and age assessment technologies to ensure that we gather the most accurate information available on each individual seeking to enter the UK." Because of the cybernetic assumption according to which human mobility is an information problem, that can allegedly be managed and solved by reducing border flows — including individuals on the move — to numbers and data points, thus filling each and every possible knowledge gap the border authorities may encounter. No more "experiments in open borders", as Starmer put it in the Foreword to the white paper; we finally have the technologies — and the political will — to close them down, selectively and automatically, for those algorithmically deemed undeserving and/or threatening to national security and UK citizens at large. AI, in this perspective, becomes a device to quell our fears of the (racialised) Other. Source: Home Office (2025) *Restoring control over the immigration system: white paper*. Available at: <https://www.gov.uk/government/publications/restoring-control-over-the-immigration-system-white-paper> (Accessed: 17 September 2026).
 - 136 Mau, S. (2022) *Sorting machines: The reinvention of the border in the 21st century*. Translated by N. Barfoot. Cambridge: Polity.
 - 137 This is what is actually happening in the United States with the heavily contested ICE operations producing abuse and violence on a systemic and daily basis. These operations fundamentally rely on AI. See and as an example. Sources: Landrum, I. (2026) 'How ICE Uses AI to Automate Authoritarianism', *Tech Policy Press*, 28

- January. Available at: <https://www.techpolicy.press/how-ice-uses-ai-to-automate-authoritarianism/> (Accessed: 17 September 2026). Iwilkinson (2026) 'ICE drives AI use case growth within Homeland Security | FedScoop', *FedScoop*, 29 January. Available at: <https://fedscoop.com/dhs-ai-inventory-mobile-fortify-palantir/> (Accessed: 17 September 2026). reporter, G.S. (2026) 'How ICE is using facial recognition in Minnesota', *The Guardian*, 27 January. Available at: <https://www.theguardian.com/technology/2026/jan/27/ice-facial-recognition-minnesota> (Accessed: 17 September 2026). Haskins, C. and Kelly, M. (2026) 'ICE Is Using Palantir's AI Tools to Sort Through Tips', *WIRED*, 28 January. Available at: <https://www.wired.com/story/ice-is-using-palantirs-ai-tools-to-sort-through-tips/> (Accessed: 17 September 2026).
- 138 Home Office (2026) *IE Facial Recognition Policy V2.0*. Available at: https://assets.publishing.service.gov.uk/media/699c763531713b50fd49c06a/IE_Facial_Recognition_Policy_V2.0.pdf (Accessed: 17 September 2026).
- 139 PublicTechnology (2025) 'Home Office trials live facial recognition to catch returning deportees', *PublicTechnology*, 7 November. Available at: <https://www.publictechnology.net/2025/11/07/public-order-justice-and-rights/home-office-trials-live-facial-recognition-to-catch-returning-deportees/> (Accessed: 17 September 2026).
- 140 Home Office (2026) *Live facial recognition deployment in November 2025*. GOV.UK, 9 January. Available at: <https://www.gov.uk/government/publications/live-facial-recognition-deployment-in-november-2025> (Accessed: 17 September 2026).
- 141 Biometric Update (2026) 'No false alerts in UK POC of live facial recognition for immigration enforcement', *Biometric Update | Biometrics News, Companies and Explainers*, 12 January. Available at: <https://www.biometricupdate.com/202601/no-false-alerts-in-uk-poc-of-live-facial-recognition-for-immigration-enforcement> (Accessed: 17 September 2026).
- 142 Atherley, J. (2026) 'Live facial recognition cameras installed at ports to catch illegal migrants trying to sneak into UK', *The Irish Sun*, 10 January. Available at: <https://www.thesun.ie/news/16366713/facial-recognition-cameras-catch-illegal-migrants-uk/> (Accessed: 17 September 2026).
- 143 Butterly, L. and Gallagher, C. (2026) 'Facial recognition technology to be trialled on passengers at Holyhead', *The Irish Times*, 22 February. Available at: <https://www.irishtimes.com/ireland/2026/02/23/facial-recognition-technology-to-be-trialled-on-passengers-at-holyhead/> (Accessed: 17 September 2026).
- 144 Butterly, L. (2026) 'Facial recognition trial on Dublin-Holyhead route scans thousands but finds no matches', *The Irish Times*, 13 April. Available at: <https://www.irishtimes.com/crime-law/2026/04/13/facial-recognition-trial-on-dublin-holyhead-route-scans-thousands-but-finds-no-matches/> (Accessed: 17 September 2026).
- 145 Home Office (2025) 'Immigration Enforcement: live facial recognition legal mandate', *GOV.UK*, 5 November. Available at: <https://www.gov.uk/government/publications/immigration-enforcement-live-facial-recognition-legal-mandate> (Accessed: 17 September 2026).
- 146 Home Office (2025) 'Live facial recognition: equality impact assessment (EIA)', *GOV.UK*, 5 November. Available at: <https://www.gov.uk/government/publications/live-facial-recognition-equality-impact-assessment-eia> (Accessed: 17 September 2026).
- 147 Home Office (2025) 'Live facial recognition: data protection impact assessments (DPIA) template', *GOV.UK*, 5 November. Available at: <https://www.gov.uk/government/publications/live-facial-recognition-data-protection-impact-assessments-dpia-template> (Accessed: 17 September 2026).
- 148 Home Office (2025) 'Live facial recognition standard operating procedures', *GOV.UK*, 5 November. Available at: <https://www.gov.uk/government/publications/live-facial-recognition-standard-operating-procedures> (Accessed: 17 September 2026).
- 149 A more analytical discussion of these policy documents is provided in the next chapter.
- 150 Lynch, D. (2024) 'Ministers will be told to use AI to screen migrants for threats, adviser says', *Yahoo Finance* (PA Media), 18 April. Available at: <https://uk.finance.yahoo.com/news/ministers-told-ai-screen-migrants-222504746.html> (Accessed: 17 September 2026).
- 151 Hall, J. (2025) *The Terrorism Acts in 2023: Report of the Independent Reviewer of Terrorism Legislation* (accessible). GOV.UK, 15 July. Available at: <https://www.gov.uk/government/publications/the-terrorism-acts-in-2023/the-terrorism-acts-in-2023-report-of-the-independent-reviewer-of-terrorism-legislation-accessible> (Accessed: 17 September 2026).
- 152 Storey, S. (n.d.) 'The UK's AI borders: Anduril's autonomous surveillance towers', *Migrants' Rights Network*. Available at: <https://migrantsrights.org.uk/projects/hostile-office/the-digital-hostile-environment/ai-borders-anduril-autonomous-surveillance-towers/> (Accessed: 17 September 2026).
- 153 McIntyre, N. and Siddons, E. (2025) 'Anduril AI weapons company lobbies UK government', *TBIJ*, 23 July. Available at: <https://www.thebureauinvestigates.com/stories/2025-07-23/selling-weapons-to-westminster-how-defence-giant-anduril-trained-its-sights-on-the-uk> (Accessed: 17 September 2026).
- 154 Home Office (2024) *Freedom of Information response: FOI/2024/07511*. 13 September.
- 155 Google. (n.d.) 'English Channel Surveillance Towers (August 2025) - Google My Maps', *Google My Maps*. Available at: <https://www.google.com/maps/d/u/0/viewer?mid=1DT0qJRzdBGqCBiYxwvLyQ042tHX1FOk&ll=51.050634111656315%2C1.0868135411399749&z=10> (Accessed: 17 September 2026).
- 156 Storey, S. (2025) 'SOAS Presentation - 26 Nov 2025', *Migrants Rights Network and the Baring Foundation*. 26 November 2025. Available at: https://docs.google.com/presentation/d/1ozuMAKDusRq6d33M9IF0yyZJe96_EORAT4jfhn6scaU/edit?usp=sharing (Accessed: 17 September 2026).
- 157 Storey, S. (2025) 'Standing at the gates of the digital hostile environment: Britain's Anduril Maritime Sentry Towers', *Samuel Storey, YouTube*, 9 April. Available at: <https://youtu.be/ziYr2S6zDTw?si=2qQOkC95l8pYhKCC> (Accessed: 17 September 2026).

- 158 Amnesty International (2023) 'Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT', *Amnesty International*, 1 May. Available at: <https://www.amnesty.org/en/documents/mde15/6701/2023/en/> (Accessed: 17 September 2026).
- 159 Poglase, K, Doherty, L, Mankarious, S and Manley, B. (2023) 'Britain's shadowy border', *CNN*, 31 July. Available at: <https://edition.cnn.com/interactive/2023/07/uk/migrant-crossings-ai-small-boats/> (Accessed: 17 September 2026).
- 160 Foreign, Commonwealth & Development Office (2025) 'UK brings forward world's first sanctions regime to smash the gangs responsible for irregular migration', *GOV.UK*, 22 July. Available at: <https://www.gov.uk/government/news/uk-brings-forward-worlds-first-sanctions-regime-to-smash-the-gangs-responsible-for-irregular-migration> (Accessed: 17 September 2026).
- 161 Meaker, M. (2020) 'Here's proof the UK is using drones to patrol the English Channel', *WIRED*, 10 January. Available at: <https://www.wired.com/story/uk-drones-migrants-english-channel/> (Accessed: 17 September 2026).
- 162 Tekever itself had actually already admitted the use of its drones to patrol the Channel in 2021. "Every day, dozens of asylum seekers and refugees set off on the dangerous journey across the English Channel to reach British soil, but small boats and treacherous conditions mean many lives are in danger along the way. We are proud to be a partner of UK authorities in fighting this kind of illegal human traffic. Drones can identify humans in distress in a much faster way and help rescue teams", said Paul Weeb, Tekever UK Managing director, back then. Source: Allison, G. (2021) 'Tekever say their drones in channel 'help prevent illegal migration'', *UK Defence Journal*, 15 September. Available at: <https://ukdefencejournal.org.uk/tekever-say-their-drones-in-channel-help-prevent-illegal-migration/> (Accessed: 17 September 2026).
- 163 Isakjee, A., Davies, T., Mayblin, L., Turner, J. and Yemane, T. (2025) 'Border security contracts linked to small boat Channel crossings', *Channel Crossings research project*. Archived at: <https://web.archive.org/web/20250430172258/https://channelcrossings.org/wp-content/uploads/2025/04/border-security-contracts-briefing-april-2025.docx-1-1.pdf> (Accessed: 17 September 2026).
- 164 Home Offices (2020) 'FW UAS Managed Service - Contracts Finder', *Contracts Finder*. Available at: <https://www.contractsfinder.service.gov.uk/Notice/def2ca3f-aed8-43ef-82e6-50f3742d99ac> (Accessed: 17 September 2026).
- 165 Jones, S and Walker, A. (2024) 'Migrants on fatal Channel crossing screamed 'we're going to die', court told', *BBC News*. Available at: <https://www.bbc.com/news/uk-england-kent-68140645> (Accessed: 17 September 2026).
- 166 Tekever (n.d.) 'AR5 – Tekever', *Tekever*. Available at: <https://www.tekever.com/ar5/> (Accessed: 17 September 2026).
- 167 Allison, G. (2021) 'Tekever say their drones in channel 'help prevent illegal migration'', *UK Defence Journal*, 15 September. Available at: <https://ukdefencejournal.org.uk/tekever-say-their-drones-in-channel-help-prevent-illegal-migration/> (Accessed: 17 September 2026).
- 168 Tekever was part of the COMPASS2020 Consortium, and one of the main beneficiaries of EU funding for that project (584.325,00 euros out of a total of 4.838.489,61), Sources: AlgorithmWatch (n.d.) 'COMPASS 2020, expanding surveillance reach through the combined use and seamless coordination of manned and unmanned assets', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/aotm-db/compass-2020-expanding-surveillance-reach-through-the-combined-use-and-seamless-coordination-of-manned-and-unmanned-assets/> (Accessed: 17 September 2026).
- 169 A paper by COMPASS2020 participants sheds light on how the SAR scenario worked: "a vessel carrying irregular migrants is in a distress situation beyond coastal waters, sending out EPIRB (Emergency Position Indicating Radio Beacon) signal in order to alert the European authorities. At the first phase of the mission, three types of assets are in the area performing persistence surveillance: the OPV (offshore patrol vessel), the Zephyr, and the A18-M. At the moment it receives the EPIRB alert, Zephyr immediately communicates this information to the operational commander that is working from the Marine Operations Center (MOC) through the COMPASS2020 Mission System (MS) replica onboard the OPV. In the following phase, the OPV will launch an AR-3 capable to collect data regarding the vessel in distress, thus enhancing the situational awareness of marine authorities concerning the risk level of the situation and allowing them to act timely and properly" Source: Bauk, S., Kapidani, N., Lukšić, Ž., Rodrigues, F. and Sousa, L. (2019) 'Autonomous marine vehicles in sea surveillance as one of the COMPASS2020 project concerns', *Journal of Physics: Conference Series*, 1357(1), article 012045. IOP Publishing. Available at: <https://doi.org/10.1088/1742-6596/1357/1/012045>
- 170 One might reasonably argue that deployments actually took place, but without the public or even the European Commission knowing. As an AlgorithmWatch investigation found, this is a structural gap in the Commission's knowledge base — one that severely affects the ability of civil society and other independent actors to scrutinise adoption and implications of immigration AI systems. Source: AlgorithmWatch (n.d.) 'The EU Spends Big on Border Tech — But Has No Idea What It Gets', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/eu-border-tech-spending/> (Accessed: 17 September 2026).
- 171 Also included in the demonstrations were a) a Zephyr "high altitude pseudo- satellite (HAPS) that fills the gap between satellites and UAVs (70000 ft)" produced by AIRBUS, and b) an A18-M by the French EXAIL ROBOTICS (also part of the consortium and granted some 416,000 in funds by the EU), described as "an autonomous underwater vehicle (AUV) that can be launched from OPV" and "capable of performing autonomous missions up to 300 m depth and it is easily transportable by plane for overseas missions". Sources: Airbus (2024) 'Zephyr High Altitude Platform Station (HAPS)', *Airbus*, 1 October. Available at: <https://www.airbus.com/en/products-services/defence/uas/zephyr> (Accessed: 17 September 2026). Exail (n.d.) 'A18-M - Autonomous Underwater Vehicle', *Exail*. Available at: <https://www.exail.com/product/a18-m->

- [autonomous-underwater-vehicle](#) (Accessed: 17 September 2026).
- 172 The University of Sheffield (n.d.) 'New research reveals billions made by companies involved in UK border security', *The University of Sheffield*. Available at: <https://sheffield.ac.uk/news/new-research-reveals-billions-made-companies-involved-uk-border-security> (Accessed: 17 September 2026).
 - 173 Turner, J., Isakjee, A., Mayblin, L., Davies, T. and Yemane, T. H. (2026) 'The border security economy in the English Channel: Small boats, racism and late imperialism', **Political Geography**, 130, article 103603. Elsevier. Available at: <https://doi.org/10.1016/j.polgeo.2026.103603> and 'Border Security Contracts: English Channel 2017-2024. Public .xlsx', *Google Docs*. Available at: https://docs.google.com/spreadsheets/d/1We0i2K72rUXm0zJe_7_nh1KB6HzBt8_/edit?pli=1&gid=1982862253%23gid=1982862253 (Accessed: 17 September 2026).
 - 174 Tussell (2019) 'Drone demonstration and development project', *Tussell*. Available at: https://client.tussell.com/award_notices/437730-6b7bdaa43eefc87ab44e9e3a8ef82f8a-drone-demonstration-and-development-project (Accessed: 17 September 2026).
 - 175 Skelton, S.K. (2023) 'New Border Force unit to deploy more surveillance tech in Channel', *ComputerWeekly.com*, 9 February. Available at: <https://www.computerweekly.com/news/365530821/New-Border-Force-unit-to-deploy-more-surveillance-tech-in-Channel> (Accessed: 17 September 2026).
 - 176 Robinson, R. (2024) 'The new £15m plan to use spy satellites to track migrants sneaking into UK on small boats', *Daily Express*, 30 December. Available at: <https://www.express.co.uk/news/politics/1994173/spy-satellites-track-migrants-small-boats> (Accessed: 17 September 2026).
 - 177 Dathan, M. (2026) 'Can facial recognition drones help combat people smugglers?', *The Times*, 6 April. Available at: <https://www.thetimes.com/uk/crime/article/facial-recognition-drones-channel-crossings-smugglers-b3s75njbt> (Accessed: 17 September 2026).
 - 178 Ibid.
 - 179 BAE Systems (2023) 'BAE Systems partners with Home Office to help identify national security risks at the UK border', *BAE Systems*. Available at: <https://www.baesystems.com/en/article/bae-systems-partners-with-home-office-to-help-identify-national-security-risks-at-the-uk-border> (Accessed: 17 September 2026).
 - 180 Sullivan, G. and Van Der Meerssche, D. (2025) 'The Legal Infrastructures of UK Border Control—Cerberus and the Dispositif of Speculative Suspicion', *Cambridge Core*, November. Available at: <https://www.cambridge.org/core/journals/german-law-journal/article/legal-infrastructures-of-uk-border-controlcerberus-and-the-dispositif-of-speculative-suspicion/E9189E07C87EED7E037D7D00098B47D6> (Accessed: 17 September 2026).
 - 181 An idea that sits perfectly with the broader HO aim of enabling “seamless” border crossing experiences thanks to algorithmic pre-screenings and biometric recognition technologies, of the likes we described in the previous pages. Cerberus might well provide the “intelligent” risk assessment capabilities that are indispensable to instantly discriminate the *deserving* from the *undeserving* of mobility at crossing points, and therefore realise the efficiency gains promised by the “uninterrupted”, “frictionless” vision of international mobility adopted — for the *deserving* — by the UK government. As we’ll argue over the next pages, the same logic is in full display in the EU as well, with striking similarities in the overall vision, in the language and tone adopted to express it, and in the technologies adopted to implement it.
 - 182 BAE Systems. (2023) 'BAE Systems partners with Home Office to help identify national security risks at the UK border', *BAE Systems*, 14 February. Available at: <https://www.baesystems.com/en/article/bae-systems-partners-with-home-office-to-help-identify-national-security-risks-at-the-uk-border> (Accessed: 17 September 2026).
 - 183 Home Office (2022) 'C22535 - Cerberus Product Development and Associated Services - Contracts Finder', *Contracts Finder*. Available at: <https://www.contractsfinder.service.gov.uk/Notice/b0c77742-492f-4dcf-8b6e-78171fbaab6c> (Accessed: 17 September 2026).
 - 184 Sullivan, G. and Van Der Meerssche, D. (2025) 'The Legal Infrastructures of UK Border Control—Cerberus and the Dispositif of Speculative Suspicion', *Cambridge Core*, November. Available at: <https://www.cambridge.org/core/journals/german-law-journal/article/legal-infrastructures-of-uk-border-controlcerberus-and-the-dispositif-of-speculative-suspicion/E9189E07C87EED7E037D7D00098B47D6> (Accessed: 17 September 2026).
 - 185 I.e. from a system based on predefined rules to one that learns them autonomously by example. See footnote 31.
 - 186 BAE Systems. (2024) 'Could AI-driven analytics transform Britain's border?', *The Times & The Sunday Times*, 26 September. Available at: <https://www.thetimes.com/static/border-control-risk-management-security-bae-systems/> (Accessed: 17 September 2026).
 - 187 Ozkul, D. (2023) *Automating immigration and asylum: The uses of new technologies in migration and asylum governance in Europe*. Oxford: Refugee Studies Centre, University of Oxford. Available at: https://www.hertie-school.org/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/Automating-immigration-and-asylum_Ozkul.pdf (Accessed: 17 September 2026).
 - 188 An almost identical version of the Cerberus vision became publicly accessible in April 2026 within the 'SRO appointment letter for Kara Claxton, October 2025'. Source: Home Office (2025) 'Cerberus programme: SRO appointment letter for Kara Claxton, October 2025 (accessible)', *GOV.UK*, October 2025. Available at: <https://www.gov.uk/government/publications/home-office-major-projects-appointment-letters-for-senior-responsible-owners/cerberus-programme-sro-appointment-letter-for-kara-claxton-october-2025-accessible> (Accessed: 17 September 2026).
 - 189 European Union (n.d.) 'European Union - EES / ETIAS', *Travel Europe*. Available at: <https://travel-europe.europa.eu/en/etias> (Accessed: 17 September 2026).

- 190 National Infrastructure and Service Transformation Authority (2025) 'NISTA Annual Report 2024-25', GOV.UK. Available at: <https://www.gov.uk/government/publications/nista-annual-report-2024-2025/nista-annual-report-2024-25> (Accessed: 17 September 2026).
- 191 Home Office (2024) 25 October 2024: Cerberus project Accounting Officer Assessment. GOV.UK, 25 October. Available at: <https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/25-october-2024-cerberus-project-accounting-officer-assessment> (Accessed: 17 September 2026).
- 192 Department for Science, Innovation & Technology (2025) 'Memorandum of Understanding between UK and OpenAI on AI opportunities', GOV.UK. Available at: <https://www.gov.uk/government/publications/memorandum-of-understanding-between-the-uk-and-openai-on-ai-opportunities/memorandum-of-understanding-between-uk-and-openai-on-ai-opportunities> (Accessed: 17 September 2026).
- 193 Booth, R. (2025) 'UK government's deal with Google 'dangerously naive', say campaigners', *The Guardian*, 9 July. Available at: <https://www.theguardian.com/technology/2025/jul/09/uk-governments-deal-with-google-dangerously-naive-say-campaigners> (Accessed: 17 September 2026).
- 194 So much that Alex Karp's manifesto, The Technological Republic, is defined by The Times as the "the AI manifesto inspiring Keir Starmer's government". Tellingly, according to the Guardian, when the Prime Minister visited Washington in February 2025, "his first stop after the White House was Palantir's office". Sources: Smyth, C. (2025) 'The AI manifesto inspiring Keir Starmer's government', *The Times*, 18 July. Available at: <https://www.thetimes.com/uk/politics/article/ai-manifesto-inspiring-keir-starmer-morgan-mcsweeney-cpxzkpt6l> (Accessed: 17 September 2026). Rose, S. and Ko, L. (2025) "Fear really drives him: is Alex Karp of Palantir the world's scariest CEO?", *The Guardian*, 18 November. Available at: <https://www.theguardian.com/technology/2025/nov/18/fear-really-drives-him-is-alex-karp-of-palantir-the-worlds-scariest-ceo> (Accessed: 17 September 2026).
- 195 University of York (2025) 'Billions made by companies involved in UK border security, study shows', *University of York*. Available at: <https://www.york.ac.uk/news-and-events/news/2025/research/billions-made-companies-border-security/> (Accessed: 17 September 2026).
- 196 Owen, C. (2025) 'New research reveals billions made by companies involved in UK border security', *University of Liverpool News*, 30 April. Available at: <https://news.liverpool.ac.uk/2025/04/30/new-research-reveals-billions-made-by-companies-involved-in-uk-border-security/> (Accessed: 17 September 2026).
- 197 ABC News (2025) 'British PM Keir Starmer outlines bid to become AI 'world leader'', *ABC News*, 13 January. Available at: <https://www.abc.net.au/news/2025-01-14/keir-starmer-lays-out-bid-for-ai-in-public-sector/104813444> (Accessed: 17 September 2026).
- 198 Clarke, L. (2024) 'UK's Keir Starmer: Don't be scared of AI', *POLITICO*, 14 October. Available at: <https://www.politico.eu/article/britain-must-run-towards-ai-opportunities-says-keir-starmer/> (Accessed: 17 September 2026).
- 199 Department for Science, Innovation and Technology and Prime Minister's Office, 10 Downing Street (2025) 'Prime Minister sets out blueprint to turbocharge AI', GOV.UK, 13 January. Available at: <https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai> (Accessed: 17 September 2026).
- 200 MacAskill, A. and Sandle, P. (2025) 'Prime Minister Starmer plans to make Britain AI "superpower"', *Reuters*, 13 January. Available at: <https://www.reuters.com/world/uk/uk-pm-starmer-outline-plan-make-britain-world-leader-ai-2025-01-12/> (Accessed: 17 September 2026).
- 201 Clarke, L. (2024) 'UK's Keir Starmer: Don't be scared of AI', *POLITICO*, 14 October. Available at: <https://www.politico.eu/article/britain-must-run-towards-ai-opportunities-says-keir-starmer/> (Accessed: 17 September 2026).
- 202 Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Business, Energy & Industrial Strategy and Department for Digital, Culture, Media & Sport (2021) *National AI Strategy*. London: HM Government. Published 22 September 2021; updated 18 December 2022. Available at: <https://www.gov.uk/government/publications/national-ai-strategy>
- 203 GOV.UK (n.d.) 'A pro-innovation approach to AI regulation', GOV.UK. Available at: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper> (Accessed: 17 September 2026).
- 204 In September 2024, the Draghi report – 'The Future of European Competitiveness', – identified an "innovation deficit" affecting the EU, and partly attributed it to the "regulatory barriers" imposed, among the "around 100 tech-focused laws" written in the bloc, by the AI Act. This led the European Commission to rewrite the digital rulebook, so that constraints on innovation in the EU could be removed. In November 2025, it therefore adopted a "Digital Omnibus", which amended and significantly watered down some of the requirements contained in the AI Act. The Omnibus has been harshly criticized by several civil society organisations. Sources: European Commission (n.d.) 'The Draghi report on EU competitiveness', *European Commission*. Available at: https://commission.europa.eu/topics/competitiveness/draghi-report_en (Accessed: 17 September 2026). Shaping Europe's digital future (n.d.) 'An agile Digital Rulebook for the EU', *Shaping Europe's digital future*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook> (Accessed: 17 September 2026). European Digital Rights (EDRi) (2026) 'Reject the proposals to undermine transparency in the AI Act - European Digital Rights (EDRi)', *European Digital Rights (EDRi)*, 11 February. Available at: <https://edri.org/our-work/ai-omnibus-reject-the-proposals-to-undermine-transparency-in-the-ai-act/> (Accessed: 17 September 2026).
- 205 Clarke, L. (2024) 'UK's Keir Starmer: Don't be scared of AI', *POLITICO Europe*, 14 October. Available at: <https://www.politico.eu/article/britain-must-run-towards-ai-opportunities-says-keir-starmer/>

- 206 Crowther, Z. (2025) 'AI Minister Kanishka Narayan: "We Want To Go Further And Faster"', *PoliticsHome*, 21 October. Available at: <https://www.politicshome.com/news/article/ai-minister-kanishka-narayan-we-want-go-faster>
- 207 Home Office (2025) 'Home Office 2030 Digital Strategy (accessible)', GOV.UK. Available at: <https://www.gov.uk/government/publications/home-office-2030-digital-strategy/home-office-2030-digital-strategy> (Accessed: 17 September 2026).
- 208 In fact, data gathered by the Ada Lovelace Institute in a December 2025 research on public attitudes show the exact opposite: the large majority of the public is skeptical about Big Tech self-regulation, and demands clear rules for AI. According to the results, 91% "feel it is important that AI systems are developed and used in ways that treat people fairly", while "84% fear that, when regulating AI, the government will prioritise its partnerships with large technology companies over the public interest". Importantly, "the public expect ongoing monitoring and clear lines of accountability", including effective "transparency reporting". Sources: Polo, N. and Modhvadia, R. (2025) *Great (public) expectations*. Ada Lovelace Institute. Available at: <https://www.adalovelaceinstitute.org/policy-briefing/great-expectations/> (Accessed: 17 September 2026).
- 209 Department for Science, Innovation & Technology (2025) 'AI Opportunities Action Plan', GOV.UK. Available at: <https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan> (Accessed: 17 September 2026).
- 210 Government Digital Service (2025) 'AI Playbook for the UK Government', GOV.UK, 10 February. Available at: <https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government> (Accessed: 17 September 2026).
- 211 Open Rights Group (2026) 'Home Office use of AI in asylum cases likely to be unlawful, legal opinion finds', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/press-releases/home-office-use-of-ai-in-asylum-cases-likely-to-be-unlawful-legal-opinion-finds/> (Accessed: 17 September 2026).
- 212 Cabinet Office (2020) '2025 UK Border Strategy', GOV.UK, 17 December. Available at: <https://www.gov.uk/government/publications/2025-uk-border-strategy> (Accessed: 17 September 2026).
- 213 Home Office (2024) 'Delivering Border Security', GOV.UK, 10 December. Available at: <https://www.gov.uk/government/publications/delivering-border-security-statement/delivering-border-security> (Accessed: 17 September 2026).
- 214 Home Office (2025) 'Restoring control over the immigration system: white paper', GOV.UK, 12 May. Available at: <https://www.gov.uk/government/publications/restoring-control-over-the-immigration-system-white-paper> (Accessed: 17 September 2026).
- 215 For a detailed explanation of this vision, cfr. Iván Chaar López's book "The Cybernetic Border", which investigates how cybernetic ideas historically informed how border surveillance and management technologies have been conceived of and adopted, from the Vietnam War to today's autonomous towers at the Southern US border. Source: López, I.C. (2024) *The Cybernetic Border: Drones, Technology, and Intrusion*. Duke University Press. Available at: <https://www.dukeupress.edu/the-cybernetic-border> (Accessed: 17 September 2026).
- 216 Government Digital Service (2025) 'Get an electronic travel authorisation (ETA) to visit the UK', GOV.UK, 28 May. Available at: <https://www.gov.uk/eta> (Accessed: 17 September 2026).
- 217 Government Digital Service (2025) 'eVisas: access and use your online immigration status', GOV.UK, 15 July. Available at: <https://www.gov.uk/evisa> (Accessed: 17 September 2026).
- 218 "Full Spectrum Dominance" is a US military doctrine that has been highly influential in the development of the foundational notions of contemporary border surveillance assemblages, both in the US and EU. It preaches the complete mastery and domination of the battlefield through pervasive, real-time information and data-driven analysis. For a deeper dive, see: Hayes, B. (2009) *NeoConOpticon. The EU Security-Industrial Complex*. Statewatch and the Transnational Institute. Available at: <https://www.statewatch.org/media/documents/analyses/neoconopticon-report.pdf> (Accessed: 17 September 2026).
- 219 Ilston, G. (2008) 'Technology brought in to strengthen Britain's borders', *Police Professional*. Available at: <https://policeprofessional.com/news/technology-brought-in-to-strengthen-britain%C2%92s-borders/> (Accessed: 17 September 2026).
- 220 Boswell, C. and Besse, J. (2023) 'The strange resilience of the UK e-Borders programme: Technology hype, failure and lock-in in border control', *Security Dialogue*, 54(4), pp. 395–413. Available at: <https://journals.sagepub.com/doi/full/10.1177/09670106231182833> (Accessed: 17 September 2026).
- 221 UK Parliament (n.d.) 'PAC warns on staggering cost of Home Office border security tech failures', *Parliament.uk*. Available at: <https://committees.parliament.uk/work/919/digital-services-at-the-border/news/152344/pac-warns-on-staggering-cost-of-home-office-border-security-tech-failures/> (Accessed: 17 September 2026).
- 222 Dearden, L. (2025) 'Revealed: Conservatives spent £134m on never-used IT systems for failed Rwanda scheme', *The Guardian*, 18 January. Available at: https://www.theguardian.com/world/2025/jan/18/revealed-conservatives-spent-134m-on-never-used-it-systems-for-failed-rwanda-scheme?CMP=Share_iOSApp_Other (Accessed: 17 September 2026).
- 223 Open Rights Group (2025) *Exclusion by design report*. Available at: <https://www.openrightsgroup.org/app/uploads/2025/12/Exclusion-by-Design-Report.pdf> (Accessed: 17 September 2026).
- 224 Harvard University Press (n.d.) *The Black Box Society*. Harvard University Press. Available at: <https://www.hup.harvard.edu/books/9780674970847> (Accessed: 17 September 2026).
- 225 Prof. Van Isacker shared it with Open Rights Group ahead of publication on the ICO's repository.

- 226 Cabinet Office, Department for Science, Innovation and Technology and Government Digital Service (n.d.) 'Find out how algorithmic tools are used in public organisations', GOV.UK. Available at: <https://www.gov.uk/algorithmic-transparency-records> (Accessed: 17 September 2026).
- 227 Ungood-Thomas, J. (2024) 'Warnings AI tools used by government on UK public are 'racist and biased'', *The Guardian*, 25 August. Available at: <https://www.theguardian.com/technology/article/2024/aug/25/register-aims-to-quash-fears-over-racist-and-biased-ai-tools-used-on-uk-public> (Accessed: 17 September 2026).
- 228 Booth, R. (2024) 'UK government failing to list use of AI on mandatory register', *The Guardian*, 28 November. Available at: <https://www.theguardian.com/technology/2024/nov/28/uk-government-failing-to-list-use-of-ai-on-mandatory-register> (Accessed: 17 September 2026).
- 229 Public Law Project (2023) 'The Tracking Automated Government register', *Public Law Project*, 12 February. Available at: <https://publiclawproject.org.uk/resources/the-tracking-automated-government-register/> (Accessed: 17 September 2026).
- 230 Or, as put by the Home Office in reply to Christoforou's FOI request, "The 'public interest' is not necessarily the same as what interests the public".
- 231 ASGI (2024) *PRAB report September to December 2023*. Available at: <https://www.asgi.it/wp-content/uploads/2024/02/PRAB-Report-September-to-December-2023--final.pdf> (Accessed: 17 September 2026).
- 232 Crerar, P. and Syal, R. (2025) 'Starmer urges Europe's leaders to curb ECHR to halt rise of far right', *The Guardian*, 9 December. Available at: <https://www.theguardian.com/law/2025/dec/09/starmer-urges-europe-leaders-update-echr-halt-rise-far-right> (Accessed: 17 September 2026).
- 233 Council of Europe (2026) 'Council of Europe foreign ministers adopt political declaration on the ECHR and migration', *Council of Europe*, 21 May. Available at: <https://www.coe.int/en/web/portal/-/council-of-europe-foreign-ministers-adopt-political-declaration-on-the-echr-and-migration> (Accessed: 17 September 2026).
- 234 Seddon, P and Casciani, D (2025) 'European ministers back ECHR plan to tackle illegal migration', *BBC News*. Available at: <https://www.bbc.com/news/articles/cx2g03gv2z6o> (Accessed: 17 September 2026).
- 235 Staff reporter (2026) 'Rightwing MEPs chant 'send them back' after controversial deportation plans are passed – video', *The Guardian*, 18 June. Available at: <https://www.theguardian.com/world/video/2026/jun/18/rightwing-meps-chant-send-them-back-deportation-plans-passed-video> (Accessed: 17 September 2026).
- 236 May, A.C. and Czymara, C.S. (2024) 'Careless whisper: Political elite discourses activate national identities for far-right voting preferences', *Nations and Nationalism*, 30(1), pp. 90–109. Available at: <https://onlinelibrary.wiley.com/doi/10.1111/nana.12985> (Accessed: 17 September 2026).
- 237 Krause, W. Cohen, D, and Abou-Chadi, T.(2023) 'Does accommodation work? Mainstream party strategies and the success of radical right parties', *Political Science Research and Methods* (Cambridge Core), January. Available at: <https://www.cambridge.org/core/journals/political-science-research-and-methods/article/does-accommodation-work-mainstream-party-strategies-and-the-success-of-radical-right-parties/5C3476FCD26B188C7399ADD920D71770> (Accessed: 17 September 2026).
- 238 Hankinson, S. (2025) 'AI critical weapon deporting migrants who treat the law optional', *Heritage*. Available at: <https://www.heritage.org/border-security/commentary/ai-critical-weapon-deporting-migrants-who-treat-the-law-optional> (Accessed: 17 September 2026).
- 239 Shahbaz, A. (2025) 'Trump's immigration crackdown is built on AI surveillance and disregard for due process', *Bulletin of the Atomic Scientists*, 21 May. Available at: <https://thebulletin.org/2025/05/trumps-immigration-crackdown-is-built-on-ai-surveillance-and-disregard-for-due-process/> (Accessed: 17 September 2026).
- 240 Singler, S. (2024) 'How to rethink tech in migration', *AlgorithmWatch*. Available at: <https://algorithmwatch.org/en/how-to-rethink-tech-in-migration/> (Accessed: 17 September 2026).
- 241 Chief among them, Prime Minister Keir Starmer — who however came to "deeply regret" his comments. Source: Mason, R. (2025) 'Keir Starmer says he 'deeply regrets' island of strangers speech', *The Guardian*, 27 June. Available at: <https://www.theguardian.com/politics/2025/jun/27/keir-starmer-says-he-deeply-regrets-island-of-strangers-speech> (Accessed: 17 September 2026).
- 242 Carroll, M. (2025) 'UK to become AI maker not taker says Sir Keir Starmer', *Sky News*. Available at: <https://news.sky.com/story/uk-to-become-ai-maker-not-taker-says-sir-keir-starmer-13381107> (Accessed: 17 September 2026).
- 243 Stewart, H. (2026) 'NHS and MoD will be urged to buy British tech to drive growth amid Iran crisis', *The Guardian*, 14 March. Available at: <https://www.theguardian.com/business/2026/mar/14/nhs-ministry-of-defence-buy-british-tech-kickstart-growth-artificial-intelligence-rachel-reeves> (Accessed: 17 September 2026).
- 244 SovAI (n.d.) 'UK sovereign AI fund: backing British AI startups', *UK Sovereign AI Fund*. Available at: <https://www.sovereignai.gov.uk/> (Accessed: 17 September 2026).
- 245 A pittance compared to the size of the industry — which, according to the AI Sector Study 2024 commissioned by the government, produced a revenue of £23.9 billion in the UK alone — and the UK's sovereign infrastructure requirements. Source: Department for Science, Innovation & Technology (2024) *Artificial Intelligence sector study 2024*. Available at: <https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2024/artificial-intelligence-sector-study-2024> (Accessed: 17 September 2026).
- 246 Department for Science, Innovation & Technology(2026) *AI Opportunities Action Plan: One Year On*. Available at: <https://www.gov.uk/government/publications/ai-opportunities-action-plan-one-year-on/ai-opportunities-action-plan-one-year-on> (Accessed: 17 September 2026).
- 247 Palantir is the target of several civil society campaigns (among them, Amnesty International's — and The Good Law Project's —). Protesters repeatedly voiced their concerns, while the Financial Times reported in April 2026 that "A growing number of NHS staff are refusing to work on Palantir's health data platform over

- ethical concerns about the controversial US tech company". As a result, ministers have been seeking advice on scrapping Palantir's contract with the NHS. Sources: Amnesty International UK (n.d.) 'No Palantir in our NHS', *Amnesty International UK*. Available at: <https://www.amnesty.org.uk/issues/international-crisis/no-palantir-in-our-nhs/> (Accessed: 17 September 2026). Good Law Project (2025) 'Stop Palantir in the NHS', *Good Law Project*, 1 December. Available at: <https://goodlawproject.org/campaign/stop-palantir-in-the-nhs/> (Accessed: 17 September 2026). Draper, J. (2023) 'Protesters blockade office of tech giant', *Yahoo! News UK*. Available at: <https://uk.news.yahoo.com/protesters-blockade-london-office-tech-095008719.html> (Accessed: 17 September 2026). Hogarth, A. (2026) 'Anti-AI protesters pressure City Council against Palantir integration with NHS', *ShefNews*, 12 March. Available at: <https://shefnews.co.uk/index.php/2026/03/12/anti-ai-protesters-pressure-city-council-against-palantir-integration-with-nhs/> (Accessed: 17 September 2026). Hughes, L. (2026) 'NHS staff boycott Palantir's data platform over ethical concerns', *Financial Times*. Available at: <https://www.ft.com/content/dbb67083-bd1d-46e9-b196-1438d54c5795?syn-25a6b1a6=1> (Accessed: 17 September 2026). Wright, O. and Hayward, E. (2026) 'Ministers seek advice on scrapping Palantir NHS data contract', *The Times*, 30 March. Available at: <https://www.thetimes.com/uk/healthcare/article/palantir-data-contract-nhs-prj8j9tm> (Accessed: 17 September 2026).
- 248 Foreign vendors the UK relies on include Microsoft, AWS, Oracle, IBM, Google, and Fujitsu. Sources: Department for Digital, Culture, Media and Sport (2024) 'Research on UK managed service providers', *GOV.UK*. Available at: <https://www.gov.uk/government/publications/research-on-managed-service-providers/research-on-uk-managed-service-providers> (Accessed: 17 September 2026).
- 249 Rikap, C., Durand, C., Paraná, E., Gerbaudo, P. and Marx, P. (2024) *Reclaiming digital sovereignty: A roadmap to build a digital stack for people and the planet*. London: UCL Institute for Innovation and Public Purpose. Available at: <https://discovery.ucl.ac.uk/10202865/> (Accessed: 17 September 2026).
- 250 Robinson, N.J. (2026) 'Palmer Luckey Is Our Most Terrifyingly Deranged Billionaire', *Current Affairs*, 31 March. Available at: <https://www.currentaffairs.org/news/palmer-luckey-is-our-most-terrifyingly-deranged-billionaire> (Accessed: 17 September 2026). Menard, C. (2026) 'Decoding the Technofascist Tendency in Palantir's Manifesto', *Byline Times*, 30 April. Available at: <https://bylinetimes.com/2026/04/30/decoding-the-technofascist-tendency-in-palantirs-manifesto/> (Accessed: 17 September 2026).
- 251 Poyares, M. (2025) 'Migrant data extractivism: Tech and borders at the limit of rights', *International Migration*, 63(4), e70065. Available at: <https://onlinelibrary.wiley.com/doi/10.1111/imig.70065> (Accessed: 17 September 2026).
- 252 Rikap, C., Durand, C., Paraná, E., Gerbaudo, P. and Marx, P. (2024) *Reclaiming digital sovereignty: A roadmap to build a digital stack for people and the planet*. London: UCL Institute for Innovation and Public Purpose. Available at: <https://discovery.ucl.ac.uk/10202865/> (Accessed: 17 September 2026).
- 253 Open Rights Group (2026) 'Home Office use of AI in asylum cases likely to be unlawful, legal opinion finds', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/press-releases/home-office-use-of-ai-in-asylum-cases-likely-to-be-unlawful-legal-opinion-finds/> (Accessed: 17 September 2026).
- 254 Section 80, Schedule 6. Source: Department for Digital, Culture, Media and Sport (2025) 'Data (Use and Access) Act factsheet: UK GDPR and DPA', *GOV.UK*, 27 June. Available at: <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa> (Accessed: 17 September 2026).
- 255 According to the Act's factsheet, "safeguards must include providing data subjects with information about significant decisions made about them and must enable individuals to make representations about them, challenge them and obtain human intervention in the taking of the decision" Source: Department for Digital, Culture, Media and Sport (2025) 'Data (Use and Access) Act factsheet: UK GDPR and DPA', *GOV.UK*, 27 June. Available at: <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa> (Accessed: 17 September 2026).
- 256 More precisely, grounds for exemption are detailed in 50C(4), and include:
- a) to avoid obstructing an official or legal inquiry, investigation or procedure
 - b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
 - c) to protect public security
 - d) to safeguard national security
 - e) to protect the rights and freedoms of others".
- 257 Moreno, D.N. and Melton, C. (2025) 'The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - DM in Law Enforcement and National Security', *Kennedys Law LLP*, 2 July. Available at: <https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-adm-in-law-enforcement-and-national-security/> (Accessed: 17 September 2026).
- 258 Pratt, G., Gillert, A., Kotecha, A. and Gordon, I. (2025) 'UK data reforms unpacked: implications for AI and other automated decision-making', *Freshfields*, 8 July. Available at: <https://technologyqu海岸.freshfields.com/post/102krow/uk-data-reforms-unpacked-implications-for-ai-and-other-automated-decision-making> (Accessed: 17 September 2026).
- 259 New York State Bar Association - NYSBA (2023) 'Automation Nation: What Happens When Algorithms Decide Entry for Immigrants and Refugees?', *New York State Bar Association - NYSBA*, 17 February. Available at: https://nysba.org/automation-nation-what-happens-when-algorithms-decide-entry-for-immigrants-and-refugees/?srsltid=AfmBOorKH9Im_DZ3M69lWnRLvsJrMsd8bDdY1fjQPW795mRHSilJbUIK (Accessed: 17 September 2026).
- 260 Javed, A., Aftab, R. and Abdul Azeez, I. A. (2025) 'Artificial intelligence (AI) in border control: Opportunity or threat? An analysis of artificial intelligence practices in controlling border', **Spectrum of Engineering Sciences**. Zenodo, version 1, 24 November. Available at: <https://doi.org/10.5281/zenodo.17696082>

- 261 Boutier, I. (2024) *AI for migration processes: A focus on the United Kingdom's approach*. UN Human Rights Office. Available at: <https://researchonline.gcu.ac.uk/ws/portalfiles/portal/90546613/90516604.pdf> (Accessed: 17 September 2026).
- 262 European Digital Rights (EDRI) (2024) '#ProtectNotSurveil: The EU AI Act fails migrants and people on the move', *European Digital Rights (EDRI)*, 13 March. Available at: <https://edri.org/our-work/protect-not-surveil-eu-ai-act-fails-migrants-people-on-the-move/> (Accessed: 17 September 2026).
- 263 Maxwell, J. and Tomlinson, J. (2022) *Experiments in Automating Immigration Systems*. Bristol: Bristol University Press. ISBN 978-1-5292-1984-5. Available at: <https://bristoluniversitypress.co.uk/experiments-in-automating-immigration-systems>
- 264 Baynes, C. (2019) 'Government 'deported' 7,000 foreign students after falsely accusing them of cheating in English language tests', *The Independent*, 14 June. Available at: <https://www.independent.co.uk/news/uk/politics/home-office-mistakenly-deported-thousands-foreign-students-cheating-language-tests-theresa-may-windrush-a8331906.html> (Accessed: 17 September 2026).
- 265 Kundaliya, D. (2019) 'System used to filter UK visa applications is biased, migrant rights groups claim', *Computing*, 30 October. Available at: <https://www.computing.co.uk/news/3083201/ai-home-office-visa> (Accessed: 28 September 2026).
- 266 Narita, K. (2024) *The digital hostile environment: migration and technology*. Doctoral thesis. Goldsmiths, University of London. Available at: <https://research.gold.ac.uk/id/eprint/38044/> (Accessed: 28 September 2026).
- 267 In February 2026, the Guardian wrote about a 26 years old software engineer of South Asian heritage arrested at his doorstep, handcuffed and held in custody for "nearly 10 hours" because an automated face recognition software mistakenly identified him with the suspect of a £3,000 burglary "100 miles away". Source: Booth, R. and Wilding, M. (2026) 'Facial recognition error prompts police to arrest Asian man for burglary 100 miles away', *The Guardian*, 25 February. Available at: <https://www.theguardian.com/technology/2026/feb/25/facial-recognition-error-prompts-police-to-arrest-asian-man-for-burglary-100-miles-away> (Accessed: 17 September 2026).
- 268 Affecting, for example, a grandmother from Tennessee, jailed for 5 months by the North Dakota police after AI-based face recognition linked her to crimes committed in the state – which she says she has never visited, and a man from Brooklyn, jailed for two days after being mistakenly identified as responsible for a flashing incident by automated face recognition software, "even though he was about eight inches taller and 70 pounds heavier than the flasher described by the victim". Sources: Sottile, Z. (2026) 'Police used AI facial recognition to arrest a Tennessee woman for crimes committed in a state she says she's never visited', *CNN*, 29 March. Available at: <https://edition.cnn.com/2026/03/29/us/angela-lipps-ai-facial-recognition> (Accessed: 17 September 2026). Stack, L. (2025) 'A wrongful arrest and worry about the accuracy of a police tool', *The New York Times*, 27 August. Available at: <https://www.nytimes.com/2025/08/27/nyregion/a-wrongful-arrest-and-worry-about-the-accuracy-of-a-police-tool.html> (Accessed: 17 September 2026).
- 269 Taylor, D. (2026) 'Two dead and one missing after trying to cross Channel to UK', *The Guardian*, 1 April. Available at: <https://www.theguardian.com/uk-news/2026/apr/01/dead-missing-after-trying-to-cross-channel-to-uk> (Accessed: 17 September 2026).
- 270 Danes je nov dan (EDRI) (2025) 'The AI Act isn't enough - European Digital Rights (EDRI)', *European Digital Rights (EDRI)*, 13 November. Available at: <https://edri.org/our-work/the-ai-act-isnt-enough-closing-the-dangerous-loopholes-that-enable-rights-violations/> (Accessed: 17 September 2026).
- 271 Cabinet Office (2025) 'National Security Strategy 2025: Security for the British People in a Dangerous World (HTML)', GOV.UK. Available at: <https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html> (Accessed: 17 September 2026).
- 272 Open Rights Group (2025) 'Written evidence submitted by Open Rights Group (BSAI0011)', *Human Rights (Joint Committee)*, UK Parliament, 22 May. Available at: <https://committees.parliament.uk/writtenevidence/140204/pdf/> (Accessed: 17 September 2026).
- 273 The Bill introduces powers to seize mobile phones from migrants, plus new offences related to small boat crossings. However, a detailed briefing published by the House of Commons Library argues that "the bill's impact assessment marks" the "expected impact" of these measures as "uncertain", "saying it wasn't possible to make a well-evidenced assessment. It says the UK would be the first country to try these methods and there isn't baseline evidence to estimate their potential success." Source: House of Commons Library (2025.) 'Border Security, Asylum and Immigration Bill 2024-25' *House of Commons Library briefing*. Available at: <https://researchbriefings.files.parliament.uk/documents/CBP-10185/CBP-10185.pdf> (Accessed: 17 September 2026).
- 274 The amendment was however not moved. Source: Hamwee, Baroness (with German, Lord) (2025) 'Baroness Hamwee's amendment, After Clause 48: Amendment 195', *Parliamentary Bills*, UK Parliament. Available at: <https://bills.parliament.uk/bills/3929/stages/19956/amendments/10024522> (Accessed: 17 September 2026).
- 275 Introduced in 2018 and only amended in 2024 after a long legal battle by the Open Rights Group and the 3million, an "immigration exemption" to data protection law allowed the Home Office to curb data rights if complying with them could result in prejudice to immigration control. Before being ruled unlawful under the Data Protection Act, the Home Office applied the exemption in 60% of immigration-related data requests. Even though the exemption can only be applied on a case-by-case basis, when necessary and proportionate, recording the reasons for adopting it and informing the data subject of its adoption, campaigners argue that "the Government did not implement any mechanism to enhance monitoring and accountability over how they are applying safeguards in practice and limitations required by Article 23(2) of the UK GDPR". These include the storage period, the category of data being included in the scope of the restrictions and the additional

- safeguards to prevent abuse of this exemption. Sources: Open Rights Group (n.d.) "Immigration exemption" ruled unlawful under GDPR', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/campaign/immigration-exemption-campaign-page/> (Accessed: 17 September 2026). Information Commissioner's Office (ICO) (2025) 'Immigration exemption: a guide', *ICO*, 9 October. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/> (Accessed: 17 September 2026). Alsherif, S. (2024) 'Government does the bare minimum to update the Immigration Exemption', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/blog/government-does-the-bare-minimum-on-the-immigration-exemption/> (Accessed: 17 September 2026).
- 276 Thus inverting the presumption of innocence for immigrants, who are effectively guilty – rather than innocent – until proven otherwise. AI and automation, as put by Indira Boutier, can be powerful tools to bring about such perversion of the law. Sources: Boutier, I. (2024) *AI for migration processes: A focus on the United Kingdom's approach*. UN Human Rights Office. Available at: <https://researchonline.gcu.ac.uk/ws/portalfiles/portal/90546613/90516604.pdf> (Accessed: 17 September 2026).
- 277 Alsherif, S. (2024) 'Why Migrants Need Digital Sanctuary', *Open Rights Group*. Available at: <https://www.openrightsgroup.org/blog/why-migrants-need-digital-sanctuary/> (Accessed: 17 September 2026).
- 278 Home Office (2026) 'Immigration Enforcement: Live Facial Recognition Legal Mandate 2.0', *GOV.UK*. Available at: https://assets.publishing.service.gov.uk/media/699c6110882eb23165f12753/IE_LFR_Legal_Mandate_2.0.pdf (Accessed: 17 September 2026).
- 279 Ibid.
- 280 Home Office (2026) Equality Impact Assessment: facial recognition v2.0. Available at: https://assets.publishing.service.gov.uk/media/699c7d0031713b50fd49c074/OFF_SEN_-_EIA_Facial_Recognition_V2.0_1_.pdf (Accessed: 17 September 2026).
- 281 Home Office (2026) *Immigration Enforcement: Live Facial Recognition Standard Operating Procedures v2.0*. Available at: https://assets.publishing.service.gov.uk/media/699c60f38eef11b95e49c036/IE_LFR_SOP_V2.0.pdf (Accessed: 17 September 2026).
- 282 Dodd, V. (2026) 'Police AI chief admits crime-fighting tech will have bias but vows to tackle it', *The Guardian*, 24 February. Available at: <https://www.theguardian.com/technology/2026/feb/24/police-ai-chief-admits-crime-fighting-tech-will-have-bias-but-vows-to-tackle-it> (Accessed: 17 September 2026).
- 283 Even more interestingly, both the legal mandate for the LFR pilots and Murray's statement were produced in February 2026. Just two months prior, the Home Office admitted that face recognition technology "is more likely to incorrectly identify black and Asian people than their white counterparts on some settings", reported the Guardian. Even more interestingly, the newspaper and Liberty Investigates found that UK police forces lobbied to use retrospective face recognition searches even though officials knew that the technology was biased: "Documents seen by the Guardian and Liberty Investigates reveal that the bias has been known about for more than a year – and that police forces argued to overturn an initial decision designed to address it." Sources: Syal, R. (2025) 'Home Office admits facial recognition tech issue with black and Asian subjects', *The Guardian*, 5 December. Available at: <https://www.theguardian.com/technology/2025/dec/05/home-office-facial-recognition-tech-issue-black-asian-subjects> (Accessed: 17 September 2026). Wilding, M. and Boffey, D. (2025) 'UK police forces lobbied to use biased facial recognition technology', *The Guardian*, 10 December. Available at: <https://www.theguardian.com/technology/2025/dec/10/police-facial-recognition-technology-bias> (Accessed: 17 September 2026).
- 284 A safeguard which, as seen before, is being both eroded (eg: the Active Human Review Exemption in the DUA Act) and ignored (eg: in the case of the wrongful arrests described in footnotes 232 and 233).
- 285 Big Brother Watch (2025) 'Stop Facial Recognition', *Big Brother Watch*, 9 December. Available at: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> (Accessed: 17 September 2026).
- 286 Statewatch (2026) 'Submission to Home Office consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies', *Statewatch*, 16 February. Available at: <https://www.statewatch.org/news/2026/february/submission-to-home-office-consultation-on-a-new-legal-framework-for-law-enforcement-use-of-biometrics-facial-recognition-and-similar-technologies/> (Accessed: 17 September 2026).
- 287 Wilding, M. and Booth, R. (2026) 'Essex police pause facial recognition camera use after study finds racial bias', *The Guardian*, 20 March. Available at: <https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias> (Accessed: 17 September 2026).
- 288 The report focussed on NEC's NeoFace V4 solution, adopted both by police forces throughout the UK and in the pilots for immigration enforcement at UK ports.
- 289 More precisely, when the face match threshold – which determines the accuracy with which faces are matched by the system – is 0.64 or higher ("Higher settings reduce errors but yield fewer face matches while lower settings give more matches with less accuracy",). Sources: Gikay, A.A. (2025) 'Policing facial recognition – between risks, misconceptions, and the need for a more honest debate', *EU Law Analysis*, 25 September. Available at: <https://eulawanalysis.blogspot.com/2025/09/> (Accessed: 17 September 2026).
- 290 AI Now Institute (2023) *Regulating biometrics*. Available at: <https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-fussey-murray.pdf> (Accessed: 17 September 2026).
- 291 Big Brother Watch (2026) 'High Court to hear landmark legal challenge against police live facial recognition', *Big Brother Watch*, 27 January. Available at: <https://bigbrotherwatch.org.uk/press-releases/high-court-to-hear-landmark-legal-challenge-against-police-live-facial-recognition/> (Accessed: 17 September 2026).

- 292 Stelter, B. (2026) 'US downgraded in democracy index as press freedom concerns grow', *CNN*, 18 March. Available at: <https://edition.cnn.com/2026/03/18/media/trump-vdem-democracy-media-report> (Accessed: 17 September 2026).
- 293 Mansoor, S. (2026) 'How ICE is using facial recognition in Minnesota', *The Guardian*, 27 January. Available at: <https://www.theguardian.com/technology/2026/jan/27/ice-facial-recognition-minnesota> (Accessed: 17 September 2026).
- 294 For example, ICE-style deportations have been promised by the Reform UK party were it to secure a win in the next general election. Source: Elgot, J. (2026) 'Reform would create ICE-style agency and end leave to remain, Zia Yusuf to say', *The Guardian*, 22 February. Available at: <https://www.theguardian.com/politics/2026/feb/22/reform-uk-ice-style-agency-end-leave-to-remain-zia-yusuf> (Accessed: 17 September 2026).
- 295 Haidari-Garmash, A. (2026) 'AI Immigration Error: Woman's Job "Hallucinated" by Canada', *RCIC News*, 25 March. Available at: <https://rcicnews.com/2026/03/ai-immigration-error-woman-s-job-hallucinated-by-canada> (Accessed: 17 September 2026). Swain, G. (2025) 'OpenAI admits AI hallucinations are mathematically inevitable, not just engineering flaws', *Computerworld*, 18 September. Available at: <https://www.computerworld.com/article/4059383/openai-admits-ai-hallucinations-are-mathematically-inevitable-not-just-engineering-flaws.html> (Accessed: 17 September 2026).
- 296 Syal, R. (2026) 'Refugee status to be temporary as Shabana Mahmood rips up rules on UK asylum', *The Guardian*, 1 March. Available at: <https://www.theguardian.com/uk-news/2026/mar/01/shabana-mahmood-to-limit-refugees-to-30-months-in-uk> (Accessed: 17 September 2026).