Alice Fill

DIGITAL PATROLLING

Emerging Bordering Practices around Europe

PREMIO CESARE ALFIERI CUM LAUDE • 2023

FIRENZE
UNIVERSITY
PRESS

PREMIO CESARE ALFIERI «CUM LAUDE»

ISSN 2612-8063 (PRINT) - ISSN 2704-5730 (ONLINE)

– 11 –

PREMIO CESARE ALFIERI «CUM LAUDE»

Alice Fill

Digital Patrolling

Emerging Bordering Practices around Europe

FIRENZE UNIVERSITY PRESS
2025

Digital Patrolling : emerging Bordering Practices around Europe / Alice Fill. – Firenze : Firenze University Press, 2025.
(Premio Cesare Alfieri «Cum Laude» ; 11)

https://books.fupress.com/isbn/9791221505771

ISSN 2612-8063 (print)
ISSN 2704-5730 (online)
ISBN 979-12-215-0576-4 (Print)
ISBN 979-12-215-0577-1 (PDF)
ISBN 979-12-215-0578-8 (ePUB)
ISBN 979-12-215-0579-5 (XML)
DOI 10.36253/979-12-215-0577-1

Graphic design: Alberto Pizarro Fernández, Lettera Meccanica SRLs
Front cover image: © wirestock|123rf.com

Peer Review Policy
Peer-review is the cornerstone of the scientific evaluation of a book. All FUP's publications undergo a peer-review process by external experts under the responsibility of the Editorial Board and the Scientific Boards of each series (DOI 10.36253/fup_best_practice.3).

Referee List
In order to strengthen the network of researchers supporting FUP's evaluation process, and to recognise the valuable contribution of referees, a Referee List is published and constantly updated on FUP's website (DOI 10.36253/fup_referee_list).

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Published by Firenze University Press
Firenze University Press
Università degli Studi di Firenze
via Cittadella, 7, 50144 Firenze, Italy
www.fupress.com

This book is printed on acid-free paper
Printed in Italy

Table of contents

Forward 7

Acronyms and abbreviations 9

Introduction 11
- 1. Digital, mobile, and smart 11
- 2. A look at the literature: digitalisation, borders, and emerging perspectives 14
- 3. Methodological considerations: a comparative and multidisciplinary perspective on digital patrolling 16
- 4. Structure of the book and case studies selection 18

Chapter 1
Digital patrolling at EU borders 21
- 1.1. Digitalising the EU borders 21
- 1.2. Defining 'digital patrolling' along smart borderwork 24
- 1.3. Situational awareness, detection, and tracking: conflicting rationales and multipurpose technologies 31
- 1.4. Information management and risk analysis: beyond filtering and pre-empting mobility 36
- 1.5. The future of digital patrolling: towards a new role for automation? 40

Chapter 2
Digital patrolling in Greece: drones flying over sea and land borders 45
- 2.1. Setting the scene: digitalisation, militarization, and experimentation 45
- 2.2. Strategic frontiers: the Evros River, the Aegean Sea, and the Turkish side of the story 47

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

2.3. National and European priorities and funding 50
2.4. Deploying drones: Frontex, EMSA, and national authorities 52
2.5. Delineating the use of drones for border patrols: a rhizomatic and vanishing regulatory framework 54
2.6. The use of drones in endemic border violence: the case of pushbacks 62

Chapter 3
Situational awareness and border enforcement in Spain: the *Sistema Integrado de Vigilancia Exterior* (SIVE) 67
3.1. Surveillance at the Pillars of Hercules and beyond: securitisation and digitalisation of Spanish border control policies 67
3.2. Deployment and maintenance: the costs of one of Europe's largest surveillance systems 72
3.3. The *Sistema Integrado de Vigilancia Exterior* in practice: situational awareness, detection, and risk analysis 74
3.4. Drones buzzing around the SIVE? 78
3.5. The legal framework: between pushbacks, the SIVE, and drones 79

Chapter 4
Navigating national, supranational, and international spheres: between digital patrolling and fundamental rights 87
4.1. From the eastern to the western route: a comparative analysis of digital patrolling 87
4.2. Technology and the law: rights at stake in digital patrolling operations 92
4.3. Human dignity in times of de-humanised surveillance 93
4.4. The right to seek protection: *non-refoulement* between access to asylum and border surveillance 96
4.5. Data protection and privacy rights: the grey area of border zones 100
4.6. Moving forward: data rights between interoperability and AI 110
4.7. The right to non-discrimination: differentiated treatment and protected grounds 114
4.8. Keeping States accountable? Sketched considerations on jurisdiction 117

Concluding remarks and pathways forward 121

List of cases, international legal instruments, and legislation 129
List of cases 129
International legal instruments and other documents 131
European Union legislation 132
National legislation 133

References 137

Index of Names 159

Forward

This book builds upon my Master's thesis, defended in June 2022 at the University of Florence. To maintain the integrity of the original work, I have not incorporated subsequent developments or contributions to the literature. However, a couple of years later, the themes discussed in these pages seem even more pressing and relevant.

In December 2023, the European Union reached a political agreement on the new Pact on Migration and Asylum, intensifying the role of risk assessments and screening procedures in migration governance. In August 2024, the Artificial Intelligence Act came into force. While it represents a partial response to some of the questions raised in this book at the crossroads between human rights protection and technological experimentation, it nonetheless largely falls short in regulating the complexities of AI in border management. Today, the digitalisation of borders, particularly in terms of surveillance and patrolling, remains a central and growing concern.

At the same time, encouraging efforts are emerging to challenge digital patrolling practices at the European Union's external borders, with cases being brought before national and supranational courts. These cases often tell the story of tragic incidents, such as the shipwreck off the coast of Pylos, Greece, in June 2023, resulting in the deaths of over 600 people. Despite the ongoing investigation, it has become increasingly clear that the vessel was detected long before the disaster through aerial patrolling activities.

The academic debate surrounding these topics has expanded considerably and continues to shape my current research, which now focuses on the datafication of human mobility in West Africa as part of my PhD studies. The reflections in this book form the foundation of my ongoing work and mark an important step in this journey.

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

This work has greatly benefitted from the vibrant collective debate within the emerging field of digital migration studies, which explores the intersections of technology, human rights, and border practices. While I cannot mention here everyone who dedicated time to explore these questions together, I am deeply grateful. My deepest thanks go to my supervisor, Veronica Federico, for her unwavering guidance, support, and invaluable advice. I am also very grateful to Georgios Glouftsios, whose insights were precious in the early stages of this project. Special thanks to Francesco Strazzari, Francesca Capone, and Luca Raineri, whose generous mentorship has inspired me since I first stepped into a university classroom. My heartfelt appreciation goes to Peter Burgess and Alice Riccardi for their invaluable supervision during my doctoral journey, as well as for encouraging me to develop my Master's thesis into this book. I am further grateful to Davide Tomaselli for his attentive reading and his cherished friendship. Finally, I would like to thank the Guido Galli Award Committee for making this publication possible. Any remaining errors, of course, are entirely my own.

Lastly, my deepest thanks go to Giulio, my family, and my friends. Your love, care, and support sustain me every day, and I am profoundly grateful to have you by my side.

Paris, September 2024

Acronyms and abbreviations

AEPD	Agencia Española de Protección de Datos
AFSJ	Area of Freedom, Security and Justice
AI	Artificial Intelligence
AIS	Automatic Identification System
APDHA	Asociación Pro Derechos Humanos de Andalucía
sBMS	Shared Biometric Matching Service
BVMN	Border Violence Monitoring Network
CAT	Convention against Torture
CCTV	Closed-Circuit Television Cameras
CEDAW	Convention on the Elimination of all Forms of Discrimination against Women
CERD	Convention on the Elimination of Racial Discrimination
CIR	Common Identity Repository
CISE	Common Information Sharing Environment
CJEU	Court of Justice of the European Union
CSDP	Common Security and Defence Policy
CRC	United Nations Convention on the Rights of the Child
CRPD	Convention on the Rights of Persons with Disabilities
EBF	European Borders Fund
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECRIS-TCN	European Criminal Records Information System-Third Country Nationals
EDPB	European Data Protection Board
EES	Entry/Exit System
EFCA	European Fisheries Control Agency

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)
Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

EFS	EUROSUR Fusion Services
EMSA	European Maritime Safety Agency
ESP	European Search Portal
EU	European Union
EU-LISA	European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EUNAVFOR MED	European Union Naval Force in the South Central Mediterranean
EURODAC	European Dactyloscopy
EUROSUR	European Border Surveillance System
FASS	Frontex Aerial Surveillance Services
Frontex	European Border and Coast Guard Agency
GCM	UN Global Compact for Safe, Legal and Orderly Migration
GDPR	General Data Protection Regulation
GHM	Greek Helsinki Monitor
HDPA	Hellenic Data Protection Authority
IBM	Integrated Border Management
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICTs	Information and Communication Technologies
IHRL	International Human Rights Law
IOs	International Organisations
ISF	Internal Security Fund
JORA	Joint Operation Reporting Application
MID	Multiple-Identity Detector
NCC	National Coordination Centre
NIMSS	National Integrated Maritime Surveillance System
PESCO	European Union Permanent Structured Cooperation
RPAS	Remotely Piloted Aerial Vehicles
SAR	Search and Rescue Convention
SIS II	Schengen Information System II
SIVE	Sistema Integrado de Vigilancia Exterior
SOC	Surveillance Operational Centre
SOLAS	Safety of Life at Sea Convention
SPATIONAV	Sistème Naval de Surveillance des Approches Maritimes et des Zones sous Jurisdiction Nationale
STS	Science and Technology Studies
UAS	Unmanned Aircraft Service
UAVs	Unmanned Aerial Vehicles
UDHR	Universal Declaration of Human Rights
UNCLOS	UN Convention on the Law of the Sea
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa Information System

Introduction

1. Digital, mobile, and smart

The 'digitalisation' of border security, which increasingly influences migration management, is a rapidly growing global phenomenon, often justified and expedited by perceived crises surrounding human mobility. Consequently, the deployment of new technologies, devices, and systems designed to enhance surveillance, monitoring, and registration processes has become a defining feature of contemporary border and migration control.

This process unfolds globally, particularly along the divides between the Global North and the Global South. One prominent example is the USA southern border in Arizona, where Integrated Fixed Towers equipped with radars, thermal cameras, and night-vision technology monitor 'suspicious' activities from up to seven and a half miles away (Aizeki et al. 2021). In addition, since February 2022, the United States has also been trialling four-legged robotic patrol dogs along its border with Mexico (Holmes 2022). In Australia, the Border Risk Identification System, operated by the Department of Immigration and Citizenship, utilises big data analytics to identify correlations and patterns, targeting so-called 'risky travellers'. In Europe, in 2019, the European Border and Coast Guard Agency (Frontex) supported a pilot project that deployed a surveillance blimp capable of remaining airborne for forty days to monitor the seas off Samos Island (Leese, Noori, and Scheel 2021; Monroy 2022). Not far, at the border between Greece and Turkey, Long Range Acoustic Devices (LRAD), or 'sound cannons', were tested in spring 2021. These devices emit sound at volumes reaching 150 decibels – equivalent to a jet engine – posing a serious risk

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

of permanent hearing loss (Gatopoulos and Kantouris 2021). Similar systems operate along the Hungarian border, where loudspeakers broadcast warnings in Farsi, Arabic, Urdu, and Serbian, notifying would-be border crossers that they are trespassing on Hungarian territory: «I'm warning you to hold back from committing this crime» (see Cockerell 2021). Additionally, in October 2021, Poland approved the construction of a €350 million wall, intended to incorporate motion sensors as the latest frontier of border security (Joly and Sandford 2021).

The introduction of thermal cameras, motion sensors, interoperable registration systems, biometric technologies, and drones in border zones reveals more than a quantitative increase in data collection and exchange, or a shift in the performance of surveillance practices. At stake is a profound transformation in how State sovereignty is exercised at borders. Indeed, digitalisation reshapes the dynamics of international travel and mobility, altering the very concept of borders by fragmenting and dislocating them (Everuss 2021, 339). Moreover, in addition to the widespread enthusiasm for technological experimentation, these innovations drive a fundamental rethinking of one of the most tangible and on-the-ground aspects of border enforcement: patrolling.

Long regarded as a core expression of modern State sovereignty and a central function of border control, integral to the filtering and sorting processes carried out at the frontiers, the practice of patrolling is in fact undergoing significant transformation due to the proliferation of new technologies. Their diffusion often unfolds within a complex and opaque web of security practices, offering fertile ground for critical enquiry into the broader dynamics of border digitalisation.

Today, borders are increasingly both mobile and omnipresent as they are designed to sort out individuals not only at territorial frontiers but also far beyond them. As Étienne Balibar (2009) observes, we are experiencing a moment of border vacillation: borders are no longer *at the border* but increasingly outsourced or subcontracted. This shift involves complex frameworks of cooperation with third States, greater engagement of private actors, the proliferation of border agencies, and the expanding mandate of International Organisations (IOs) in border-related issues – trends further amplified by the integration of technologically advanced systems. Borders, as a result, take on new shapes. Leanne Weber's (2006) notion of «mobile borders», which captures the decoupling of border control from physical borders, illustrates this evolving landscape and highlights the pivotal role of new digital technologies in this domain.

The digitalisation of borders, exemplified by both the convergence of biometric databases and high-tech barriers – often referred to as 'smart borders' – primarily aims to enhance the efficiency of mobility control and filtering. Overall, these technologies are designed to prevent the entry of 'undesirable' individuals while facilitating seamless passage for pre-cleared travellers. Operating within a pre-emptive and anticipatory logic, they are presented as a one-size-fits-all solution for managing future indeterminate threats, positioning security measures around mobility in an increasingly proactive mode (Suchman, Follis, and Weber 2017).

Clearly, digitalisation in this field does not unfold in a political or legal vacuum. Instead, it reproduces existing power asymmetries and social hierarchies, mirroring broader drifts in migration governance that encompass restrictive procedures, practices, and legislation, which *de facto* limit access to international protection (see Pannia et al. 2018). The use of new technologies in border control is, therefore, neither neutral nor incidental, nor is it the use of *certain* technology to perform *certain* functions in a *certain* context. Rather, as technology is also socially constructed, it reflects how digitalisation is shaped by and embedded within broader governance frameworks.

While border digitalisation is a global trend, often embedded in regional initiatives that transcend national boundaries, the level of cooperation and coordination achieved in the European Union (EU) has not been replicated anywhere so far (Topak and Vives 2018). This makes the EU and its Member States, which are central to this book, especially relevant. Although efforts to harmonise border policies in regions such as North America are notable, the EU's integrated approach stands apart in both scope and impact. Thus, this study focuses on Europe, where long-standing dynamics of externalisation, criminalisation, and privatisation in border and migration management are deeply entangled with the relatively recent digitalisation process.

In the EU, the increasing interest (and investment) in next-generation border technologies, often enhanced by Artificial Intelligence (AI), warrants closer scrutiny at least for two reasons. First, the digitalisation of borders is shaped by socio-technical interactions embedded in a complex interplay between legal obligations, societal values, and technological constraints (Burgess and Kloza 2021)[1]. Especially from a human rights perspective, this makes the consequences of their integration far from straightforward and inherently multifaceted. Second, the push for *smarter* border security, driven by converging narratives and practices around technology deployment across various legal systems, extends beyond border zones. It systematically spills over into other areas of society,

[1] The emphasis on the socio-technical dimensions of smart borders stems from efforts to reconcile the long-standing debate between essentialism and instrumentalism, revitalised by the recent "new materialist" turn in critical security studies. In brief – and with the caveat that this simplification may not fully capture the nuances of these positions – essentialist perspectives assert that technological development drives social change. According to this view, the emergence of new technologies directly triggers dynamics that shape political decisions made by States and social actors (see, for instance, Schweller 2014, 116). In contrast, instrumentalism challenges technological determinism by positing that technologies are passive and neutral tools, integrated into a socially constructed reality: it is social actors who ultimately harness technology to achieve specific objectives (see, among others, Herz 1976). Scholars such as Geoffrey Herrera (2006) and Stefan Fritsch (2011) have sought to bridge these two approaches, arguing that while technological innovations carry material consequences, those consequences are embedded within a social framework where human agency remains paramount. In this study, it is argued that such a perspective – acknowledging both the particularities of new technologies and the *ensemble* of social implications of border control – is especially fruitful for examining the digitalisation of borders.

meaning that the technological experiments carried out at the borders demand particular attention due to their broader implications.

Building on these premises, the book aims to critically examine the digitalisation of borders through the lens of 'digital patrolling', contributing to the broader discourse on border surveillance and digitalisation. By adopting a comparative approach within the EU context and engaging with an emerging and dynamic body of literature, this study seeks to provide new insights into the evolving field of border digitalisation.

2. A look at the literature: digitalisation, borders, and emerging perspectives

Notably over the last decade, critical security scholars, science and technology studies (STS) researchers, and political geographers have significantly contributed to the growing body of literature that examines the impact of digitalisation on the border-crossing experience (see Amoore 2006; Bigo 2014; Dijstelbloem and Broeders 2016; Leese 2016). This vibrant and multidisciplinary debate has led to the development of new subfields, such as digital migration studies (see Candidatu, Leurs, and Ponzanesi 2019; Leurs and Smets 2018; Sandberg et al. 2022).

At the intersection of critical security studies and STS, this literature has illuminated how material allowances and constraints shape security practices[2], while also considering the subjectivity and agency of both those who *operate* the border and those who *cross* it (see Amicelle, Aradau, and Jeandesboz 2015).

Borders digitalisation has been described as a shift towards «techno-securitisation» (Marin 2016), a process of «smartening» of border security (Jeandesboz 2016), shaped by the «datafication» of mobility and migration management (Broeders and Dijstelbloem 2016), the diffusion of «techno-borderscapes» (Godin and Donà 2021), and the emergence of new forms of «dataveillance» (Degli Esposti 2014; Peoples and Vaughan-Williams 2010, 162) – defined as the monitoring and mining of multiple data types to identify potentially risky groups and individuals.

As previously mentioned, digitalisation and high technologisation of borders also fit within – and cannot be adequately understood aside from – a widely documented shift towards the criminalisation and containment of non-pre-vetted or unauthorised travellers through risk-based taxonomies, the externalisation of border control, and the outsourcing of migration management to private companies, international organisations, and third countries (see Csernatoni 2018, 177; Giuffré and Moreno-Lax 2019; Ferraris 2020; Nagore Casas 2019).

These strategies intertwine with forms of contactless, remote, and de-territorialised control, often described as preventive «*non-entrée*» policies and cooperative deterrence mechanisms, which also contribute to the shrinking of access to asylum and international protection (Mountz 2020; Tholen 2010, 273). Un-

[2] On the 'materiality turn' in migration studies and STS, see Stephan Scheel, Evelyn Ruppert, and Funda Ustek-Spilda (2019).

der this frame, increasingly hard-line and intrusive technologies for policing the European Union's periphery are being justified and encouraged. Scholars have termed this shift «the transformation of the EU into a technological fortress» (Marin 2011), describing it as a deliberate security strategy for controlling migration within «emergent, recursively performed, and mutable» digitalised borders (Glouftsios 2021a, 9).

Karolina Follis (2017) describes this approach as a project of trans-territorial expansion, enabled by technologies that facilitate surveillance and governance in previously 'unseen' spaces beyond territorial borders, in the so-called 'pre-frontier' area, encompassing seas and lands adjacent to, but outside of, EU Member State jurisdiction. In this context, digitalisation enables forms of strategic «borders manipulation» (Weber 2006, 22), allowing for the shifting of frontiers in line with evolving security priorities.

These technological innovations thus challenge the notion of borders while raising significant concerns about the safeguarding of fundamental rights of people on the move. The Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance's September 2021 report highlighted how the digitalisation of migration policies and border enforcement often occurs with little regard for human rights abuses, racially discriminatory structures, and «experimental risks» (Human Rights Council 2021, para. 35). This is even more alarming as this context diverges significantly from other domains of social life similarly affected by the expansion of technological infrastructures. Firstly, people on the move often possess fewer rights and enjoy limited legal protections. Secondly, States still retain broad discretionary authority in matters of border and immigration enforcement, powers that can be largely expansive and at least partially shielded from judicial review.

Echoing the Special Rapporteur's solicitude, at the European level, a resolution adopted by the European Parliament on 6 October 2021 concerning AI in criminal law and its use by police and judicial authorities highlighted serious concerns regarding the use of biometric data and facial recognition technologies within law enforcement practices (European Parliament 2021). These developments have in fact spurred criticism, particularly regarding the risk of indiscriminate mass surveillance in public spaces. In light of these concerns – but mindful of the significant disparity between the rapidity of technological advancements and the slower pace of legislative and regulatory frameworks – the proposed Artificial Intelligence Act recognises the need to classify AI systems used in migration, asylum, and border control as 'high-risk' (European Commission 2021, 10).

The digitalisation of border security – along with its attendant risks and potentials – has thus begun to attract attention in both academic literature and among international bodies and institutions, with discussions unfolding from diverse perspectives and across different normative schemes. Scholars have engaged with various facets of the border network, exploring the «technopolitics of border control» (Dijstelbloem 2021), the changing role of security professionals (Bigo 2014), the «dronisation» of borders (Csernatoni 2018, 178), and the deployment of satellite technologies for external border surveillance (Słomczyńska and Frankowski 2016). Other areas of enquiry include the expansion of biometric databases (Scheel 2019), the datafication of migrant populations (Broeders and Dijstelbloem 2016), the introduction of risk analysis algorithms (Amoore 2006), and the emergence of new rationalities within «deep border» regimes through machine learning (Amoore 2021; 2023). Additionally, attention has been drawn to large-scale information systems (Glouftsios 2021b), digital mapping interfaces aimed at visualising border zones and transboundary flows (Tazzioli and Walters 2016), and the discriminatory outcomes engendered by the datafication in this field (Leurs and Shepherd 2017; Broeders and Dijstelbloem 2016). On the other hand, human rights bodies have underscored the 'protection crisis' that the digitalisation process risks exacerbating.

3. Methodological considerations: a comparative and multidisciplinary perspective on digital patrolling

While patrolling is not absent from these discussions on border digitalisation, its transformations have rarely been treated as a distinct and essential lens of analysis. This work seeks to address this gap expanding the research agenda in this field. The value of this focus lies in exposing the frictions and contradictions within State-led border patrol activities, where security logics and border violence intersect with humanitarian aims, such as coordinating search and rescue operations at sea.

Within the scope of this analysis, digital patrol systems refer to a wide range of technologies deployed at and before the borders, including unmanned aircraft, drones, satellites, offshore sensors, thermal cameras, radars, autonomous surveillance towers equipped with infra-red cameras, high-resolution imagery, smart walls, and geographic information systems. It should be noted that this conceptualisation of patrolling deliberately centres on State-led activities in border control, which overlap significantly with migration management. Patrols conducted by non-State actors, including humanitarian organisations, are thus beyond the scope of the study[3]. Focusing on the European Union, the book endeavours to define and preliminarily classify the forms of digital patrolling implemented at various stages of *borderwork*[4]. It is thus based on the analysis of diverse 'bordering' strategies at both European and national levels showcasing the digitalisation of patrolling activities, with a particular emphasis on drone deployment at external borders and the functioning of integrated surveillance systems[5].

[3] For example, the work of AlarmPhone, particularly the Alarm Phone Sahara (2021) division, is noteworthy. This group periodically organises solidarity patrol operations in the Sahara Desert to locate and rescue migrant people in distress.

[4] Chris Rumford (2008) effectively describes 'borderwork' as the process of «envisioning, constructing, maintaining and erasing borders».

[5] On the relevance of the term 'bordering' to analytically capture the continuous processes of fixating and regulating mobility, see Nina Amelung, Rafaela Granja, Helena Machado (2021) and Martina Tazzioli (2018).

This research focuses on three central aspects. Firstly, it seeks to define and contextualise digital patrolling, tracing its proliferation across the EU's external borders. Secondly, it examines how and under which conditions Member States are advancing digital patrolling strategies and technologies as part of their broader border digitalisation efforts, specifically through a comparative analysis of this phenomenon in Spain and Greece. Finally, the study investigates the implications of digital patrolling for the rights of people on the move, expanding the analysis from the case studies to both European and international levels. Thus, it is questioned whether legal frameworks in place – national, European, and international – provide sufficient safeguards against the risks posed by digital patrolling, or whether they are instead facilitating indiscriminate digitalisation at the borders while being largely devoid of necessary protection measures.

This research adopts a multidisciplinary approach, engaging with a broad range of literature and sources. It draws on an extensive review of both primary and secondary materials, encompassing national and EU legislation, case law, reports, and policy documents. The triangulation of diverse materials is crucial for uncovering patterns, paradoxes, and rationales that reveal far-reaching and persistent tendencies, often greater in scope than individual data points might suggest. While not claiming exhaustive coverage, this approach resembles the construction of a mosaic, where each component contributes to a more complex and nuanced picture.

Of course, examining specific technologies, national policies, and legal frameworks within a meaningful and coherent dialogue presents significant challenges. To address such complexities, the study adopts a comparative perspective that builds conceptual bridges across disciplines and spaces[6]. Indeed, the comparative perspective inherently favours the integration of multidisciplinary approaches by examining diverse legal systems, cultures, and practices, thereby supporting a dynamic understanding of how different disciplines interact within specific legal contexts. As socio-legal methodologies suggest, a comparative approach is especially valuable when addressing cross-border technological issues, as it integrates non-legal knowledge into legal research, fostering a form of «methodological pluralism» that surfaces the global challenges underlying local developments (see Guerra 2018; Scarciglia 2015). In this sense, this book not only aims to advance the literature on digital patrolling but also to offer insights into the broader processes of border digitalisation within the European Union, through the analysis of the key case studies of Greece and Spain.

Engaging with this complexity offers significant promise: if digital borders are increasingly invasive and pervasive compared to physical barriers like barbed wire, their full impact is often concealed behind the veil of secrecy surrounding surveillance technologies (see Pallister-Wilkins, Goede, and Bosma 2020). This holds especially true in the context of border control and international mobility.

[6] The relationship between social sciences and comparative public law, along with the fruitful intersections that arise from it, is greatly discussed by Ran Hirschl (2014).

As Tazzioli (2021) further observes, digital forms of border violence frequently remain obscured, operating beneath the threshold of political visibility. This opacity presents a notable challenge for research in this area, making it difficult to fully grasp the implications of digital surveillance practices.

The limitations imposed by this opacity are compounded by the constraints of this study[7]. Nevertheless, these challenges will be critically addressed on a case-by-case basis, acknowledging the potential gaps while drawing insights from the available sources. In carefully navigating these limitations, this research aims to offer a nuanced understanding of how the digitalisation of border control is reshaping contemporary practices of surveillance and mobility management.

4. Structure of the book and case studies selection

The book is structured into four chapters. Chapter 1 aims to establish the theoretical framework through which the process of digitalisation of border patrols is examined. Specifically, it scrutinises the various capability areas underpinning border security functions, enabled or reconfigured by digitalisation in this field. These capabilities include situational awareness, detection and tracking, information management, and risk analysis, all constitutive to the digitalisation of patrolling. The chapter also offers an analysis of the European Border Surveillance System (EUROSUR) and the deployment of drones at the EU's external borders, alongside a reflection on future developments driven by increased investment in automated patrolling systems.

Chapters 2 and 3 present a cartography of emerging patrolling systems, focusing on case studies at the EU level and in two Member States: Greece and Spain. These countries, which have been interested in the most significant investments in border digitalisation, are emblematic «surveillance sandbox[es] at the frontiers of Europe» (Molnar 2022, 54). Located along the Eastern and Western migratory routes, they both provide invaluable insights into the digitalisation of border patrols, allowing for an exploration of how this process intertwines with national and European policies.

In both case studies, the analysis traces the specific ways in which digitalisation unfolds along the most critical sections of their external borders, highlight-

[7] This work has largely been written during the Covid-19 pandemic, which has restricted the ability to collect certain types of primary data, for instance through fieldwork. To gain a more comprehensive understanding of the phenomena under investigation as they unfold on the ground, I conducted eight in-depth interviews with a diverse range of stakeholders. These participants included researchers and academics, as well as journalists and activists from non-governmental organisations. The interviews, conducted online and lasting between 40 and 90 minutes, were designed with a purely exploratory purpose. As such, they are not directly relevant to the research design of the book and will not be explicitly referenced within its pages. Nonetheless, they have been invaluable in informing the factual reconstruction of recent developments related to the digitalisation of border patrols and in contextualising them.

ing the peculiarities of different patrolling systems. A thorough examination of the legal framework underpinning this digitalisation follows, identifying regulatory gaps and discrepancies between law and practice.

Finally, chapter 4 offers a comparative analysis of the findings from the case studies, with a particular focus on the tensions between digital patrolling and the obligation to respect and protect the fundamental rights of those subjected to such surveillance. From this, the discussion examines the broader implications for human rights from both European and international legal perspectives. Outlooks around human dignity, the right to international protection, privacy and data protection, as well as the principles of equality and non-discrimination, are discussed. The chapter concludes with reflections on the challenges of holding States accountable in times of digitally enhanced border surveillance.

To conclude and move forward, a few remarks concerning the selection of case studies are necessary. The decision to focus on Greece and Spain stems from the need to explore how the Member States that are most exposed to migratory flows are progressively digitalising their border patrol strategies, thus intertwining border security and migration policies to an increasingly indistinguishable degree (Topak and Vives 2018). At present, there are three primary migratory routes towards Europe: the Eastern, Western, and Central routes[8].

Although the Eastern route affects not only Greece but also Croatia and Bulgaria, Greece has seen the most notable investments in border digitalisation. The country has, in fact, increasingly relied on technological experimentation to secure its maritime and land borders. This trend is particularly evident in the growing use of drones for patrols.

On the Western route, Spain stands out as a crucial case study for several reasons. First, Spain remains the primary European destination for people on the move travelling via the Atlantic route. Its geographical position, coupled with the location of the Canary Islands and the enclaves of Ceuta and Melilla, has driven the development of increasingly sophisticated remote surveillance systems since the early 2000s. The *Sistema Integrado de Vigilancia Exterior* (SIVE) is particularly noteworthy, often regarded as the forerunner of EUROSUR. As will be discussed, the SIVE deeply exemplifies the process of digitalising border patrols, particularly through its capabilities in situational awareness, detection, and risk analysis.

The Central Mediterranean route, which remains the deadliest and most heavily traversed route to Europe in 2022, is not the focus of a specific case study in this analysis for two reasons. First, the Member States along this route have made few recent advances in digital border patrolling, instead prioritising cooperation with third countries. While systems akin to Spain's SIVE have been implemented, such as France's *Système Naval de Surveillance des Approches Mari-*

[8] From 2016 – the year after the so-called refugees' crisis – until April 2022, 413.847 arrivals have been recorded from the route Eastern, 208.030 from the Western, and 450.501 from the Central route.

times et des Zones sous Jurisdiction Nationale (SPATIONAV)[9], they are primarily deployed outside the Mediterranean. France's digital patrolling initiatives, for example, focus more on internal borders with Italy and Spain, on the Calais region and the English Channel, in close collaboration with UK-led border control operations (Akkerman 2021, 154; Bonnevalle 2022)[10]. Such «internal externalisation» of border control (Barbero and Donadio 2019), gaining momentum since Brexit, lies beyond the scope of this study. Secondly, along the Central Mediterranean route, patrolling strategies and their digitalisation, are marked by a high level of cooperation, mainly coordinated by Frontex[11]. This dynamic highlights the role of «intermediary or hybrid agencies» (Bigo 2006, 391), operating between police and military functions, especially in response to perceived security threats at Europe's borders. Given the predominance of Frontex-led operations – which, while integral to the broader context of this study, play a different role – the Central Mediterranean route is less relevant for a comparative analysis focused on the Member States' initiatives in digitalising border patrols at the EU's external borders.

[9] The SPATIONAV is a sea surveillance integrated system which produces a real-time operational picture fusing data from over 10.000 sources and connecting over 50.000 additional European and international tracks via a cyber-secured gateway. Launched in 2002, it is mainly based upon information collected by the French Navy and the Maritime Gendarmerie through a network of radars, cameras and infrared. The *Sistème* has a regional architecture based on three main hubs: SPATIONAV Channel/Atlantic, SPATIONAV Mediterranean, and SPATIONAV Antilles-Guyana. Moreover, France has recently started deploying drones to control its borders, and the data thus collected are very likely to be merged into the SPATIONAV.

[10] In addition to the surveillance systems supporting patrolling activities in the Mediterranean, mention should be made of the Finnish *Merivalvonnan tietojärjestelmä* (Maritime surveillance system), MEVAT. SIVE, SPATIONAV and MEVAT are to date the most advanced integrated and remote surveillance systems in Europe. Similar systems, but with a lower level of technical development and a smaller surveillance area, are also widespread among other EU Member States. In Italy, for example, this surveillance role is covered by the Vessel Traffic Service (VTS).

[11] Remarkably, since Frontex took over the Central Mediterranean surveillance with Joint Operation Hermes in 2011, its operations have been defined by broad mandates, prioritising border control over life-saving interventions at sea. Currently, Operation Themis, which replaced Operation Triton started in 2014, represents a key shift in digital border patrols, particularly with the transition from maritime to aerial surveillance marked by the 2020 launch of Operation Irini. As will be discussed, this change has significant implications for SAR capabilities. Moreover, the new aerial surveillance systems, including Multipurpose Aerial Surveillance (MAS) and satellites, are now used to detect migrant boats and assist third-country authorities, such as the Libyan Coast Guard, in conducting interception and return operations. These practices expose migrant people to severe human rights abuses today thoroughly documented, including arbitrary detention in inhumane conditions, where people on the move intercepted are denied basic rights.

CHAPTER 1

Digital patrolling at EU borders

1.1. Digitalising the EU borders

«Leonardo's Falco EVO drone is used to monitor irregular migration during Frontex operation» headlines a Leonardo press release, published in July 2019. The drone, it reads, helped identify a «'mothership' trawler as 81 illegal migrants were transferred to smaller boats». Without dwelling on the fact that the persons on board are *a priori* identified as 'illegal migrants' and not, for instance, as potential asylum seekers, similar reports on the use of Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aerial Vehicles (RPAS) – commonly called drones – and other surveillance tools for the control of the external borders of the European Union seem bound to become more and more present. According to an interview released by an official from Frontex Press Office on a review specialised in unmanned systems, in 2022, Frontex aerial surveillance planes and drones detected over 35.000 migrant people attempting to cross the Mediterranean Sea and heading to Europe (Gurierrez 2022).

The digitalisation of the European Union's borders is frequently depicted by actors engaged in *borderwork* through its substantial irreversibility. This idea is underpinned by a combination of path dependency, which propels the further dissemination of border and migration digitalisation as new technologies are incorporated into bordering practices, and a «technological solutionist» approach (Oliveira Martins and Jumbert 2020) or «techno-solutionism» (Morozov 2013), wherein every technological challenge is met with increased digitalisation, and border issues are framed as requiring technological solutions. Noteworthy in this context are the two contract award notices for aerial surveillance services

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

issued in August 2021, directed at Frontex, amounting to €84.5 million[1]. On the one hand, Frontex designates drones as state-of-the-art instruments to enhance the effectiveness of border patrols and search and rescue operations. On the other, various nongovernmental organisations (NGOs) and humanitarian groups contend that these measures predominantly reflect a calculated strategy to perpetuate illegal pushbacks (Alarm Phone et al. 2020; Mazzeo 2021), thereby violating the principle of *non-refoulement* enshrining the right not to be removed, expelled or extradited to a State where there is a severe risk of being subjected to death penalty, torture, and other inhuman or degrading treatments.

Investments promoting border digitalisation and relying on technological solutions to address migration challenges are often spurred by situations framed in public discourse through the lenses of crisis and emergency. At the EU level, the debate on the digitalisation of borders commenced in 2002 with the development of the EU Integrated Border Management (IBM), framed as an operational supplement to Schengen cooperation and aimed at enhancing collaboration among Member States at the external borders (see Hanke and Vitiello 2019). The premise was that the freedom of movement within the Schengen zone necessitated integrated efforts in border governance to prevent external threats from penetrating the area.

In 2007, the EU Integrated Maritime Surveillance was adopted to promote coordination in monitoring Europe's coasts, followed by the launch of the construction of a Common Information Sharing Environment (CISE) in 2014 (European Commission 2014). In February 2008, shortly after the so-called 'cayuco crisis' in the Canary Islands, the European Commission (2016a) presented a New Borders Package aimed at enhancing the governance of the external borders through increased digitalisation. However, it was the so-called 2015 'migration crisis' that marked the pivotal moment for the adoption of an increasingly integrated smart borders system. In April 2016, a revised legislative proposal for the Smart Borders Package was approved, comprising measures to establish an Entry/Exit System (EES)[2] and to implement significant modifications to the Schengen Borders Code[3], aimed at fighting irregular migration and facilitating border crossings for 'pre-vetted' and 'trusted' non-EU travellers (European Commission 2016a; 2016c; 2016b).

[1] See Tenders Electronic Daily (2021), 'Services - 395423-2021. Poland-Warsaw: Frontex Surveillance Aircraft Services for Border and Coast Guard Functions (FSA I) 2021/S 149-395423, Contract Award Notice' and 'Services - 395424-2021. Poland-Warsaw: Frontex Surveillance Aircraft Services for Border and Coast Guard Functions (FSA I), 2021/S 149-395424, Contract Award Notice'.

[2] Regulation no. 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, 30 November 2017.

[3] Regulation no. 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), 9 March 2016.

Since then, information systems have been deployed both *at* and *before* European borders. At the border, the EU Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (EU-LISA) manages three major information systems[4]: the European Dactyloscopy (EURODAC)[5], the Schengen Information System (SIS II)[6], and the Visa Information System (VIS)[7]. As argued by Sandro Mezzadra and Brett Neilson (2013), these large-scale IT information systems should be fully understood as bordering practices.

Before the border, information is exchanged and stored through the European Border Surveillance System (EUROSUR)[8], which aims to make visible irregular movements across land and maritime borders. Today, new systems such as the Passenger Name Record (PNR)[9] and the European Travel Information and Authorisation System (ETIAS)[10] are also being implemented. The significance and scope of these databases have increased dramatically with the approval of Regulation 2019/818, which establishes a framework for interoperability between EU information systems in the fields of police and judicial cooperation, asylum, and

[4] EU-LISA is an Agency of the European Union mandated to provide long-term solutions for the operational management of large-scale IT systems. It was established in 2011 by Regulation no. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. In 2018, the Agency has been given a wider mandate as enshrined by Regulation no. 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA).

[5] Regulation no. 603/2013 on the establishment of Eurodac for the comparison of fingerprints, 26 June 2013.

[6] Regulation no. 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), 20 December 2006. In December 2019, the three Regulation no. 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals, Regulation no. 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Regulation no. 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters entered into force: when fully operational, they will repeal the current system with SIS III. The most relevant novelties that will be introduced concern the mandatory registration of entry bans and return decisions, the full access by EUROPOL, and the possibility to process palm prints and DNA data.

[7] Regulation no. 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), 9 July 2008.

[8] Regulation no. 1052/2013 establishing the European Border Surveillance System (Eurosur), 22 October 2013.

[9] Directive no. 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 27 April 2016.

[10] Regulation no. 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS), 12 September 2018 and Regulation no. 2018/1241 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), 12 September 2018.

migration[11]. Once again in an emergent context, recent facts associated with the Covid-19 pandemic have significantly accelerated the digitalisation of border enforcement and migration management. This transformation has coincided with a surge in border violence, largely justified under the pretext of what Maurice Stierl and Deanna Dadusc (2021) have termed the «Covid excuse».

Building on these developments, this chapter aims to define and investigate the modes of digital patrolling carried out at various stages of *borderwork*. First, it provides a critical mapping of the operations conducted through smart borders under the overarching concept of digital patrolling, thereby offering insights into the rationale behind the digitalisation of borders. The objective is to underscore the specificities and distinctions that the *smartening* of particular segments of borderwork entails or might entail. Second, the chapter endeavours to problematise the articulation of operations associated with digital patrolling by examining different tools and systems currently in use at European borders, including devices and systems currently under trial. To do so, the focus shifts to the *capability areas* enabled or (re)assembled by the digitalisation of patrolling. According to the terminology used in the latest Frontex report on Artificial Intelligence, capability areas denote selected skills employed to execute the corresponding border security functions, encompassing the work facilitated by various technologies (Frontex 2021).

The chapter is structured as follows. The first section proposes a definition of border patrolling, emphasising its positioning within the framework of border digitalisation. Engaging with the literature, it offers an overview of the capability areas shaping digital patrolling: situational awareness, detection and tracking, information management, and risk analysis. Each area is examined and articulated in relation to the deployment of drones at external borders and the functioning of EUROSUR. The aim is to elucidate the logic behind the progressive digitalisation of patrolling, showing how this shift can profoundly transform borderwork. Lastly, in light of the growing emphasis on achieving higher levels of automation, a brief discussion on potential future developments in digital patrolling is proposed.

1.2. Defining 'digital patrolling' along smart borderwork

Border patrol can be understood as the array of control and surveillance practices carried out at the external borders and adjacent zones to safeguard border areas, primarily by preventing irregular crossings. At the EU level, this definition aligns with the primary aim of border surveillance as delineated by the Schengen Borders Code, *i.e.* to prevent unauthorised border crossings, to counter cross-border criminality (for instance, related to terrorism, smuggling, or other illicit traffic), and to take measures against persons who have illegally

[11] Regulation no. 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, 20 May 2019.

crossed the border[12]. Border patrolling, therefore, includes measures to counter such activities also through intelligence, surveillance, and reconnaissance missions. At the same time, however, patrolling can cover search and rescue operations (SAR) as well as specific environmental missions to address issues such as oil spills, deemed particularly dangerous for border areas. Patrolling, therefore, necessarily appears multipurpose and – consequently – ambiguous, or at least non-neutral, about the diverse objectives it pursues.

As noted in the introduction, this definition is partial as it lies on an understanding of patrolling limited to the expression of State sovereignty in border areas. This approach acknowledges that such sovereignty is fragmented and redistributed among multiple actors (see Bigo 2022), but it leaves aside other forms of patrolling whose existence and significance should not be overlooked. For instance, it does not encompass patrol activities carried out within and across State territory for purposes similar to those justifying border patrols. Louise Amoore argues in this regard that border spaces are becoming «feature spaces», with the result that border policing activities potentially enter every space – «the city street, the university campus, the clinic» (Amoore 2021, 4). Similarly, this definition does not cover patrolling activities conducted by organisations or civil society associations under rather opposite rationales, notably to provide support along the migratory routes.

If this approach does not fully engage with the ambivalence of «digital passages and borders» (Latonero and Kift 2018), exploring digital border patrol within a narrowly defined angle can contribute significantly to critically unravelling the implications of digitalisation. Patrolling, in this context, represents in fact a mechanism through which terrains and spaces are actively reorganised through the exercise of sovereignty manifested in border control. The underlying rationales of this reorganisation can tangibly impact pre-border zones, redefine migratory routes, and attempt to reshape the rules and practices governing human mobility (see Scheel, Ruppert, and Ustek-Spilda 2019, 584).

Rogier van Reekum (2019, 629) argues that the practice of patrolling in migration and border governance is intrinsically linked to processes of visibility: it centres on rendering both the movements of people and the inherent violence of border enforcement visible. Patrolling does not merely aim at «enacting the 'really real' border»; rather, it involves «encountering life in webs of terrains and tactics», intersecting the vision afforded by the tactical domain with the specificities of individual border areas. This encounter, increasingly digitally mediated, can take different shapes or even be circumvented altogether through various externalised forms of expulsion or abandonment, exemplified by the instance of boats left to die. Therefore, patrolling becomes a matter of managing, maintaining, and scrutinising, increasingly reliant on data collection. This process breaks down space into digital fragments produced by and through digital patrolling, which are presented as neutral and self-evident.

[12] Schengen Borders Code, no. 2016/399, Article 13(4).

In summary, digital patrolling extends to the intersections between the proposed understanding of border patrolling and the capabilities along which smart borders are articulated. It emphasises the complex interplay between digital borders and their physical and geographical counterparts, resulting in something emergent and new.

1.2.1. A look at the literature: defining capability areas

At this juncture, it is relevant to revisit the capability areas introduced by smart borders, establishing a dialogue between the various taxonomies examined in the literature. Richa Kuman (2020), for instance, presents an interesting classification of the tools that, when assembled or deployed, facilitate the functioning of smart borders. Her focus lies primarily on the differences and interactions between aircraft and drones, biometric communication systems, port access control systems, information and communication technologies (ICTs), radio frequency identification systems, and perimeter security systems designed to detect movement and prevent unregulated border crossings. The concept of «perimeter security systems» partially overlaps with the proposed definition of digital patrolling systems, as it encompasses tools that enable the surveillance of both border and pre-frontier areas.

Shifting the focus to the operations conducted by digitalised borders, van Reekum (2019, 625) identifies three primary domains of deployment: patrolling, recording, and publicising. The latter two are linked respectively to the production of documentary objectivity and the pictorial capture of fleeting realities. Here, the notion of patrolling is thus shaped in conjunction with the ability to build an archival memory and to make it public, carefully selecting what should be displayed and what should remain unseen.

Contrastingly, the 2021 report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance identifies six areas where the digitalisation of borders is having implications not only quantitatively – due to the extent and complexity of the data collected – but also qualitatively (Human Rights Council 2021)[13]. From a notably different perspective, Frontex (2021, 18) identifies five key capability areas resulting from the analysis of border security functions: situational awareness, information management, communication, detection/identification, training and exercise. In this context, particular emphasis is placed on the ability of smart borders to enhance States' capacity to act and increase the comprehensiveness of surveillance of border areas in a particularly broad sense.

These considerations can be critically mobilised to engage in a broader and overarching study of the capability areas of digital patrolling, highlighting their

[13] The reference is, in particular, to the use of online platforms, racial profiling, biometric data collection and digital identification systems, language recognition systems, mobile data extraction, and social media intelligence on migrant and refugee populations.

peculiarities with respect to different patrolling systems, and serving as a valuable analytical tool for the examination of case studies.

1.2.2. Operationalising the digitalisation of patrols

In an effort to contribute to existing taxonomies, two primary functions driving the rationale behind border digitalisation are here identified, along with seven key capability areas where smart borders are applied. Among these, four areas are particularly relevant for unpacking the notion of digital patrolling and will be further examined.

The two overarching capability areas in border and migration control, significantly expanded by digitalisation, are the deepening of control and surveillance capabilities at the borders and in the pre-frontier areas, and the enhanced filtering and sorting of international mobility. Given the impossibility of merely blocking 'unwanted' flows, the core aim is here to establish varied patterns of social sorting or triage between trusted and untrusted travellers. These patterns are increasingly based on data-driven knowledge and mediated by technologically intensive practices.

Control and surveillance, together with filtering and sorting, aim to identify individuals or groups deemed threatening or risky, often due to racial and other implicitly or explicitly discriminatory factors. This identification is framed as a precondition for facilitating the movement of trusted persons, those who generally have full access to the global mobility architecture, can travel by plane, easily apply for visas, and whose mobility is generally expected to be 'positive'. Digitalisation is intended to make their travel as seamless as possible, while others are even more forcibly kept outside legitimate means of movement.

As the exclusionary practices inherent in borderwork are designed to classify individuals based on desirability and belonging, datafication can elevate these practices to new levels (Bosworth 2008; Ferraris 2020; Glouftsios 2021). Smart borders are in fact sites where biometric identification and predictive analytics interact to shape decisions on exclusions and admissions. Huub Dijstelbloem (2021, 181) describes the resulting modalities of surveillance and filtering as turning borders into «extreme infrastructures», places where technological mediation naturalises and normalises exceptional situations crystallising at the borders, often particularly violent, through the exasperation of inclusion and exclusion processes.

To explore these two main axes – control and surveillance of borders and pre-frontier areas, alongside filtering and sorting – seven key capability areas of smart borders can be identified: screening, scanning, identification, and authentication; application of predictive analytics; communication; situational awareness; detection and tracking; information management; and risk analysis.

The first capability area, involving screening, scanning, identification, and authentication, encompasses tasks typically executed by large-scale IT systems such as SIS II, VIS, and EURODAC. Screening and scanning processes aim to identify individuals and other targets involved in border operations or authenticate their identities, and should thus be considered together. Unlike generalised and extensive surveillance, smart borders enable «hyper-individualisation» in policing persons and entities (Latonero and Kift 2018, 6). Classical examples tied to this capability area include the collection and processing of biometric data, digital identity authentication, and Automated Border Control (ABC) systems. These systems authenticate machine-readable electronic travel documents to detect cases of identity fraud – a process that is often built on non-neutral operationalisations of suspicion around unwanted or unsolicited mobility. Additionally, the use of facial recognition technologies for applications that go beyond mere identification, such as emotion recognition in lie detector trials, also falls within this spectrum.

The second area, concerning the application of predictive analytics, encompasses all analyses conducted on travellers, as well as background archiving and recording processes. For example, Passenger Name Record (PNR) data is analysed to support authorities through criminal intelligence information, primarily detecting travellers deemed potentially risky or suspicious. This area also includes social media intelligence and data extraction processes from mobile phones, which are used both predictively and as verification tools in border security as well as in access to international protection.

Thirdly, the communication capability area involves technologies that facilitate information sharing in border control contexts, for instance ensuring secured communications and wireless broadband data links (Frontex 2021, 18).

These three capability areas – screening, scanning, identification, and authentication; predictive analytics; and communication – fall outside the cross-sectional work of digital patrolling and will therefore not be further discussed here. Instead, the last four areas will be addressed in detail. Firstly, the promotion of situational awareness is crucial in patrolling, serving as the conceptual and operational prism that allows «the intermingling of vision and action» (Dijstelbloem, van Reekum, and Schinkel 2017). EU agencies' operational documents often describe situational awareness as the capacity to identify anomalies and track everything that crosses EU borders (Loukinas 2017, 8) – a prerequisite for prompt and targeted interventions. Enhancing situational awareness is indeed EUROSUR's central mission and a dominant narrative in the discourse on the deployment of military surveillance systems and techniques, within which various perimeter security systems, notably drones, are embedded (Csernatoni 2018, 183).

Similarly, processes of detection and tracking are core functionalities in digital patrolling and one of the main objectives pursued through the digitalisation of borders. In the realm of migration, detecting and tracking vessels in distress or suspected of conducting illegal cross-border activities in near real-time is perhaps the most evident manifestation of what William Walters (2016) famously calls «the dream of *live governance*». Thus, the digitalisation of detection and tracking implies a shift from reactive to proactive border patrolling, expanding the spatial and temporal dimensions covered by persistent surveillance of populations identified as risky. Situational awareness, detection, and tracking are closely intertwined, as situational awareness provides the framework of possibility for detection and tracking (Suchman, Follis, and Weber 2017). Drones, satellite-based services, and data fusion services provided by Frontex play a major role here, and their capacity to detect and track suspicious objects beyond borders has garnered increased attention.

The information management capability area – which includes data mining, exchange, and fusion – extends to both ICTs, such as the interoperability between different databases, and digital patrolling. In digital patrolling, the exchange of information from EU countries to third countries within the framework of joint patrols and data analysis converging to EUROSUR is particularly relevant. Regardless of the level of digitalisation achieved, border patrolling is in fact fundamentally a data practice: it is first and foremost about collecting information regarding what is happening in the border areas and reacting to it. However, with digital patrolling, the data dimension becomes even more crucial, to the point that emerging forms of patrolling have been described as «performing the datafication of space and its encounter of bodies» (van Reekum 2019, 630–31). Data mining, exchange, and fusion in border and pre-frontier areas can indeed result in unprecedentedly data-intensive practices that shape the understanding of both the territory to be patrolled and the people on the move who traverse such territory.

The seventh and final capability area concerns risk analysis and the adoption of pre-emptive mechanisms. This is particularly significant because, often relying on deterrence narratives, it supports processes of categorization and classification that differ from those of identification: individuals belonging to specific groups or possessing certain characteristics should be dissuaded from attempting to reach EU borders, as access will not be granted to them. In this field, anticipating risks based on past trends and generalizing potential individual behaviour is deeply problematic, especially from a fundamental rights perspective. This understanding of risk allows in fact for the development of 'parallel border regimes', different for different categories of people, where violations of the principle of non-discrimination are likely to occur (Human Rights Council 2021, para. 10).

Nevertheless, archiving migratory events through mapping and monitoring digital interfaces, which enable the production of future-oriented spaces of governmentality, is increasingly central to the development of smart borders. At the EU level, examples of such mechanisms include EUROSUR, the Joint Operation Reporting Application (JORA, a data collection and exchange system used in joint operations), and the Vessel Detection Service provided by the European Maritime Safety Agency (EMSA), which processes archival data on migratory routes, past incidents, and interceptions (Glouftsios and Panagiotis 2022; Tazzioli 2018, 2). Here, the key difference with the second capability area lies in the immediate connection between risk analyses and patrolling activities, with risk being understood as a tool to better target patrolling efforts.

Table 1 – Capability areas in digital borderwork and capability areas defining digital patrolling.

Overarching capability areas in *borderwork*	Description in digital borders operations
Control and surveillance of border and pre-border areas	The capability of deploying advanced control and surveillance technologies is increasingly 'far away' in space and time from geographical borders, in a preventive logic.
Filtering and sorting	The capability to perform data-based or (semi-)automated *triage* between trusted and untrusted travellers.

Capability areas in digital *borderwork*	Description in digital borders operations	Examples in use or tested in the EU	
Screening, scanning, identification, and authentication	The capability to screen and scan information to identify individuals and other targets involved in border operations, and/or to authenticate their identities.	SIS II, VIS and EURODAC Automated Border Control Different forms of document authentication	
Application of predictive analytics	The capability to manage data in order to facilitate pattern recognition with a future-oriented approach, also utilising AI-based systems.	PNR Social media intelligence Data extraction from mobile phones	
Communication	The capability to collate information for communication purposes in a digitally-mediated manner, enabling information sharing in border surveillance.	Secured communications Wireless broadband data links Chatbots and virtual agents	
Situational awareness	The capability to collect, fuse, and analyse various types of data originating from different sources at the border and in the pre-frontier area, aimed at enhancing response capabilities.	AI-enabled surveillance towers Drones Border surveillance systems (EUROSUR, SIVE)	**CAPABILITY AREAS DEFINING DIGITAL PATROLLING**
Detection and tracking	The capability to detect and track individuals and/or objects at, and before, the border within a framework of enhanced situational awareness.	Satellite and drones-based services Robotic border patrol agents Border surveillance systems	
Information management	The capability to manage and exchange information among different stakeholders, including outside the EU, thereby facilitating joint operations while ensuring secure and interoperable systems.	Data fusion services Geospatial data analytics	
Risk analysis	The capability to generate risk taxonomies with the aim of assessing the impact of an event at the border or pre-border area, and categorising people on the move, adopting a pre-emptive and deterrent approach.	Early warning technologies Joint Operation Reporting Application Vessel detection services	

1.3. Situational awareness, detection, and tracking: conflicting rationales and multipurpose technologies

After discussing the proposed taxonomy, the analysis now shifts to the different modes of digital patrolling, focusing on exemplar technologies and functionalities. In particular, the transition from a 'patrolling-driven' to an 'intelligence-driven' strategy in border control (Dijstelbloem 2021, 105), resulting from increased technological mediation for surveillance purposes, is problematised. Attention is given to the technical and political justifications for this shift. As previously mentioned, the capability areas of situational awareness, detection, and tracking are interrelated and complementary within various devices and systems that facilitate digital patrolling and should thus be studied together. To illustrate how these capability areas are articulated throughout the digitalisation process, the functioning of EUROSUR and the deployment of drones at the borders are here discussed.

1.3.1. EUROSUR, the 'system of systems'

Among integrated border surveillance systems at the European Union level, EUROSUR stands as a textbook example. Operational since December 2013, it was immediately hailed as the future of border and migration management, designed to decouple surveillance from patrolling and deliver the right information to the right person, at the right time, and in the right format (Bellanova and Duez 2016, 12; Tazzioli and Walters 2016, 450).

EUROSUR is often described as a 'system of systems', integrating various mechanisms aimed at curbing irregular migration while safeguarding migrants' lives. It is deemed achieving this by establishing a common framework for information exchange and cooperation between EU Member States and Frontex. The Surveillance System comprises national hubs, the National Coordination Centres (NCCs), connected through a secure communication network with each other and with Frontex. In practice, EUROSUR compiles and visualises maps by integrating data from sources such as radars, drones, satellites, intelligence reports, and sensor systems (Jeandesboz 2017). Using this data, and combining the National Situational Pictures created by the NCCs, the EUROSUR Fusion Services (EFS) generate the European Situational Picture (ESP) and the Common Pre-frontier Intelligence Picture (CPIP).

According to Article 3(d) of Regulation 1052/2013, EUROSUR aims to «support the Member States in achieving full *situational awareness* at their external borders and enhancing the *response capability* of their law enforcement authorities» (emphasis in original). Situational awareness here is broadly defined as the capacity to monitor, detect, identify, and track irregular cross-border activities to find «reasoned grounds for reaction measures on the basis of combining new information with existing knowledge». Notably, the system promotes an overtly *extraterritorial* approach to situational awareness, detection, and tracking in the pre-frontier area: the CPIP is in fact derived directly from information gathered through the surveillance of territorial waters in third countries, some of which have alarming human rights records concerning people on the move (Marin and Krajčíková 2016, 119).

The EUROSUR mandate thus enables the replacement of border patrolling with the analysis of interactive maps. These maps, through their aggregated data, mediate the border agent's perspective of the situation at and before the frontier, directly from an operations room. Consequently, patrolling becomes digitally mediated, undergoing significant transformations. Scholars have accordingly described situational awareness as a form of «operational vision», indicating that the visibility produced by technologically mediated monitoring practices is not solely for knowledge production but also for managing and governing the detected events (Tazzioli and Walters 2016). This digital and EUROSUR-mediated evolution of situational awareness, detection, and tracking thus alters significantly the understanding of border patrolling.

Furthermore, making previously unreachable areas visible and governable facilitates a remote-control logic that challenges also patrolling rules. The increased likelihood of being «policed at distance» (Bigo and Guild 2005, 234) raises significant concerns regarding the actions (*i.e.*, the direction in which the enhanced reaction potential is aimed) that heightened situational awareness may prompt and trigger, as well as the practical implementation of early detection tactics. While a comprehensive assessment of the known casuistry is beyond the scope here, it is pertinent to highlight that drones might be used in identifying the optimal moment for an interception at sea – irrespective of who actually carries out the operation, and the objective of such operation (Follis 2017, 17).

The above-mentioned report by the Special Rapporteur and accounts by various human rights organisations indicate in fact that surveillance drones, deployed within the EUROSUR framework in the Mediterranean, can be (and are) used to inform the Libyan coastguard about when and where to intercept potential asylum seekers and migrant people's boats heading to Europe, to bring them back. This coordination of 'pullback' operations from a distance exposes detected individuals to severe violence and human rights violations in Libya (Alarm Phone et al. 2020; Human Rights Council 2021; Monroy 2021). The effects of enhanced detection and tracking can thus be extremely direct for people on the move.

1.3.2. Drones' sightless vision, at a distance

Drones have become increasingly significant within the European borders network, necessitating a thorough examination of their integration and the underlying logic of their deployment – especially within the set of capabilities areas here under analysis. Similar to integrated border surveillance systems, drones operating at and beyond external frontiers contribute substantially to situational awareness in pre-frontier areas. They intersect visibility and action, where the core of digital patrolling lies, and play a crucial role in fostering a mediated perception of space and events (Dijstelbloem 2021, 103).

The use of drones for border and migration control represents one of the most interesting instances of military-style UAVs being utilised in the civilian domain – a transformation that Luisa Marin (2017b) describes as a true metamorphosis. Like for military surveillance technologies, the 'sightless' vision enabled by real-time monitoring allows not only to observe objects but also to target them and act proactively on processes and events (Csernatoni 2018; Follis 2017).

First of all, drones should thus be seen as proactive data collection technologies, versatile enough to serve security, humanitarian, environmental, and law enforcement purposes (Loukinas 2021). Through the data collected, drones assist in detection and tracking operations, reducing the need for public agents to undertake difficult and time-consuming border control tasks. This perspective is central to the digitalisation of patrolling and is evident in the context of EUROSUR, where there is a growing emphasis on using remotely piloted aircraft to monitor external land borders and pre-frontier areas. The aim is to detect, classify, and track all targets of interest «as fast as possible and for as long as possible» (Follis 2017, 11).

Studying the exact functions of drones used for digital patrolling is challenging due to limited access to detailed information, often restricted for commercial and security reasons. Nevertheless, an overview of the main advancements in this field can offer a general understanding of the phenomenon's scope. The European Union has explored funding research programmes on drones for border surveillance since the early 2000s, with widespread deployment starting around 2016. Currently, while the three European agencies – Frontex, EMSA (European Maritime Safety Agency), and EFCA (European Fisheries Control Agency) – do not directly own UAVs, they lease drone services from private companies to Member States. This process is significantly facilitated by inter-agency agreements to share reconnaissance capabilities, including the use of drones (Loukinas 2021; Peter and Jo 2020).

In 2017, EMSA established drone services to support Member States' coast guard activities. A subsequent pilot project, involving Frontex, aimed to create operational and technical synergies between different European Coast Guards and the three agencies. Greece, Italy, and Spain were identified as key host States for this initiative. The deployment of RPAS coordinated by EMSA, alongside fixed-wing aircraft managed by Frontex for patrol purposes, was considered a success of interagency cooperation.

Later in 2017, a pilot was conducted under the Frontex Aerial Surveillance Services (FASS) framework contract. In the following months, support extended to the Balkans, Aegean Sea, Black Sea, Slovakia, Poland, southern Portugal, and Denmark, as well as to joint operations such as Themis and Poseidon (Frontex, EMSA, and EFCA 2018). Remarkably, the FASS leased aircraft contributed data to the EUROSUR Fusion Services (Council of the European Union 2018; Frontex 2020a; Monroy 2021). However, specific information about the aircraft used within the FASS remains commercially confidential, further complicating the study of drone functionalities for digital patrolling.

Currently, EMSA retains a fleet of various types of drones lent free of charge to Member States to support coastguard monitoring around the European Union, with flights originating from an EU or EFTA country (Frontex 2020b). These drones primarily support general maritime surveillance or, in some cases, pollution and emissions monitoring. According to EMSA's 2022 Agency Outlook, it is committed to continuing RPAS services to Member States and EU agencies, supporting all types of maritime authorities (European Maritime Safety Agency 2022). Furthermore, EMSA plans to develop multipurpose regional services to facilitate operational capability sharing among neighbouring coastal States using RPAS, with extended capabilities.

Conversely, Frontex is authorised to deploy drones, airborne surveillance technologies, or other assets for detection and tracking within the territorial waters of EU Member States exclusively upon obtaining consent from the pertinent country. However, these restrictions do not apply to surveillance operations in the pre-frontier area, reflecting the extraterritorial nature of Frontex's operations, where the agency takes the initiative independently of State involvement (Follis 2017, 8; Peter and Jo 2020, 17). Despite Frontex's long denial of using drones in its operations, there is evidence that it has leased drones to State authorities and used the collected information since at least 2018 (Glouftsios and Panagiotis 2022).

1.3.3. Divergent logic, multipurpose considerations, and militarization

The analysis of EUROSUR and the deployment of drones at the European Union level, focusing on the capability areas shaping digital patrolling, has led to the identification of different emerging trends and insights regarding the evolving modalities of border control. These trends, introduced above, merit additional scrutiny.

Firstly, there are substantial ambivalent and divergent logics underlying and justifying digital patrolling: in particular, tensions exist between the security-oriented rhetoric built on the potential of drones to enhance situational awareness at borders and a discourse aimed at reaffirming the role such technologies can play in rescuing migrant people in distress or dismantling smuggler networks. This is particularly relevant to the use of drones for border and pre-frontier patrols, where the discussion revolves around the distinction between so-called 'security drones' and 'humanitarian drones' (Peter and Jo 2020). Notably, humanitarian drones often refer to those employed in search and rescue missions, for example during operations such as Mare Nostrum, or those flown by NGOs. Additionally, there have been attempts to promote the testing of semi-automatic systems using Earth Observation data to enhance surveillance and support SAR operations, which, however, posed severe political and legal issues regarding the use of collected data (Loukinas 2021; Marin 2017a). This ambivalence and mixture of rationales underpin what Sanja Milivojevic (2016, 87) describes as «the drone dilemma» – a concern that can be generalised to digital patrolling more broadly and is reflective of what is often described as the humanitarian-security nexus. This nexus, also referred to as the «care and control continuum» marking the governance of 'undesirable' populations (Agier 2008), deeply shapes bordering practices well beyond digital patrolling.

The rationale underlying differentiations among drones based on their use is that they are neither inherently good nor bad; their impact depends, in fact, on their utilisation. While this perspective is, of course, pertinent in emphasizing the role of the context in which technologies are embedded as being of the utmost importance, it obscures the far-reaching implications of drone deployment *per se*. The line between humanitarian and security purposes is in fact extremely blurred. On the one hand, drones could play a crucial role in saving lives at sea – for example, by delivering water or life jackets (Loukinas 2017, 12). On the other hand, as Follis and Marin (2017, 11; 2016, 129) note, even when drones are deployed with humanitarian intent, successful rescue operations should not be assumed merely due to enhanced situational awareness, tracking, and targeting capabilities. Such operations in fact always require additional resources connected to the rescue operation, which – as dramatic news cases systematically show – cannot be given guaranteed. There is very little or no evidence that enhanced awareness of boats in distress results in prompter saving efforts. Critics from academic and humanitarian spheres have indeed raised concerns that even 'humanitarian drones' may not primarily serve rescue purposes but rather enhance capabilities to *hunt* people on the move, thereby improving reaction capacities against unwanted mobility. What is sure, is that the digitalisation of patrols is not preventing people from dying in border-crossing situations.

Furthermore, the transition to aerial surveillance over naval patrols has been criticised as an attempt to evade international legal obligations applicable to vessels but, currently, not to drones (Howden, Apostolis, and Loewenstein 2019; Oliveira Martins and Jumbert 2020). Thus, the digitalisation of patrolling could deepen accountability gaps. A notable example in this sense is the European Union Naval Force in the South Central Mediterranean (EUNAVFOR MED) Operation Sophia which, despite lacking a humanitarian mandate, saved over 45.000 lives between 2015 and spring 2019 merely by adhering to the International Law of the Sea. Its replacement, Operation Irini, shifted focus to monitoring the UN arms embargo on Libya, replacing naval ships with aerial operations conducted by aeroplanes and drones, that resulted in fewer sea rescues. This shift occurred amidst a sharp criminalisation of solidarity toward people on the move, particularly against humanitarian NGOs at sea, thus significantly amplifying such consequences.

Similar concerns have been raised regarding EUROSUR's contribution to rescue operations. Evidence suggests that the timing and practices of data entry into the system are often incompatible with rescue operations, being instead useful to serve risk rating and analytics purposes. Data are in fact frequently entered with significant delays, *de facto* making real-time incident response impossible: there is a mismatch between the information collected for border control and that necessary for rescue operations. Based on this, critical literature has often depicted humanitarian objectives in border digitalisation as a pretext to justify the integration of drones and other digital patrolling systems into border management, further consolidating the securitisation of European borders (Marin

2017a). In fact, delays in data entry and sharing through EUROSUR are not solely attributable to technical limitations; rather, they reflect the underlying logic and priorities shaping EU border management. And the primary objective appears to be intercepting and tracking as many migrant people as possible before they reach Member State jurisdictions, aligning with a preventive approach (Jumbert 2018). In contrast, the organisation of timely rescue operations appears to be of comparatively lower priority.

Overall, it is nevertheless challenging to determine whether data collected by drones – or as Loukinas (2021) suggests, by «multipurpose drones» – primarily enhance patrols for security reasons, dismantle trafficking, facilitate illegal pushbacks, make SAR operations more efficient, or help contain maritime pollution (Marin 2017a).

Interestingly, moreover, these multipurpose tools in border patrols are often praised for their expected efficiency. Justifications for drone procurement and deployment frequently emphasize operational benefits such as reduced personnel costs, enhanced tracking and detection accuracy, extended operational duration, increased patrolling capacity compared to manned vehicles, and the ability to patrol complex or hazardous areas (Marin and Krajčíková 2016; SESAR 2016). Reports from Frontex and EMSA, for instance, overly assert the potential of digitalisation to address all the «various challenges that the EU external border management might face in the coming years» (Frontex 2021). While this narrative can support increased funding for drone research and leasing, it overlooks the frictions and errors that digital patrolling does not eliminate, as well as the transformative impact that drone use in border security can have on migration governance.

First, it is thus essential to recall that digitalisation and smart borders, though often presented as infallible, are prone to disruptions and subversion (Everuss 2021; Glouftsios 2021). For example, drones' surveillance gaze is neither perfectly timely nor uninterrupted and is susceptible to human error, thus not solving 'all' patrolling issues. Drones' 'vision' is in fact limited and flawed due to cost constraints preventing 24/7 operation and technical limitations necessitating a trade-off between image quality and coverage area. Accidents can also significantly compromise border management operations. Thus, the 'dronisation' of borders is simply not a *panacea* for all patrolling problems.

Here, as Follis (2017, 12) rightly notes, the central issue is not only the adoption of military technologies *per se* but the paradigm shift it brings in border security, where migrant people are detected and treated as 'targets' moving through space, trackable beyond EU Member States' jurisdictional boundaries.

1.4. Information management and risk analysis: beyond filtering and pre-empting mobility

Two more capability areas – information management and risk analysis – enable border patrolling through increased technological mediation. The interconnection and interdependence of different segments of borderwork, particularly in collecting information via drones and tools that integrate into EUROSUR, have been partially addressed in previous sections. However, the mechanisms of data exchange and fusion that underlie digital patrolling, as well as the growing role of risk analysis and rating processes, should be further explored.

Firstly, data exchange and circulation are central to the increasingly externalised and outsourced management of borders and human mobility. This trend highlights the role of third-countries, agencies, and private companies also in patrolling schemes, having an impact on the use of drones and EMSA's vessel detection service within the EFS framework, the routine satellite surveillance of maritime flows in pre-frontier areas and third countries, and the use of EUROSUR data. Notably, several EUROSUR contact points with Frontex headquarters in Warsaw exist not only within Member States but also in North African countries such as Morocco, Algeria, and Libya. Here, data collected by satellite stations, coastal surveillance stations, and remote surveillance platforms converge (Glouftsios and Panagiotis 2022). Remarkably, some information shared by third countries flows directly into National Situational Pictures thanks to bilateral agreements. While these arrangements are often shrouded in secrecy and generally lack substantial public oversight, their scope is deemed growing as the volume of data-sharing practices is likely to escalate rapidly.

Moreover, the exchange of surveillance information with third-country authorities, including satellite information for example under the EU's Copernicus space programme (see Słomczyńska and Frankowski 2016)[14], demonstrates how data sharing fragments patrolling, refining mechanisms for filtering 'undesirable' mobility and strengthening the surveillance of key areas of interest. For Frontex's activities, cooperation with third countries typically involves working arrangements where information exchange and risk analysis are crucial. These arrangements allow data collected by drones and other digital patrolling tools in the pre-frontier area to be accessible to neighbouring third-country authorities[15].

Additionally, through the Maritime Simulation Module Service (MSMS), images captured via digital patrolling also converge on EUROSUR. The MSMS works to facilitate predictions on suspicious or abnormal vessel movements through ship reporting systems like the Automated Identification System (AIS) and EMSA-developed algorithmic analysis. Once again, these systems aim to identify and make visible (and potentially governable) events occurring before the border (Glouftsios and Panagiotis 2022; Monroy 2021).

The digitalisation of patrolling through information sharing with third countries is particularly problematic, and has faced criticism. EUROSUR's Regulation in Article 20(5) states that «[a]ny exchange of personal data with third

[14] Copernicus is the EU's Earth observation programme, managed by the Commission in partnership with the Member States, the European Space Agency (ESA), and other centres and organisations. It collects vast amounts of global data from satellites and ground-based, airborne, and seaborne measurement systems.

[15] The conclusion of an agreements is unnecessary if communications exchange occurs, per the Law of the Sea, with the nearest Maritime Rescue Coordination Centre (MRCC).

countries in the framework of EUROSUR shall be strictly limited to what is absolutely necessary for the purposes of this Regulation» and must comply with data protection provisions. This is crucial especially if the data could allow to identify individuals or groups seeking international protection or at serious risk of fundamental rights violations. However, information exchange – though limited and conditional – remains possible and is not immune to potential creep. Monitoring the use of shared information by third authorities is challenging, and there is sporadic reporting of how the data is used in practice, especially concerning migrant people and asylum seekers' rights in third countries (Marin 2020).

1.4.1. Between deterrence and sorting

These considerations are particularly relevant within the discourse on deterrence and prevention, which informs much of the information management capability under digital patrolling. Frontex's focus on preventive surveillance operations aligns with this perspective: the CPIP itself, which results from merged data from diverse sources, aims to situate the present within an anticipatory matrix (Csernatoni 2018, 180; Walters 2016, 807). This approach shapes border policies regarding potential flows, transcending territorial boundaries, and emphasizing migration patterns and routes over individual rights as a way to frame migratory phenomena (Jeandesboz 2017, 3).

Remarking on these shifts, Martina Tazzioli (2018, 11) shows how the functioning of monitoring systems like EUROSUR is expected to deter people on the move from embarking on non-pre-authorised border crossings. Notably, this deterrence is framed as evidence of the humanitarian vocation of border digitalisation: by significantly increasing detection and interception probabilities, EUROSUR would reduce departures and, consequently, deaths at the EU's external borders.

In his ethnography on the patrolling of 'clandestine migration' in the Euro-African borderlands, Ruben Andersson (2014, 128) highlights that border patrols tend to be highly visible, as the mere sight of police ready to thwart any boat journey to Europe serves as a deterrent. However, digital patrolling alters this dynamic. In a remotely controlled pre-frontier space filled with «technological deterrents» (Csernatoni 2018, 178) capable of collecting, exchanging, and assembling information in close-to-real time, traditional visible signs of security such as fences and patrol troops become less relevant. Instead, precisely the «double invisibility of drones» – as described by Loukinas (2017, 15) – emerges as a promising surveillance tool: drones are often undetectable from the ground, and even if seen, it is almost impossible to discern who operates them and for what purposes data is collected. This results in a «chilling» (Marin and Krajčíková 2016, 118) or self-disciplining effect, normalising pervasive surveillance levels and discouraging even legitimate actions, such as reaching the EU borders to seek international protection. Digital patrolling, therefore, can be more intrusive than traditional methods. However, the effectiveness of such deterrence would require further investigation. In fact, if a lesson can be drawn from migration and border control policies, it is that people on the move are rarely deterred by harsh conditions and violent or dangerous terrains (van Reekum 2019, 629). What happens instead, is that they are pushed towards more hazardous routes. In this sense, migration is largely 'incorrigible': people tend to adapt and reinvent strategies of movement despite structural changes in border policies (Tazzioli 2018, 4).

These strategies – such as route selection, departure points, and transport specifics – become targets of risk analysis, the last dowel of this excursus through the capability areas enhanced by digital patrolling. The vessel detection service and EUROSUR are again particularly significant here. The former processes archival data to identify areas of interest based on risk analysis, accounting for patterns and trends in «illegal immigration» and cross-border crimes (European Commission 2015, 11). As mentioned, these calculations extend over geographically dispersed areas, beyond the jurisdiction of the Member States (Glouftsios and Panagiotis 2022).

Similarly, EUROSUR's operational maps collect information from third countries and the pre-frontier area, fragmenting the external borders of each Member State into more manageable 'border sections' with assigned risk levels: its dynamic situational pictures use red, yellow, and green lines to reflect the 'migratory risks' to which different border sections are exposed (Tazzioli and Walters 2016, 456). These evaluations, based on past events and possible future migratory scenarios, are driven by Frontex and relate to the (present or future) border stress affecting specific frontiers, ranking different border events by their «expected governability» (Tazzioli 2018, 11).

Besides assessing border area risks, EUROSUR reinforces external borders by classifying and categorizing groups of people (Latonero and Kift 2018, 2). EMSA drones, for instance, can gather data on the number of people or activities on detected vessels, during day and night (Loukinas 2017, 8). Risk analysis in digital patrolling thus goes in the direction of classifying people into risk groups – such as citizens, (presumed) criminals, and irregular migrants. However, these categories remain extremely fluid: the term 'irregular migrant', for instance, often remains vague and extends to asylum seekers attempting to reach Member States. Before the border, different statuses are in fact blurred, making it almost impossible for asylum seekers and other people in need of protection to be recognised within the 'mixed flow' (Peoples and Vaughan-Williams 2010, 141). While human-conducted forms of patrolling allow to encounter people, making it possible (at least in theory) to carry out individual assessments in line with fundamental rights and international protection standards, this step can easily be bypassed through digital patrolling and its pre-emptive outlook.

This represents one of the prominent features of modern surveillance: borders and bodies are reshaped into patterns of social sorting, made visible through maps, scores, alerts, and other data derivatives defining risky behaviours (Muller 2011, 92). Risk assessment thus legitimises suspicion against specific groups simply by categorizing them, a process that is not politically neutral but results from specific choices: this approach is about uncertainty and probability, not about rights.

1.5. The future of digital patrolling: towards a new role for automation?

In mapping the landscape of digital patrolling, the rapid progression of border digitalisation has emerged quite clearly. As new technologies and increasing automation gain prominence in European policy documents and discourses, it is pertinent to indulge in some preliminary reflections on the future trajectories of digital patrolling by having a look at the current research and development initiatives across Europe.

In discussions on digital border patrolling, a central focus lies on the increased efficiency that new patrolling systems may offer, alongside an advocacy for expanding reliance on advanced technological expertise and state-of-the-art surveillance technologies. This approach positions technological 'solutions' as responses to perceived security 'problems' associated with managing migratory flows at the EU's periphery. According to Raluca Csernatoni (2018, 191), studies and projects aimed at enhancing digital patrolling often promote a narrative focused on effectiveness and cost-efficiency, thereby normalising the use of emerging surveillance technologies while advancing militarization and military rhetoric in border management. This perspective is underpinned by a belief in the infallibility of technology, termed the «EU's border technology fix» by Panagiotis Loukinas (2021, 4), which drives a push towards digitalisation.

In the aforementioned Frontex report on AI-based capabilities, alongside existing technologies such as surveillance towers, maritime domain awareness, and small unmanned aircraft systems, significant attention is given to technologies currently in development. Notably, these include new automated border control systems and diverse robotic systems (Frontex 2021, 23). These studies underscore how borders are increasingly viewed as prime sites for experimentation, to the extent that, as Claudia Aradau (2020) suggests, experimentality has become a primary rationale in the governance of border zones, leading to a «laboritazation of borders» (Bourne, Johnson, and Lisle 2015). The selection of border areas and vulnerable groups, such as migrant people and asylum seekers, for technological testing raises numerous ethical and legal concerns. This choice is particularly troubling given the stark power imbalances and the significant barriers these individuals face in asserting their rights or challenging violations arising from such experimental practices.

1.5.1. Which *Horizons*? European research priorities in digital patrolling

An intriguing perspective on these developments can be found in research projects funded at the European level, which further accelerate the digitalisation of patrolling. This 'laboratory' is for example provided by projects funded under the Horizon2020 scheme, succeeding the 7th EU Framework Programme. Although, as William Walters (2016, 813) cautions, when engaging with minor shifts in the present, effervescent assemblages should not be mistaken with durable apparatuses, trends towards growing automation are likely to persist and are indeed rooted also in research and development programmes.

Specifically, funding for these projects is provided through the European Security Research Programme (ESRP), which comprises a €1.3 billion component of the Horizon Europe research and development programme for the 2021-2027 financial period (European Commission 2021b)[16].

Since 2015, several projects have explored the use of autonomous drone technologies in border networks to enhance situational awareness systems. On digital patrolling, particularly notable is ROBORDER[17]. Funded with approximately €8 million under the Horizon 2020 framework in May 2017 and concluded in September 2021, ROBORDER aimed to develop and demonstrate a fully functional autonomous border surveillance system using 'swarms' of unmanned mobile robots to improve detection capabilities for early identification of illegal border activities. This system, comprising aerial, water surface, underwater, and ground vehicles, also aimed to detect maritime pollution and oil spills. The project's significance lies in its promise to find a solution to virtually all the challenges border authorities face in patrolling the EU borders, particularly when dealing with heterogeneous threats across vast areas. The adaptable sensing and robotic technologies developed in this project are designed to enhance interoperability and flexibility as never before in diverse operational and environmental settings.

Demonstrations have been conducted in various sites: in Greece, for detecting unauthorised sea border crossings; at the Bulgarian-Turkish borders, for detecting unauthorised land border crossings and signals from trespassers; in Hungary, for developing autonomous systems for patrolling hard-to-reach areas; and at the Estonian-Russian borders, for tracking smuggling activities. Additional pilots, conducted in Portugal, included early identification and tracking of illegal communications, as well as the detection of pollution and other incidents at the borders (ROBORDER 2021).

While autonomous technologies are already in use in border monitoring, with Frontex testing unpiloted military-grade drones in the Mediterranean and the Aegean, if ROBORDER's outcomes were effectively implemented, the level of automation in border patrolling would significantly advance. This would lead to the further decentralisation of border zones into various layers of surveillance and tighter integration of migration, criminal and national security concerns through military (or quasi-military) autonomous technologies. The future of digital patrolling would thus increasingly focus on risk calculation and managing vast amounts of information, turning people on the move into security objects.

ROBORDER is not unique in its objectives and methods. Among others, it has in fact been complemented by CAMELOT, a Horizon 2020 project which

[16] The current ESRP follows from the €1.7 billion security component of the EU Framework Research Programme Horizon 2020, 2014-20 and its €1.4 billion predecessor within the FP7, 2007-13.

[17] Autonomous swarm of heterogeneous robots for border surveillance (ROBORDER), Grant agreement ID: 740593. 1 May 2017 – 31 August 2021.

developed systems for managing the data collected by the 'swarms'[18]. Another ongoing project, COMPASS2020, aims to demonstrate the combined use and seamless coordination of manned and unmanned assets in maritime surveillance operations, improving drone capabilities for maritime tasks and focusing on software development for data fusion and risk analysis[19]. Similarly, BORDERUAS, launched in June 2020, explores data processing, fusion, and interpretation methods to support detection and tracking in rugged terrain, with the goal of enhancing patrolling efficiency along the EU's external borders – amounting to over 42.000 km of coastline and around 9.000 km of land borders, as recalled by the project[20].

A more recent example is «NESTOR – An Enhanced Pre-Frontier Intelligence Picture to Safeguard the European Borders»[21], an 18-month project with a budget exceeding €6 million, coordinated by the Hellenic Police. Starting in November 2021, NESTOR aims to establish a next-generation holistic border surveillance system that provides pre-frontier situational awareness beyond maritime and land borders, perfectly adapting to different geographies to obtain unprecedented situational awareness (European Commission 2021a). This will be achieved through a combination of sensing technologies, intelligent radar systems, wide-area visual surveillance services, UAVs, and thermal and optical cameras, with data fused through advanced AI analysis. The project's infographics clearly illustrate the interconnection of various technologies for patrolling and the convergence of collected information in dedicated data analysis centres, which are central to decision-making and operational capabilities on the ground.

Projects related to border digitalisation have sometimes faced legal challenges due to their potential consequences. One notable case is iBorderCtrl, a project involving lie-detecting technologies[22]. Funded through Horizon 2020 with €4.5 million and concluded in August 2019, iBorderCtrl developed and tested an AI-based interviewing system for border control, using a webcam to analyse travellers' micro-gestures to detect deceit. In March 2019, iBorderCtrl was brought before the General Court of the Court of Justice of the European Union (CJEU) by the Member of the European Parliament Patrick Breyer, after the European Commission refused to grant open access to relevant docu-

[18] C2 Advanced Multi-domain Environment and Live Observation Technologies (CAMELOT), Grant agreement ID: 740736. 1 May 2017 – 30 April 2021.

[19] Coordination of Maritime assets for Persistent and Systematic Surveillance (COMPASS2020), Grant agreement ID: 833650. 1 May 2019 – 31 October 2021.

[20] Semi-autonomous border surveillance platform combining next generation unmanned aerial vehicles with ultra-high-resolution multi-sensor surveillance payload (BorderUAS), Grant agreement ID: 883272. 1 June 2020 – 31 May 2024. For other Horizon 2020 projects relevant to digital patrolling in progress see https://roborder.eu/related-projects/.

[21] An Enhanced Pre-Frontier Intelligence Picture to Safeguard the European Borders (NESTOR), Grant agreement ID: 101021851. 1 November 2021 – 30 April 2023.

[22] Intelligent Portable Border Control System (iBorderCtrl), Grant agreement ID: 700626. 1 September 2016 – 31 August 2019.

ments, raising concerns about bias in exclusion decisions[23]. While the Court protected the commercial interests of the project, it acknowledged the public interest in democratic oversight of surveillance technologies and the need for public discussion on their development with public funds (see also European Digital Rights 2021).

Attention and funding for innovative and increasingly autonomous modes of digital patrolling (and bordering, more broadly) are thus rapidly growing and raising concerns. Further research is necessary to ensure that technological advancements are accompanied by serious reflection on the legal, political, and ethical implications they entail. While many projects invoke a human rights discourse, they often do so in instrumental ways that primarily serve to legitimise their trials.

In conclusion, the analysis proposed in this chapter suggests that the integration of high-tech solutions in patrolling strategies often indicates a failure to address the complexities and polyhedralities of migration. The almost spasmodic pursuit of surveillance automation and deployment of military or semi-military technologies at borders seem to cement a blurred convergence of border control, migration management, and access to international protection, reflecting a failure to develop broader (while, maybe, less *multipurpose*) approaches and policies on mobility and access to international protection. The «securitised transformation of Europe's borderscapes», as Martin Lemberg-Pedersen (2013) describes it, frames migration as an existential threat to security: it might be argued that the digitalisation of patrolling represents a continuation of migration and asylum policies (or, rather, their obstruction) by other means.

[23] CJEU, *Breyer v. Commission*, Case T-158/19, 15 March 2019.

CHAPTER 2

Digital patrolling in Greece: drones flying over sea and land borders

2.1. Setting the scene: digitalisation, militarization, and experimentation

Despite the scarcity of official documentation, evidence shows that drones are being utilised for border surveillance in several critical frontier areas in Greece (Molnar 2022). However, delineating the specifics of the deployment of Remotely Piloted Aircraft Systems – such as the technical attributes of these systems, the authorities responsible for their operation, and the modalities of their integration into border patrol operations – presents significant challenges. This difficulty is primarily due to the pervasive secrecy shrouding the digitalisation of patrols, both at the European level and, even more so, within national jurisdictions. As a result, a careful triangulation of fragmented information sourced from expert analyses, media reports, and procurement tenders is necessary.

Given this complexity, the analysis of the broader context within which these new surveillance technologies are being deployed becomes particularly valuable. The decision to experiment with new patrolling systems is, in fact, not merely a technical or operational matter; rather, it is deeply embedded within and shaped by the surrounding political, social, and legal contexts. A critical understanding of the situation at the Greek borders allows for a series of deductive inferences about the use of unmanned aerial vehicles, enabling a partial reconstruction of the phenomenon and suggesting paths to get around the limited access to primary sources. The opacity and inscrutability surrounding these developments are after all characteristic of new and evolving bordering practices that are taking place in the proximities of the military domain – areas that have been largely shielded from public scrutiny and judicial investigation.

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

In light of these challenges, to have a better understanding of this worn-out section of the mosaic, a comprehensive understanding of digital patrolling in Greece requires a broader perspective, a step back to take a look at the whole picture. This entails retracing the political and geopolitical role of border enforcement in Greece and examining the intersecting processes of technologisation and militarization that define this landscape.

The analysis thus begins by situating digitalisation within the wider legal and political frameworks that have shaped the militarization and experimentation along Europe's external borders. Attention then turns to the strategic importance of these border regions, particularly concerning the allocation of funds aimed at advancing digital surveillance initiatives. Special focus is given to the deployment of drones by European agencies and national authorities for border monitoring. Following, the regulatory frameworks – positioned at the intersection of migration law and border control – governing the digitalisation of patrols and the use of drones are critically explored. Finally, these trends are considered against the backdrop of the endemic violence that has characterised the Greek borders in recent years.

2.1.1. European shield: «nobody gets through»

The strategic significance of Greece's borders extends far beyond national interests, encompassing animated concerns for the European Union as a whole. This was starkly evident in early March 2020, during a period of heightened tension between Greece and Türkiye, following President Recep Tayyip Erdoğan's declaration that Türkiye would open its borders to Europe. Upon her arrival in Greece, European Commission President Ursula von der Leyen commended Athens for serving as «our European ασπίδα» (shield) (European Commission 2020b). This designation underscored Greece's role as a crucial defensive barrier for Europe. Concurrently, however, Greece took the controversial step of suspending all asylum application procedures for individuals arriving from Türkiye for a month (Human Rights Watch 2020). This measure, far from being commendable, raises significant human rights concerns. According to a major investigation conducted by *Der Spiegel*, when Türkiye ceased intercepting people attempting to cross the borders, Greek officers were instructed with a clear directive: «nobody gets through» (Christides et al. 2021).

This development is neither unprecedented nor unexpected; it reflects a longstanding dialectic between Greek and European institutions regarding migration. At least since 2010, the Greek governments have in fact tended to present the migratory pressure at the Greek-Turkish border as a European problem, one that necessitated a strong response from EU institutions (Carrera and Guild 2010).

However, this strategic approach towards Greece's borders is not solely determined by geographical considerations. Over the past few decades, these borders have increasingly been regarded as a privileged testing ground for new technologies and surveillance mechanisms. Petra Molnar aptly describes Greece as «a surveillance sandbox at the frontiers of Europe» (2022, 54). This experimental turn has prompted warnings from organisations such as Euro-Med Human Rights Monitor, which caution against the potentially dangerous and discriminatory outcomes stemming from the experimental use of digital technologies at Greek borders, especially those deployed with «a clear deterrence aim» (Euro-Med Monitor 2021). A particularly striking example is the use of Long Range Acoustic Devices (LRADs), or 'sound cannons', whose deployment along the Turkish border was extensively documented during the summer of 2021. These devices appear to be part of a broader array of experimental digital barriers that were implemented and tested especially during the challenging months of the Covid-19 pandemic and the associated lockdowns, thus largely beyond public scrutiny.

2.2. Strategic frontiers: the Evros River, the Aegean Sea, and the Turkish side of the story

In examining the patrolling systems along the Greek-Turkish border, two key areas stand out: the Evros region, where the eponymous river demarcates the border, and the Aegean Sea, where Greek islands – frequently spotlighted due to the dire conditions in hotspots such as Chios, Samos, Leros, and Kos – stretch towards Türkiye. These *borderzones* are characterised by dense patrolling systems that, at the edges of these highly militarized regions, often give rise to extreme violence (Topak 2021, 6). The Evros border, which spans 206 kilometres, periodically draws national and European political attention, emphasising its geopolitical significance. This region is marked by the wide, fast-flowing Evros River, which branches into several streams, some of which are punctuated by small islands. Winter conditions are harsh in the area, with temperatures falling to ten degrees below zero. The Evros border is now a military exclusion zone, heavily monitored with cameras, searchlights, night-vision equipment, and sensors (Euro-Med Monitor 2021). Information from this zone is tightly controlled, with little available beyond what is officially released by the Ministry of Interior. Recently, several NGOs have raised concerns about an 'information blackout' from Evros, as access for researchers, human rights activists, and humanitarian workers has become increasingly restricted.

Since 2011, following the designation of the Evros route as a primary gateway to Europe for migrant people (Topak and Vives 2018), Greek authorities have fortified the border with a steel wall at key crossing points, built under the newly approved Integrated Border Management Programme for Combating Illegal Immigration (see Papatzani et al. 2020). The Programme, aimed at protecting both EU and national borders and reducing irregular migration, continues to have far-reaching implications. In May 2022, the wall extends over 38 kilometres, with plans to expand it by at least another 30 kilometres by the end of the year, incorporating more advanced surveillance technologies with substantial support from the European Union (Bathke 2021).

In the summer of 2012, Greek authorities supplemented the wall's construction with *Operation Aspida* (Shield), which significantly increased the number of border officials and mainly resulted in the shifting of migratory routes from Evros to the Aegean Sea (Koca 2020; UN Office of the High Commissioner for Human Rights 2012). By September 2020, amidst heightened tensions with Türkiye and the instrumentalization of migrant people as political leverage, the Ministry of Civil Protection announced an escalation in the armament of the Evros border. This included the deployment of four drones for aerial surveillance, fifteen thermal cameras to detect nighttime migratory flows, ten armoured jeeps, and five inflatable boats to enhance patrols (e-evros.gr 2020). There is in fact evidence that drones, alongside other surveillance technologies such as night-vision goggles, thermal cameras, laser rangefinders, and pulse radars, are being tested and utilised in the Evros region (Molnar 2022). Moreover, since 2021, Frontex has introduced advanced aerostats in the area, capable of remaining airborne for up to forty days, marking a significant innovation in border surveillance (Monroy 2022b).

Similarly, surveillance in the Aegean Sea has intensified steadily over the years. Maritime borders are increasingly monitored by vessels and air units equipped with digital patrolling technologies, enhancing detection, tracking, and risk analysis capabilities, and fundamentally enlarging the scope of situational awareness in the region. Much like the Evros border, the Aegean Sea has seen a shift from intensive physical patrols to remote controls. The literature extensively discusses how this push for greater efficiency through technologically advanced and *smart* systems is largely driven by exclusionary rationales, aiming to effectively keep people out (Topak 2014).

Already in 2009, the Greek Coast Guard began utilising the Automatic Identification System (AIS), a tracking mechanism for ships and boats, instrumental also in identifying vessels used by people on the move heading to islands such as Lesbos, Chios, Samos, or Patmos, which lie just a few kilometres from Türkiye. The introduction of the Integrated Border Management System, comprising the Surveillance Operational Centre (SOC), has accelerated the shift towards digital and remote patrolling. This system allows multiple border sections to be monitored simultaneously and communicates with patrol units by analysing real-time data from various surveillance sources. The SOC is linked to the Greek National Coordination Centre (NCC), which, as discussed in the previous chapter, transmits data to EUROSUR, contributing to the European Situational Picture and the Common Pre-frontier Intelligence Picture. The rationale behind this development is rooted in a preventive approach to border control. As reported by Özgün E. Topak (2014, 826), the SOC is in fact particularly valuable for its ability to monitor border situations and direct patrol units precisely to locations where migrant people are approaching.

Moreover, it should be noted that the digitalisation of patrols extends beyond the Greek side of the border. On the Turkish side, border areas are also subject to intense surveillance. The increasing digitalisation and militarization of Turkish border regions sometimes align with Greek efforts to contain and limit arrivals, while at other times, they contribute to documenting Greek border operations, including pushbacks.

The use of advanced security technologies in Türkiye dates back to 2011, when the country became the world's largest refugee host following the outbreak of war in Syria. The European Union played a significant role in modernising the Turkish-Greek border, supporting the establishment of additional patrols at both sea and land borders. In May 2012, Turkish authorities signed a memorandum of understanding with Frontex to prevent irregular migration and update border surveillance systems through cooperation in risk analysis, training, research, and development (Frontex 2012). Once again, on all sides, these operations were justified with references to both security threats and humanitarian concerns for the lives of people on the move in border areas (Koca 2020).

Of course, such technical agreements should be viewed within the broader framework of cooperation between Greece, the European Union, and Türkiye on migration management and control. In this context, the conclusion of the EU-Türkiye Statement stands out as a pivotal moment. Agreed upon in March 2016 during the height of the so-called 2015 refugee crisis, the Statement was signed by Türkiye and the Member States gathered within the Council – the latter acting on behalf and in the interest of the Union, despite not in the Council capacity – under a nebulous legal framework. The Statement remains central to the EU's externalisation strategy. Through this controversial and debated agreement, Türkiye was declared a 'safe third country' under Article 38 of the Asylum Procedures Directive[1]. In essence, Türkiye committed to receiving and protecting approximately three million Syrian refugees in exchange for substantial funding and the initiation of visa liberalisation negotiations for Turkish citizens (see Favilli 2018). A 'fast-track' border procedure was introduced in Greece by Law 4375/2016-55 (Art. 60 para. 4)[2], *de facto* establishing hotspots at external borders to facilitate the Statement's implementation. The core of the Statement lies in a non-arrival policy, with Türkiye pledging to take all necessary measures to shut down maritime and land routes to Europe (Petracou et al. 2018). This commitment includes enhancing surveillance capabilities and adopting a preventive border control approach using advanced technologies. Consequently, there have been several reports of joint patrol operations between Greek and Turkish forces, where people on the move intercepted by Greek remote patrolling systems have been apprehended by Turkish patrol units.

Recently, Türkiye has also developed a sophisticated drone surveillance system over its border areas. According to a map published by a local newspaper in Evros, Turkish drone patrols have significantly increased since 2019, with extended flight hours along the Greek border (e-evros.gr 2021b). During periods of heightened tension with the EU, Türkiye has publicly highlighted numerous instances of violence and violations of the *non-refoulement* principle by the Greek Coast Guard in the Aegean Sea. Various videos circulated online

[1] Directive no. 2013/32 on common procedures for granting and withdrawing international protection (Asylum Procedures Directive), 26 June 2013.

[2] Law no. 4375/2016 on the organization and operation of the Asylum Service, the Appeals Authority, the Reception and Identification Service, the establishment of the General Secretariat for Reception, the transposition into Greek legislation of the provisions of Directive 2013/32/EC, 3 April 2016.

by the Turkish Armed Forces, supported by drone footage, document push-back operations carried out by Greece[3], illustrating a new 'materiality' and 'visibility' in digital patrolling that may lead to emerging forms of public scrutiny (İşleyen 2021). Not surprisingly, similar processes of drone surveillance, image collection, and public dissemination have also been employed by Greek authorities against Türkiye.

2.3. National and European priorities and funding

Investing heavily in state-of-the-art technologies for border patrolling is resource intensive. Over the years, the European Union has provided substantial support to address the border security needs expressed by Greek governments. The shift toward smart patrol systems emerges clearly when examining the projects, actions, and tools developed within the framework of European funds dedicated to border surveillance.

During the 2007-2014 financial period, the European Borders Fund played a significant role in supporting the purchase and use of coastal patrol vessels, particularly favouring very high-speed coastal patrol vessels (VHSCPVs) and high-speed boats for special operations (HSBSOs), which are mainly useful for rapid patrols at night (External Borders Fund 2007). Additionally, since 2007, several motion sensors have been installed in areas close to the borders, indicating a gradual shift toward technologically enhanced border control.

This trend continued under the Internal Security Fund (ISF) for the 2014-2020 period[4], where significant emphasis was placed on developing and installing the Maritime Borders Surveillance System and extending the automated surveillance system at the Greek-Turkish border (Hellenic Ministry of Citizen Protection 2015, 36). These measures have led to increasingly remote management of surveillance, aimed at preventing unauthorised mobility, that include the installation of cameras and radars capable – according to media reports (e-evros.gr 2021a) – to monitor up to 15 kilometres into Turkish territory. The strategic objectives outlined by the Greek government under the ISF prioritised improving national situational awareness capacities and enhancing integrated border management within the EUROSUR framework, with a focus on promoting automated surveillance systems. The goal was to transition from a man-based to a technologically assisted surveillance system, with significant contributions from Frontex (Hellenic Ministry of Citizen Protection 2015).

A key funding priority under the ISF was the deployment of a National Integrated Maritime Surveillance System (NIMSS), a network of integrated sur-

[3] See, e.g., "Drone footage shows Greece pushing back asylum seekers in Aegean – 05.04.2021", available at: https://www.yenisafak.com/en/video-gallery/news/drone-footage-shows-greece-pushing-back-asylum-seekers-in-aegean-2206349

[4] For a compendium of key documents on national legislation for the use of ISF funds, see (only in Greek): https://www-ydeap-gr.translate.goog/isf-b-v-tameio-esoterikis-asfaleias-synora-kai-theoriseis/nomiko-plesio1/?_x_tr_sl=el&_x_tr_tl=it&_x_tr_hl=it&_x_tr_pto=sc

veillance stations connected to an operational control centre. Although the NIMSS was expected to be fully operational by mid-2021, delays in the tender process mean that the first surveillance stations are expected to be fully functional by 2023 (Hellenic Ministry of Citizen Protection 2015). According to national security advisors, the NIMSS will significantly enhance border surveillance while minimizing unnecessary involvement of patrol vessels (Dokos 2021). Additionally, the Greek authorities have procured unarmed drones for surveillance of the sea borders in the East Aegean, as acknowledged by the European Commission (Lagos 2019).

The ISF also supported the purchase of hardware and software for risk assessment analysis aimed at preventing illegal entries at the borders. The national program defined by the Greek Ministry of Citizen Protection explicitly mentions the deployment of new technological equipment, such as mobile scan units, mobile heartbeat detection devices, Closed-Circuit Television Cameras (CCTV) systems, and UAVs to detect illegal migrants (Hellenic Ministry of Citizen Protection 2015, 18). This is one of the few governmental sources that explicitly outlines the intention to systematically integrate drones into the patrol system, with policy objectives focused on strengthening preventive policing and containing migrant people before they reach the EU's external borders (see also Human Rights Watch 2022).

Without taking into account the allocation of additional funds under the Borders Emergency Assistance (in particular in 2019), Greece benefited from almost €167 million under the ISF, second only to the €195 million allocated to Spain (European Commission 2020a). Recently, Greece has invested heavily in technology-led policing and border management, including advanced facial recognition and biometric processing software. Police officers have also been provided with smartphone-sized devices capable of collecting and storing such data (Chelioudakis 2020). A 'Smart Policing Program', aimed at increasing the efficiency of identification systems for third-country nationals, was also introduced by the Hellenic Police in April 2021 (European Union 2021). This program has faced criticism from various organizations for non-compliance with fundamental rights, in particular with the principle of non-discrimination, and the most basic privacy and data protection provisions (Human Rights Watch 2022).

Looking ahead, the initiatives funded under the 2021-2027 Integrated Border Management Fund indicate a persisting trend towards the use of increasingly advanced technologies to enhance the automation of patrolling activities. This is also supported by a recent draft decision by the EU Commission, which calls for Greece to further enhance its surveillance capabilities at land and sea borders by increasing reaction capabilities and deploying additional thermovision vehicles, cameras, helicopters, and drones (together with «a number of service dogs»)(European Commission 2022). Although the draft also emphasizes the need for Greece to strengthen the fundamental rights component of border management and to investigate pushback allegations, it highlights that the Greek authorities will need to further tighten controls at the borders.

2.4. Deploying drones: Frontex, EMSA, and national authorities

Following this overview of the advanced bordering practices in Greece, it is possible now to focus on the specific role and deployment of Unmanned Aerial Vehicles.

In Greece, the deployment of UAVs for border surveillance is mainly attributed to European agencies like Frontex and the European Maritime Safety Agency, although national authorities also operate drones in various border areas, particularly in the Evros region. In the European Union, competencies in the field of border security and control remain in fact closely linked to the exercise of State sovereignty. Thus, once advanced surveillance tools such as UAVs are introduced for security purposes by EU agencies, national authorities are likely to expand their use and claim more competencies over them. In this case, Frontex and EMSA have been pivotal in integrating drones into patrol systems.

Frontex's involvement at the Greek borders became significant in 2010, when the Greek government requested specific assistance, leading to the deployment of the Agency's Rapid Border Intervention Teams (RABITs)[5]. This operation, the first of its kind in Europe, ended in March 2011 but marked the beginning of Frontex's sustained presence in Greece, particularly in the Evros region. The Agency contributed to the militarization of patrol systems and the increasing preference for remote surveillance tools in the area (Topak and Vives 2018). Frontex has also been instrumental in establishing a risk management approach to border control, focusing on future-oriented, remote interventions designed to «secure unknown futures» (Amoore 2013, 153).

Since 2010, several operations have taken place at the Greek-Turkish borders, with Joint Operation Poseidon being particularly significant. Initially aimed at controlling the maritime borders between Greece and Türkiye, this operation was reinforced in 2016 to assist Greek authorities with enhanced border surveillance capabilities and a higher number of officers (Ilias et al. 2019, 25). More recently, between March and October 2020, Frontex launched the Rapid Border Intervention Aegean 2020 and the Rapid Border Intervention Evros 2020 operations at the Greek-Turkish land and sea borders (Frontex 2020). Currently, Frontex operates under the multipurpose Operation Poseidon, covering both Greek sea borders with Türkiye and the Greek islands (Frontex 2021b). Despite the absence of official statements, there is evidence that UAVs have been deployed in these operations (see Monroy 2020). Moreover, there is evidence of collaboration between Frontex and Greek authorities aimed at indiscriminately reducing arrivals, even at the expense of potential international protection applicants. This was highlighted during a meeting in May 2021 between Greek Prime Minister Kyriakos Mitsotakis and Frontex head Fabrice Leggeri, where

[5] At EU level, Member States can initiate joint operation and rapid interventions with the possibility for Frontex to intervene at the external border of a Member State, as foreseen in Regulation no. 2016/1624 on the European Border and Coast Guard, replaced in 2019 by Regulation no. 2019/1896.

they complimented each other over cooperation resulting in an 80% reduction of arrivals to Greece in 2020 and a further 72% reduction registered until the spring of 2021 (European Council on Refugees and Exiles 2021).

EMSA's public communication is more transparent regarding its use of drones to support Member States in enhancing maritime surveillance capabilities. For example, EMSA records indicate that, in 2019, Greece was provided with remote-controlled surveillance aircraft for a total of 155 flight hours, designated for use by both the Hellenic Coast Guard and Frontex (European Maritime Safety Agency 2021). EMSA's 2022 Agency Outlook confirms the continued provision of Remotely Piloted Aircraft System services to Member States and EU agencies, with plans to develop multipurpose regional services for operational capability sharing among neighbouring coastal states (European Maritime Safety Agency 2022). While in 2022 these systems are primarily intended for monitoring oil spills, the same national and European agencies involved in maritime border surveillance are the final users of these drones, raising concerns about the potential extent of their use beyond EMSA's stated objectives.

At the national level, the deployment of drones is closely tied to Greece's security apparatus, including the Armed Forces, Police Services, and the National Intelligence Service. In 2017, the Greek Deputy Minister of Citizen Protection announced that the Hellenic Police had been equipped with drones for border surveillance, aiming to intensify border controls with Türkiye (Loukinas 2017). More recently, in 2020, the Hellenic Police also procured two drones for border patrols under the HEFESTOS project (Hellenic anti-Fraud Equipment and relevant training for Strengthening the Operability against Smuggling) (Hellenic Republic Ministry of Civil Protection 2020; Homo Digitalis 2020b). The Western Greece Region as well procured UAVs for security forces, intended for various purposes, ranging from environmental and civil offence detection to smuggling prosecutions, and area surveillance (Region of Western Greece 2020). In November 2021, the Greek Navy purchased five unmanned helicopters for maritime security and surveillance, specifically the New Alpha 900, known for their redundancy in critical systems, making them suitable in particular for target acquisition and reconnaissance operations (McNabb 2021). Additionally, media reports suggest that Greece will soon lease two more Heron-1 UAVs from an Israeli company to enhance surveillance in the Aegean, explicitly meant to manage a potential new wave of migrant people and asylum seekers (see Monroy 2022a). These developments underscore the increasing, albeit partially opaque to public scrutiny, presence of drones in Greek border surveillance.

From an organizational perspective, the introduction of new surveillance systems has created a significant divide between Greek agencies and officials working remotely from operational centres and those conducting physical patrols on the ground. This divide, as highlighted by Dijstelbloem et al. (2017), exacerbates the risk of a divergence in the perception of situations 'remotely' versus 'on the ground', potentially having serious consequences from a fundamental rights perspective. The growing reliance on digital patrolling reduces direct *encounters* between patrols and migrants, which could, on the one hand, limit episodes of violence and arbitrary conduct but, on the other, contribute to the dehumanization of border enforcement, a concern that will be further explored in chapter 4.

2.4.1. From borders to camps

The use of drones for monitoring migrant populations in Greece extends beyond the borders with Türkiye, encompassing surveillance over 39 migrant and refugee camps across the Greek mainland and islands. This panoptic surveillance expands the concept of patrolling presented in this book.

Central to this security apparatus is the 'Centaur' system, an integrated digital platform for electronic and physical security management deployed within and around targeted facilities. This system utilizes cameras and motion analysis algorithms to monitor camps (Statewatch 2021; Petridi 2021). Notably, Centaur is fully funded by the EU's Recovery and Resilience Facility, intended to support Greece's digital transition (Hellenic Ministry of Digital Governance 2021; see also Geese and Marquardt 2021). The presence of seven patrolling drones, magnetic gates equipped with thermographic cameras, x-ray machines, and security cameras at the camps' entry and exit points has been reported by various media and NGO sources (Emmanouilidou and Fallon 2021; European Council on Refugees and Exiles 2021). All data gathered is transmitted to a control centre at the Ministry of Migration and Asylum in Athens, further centralizing surveillance efforts (Monroy 2022a).

From the perspective of State security in border enforcement, particularly in Greece, where borders and terrain twist in particularly inaccessible areas, drones offer undeniable advantages – especially when the costs associated with testing and deploying new technologies are at least partly borne by European funds. Drones' ability to operate in darkness, traverse difficult terrain, and collect real-time information makes them a valuable asset that authorities are unlikely to relinquish in the future. Drones also significantly reduce communication errors between units, allowing for the collection and, in some cases, the AI-assisted analysis or filtering of large volumes of data, which would otherwise require a disproportionate deployment of personnel. However, this vast accumulation of data also raises crucial concerns about how the information collected is processed, stored, and used.

2.5. Delineating the use of drones for border patrols: a rhizomatic and vanishing regulatory framework

Just as the analysis of the integration of drones in border patrols, reconstructing the regulatory framework governing the use of drones for border patrols is fraught with challenges. The complexities arise from several factors: the limited and fragmented information available on these regulations, the operational and technical nature of the existing framework, and the ongoing development of new legal structures, which make the regulatory landscape appear rhizomatic – an interconnected and somewhat elusive system that is difficult to analyse comprehensively (Marin 2017). Furthermore, the novelty of digital patrolling means that there is a lack of case law directly addressing the use of drones in border surveillance.

Under these circumstances, to understand the regulatory context in which drone use for border patrols is situated, as for the previous paragraphs, it is useful to first explore the broader trends in Greek migration law and border control policies. This exploration highlights once again the increasing securitization and militarization of borders and the corresponding reduction in protection for people on the move.

2.5.1. Greek migration law: rights shrink, barriers multiply

Recent developments in Greek migration law reveal a consistent trend toward the reduction of rights and protections for non-EU nationals, including migrant people, asylum seekers, and recipients of international protection. This shift, as discussed, has been accompanied by a tightening of border controls, reflecting a broader logic of militarization and deterrence (Pannia et al. 2018; Petracou et al. 2018). Notably, significant changes have been made in both national asylum and immigration legislation and border surveillance laws. While these are distinct areas of law, their developments are interconnected, particularly as stricter border surveillance is often aimed at preventing people on the move from reaching Greek territory.

One of the most significant legislative changes in recent years is Law 4636/2019 on International Protection, which was later amended by Law 4686/2020[6]. It codified existing legislation on the recognition of beneficiaries of international protection, asylum procedures, reception conditions, and judicial protection (Greek National Commission for Human Rights 2021). However, this legislative framework has been widely criticized as a regression in terms of migrant people's rights by both the Greek National Commission for Human Rights (GNCHR) and the UN Refugee Agency (UNHCR 2019).

The concerns surrounding this legislation focus particularly on the broadening and intensification of detention measures, which contribute to the criminalization of asylum seekers, and the introduction of stricter deadlines that accelerate asylum procedures without providing adequate safeguards, especially for applicants in particular conditions of vulnerability (Greek National Commission for Human Rights 2020; Papatzani et al. 2020). The impact of Law 4686/2020 was further exacerbated by the Covid-19 pandemic, particularly following the suspension of asylum applications between February and March 2020, a move justified by the tense political situation at the Greek-Turkish border (Greek National Commission for Human Rights 2021).

[6] Law no. 4636/2019, on international protection and other provisions, 1 November 2019 and Law no. 4686/2020, improvement of the migration legislation, amendment of Law 4636/2019, 4375/2016, 4251/2014 and other provisions, 12 May 2020.

In September 2021, the Greek Parliament passed Law 4825/2021, which amended procedures for deportation, return, residence permits, and asylum applications[7]. This law has raised alarms among various organizations as it further entrenches security measures, thus reducing safeguards against detention and increasing the risk of deportation to countries where individuals may face persecution or human rights violations. The Commissioner for Human Rights of the Council of Europe also expressed concern, particularly regarding Article 40, which *de facto* prohibits NGOs from conducting or supporting sea rescue operations (Commissioner for Human Rights 2021a).

These legislative changes illustrate a broader trend in Greek migration law: a shift away from protecting the rights of migrants and toward a securitized and exclusionary approach. This trend mirrors the increasingly complex and fragmented regulatory framework governing drone use in border patrols, highlighting the challenges of balancing security with human rights in border management.

2.5.2. Regulating border surveillance

The emerging regulatory framework for border surveillance in Greece also mirrors this broader, concerning picture[8]. This framework can be broadly categorised into two distinct branches: one governing the relationship with Frontex, the other dealing with domestic regulations.

Law 3902/2010[9], which transposes Council Regulation 2007/2004, defines the cooperation modalities between Frontex and Greece for hosting the Agency's Operational Office. Additionally, Regulation 1168/2011 outlines the conditions under which Frontex may engage in border surveillance operations when heightened technical and operational assistance is required[10].

On the domestic side, Law 4249/2014 establishes the Hellenic Police's responsibility for border protection through its Border Protection Directorate,

[7] Law no. 4825/2021, reform of deportation and return procedures of third country nationals, attracting investors and digital nomads, issues of residence permits and procedures for granting international protection, provisions within the competence of the Ministry of Migration and Asylum and the Ministry of Citizen Protection and other emergency provisions, 4 September 2021.

[8] See Ilias et al. (2019, 22) for a comprehensive reconstruction of the Greek national legal framework on border surveillance.

[9] Law no. 3838/2010, on Current Provisions related to Greek Nationality and the Political Participation of Expatriates and Legally Residing Immigrants, 24 March 2010.

[10] Council Regulation no. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 26 October 2004 (no longer in force) and Regulation no. 1168/2011 amending Council Regulation (EC) no. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 25 October 2011 (no longer in force).

as stipulated in Article 18[11]. Further, Law 4332/2015[12] reaffirms that the Greek Police and Coast Guard, as reorganised by Law 4249/2014, are charged with the surveillance of both land and maritime borders (Article 8).

In this context, the ongoing militarization of border surveillance has recently gained new momentum. Law 4650/2019 marks a significant step in this direction[13]. Among other provisions, the law establishes the Unified Border Surveillance Body, tasked with the comprehensive monitoring and control of external borders. The Surveillance Body reports directly to the newly created National Coordinator for the treatment and management of the «immigration-refugee issue», as provided by Article 11. Moreover, the law facilitated the deployment of new law enforcement units in border areas and authorised the hiring of an additional 400 border police patrol officers at various entry points across the country (Human Rights 360° 2020).

The regulatory framework governing surveillance systems is anchored in Law 3917/2011, which addresses the retention of data generated or processed by surveillance systems used to capture or record audio or video in public spaces[14]. It is important to note that Chapter A of this law transposes Directive 2006/24 (the Data Retention Directive)[15], which was later declared invalid by the Court of Justice of the European Union in two parallel cases raised in Ireland and Austria[16]. The CJEU ruled that the directive failed the proportionality test, infringing on the rights to privacy and data protection as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR)[17]. Legal scholars have further argued that drone imagery captured by the Hellenic Police does not fall within the scope of video surveillance systems as defined by Law 3917/2011, highlighting the inadequacy of what is widely regarded as the legal basis of drone surveillance (Homo Digitalis 2020a, 21).

[11] Law no. 4249/2014, Reorganization of Greek Police, Fire Brigade and the General Secretariat for Civil Protection, upgrade of the Services of the Ministry of Public Order and Citizen Protection and regulation of other matters concerning the Ministry of Public Order and Citizen Protection, 24 March 2014.

[12] Law no. 4332/2015, Amendment of the provisions of the Greek Nationality Code – Amendment of Law 4521/2014, 9 July 2015.

[13] Law no. 4650/2019, Regulations of issues of the Ministry of National Defence and other provisions, 17 December 2019.

[14] Law no. 3917/2011, Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the obtaining or recording of sound or image at public areas and relative provisions, 21 February 2011.

[15] Directive no. 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications (Data Retention Directive), 15 March 2006 (no longer in force).

[16] CJEU, Joined Cases Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12 and C-594/12, 8 April 2014.

[17] An in-depth commentary on these cases can be found in Podkowik, Rybski, and Zubik (2021).

In 2019, new regulations were introduced to specifically govern the use of drones by the Hellenic Police. Initially justified as a public health measure to enforce pandemic-related movement restrictions, these provisions were not limited to areas most at risk of Covid-19 transmission (Chelioudakis 2020). In fact, Presidential Decree 98/2019 significantly expanded the Police's authority to use drones, extending their deployment to monitor migration in border regions – a clear departure from the original pandemic-related rationale[18]. The decree outlines three scenarios in which drones may be deployed: to provide aerial support to police operations (though the nature of this support is not specified), to survey areas under local police jurisdiction, and to relay information to ground forces during specific missions, including those aimed at crime prevention and «tackling illegal immigration in border regions» (Homo Digitalis 2020a).

Before this decree, the Hellenic Police's use of drones was confined to monitoring traffic on motorways and observing forests to detect potential fires, as per Presidential Decree 21/2017[19], which established the Unmanned Aircraft Service (UAS) within the Directorate of Special Police Forces (Homo Digitalis 2020b). Notably, the drones available to the Hellenic Police are equipped with high-resolution cameras, thermal imaging for night operations, and photogrammetry capabilities for high-resolution mapping. There are also indications that these drones may soon be outfitted with systems for intercepting telephone conversations, interfering with mobile signals, and positioning them. The expanded mandate, coupled with enhanced technological capabilities, has raised significant concerns regarding data protection.

2.5.3. Images, photos, and videos from the sky: which protection?

The deployment of drones in policing and border management inevitably involves the collection of images and videos of individuals. When these images allow for the identification of persons, whether directly or indirectly, the reception, collection, storage, retention, and transmission of such data constitute personal data processing[20]. This process must adhere to specific legal safeguards. The Hel-

[18] Presidential Decree no. 98/2019, Organisation and structure of the Drone Service, 25 October 2019. The Decree introduces significant changes to Article 25 of Law 2800/2000 regulating the operating provisions regarding air means deployed by Security Forces and covering in particular the suppression of fires and the rescue of victims in case of disasters.

[19] Presidential Decree no. 98/2019, Organisation and structure of the Drone Service, Establishment of Procurement Directorates and History of the Hellenic Police and Unmanned Aircraft Service, 21 March 2017.

[20] Personal data, according to the definition provided by Article 4 para.1 of the Regulation No. 2016/679 (General Data Protection Regulation), means «any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person».

lenic Data Protection Authority's (HDPA) latest Annual Report acknowledges the operational use of unmanned aircraft by the Hellenic Police and the establishment of Unmanned Aircraft Systems, highlighting that drones inherently process image, and potentially audio, data capable of identifying individuals (Hellenic Data Protection Authority 2021, 118). Despite the fact that European data protection provisions are to be considered applicable, Presidential Decree 98/2019 remains notably vague regarding the specifics of data storage and processing, merely stating that images from unmanned aircraft are processed according to existing legislation (Homo Digitalis 2020d).

In correspondence with the Hellenic Police, the HDPA emphasised that under Law 4624/2019[21], which transposes the EU Directive 2016/680 on the protection of natural persons concerning the processing of personal data (Law Enforcement Directive)[22], authorities are obliged to process personal data lawfully and only to the extent necessary for their tasks (see Hellenic Data Protection Authority 2021, 119). Lawful processing requires that Member States enact clear laws specifying the objectives and purposes of such data processing (Article 8, EU Directive 2016/680).

The HDPA specifically refers to Articles 65 and 67 of Law 4624/2019, which mandate that before engaging in processing activities involving new technologies such as UAVs, the Hellenic Police must consult the HDPA and conduct an impact assessment on personal data protection[23]. The HDPA's Decision 65/2018 identifies scenarios where such assessments are mandatory, which include cases of systematic and large-scale processing for monitoring, observation, or control of individuals via video surveillance systems or other data processing methods (Hellenic Data Protection Authority 2018). The impact assessment should provide a detailed description of the operations, evaluate the risks posed to the rights and freedoms of the data subjects, outline measures to mitigate these risks, and specify safeguards and security measures to ensure the protection of personal data[24].

The HDPA's Decision 65/2018 also underscores the absence of a robust legal basis necessary for the lawful deployment of drones by the Hellenic Police. Law

[21] Law no. 4624/2019, On the Hellenic Data Protection Authority, the implementation of Regulation 2016/679 and the transposition of Directive 2016/680, 29 August 2019.

[22] Directive no. 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive), 27 April 2016.

[23] Homo Digitalis (2020a, 23) offers an in-depth analysis of the specificities of 'new technologies', proceeding by analogy from the *List of types of processing operations subject to the requirement to carry out a data protection impact assessment* (2018) published by the Hellenic Data Protection Authorities and addressing the provisions of the GDPR. The list is considered a relevant guide in interpreting the provisions defined by Directive 2016/680 apply. In fact, the Authority explicitly states that a relevant example of systematic and large-scale processing is given by the processing of data through drones.

[24] On impact assessment and new technologies in border control, see also Burgess and Kolza (2021).

3917/2011, Article 14(4), stipulates that the procedure and conditions for operating surveillance systems, including proportionality criteria, types of personal data processed, and security measures, must be established by a Presidential Decree[25]. However, since Presidential Decree 98/2019 fails to reference these obligations or incorporate safeguards to prevent misuse or abuse of drone technology, the HDPA argued that the decree effectively renders the regulations governing drone use by the Hellenic Police inactive and the protections under Law 4624/2019 and Directive 2016/680 ineffective (Hellenic Data Protection Authority 2021, 119). As a result, the general provision in Decree 98/2019 stating that image processing by drones is conducted «in accordance with the applicable legislation» remains void and largely unenforced.

A report by the Greek NGO Homo Digitalis (2020a, 22), which advocates for digital rights, similarly highlights the lack of defined procedures and conditions for drone use, criteria for maintaining proportionality, and guidelines for data collection, storage, and transmission within the national legal framework[26].

In response to these regulatory gaps, Presidential Decree 75/2020, adopted in September 2020[27], provides rules for the use of surveillance systems to capture or record audio or video in public spaces, based on Law 3917/2011, Article 14(4)[28]. The Decree's definition of «surveillance systems» includes mobile vehicles operated by individuals or other vehicles of any kind, whether manned or unmanned. In accordance with Article 14 paragraph 1 of Law 3917/2011, Article 3 of the Decree outlines the purposes for which surveillance systems can be installed, ranging from national defence to the prevention and suppression of crimes against public order.

The HDPA (2020), when reviewing the draft Decree, interpreted its provisions in light of the General Data Protection Regulation (Regulation 2016/679)[29], Directive 2016/680, and Law 4624/2019. The Authority reiterated that surveillance systems, including UAVs, must comply with data protection legislation, considering the specific context in which these technologies are used. Although not detailed here, the Aviation Law framework is also relevant: on this point,

[25] Notably, the explanatory memorandum accompanying draft law 3917/2011 clarifies that the provisions established by the act do not apply in situations where the processing of personal data is unfeasible, such as in cases involving systems that capture remote images without the capability to enlarge and identify individuals or other information pertaining to natural persons.

[26] It is also worth noting that Homo Digitalis (2020e) submitted an official inquiry regarding the use of drones by the Hellenic Police. However, it appears that no response has been received to date.

[27] Presidential Decree no. 75/2020, Use of surveillance systems obtaining or documenting sound and pictures in public places, 10 September 2020.

[28] Although it falls beyond the scope of this analysis, it is worth mentioning that this Decree has been strongly criticised by several organisations, such as Amnesty International (2021), for infringing or potentially infringing on the right of assembly and expression.

[29] Regulation no. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 27 April 2016.

the HDPA, as indicated by the Greek Civil Airport Service's Decision on the general framework for Civil Aviation Authority flights, reiterated the limits of drone use to specified and justified purposes, with restrictions on geographical and temporal scope.

Additionally, the HDPA highlighted that any additional equipment or software used to enhance surveillance by «further processing of the image and sound», for instance in cases of facial recognition, constitutes distinct processing activities that must adhere at every single stage of the process to the principles of lawfulness and data protection (Hellenic Data Protection Authority 2020, 17). This is particularly critical when dealing with border surveillance and digital patrolling, where transparency is often lacking, and significant uncertainties persist regarding the processing of data collected by drones.

Furthermore, Article 12 of Presidential Decree 75/2020, which outlines the procedures for deciding on the deployment of surveillance systems, has recently been the focus of reports documenting widespread violations. The Decree requires the competent authority (with the status of the *controller*) to issue a decision for each surveillance operation, specifying activation time, duration, scope, system characteristics, and feasibility. However, data collected by NGOs indicate that the Hellenic Police has repeatedly violated these obligations (at least sixty-four times between November 2020 and May 2021), failing to provide adequate justification or transparency for its use of surveillance systems, thus endangering privacy rights (Homo Digitalis, Reporters United, and The Press Project 2021). In deviation from the relevant disclosure obligations, publicly accessible decisions regarding the use of surveillance systems remain vague and generic, which reasonably raises concerns as to whether such decisions are issued at all, much like the associated data protection impact assessments[30].

While these concerns have largely focused on the use of drones during the pandemic, even fewer safeguards will likely be applied to non-citizens, particularly in border areas designated as military zones, where legal provisions are even less clear, and public scrutiny mechanisms dissolve.

Moreover, the use of drones extends beyond the general processing of personal data. In fact, the images captured by UAVs often qualify as *sensitive* personal data, revealing information such as ethnic origin or religious beliefs, which could lead to discriminatory actions. There is also the potential for biometric data processing, particularly in the case of drones equipped with high-resolution cameras. Biometric data, as defined by Directive 2016/680 (Article 3) and transposed into Greek Law 4624/2019 (Article 44), include personal data derived from specific technical processing of natural, biological or behavioural characteristics: not only fingerprint data but also facial images that *could* (at least technically) be collected by the drones currently in use for patrolling the Greek borders. Notably, the HDPA has clarified that Law 3917/2011 does not

[30] At the time of writing, the Hellenic Police Service has denied access to these operating decisions even after requests for access have been issued by directly interested citizens.

cover the use of facial recognition and related identification technologies, which should be treated as separate data processing activities.

Nonetheless, under the 'Smart Policing Program', the Hellenic Police Directorate of the Ministry of Citizen Protection signed a contract in 2019 with the Greek company Intracom Telecom (2019) for a facial recognition software, which could be used in both drones and body-worn cameras. However, information on this software remains scarce, while the lack of transparency surrounding the purchase has been criticised. Homo Digitalis has called for further scrutiny, leading to an ongoing HDPA investigation into the Smart Policing Program and the Intracom Telecom contract (Fallon 2020). Adequate and necessary safeguards should indeed be imperative to balance the often secretive nature of border security measures against the risk of abuses. Yet, no conclusions have been drawn at the time of writing.

The NGO's concerns particularly focus on the collection of biometric data indicated by the contract without the necessary legal provisions, as required by the GDPR, which mandates that such data collection must be strictly necessary and subject to appropriate safeguards (Article 10) (Homo Digitalis 2020c). The absence of a robust regulatory framework raises the risk that drone use could result in unduly restrictive measures on individual rights, lacking the general and objective definition required by Greek case law (Hellenic Data Protection Authority 2020, 8). In border regions and migrant camps, these limitations could disproportionately affect vulnerable groups. Moreover, as repeatedly emphasised by the HDPA, restrictions on individual rights must be justified by compelling reasons of public interest and must be appropriate and clearly related to that purpose. Such restrictions should not infringe upon the essence of the right, nor should they grant excessive discretionary power. This aligns with the principles of legality, objectivity, and transparency that govern data processing.

In summary, the current regulatory landscape fails to fully integrate the principles of legality, necessity, and proportionality in the use of drones, especially in border areas. Moreover, despite a rather recent, complex, and evolving legal framework, a significant gap remains between the established rules and their implementation, leading to a deep disconnect between «the laws and real life» (Ilias et al. 2019). The analysis of reports, opinions issued by the HDPA, and tenders reveal ongoing transparency issues in digital patrolling and data processing, especially concerning sensitive and biometric data.

2.6. The use of drones in endemic border violence: the case of pushbacks

The deployment of drones for border surveillance in Greece must thus be critically examined within a context characterised by a lack of transparency, particularly in militarized zones, and within a regulatory framework that remains vanishing. This practice also aligns with a broader strategy aimed at limiting access to third-country nationals under the guise of migration prevention. Moreover, in recent years Greece has gained notoriety for the widespread use of indiscriminate violence and *refoulement* at its external borders. While the fourth chapter will provide a more detailed examination of the rights at risk in digital patrolling, it is wise to first outline some of the most notable instances of pushbacks that have precluded the possibility of lodging claims for international protection. In this context, the digitalisation of border patrols through the use of drones raises significant concerns, particularly regarding the facilitation of these illegal expulsions.

Over time, the evidence of systematic and violent pushbacks has become increasingly irrefutable. To focus on recent developments, in February 2021, the Greek National Commission for Human Rights (GNHCR) submitted a report to the UN Special Rapporteur on the Human Rights of Migrants, highlighting the growing number of recorded pushbacks (Greek National Commission for Human Rights 2021). The GNHCR noted that, despite numerous complaints lodged by organisations such as the Hellenic League for Human Rights and the Greek Council for Refugees since 2017, no Greek court has yet had the opportunity to rule on the issue. However, several complaints regarding border violence and pushbacks in contravention of the *non-refoulement* principle are currently under examination by the European Court of Human Rights[31].

In April 2021, the Greek Ombudsman released an interim report as part of an investigation initiated in 2017, condemning the relevant authorities for their failure to adequately investigate allegations of pushbacks at the Greek-Turkish land border (Ombudsman 2021). The Greek Helsinki Monitor (GHM) in May 2021 filed a criminal complaint concerning 147 pushbacks involving over 7.000 individuals between March and December 2020. This complaint was subsequently forwarded by the Supreme Court prosecutor to first-instance prosecutors for further investigation. The gravity of these incidents has prompted scrutiny and calls for investigations from both the Council of Europe's Commissioner for Human Rights, Dunja Mijatović, and the EU Commissioner for Home Affairs, Ylva Johansson (Commissioner for Human Rights 2021b). However, despite persistent calls from the United Nations High Commissioner for Refugees (UNHCR) and the European Commission for a rights-monitoring mechanism at Greek borders, the Greek Migration Minister formally rejected such a mechanism in October 2021, citing concerns over national sovereignty (European Council on Refugees and Exiles 2021).

These violations are not limited to Greek authorities alone; Frontex has also been implicated. In October 2020, an investigation by a consortium of media outlets including Lighthouse Reports, Bellingcat, Der Spiegel, ARD, and Asahi TV claimed that Frontex was complicit in and aware of several illegal pushbacks and collective expulsions of asylum seekers in the Aegean Sea (Bellingcat 2020). This revelation prompted an internal investigation by the Frontex Management Board, which could not definitively rule out the agency's involvement in pushbacks (Frontex 2021a). By July 2021, the European Parliament published a re-

[31] See in particular ECtHR, *L.A. and Others against Greece and A.A. against Greece*, Applications nos. 12237/20 and 12736/20, lodged on 5 March 2020 and 7 March 2020.

port following a fact-finding investigation into Frontex's alleged fundamental rights violations, concluding that while there was no decisive evidence of direct pushback operations by Frontex, the agency failed to address substantial evidence of fundamental rights violations at Greek borders (European Parliament 2021). Today, Frontex continues to be at the centre of different investigations and legal actions in the country[32].

Against this backdrop, the digitalisation of border patrols, including the use of drones by both Greek authorities and Frontex, raises profound concerns. While instances where drones have facilitated rescue operations at sea are occasionally publicised in government and agency press releases, the use of drones in supporting illegal pushback operations remains shrouded in secrecy. To fully understand the purposes behind drone deployments, it would be essential to have a comprehensive view of other assets contributing to border patrols. For example, if it could be established that drones are primarily used to enhance situational awareness within existing surveillance frameworks to support other units already on the ground or at sea, it would suggest that they are an integral part of broader border control mechanisms. Conversely, if drones are found to be replacing conventional patrols, it would indicate a shift in priorities away from rescue operations at sea. However, accurately reconstructing the operational landscape remains challenging, highlighting the need for further investigation.

In a context marked by widespread and often violent expulsions, it is reasonable to surmise that the deployment of advanced surveillance technologies, including drones, will reinforce these established practices. Nonetheless, there is currently no documented case of a pushback operation being directly facilitated by drone-collected data. Given the covert nature of such operations, it is highly unlikely that official sources would acknowledge this dynamic, and no judicial proceeding has addressed the issue to date.

Nevertheless, testimonies collected by organisations such as the Border Violence Monitoring Network (BVMN) provide a glimpse into the potential implications of drone surveillance in border control. Although BVMN does not specialise in new technologies, the network has in fact documented episodes that substantiate the fears of human rights activists on the use of drones for border control.

[32] Consider for example the action for damages brought against Frontex before the Court of Justice, alleging the illegal deportation of a Syrian family to Türkiye and the violation of their fundamental rights. According to Front-LEX, the organisation promoting the legal action, «despite undisputed and overwhelming evidence for serious and persisting violations of fundamental rights, FRONTEX and its Executive Director, Fabrice Leggeri, have failed to terminate the Agency's activities in the Aegean Sea, in flagrant infringement of the EU Charter of Fundamental Rights, the Treaty on the Functioning of the EU and Frontex Regulation» (Prakken d'Oliveira Human Rights Lawyers 2021). Furthermore, in February 2020, the GHM lodged a complaint against the violent expulsions and lawlessness occurring at the sea borders (Pagoudis 2022).

According to BVMN, for instance, on 6 October 2021, a group of approximately 200 people, including minors, attempting to cross the Evros River from Türkiye to Greece reported encountering a drone overhead (BVMN 2020). Shortly after, they were intercepted by Greek officers, their belongings were confiscated, and they were detained without food or water. The day after, they were forcibly returned to Türkiye across the Evros River, where Turkish military personnel were waiting. Similarly, on 27 August 2020, a drone reportedly facilitated the pushback of nearly 80 individuals in the same region, who were stripped of their personal belongings, including valid UNHCR-issued *Khartias* (temporary residence permits), before being expelled (BVMN 2020). Comparable incidents have also been reported at the Croatia-Bosnia border (BVMN 2019). Moreover, evidence suggests that when political conditions permit, drones and radars are also employed by Turkish authorities to carry out *pullbacks*, intercepting people on the move before they reach Greek territory, thereby systematically curtailing their chances of seeking asylum (İşleyen 2021, 1094).

Many scholars and organisations argue that these cases are not isolated incidents but reflect a broader strategy in which drones are used to intercept, apprehend, and push back people on the move, either directly or indirectly (Topak 2014, 824). What is indisputable is that the digitalisation of border patrols has not reduced recorded deaths during border crossings. Furthermore, the narrative that advanced surveillance technology enhances rescue operations is contradicted by numerous documented cases where Greek authorities have allegedly used distress signals to locate and push back migrant boats, rather than rescue them (ProAsyl 2013, 28). Reports also suggest that Frontex's surveillance technology is utilised to oversee illegal pushbacks, suggesting that further examination of the intersection between technology and human rights violations in the activities conducted by the agency is necessary (Habib 2021). These observations gain further significance when considered alongside recent ethnographic research by Covadonga Bachiller López (2022), which accurately describes Frontex's role in early detection tactics aimed at deterrence and externalisation, systematically performed by Frontex in collaboration with the Hellenic Coast Guard since early 2020.

In conclusion, while the use of drones in pushback operations is widely suspected, it remains today difficult to definitively prove. The deployment of these technologies in such operations could be described as a 'common secret', understood by many but officially acknowledged by none. The increasing reliance on drones for border surveillance, within a context of endemic border violence, thus raises profound ethical and legal concerns that require urgent attention and further investigation.

CHAPTER 3

Situational awareness and border enforcement in Spain: the *Sistema Integrado de Vigilancia Exterior* (SIVE)

3.1. Surveillance at the Pillars of Hercules and beyond: securitisation and digitalisation of Spanish border control policies

Non plus ultra: the mythological Pillars of Hercules, representing the Calpe and Abila mountains that flank the Strait of Gibraltar, were once considered the limits of the known world – the outer boundary, impossible to cross. Today, this same strait is one of the most monitored and securitized borders in Europe and embodies the violence that often marks the lines dividing the global North and South. However, despite the sophisticated systems in place to deter migration, people continue seeking to cross, echoing the *folle volo* – the daring journey beyond humanity's unsurpassable threshold, famously depicted in the Divine Comedy[1].

People on the move attempting to enter Spain typically follow three main corridors: the autonomous cities of Ceuta and Melilla, the Strait of Gibraltar, and the Canary Islands. Interestingly, over time, enhanced surveillance and border enforcement in one corridor have often led to increased pressure on the others, resulting in shifts in migration strategies rather than a reduction in the overall number of attempts to cross the border (Godenau and López-Sala 2016, 7).

This chapter focuses on the digitalisation of border surveillance in Spain, specifically through the implementation of the *Sistema Integrado de Vigilancia Exterior* (SIVE). The analysis begins by examining the digitalisation process

[1] Dante Alighieri, 'La Divina Commedia', *Inferno,* Canto XXVI, v.125.

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

within the broader context of migration routes to Spain, highlighting the militarization of Ceuta and Melilla, and the cooperative networks involved in monitoring the Strait of Gibraltar and the Canary Islands. This enquiry provides an in-depth look at the SIVE's functionality and its multifaceted impact, concluding with an exploration of the legal framework within which the system is operated.

3.1.1. Ceuta and Melilla, imagining and contesting the *frontera inteligente*

The autonomous cities of Ceuta and Melilla, two Spanish enclaves on the African continent, are located approximately 100 kilometres from the Algerian-Moroccan border. These enclaves, unlike other Spanish external borders, which are predominantly maritime, have land-based borders, making them unique within the European context. These borders, in fact, demarcate regions characterised by profound economic and social disparities[2], that have prompted scholars to draw comparisons between the dynamics observed in Ceuta and Melilla and along the USA-Mexico border (Carling 2007).

In fact, such a geographical location, situated between continents, makes the border zones before the enclaves fraught with tensions, violence, and contradictions, largely crystallized in the iconic militarization and securitisation of the area, marking deep territorial ruptures. Moreover, numerous exceptional provisions characterize the area: as an example, it should be noted that – despite Ceuta and Melilla being part of the Schengen Area – Spain reserves the right to conduct checks on citizens travelling from the enclaves to the mainland. Nevertheless, both enclaves remain crucial transit hubs.

The physical border infrastructure in these cities is formidable, with multiple high barbed-wire fences marking a large *no-go-zone* on the Spanish side of the border. Within this space, the Spanish *Guardia Civil* is the only authorised actor. In Ceuta, there are three distinct fences: the first, covered with barbed wire, is controlled by Morocco; the second, standing ten metres high, is monitored by the *Guardia Civil* and purportedly separates a 'neutral area' carved out from Spanish territory; the third encloses a zone where regular patrols are conducted by *Guardia Civil* agents (BVMN 2021). The area between these fences has gained notoriety for forceful policing operations. Pushbacks, which will be further discussed below, represent some of the most severe manifestations of such activities. Furthermore, the intensification of border enforcement in Ceuta and Melilla is periodically exacerbated, notably in instances when mobility provisions are further curtailed. For instance, during the Covid-19 pandemic, the decline in legal mobility options significantly increased the hazards associated with migration to the enclaves: as crossing the borders at Beni Enzar (Melilla)

[2] In Spain, the per capita income adjusted for the cost of living is approximately five times higher than that estimated in Morocco. Although this parameter has clear limitations, as it does not account for factors such as the welfare state, the rule of law, or guarantees of individual freedom when assessing the quality of life, the stark economic disparity remains relevant.

and El Tarajal (Ceuta) became nearly unattainable, a greater number of people resorted to maritime attempts or swimming to reach the autonomous cities, occasionally with fatal outcomes (Spanish Refugee Aid Commission 2021, 80).

Once again due to their 'exceptional' location, since the early 2000s, the two enclaves have become key sites for technological experimentation and the deployment of state-of-the-art surveillance systems. A significant development in this trajectory occurred in December 2021, when the Spanish government established an inter-ministerial commission to promote a new '*frontera inteligente*' (smart border) in Ceuta and Melilla. Touted as a progressive step in combating illegal trafficking, this initiative also includes provisions for the use of facial recognition cameras in border areas (Martín and González 2021). However, the implementation of this new bordering model has encountered substantial obstacles and tensions. Over fifty civil society associations and organisations expressed opposition, signing a letter asserting that the *frontera inteligente* would significantly violate human rights and increase the risk of discrimination and criminalisation of migrant people. To mitigate these risks, the letter advocates for European standards on AI and data protection to be applied also in security-related domains, emphasising the need to obtain informed consent from people subjected to facial recognition systems before their deployment, and stressing that human rights considerations must be systematically integrated into border actions (Frontera Digitales 2022). While these points remain largely unaddressed, the project is still ongoing.

3.1.2. Between the Straits and the Canaries: surveillance systems, third States, and European Agencies

Besides Ceuta and Melilla, the two key migratory corridors towards Spain traverse the Strait of Gibraltar and the Canary Islands, which lie in front of southern Morocco. In these regions, Spain has implemented one of the most extensive maritime surveillance systems that can be found in the European Union. Unlike the enclaves of Ceuta and Melilla, where physical barriers play a significant role in border enforcement, Spain's maritime borders rely significantly on advanced situational awareness mechanisms. This partly explains Spain's early adoption of sophisticated surveillance technologies designed to enhance situational awareness and reaction capabilities at its external borders, establishing the country as a model for other EU Member States, including Romania, Portugal, and Finland, as well as for the European Union itself (European Union Agency for Fundamental Rights 2013, 59).

In response to the increased migratory pressure through the Strait of Gibraltar from 1999 onwards, Spain was in fact among the first EU States to integrate advanced surveillance systems into its border control strategy. That year, the Spanish government launched an ambitious surveillance enhancement plan with a budget of €150 million for a five-year period. At the core of this plan was the implementation of the *Sistema Integrado de Vigilancia Exterior* (SIVE), a surveillance system overseen by the *Guardia Civil*. The SIVE was designed to improve the surveillance of Spain's southern border, engaging in two main 'fights': drug trafficking and irregular migration (Guardia Civil 2010). From its inception, the SIVE was recognised as one of the most advanced border surveillance systems in Europe.

Originally intended to only be deployed in the Strait of Gibraltar, the SIVE's scope has gradually expanded. While its functioning will be further discussed below in this chapter, it is important to note that from the outset the system's high costs sparked significant controversy. Humanitarian NGOs have largely criticised the expenditure, arguing that significant funds were unjustifiably allocated for a system with repressive objectives. Research by Jørgen Carling estimated that during its first five years of operation, the SIVE cost approximately €1.800 per migrant reportedly intercepted (Carling 2007). In response to these criticisms, the Spanish government framed the adoption of the SIVE as a 'necessary' measure, ostensibly driven by EU mandates to achieve more effective border surveillance and paired with the impossibility of the deployment of a substantial number of officers for border enforcement. Additionally, the government sought to reassure civil society by emphasising the humanitarian vocation of the system and its role in combating smuggling while supporting sea rescue operations (Fernández Jurado and Sabariego Rivero 2006).

Besides technological deployment, a crucial component of Spain's border control strategy in the western Mediterranean involves extensive cooperation with different stakeholders, including the private sector, third states, and European agencies.

First, investigations have in fact highlighted the significant role of technology and consulting firms in the digitalisation of Spain's borders (PorCausa 2020b). Among them, Indra – a Spanish company that supplies the SIVE and similar maritime border surveillance systems in Latvia, Portugal, and Romania – plays a particularly prominent role (Akkerman 2021, 156).

Second, Spain's cooperation with third countries, particularly in North and West Africa, has historically been a cornerstone of its border control (and migration pre-emption) efforts, both through bilateral agreements and under EU auspices. Indeed, cooperation with Morocco, Algeria, Senegal, Mauritania, and Mali has long been central for both containing migratory flows and facilitating repatriations and returns through ad hoc agreements[3].

The strategic importance of these partnerships is such that, in 2012 alone, the Spanish government allocated €12 million towards cooperation with police forces in these countries (Godenau and López-Sala 2016)[4]. In this regard, a 2015 Frontex report praised the effectiveness of Spain's cooperation with Senegal, Mauritania, and Morocco, noting that it had significantly reduced migratory pressure on routes to the Canary Islands and southern Spain (Frontex 2015, 6).

[3] It should also be noted that until 1991 citizens of North African countries entering Spain were not subjected to visa requirements.

[4] More recent aggregate data could not be retrieved.

The Seahorse Mediterranean operations, conducted under the Seahorse Mediterranean Network, clearly exemplify such cooperation.

This programme, led by Spain through the *Guardia Civil* and funded by the European Commission, aims to enhance information exchange in the Mediterranean region within the EUROSUR framework. It involves seven EU Member States (Spain, Italy, France, Malta, Cyprus, and Portugal) and several North and West African countries. Operations have included Niger, Mali, Burkina Faso, Senegal, Gambia, Guinea-Bissau, Guinea Conakry, Mauritania, Cape Verde, and Morocco. The Seahorse Mediterranean operations are frequently discussed in academic literature as examples of extraterritorial border control processes, illustrating how «informal and itinerant bordering assemblage of institutions, state authorities, and policies» operate (Casas-Cortes, Cobarrubias, and Pickles 2016, 2). In the Spanish context in particular, the digitalisation of border patrols is inseparable from and impossible to grasp outside of this dense network of cooperation, externalisation, and outsourcing arrangements that characterise Spain's approach to maritime border surveillance.

Within this network, the strategic partnership with Morocco is particularly crucial due to geographic proximity. Since the early 2000s, Morocco has progressively aligned itself with Spanish and European priorities of curtailing irregular migration and criminalising mobility. The adoption of the 2003 Law on Entry and Residence of Foreigners in the Kingdom of Morocco and Irregular Emigration and Immigration, which includes only minimal provisions for migrant people's rights, has been a key development in this context[5]. More broadly, the cooperation between Morocco and the EU on migration issues continues to be anchored in an Action Plan amended in 2005, which aims to harmonise national legislation with international asylum and refugee protection standards, while simultaneously combating irregular migration to and through Morocco[6]. Under this framework, Morocco established the Migration and Border Surveillance Directorate and the Migration Monitoring Centre to enhance its capacity to fight 'illegal' migration and human smuggling.

In 2013, the EU and Morocco signed an Association Agreement on Mobility, launched in 2019. Between 2013 and 2020, the European Union provided Morocco with €342 million in migration-related support through the EU Emergency Trust Fund for Africa and the European Neighbourhood Instrument (PorCausa 2020b, 8). Additionally, under pressure from Spain, in 2018 the EU agreed to allocate €140 million to strengthen Morocco's border management capabilities (Statewatch 2019). In December 2019, the European Commission granted a further €389 million for border management activities as part of the Euro-Moroccan partnership for shared prosperity. Remarkably, such cooperation has so far not resulted in better protection standards for migrant people

[5] Law no. 02/03, Entry and stay of foreigners into the Kingdom of Morocco, irregular emigration and immigration, 20 November 2003.

[6] Association Council, UE-MA Action Plan 2702/1/05, 27 July 2005, para. 48.

and asylum seekers in Morocco, but only in enhanced border enforcement capabilities. It is thus not surprising that legal scholars are strongly questioning the suitability of the *de facto* integration of Morocco into Spain's border control and protection system (Spanish Refugee Aid Commission 2017).

Lastly, coordination with European agencies, particularly Frontex, is another critical element of Spain's border control strategy. Frontex has been active in Spain since 2006, the year of the 'cayuco crisis', when a surge in departures from Senegal and Mauritania to the Canary Islands using traditional fishing boats was registered. Since then, Frontex has provided technical and operational support for both the digitalisation of border surveillance and the deployment of patrols to deter migration attempts along the West African coast. Over the years, Frontex officers have participated in several joint operations, including Hera, Indalo, and Minerva, all aimed at bolstering Spain's maritime border security (Godenau and López-Sala 2016, 10). Particularly relevant is Operation Indalo, which seeks to enhance aerial and maritime surveillance capabilities to enable the early identification of migrant boats. Currently, more than 250 Frontex officers are deployed in Spain as part of the Indalo operation to support the country in managing the Western Mediterranean migratory route (Frontex 2021). Furthermore, Frontex is now also present in the Port of Ceuta as part of a new joint mission (BVMN 2021).

Having outlined the extensive network of actors involved in border surveillance at Spain's external borders, it is now crucial to delve deeper into the resources necessary for the operation of these border enforcement mechanisms. This includes an analysis of national and European funding strategies, with a particular focus on the SIVE and the broader digitalisation of patrols along the Atlantic coast.

3.2. Deployment and maintenance: the costs of one of Europe's largest surveillance systems

Evaluating the operational functioning of the *Sistema Integrado de Vigilancia Exterior* also requires outlining the financial resources, predominantly borne by European funds, required for the maintenance and replacement of its equipment, which now has been in use for over two decades.

As discussed in the Greek case study, the European Borders Fund (EBF) – covering the 2007-2014 financial period – was established to support national actions under five strategic priorities. Among these, the development and implementation of national components for a European Surveillance System at the external borders, as well as the establishment of a permanent European Patrol Network for the southern maritime borders, were particularly salient (European Commission 2014). As articulated in Spain's national report on the EBF, the efficacy of the SIVE is intrinsically linked to the achievement of these priorities, thus justifying continued financial support (Spanish Ministry of the Interior 2012). Out of the total €630 million allocated to Member States under the EBF during the 2007-2010 period, Spain, Italy, and Greece, received nearly half, with

Madrid alone obtaining approximately €134.5 million. This funding enabled Spain to procure a substantial number of surveillance components, primarily for the expansion of the SIVE. According to a European Commission report, these investments facilitated the interception of 5.279 migrant people within the specified financial period (European Commission 2014).

The 2013 national annual programme on the EBF provides one of the most comprehensive insights into the technical and operational life of the SIVE. In the programme, the Spanish Ministry of Interior emphasised the critical role of European financial support in maximising the system's technological development. Moreover, it outlined the strategic importance of enhancing SIVE's capabilities to advance the automation of border controls, thereby improving security while reducing operational costs and reliance on human resources (Spanish Ministry of the Interior 2013, 13). This emphasis on automation and the integration of AI into security protocols highlights the shifting priorities in border management.

Under the Internal Security Fund for 2014-2020, the digitalisation of border patrols in Spain was further accelerated through additional financial support, including from the Borders Emergency Assistance. This emergency funding, totalling €52 million in 2018 and 2019, was allocated to Spain, Greece, Hungary, Croatia, and Belgium to bolster border control efforts. In Spain, it once again primarily supported initiatives aimed at contrasting 'illegal' migration (European Commission 2021). Specifically, in 2018, over €6 million was dedicated to the maintenance and expansion of the SIVE, including repairs to its radars and sensors (Spanish State Secretariat for Security 2018). The investments continued over the following years, with approximately €3.6 million in 2019 and over €8.5 million in 2020 being allocated for similar purposes (Spanish State Secretariat for Security 2019). Furthermore, in 2020, an additional €1.4 million was earmarked to promote the digitalisation of borders and the development of automated smart borders (Spanish State Secretariat for Security 2020).

Tracking the precise allocation of funds within security-related projects is inherently challenging due to the opacity surrounding such expenditures. Nonetheless, a study by the *Fundación PorCausa* – a Spanish investigative foundation working on migration – offers revealing insights into the financial scale of migration control between 2007 and 2017. During this period, Spain spent approximately €896 million across 943 public contracts, with 97% of these funds aimed at enhancing border protection, surveillance, detention, and the expulsion of irregular migrants (PorCausa 2020a). A later analysis covering the 2014-2019 period shows that at least €660.4 million were awarded to companies involved in the contrast of migration through 1.677 public contracts, many of which raised transparency concerns[7]. Most recently, in March 2022, the Spanish Council of Ministers authorised the Secretary of State for Security to conclude a contract

[7] All these contracts are collected and published by *porCausa* at https://docs.google.com/spreadsheets/d/1mEOHIKwFyGfiha5GJ0HkTpc08mDZc-I6hGpUFf2oDno/edit#gid=1367307146

valued at €25.7 million for further upgrading the SIVE's capabilities in Cadiz, Algeciras, and Ceuta (Carrasco 2022).

These figures illustrate a sustained and growing interest in advancing the digitalisation of border surveillance and patrolling systems, facilitated also by the allocation of emergency funds and contracts that often escape public scrutiny. Moreover, as evidenced in the case of Greece, EU funding mechanisms not only shape national policy orientations but also promote a convergence of approaches among Member States on border technologies.

3.3. The *Sistema Integrado de Vigilancia Exterior* in practice: situational awareness, detection, and risk analysis

Together with the investments it involves, the *Sistema Integrado de Vigilancia Exterior* carries significant expectations. Remarkably, the SIVE represents a prime and textbook example of digital patrolling systems as discussed in the first chapter, designed to enhance situational awareness and improve targeted detection along and beyond maritime borders. Essentially, the operational scope of the SIVE is closely aligned with the rationale underpinning the deployment of EUROSUR, which was indeed partially modelled on it (Ellebrecht 2020, 217).

Technically, the SIVE functions as an operational system that facilitates the surveillance of sea borders and surrounding areas. It shares real-time information with control centres through a network of fixed stations and mobile units equipped with still cameras, heartbeat detectors, CCTV cameras, night vision devices, infrared optics, long-range radar systems, and thermal cameras positioned along Spain's coastal areas (Jumbert 2018, 16; Spanish Ministry of the Interior 2012). When weather conditions are favourable, the SIVE detects migrant boats within a range of 10 to 25 kilometres from the shore, capturing high-quality photographs and videos. Once a target is detected, an alert is sent to the *Centro de Mando y Control* in Algeciras, which monitors the situation remotely. Smaller control centres are also located in Cadiz, Malaga, and Ceuta, though the exact locations of the SIVE stations remain classified (González 2018).

As a boat approaches within 5 kilometres of the coast, the control centre can estimate the number of passengers, the vessel's course, and its expected time of arrival. This information, gathered from multiple sources, is fused, processed based on risk criteria, and then relayed to patrol units (such as helicopters, boats, or other vehicles) or other entities, such as the Maritime Rescue, the Red Cross, or the National Police Corps. As previously mentioned, the entire system is operated by the *Guardia Civil*, a joint military and civilian police force responsible for the Coast and Border Service and the Maritime Service (Catalán 2014).

The primary objective of the SIVE is to efficiently detect and apprehend individuals attempting to enter Spain, blending a deterrence-based approach with a discourse that encompasses both trafficking and humanitarian concerns (Carling 2007). More precisely, according to the Spanish Ministry of the Interior (2013, 11), the purpose of the SIVE is to ensure coverage of the European

Union's southern border, thereby enhancing the *Guardia Civil*'s effectiveness in performing its duties.

Despite the focus on irregular immigration and drug trafficking being its primary objectives, the SIVE is often praised for its versatility. The system is in fact also aimed at combating terrorism, intelligence gathering, countering illegal fishing and piracy, protecting marine and land resources, conducting search and rescue operations, and ensuring port security (Fernández Jurado and Sabariego Rivero 2006). Over time, the system's operational scope has thus expanded considerably.

Also in geographic terms, SIVE's coverage has grown since its initial deployment in 2002 around the Strait of Gibraltar. It now spans the entire Spanish Mediterranean coast, the Balearic Islands, and the Canary Islands. The system's expansion began with three fixed detection stations in Fuerteventura and later extended also to Lanzarote, Gran Canarias, and the Atlantic coasts (European Union Agency for Fundamental Rights 2013, 59). Beyond Spain, just like the EUROSUR, SIVE's operational reach has extended also to non-European countries, reflecting externalisation ambitions. Since 2006, coordination centres have been established in Mauritania, Senegal, Guinea, and Cape Verde to foster interoperability and information exchange in pre-frontier areas, aligning with broader European policy objectives often supported by Frontex (Markard 2016, 612).

Interestingly, the continuous expansion of the SIVE has often led to the deflection (and not suppression) of migration routes, resulting in a 'cat-and-mouse' game that does not offer a definitive solution to migration governance challenges[8]. Migrant people have increasingly resorted to longer, more hazardous routes, away from both border surveillance and rescue systems (Spanish Refugee Aid Commission 2017).

3.3.1. Controversial impact assessments and resistance strategies

The design of the SIVE's digital patrolling scope is fundamentally rooted in two core principles: early detection and central command (Carling 2007). These principles support the system's objectives of enhancing situational awareness and response capabilities, which are structured along three functional axes: detection, coordination and centralization, and interception. However, different assessments of the impact of the SIVE often reveal frictions and contradictory outcomes.

Since its deployment, the System has been lauded within border industry circles as a successful example of border control, contributing to a significant reduction in the number of migrant people along the routes under its surveillance (Alscher 2005). However, the overall fluctuations in the number of arrivals in Spain can-

[8] To provide an example, according to the *Asociación Pro Derechos Humanos de Andalucía* (APDHA) (2022, 52), the decrease in the arrival of migrants on the coast of Cádiz registered between 2002 and 2005 was almost totally compensated by the increase in the arrivals that took place in the years 2005-2007 in the Canary Islands.

not be strictly correlated with the digitalisation of patrolling along the Western Mediterranean route. These fluctuations often reflect other variables, such as the political dynamics of cooperation on migration and border control with Senegal, Mauritania, and Morocco, as well as weather and sea conditions. This should not result in underestimating the role of the SIVE, but rather emphasise the importance of the framework in which it operates: a broader context where the deterrent effects of advanced surveillance systems are often outweighed by the impact of 'old-fashioned' migration containment and border externalization policies. Bringing it all together, Dirk Godenau and Ana López Sala (2016) effectively describe border digitalisation strategies and cooperation with third countries at Spain's maritime borders as a complex and multi-layered deterrence strategy.

Moreover, this success narrative of arrival reduction often overlooks the aforementioned deflection of migratory flows toward more dangerous routes, which increases the risk of fatalities. For this reason, Carling (2007) argues that the effectiveness of the SIVE should be evaluated not only by its ability to reduce unauthorised entries but also by its capacity to reduce fatalities. In any case, there do not seem to be any sharp trends. In fact, despite the expansion of SIVE, data from the Spanish Ministry of Interior show a fluctuating number of arrivals, with more than 64.000 arrivals recorded in 2018 – one and a half times the number in 2017, and double that of 2016. By 2019, arrivals fell to 32.000, to rise again in 2020, suggesting that these fluctuations are just not correlated with SIVE's activities (Asociación Pro Derechos Humanos de Andalucía 2021, 10).

Challenging Carling's (2007) conclusion that the migrant mortality rate had decreased since the deployment of the SIVE, the *Asociación Pro Derechos Humanos de Andalucía* (APDHA) (2021) reported over 1.700 deaths in 2020 among people attempting to reach Spain. In 2021, this number rose to 2.126, a record high (Asociación Pro Derechos Humanos de Andalucía 2022). According to different estimates, by mid-September 2021, more than 1.025 people died or went missing at sea while trying to reach Spanish shores – most of them in the Atlantic, apparently being unidentified by the SIVE (see El Día 2009; Martín 2021). As is often the case with fatalities during migratory journeys, these numbers are likely under-reported.

Although it is not possible here to clearly establish whether this is due to inefficiencies of the system or specific priority settings, the effectiveness of the SIVE in sea rescue operations is thus undeniably limited. Recently, civil society groups and the Canary Islands Government Delegation have vocally criticized the high costs of a system that simply fails to prevent tragic accidents. Therefore, they have called on the *Guardia Civil* to provide a «concrete, clear and forceful» report on SIVE's functioning, effectiveness, and technical status (González 2018). At present, no official reply on this matter is known.

In 2011, the SIVE was responsible for only one-sixth of rescue operations, with most alerts coming from private individuals, aid workers, other boaters, or Frontex's Operation Indalo (European Union Agency for Fundamental Rights 2013, 59). While more recent data could not be retrieved, the trend seems to be consistent. According to the APDHA (2021, 51), this would corroborate the ineffectiveness of the SIVE and its role in exacerbating the suffering of migrant people, pushed toward more dangerous routes. But this is not the only way the SIVE influences migration strategies. Notably, the System struggles to detect small and lightly structured boats: for this reason, trying to reduce the chances of being intercepted, migrant people increasingly resort to small vessels often camouflaged as fishing boats, thus significantly heightening the risk of accidents at sea. Moreover, as people on the move are often informed that Spanish surveillance systems will detect their boats and that those in command will face severe consequences, they sometimes discard their boat engines shortly after leaving Moroccan waters. This is done in the (optimistic) hope of making the boat driver unidentifiable and of being detected by the SIVE system and rescued, rather than being pushed back (Fisher 2018, 73). These examples show how migrant people are not just 'being surveilled' but manage to challenge one of Europe's most expensive coastal surveillance systems, sometimes successfully undermining its effectiveness. Of course, this comes with extremely high risks.

Moreover, despite continuous maintenance and heavy investment in new technologies, the SIVE remains plagued by blind spots. Malfunctions are frequent, either due to rapid obsolescence of the systems or sabotage of cameras and radars by people on the move. From a socio-technical perspective, Daniel Fisher (2018) pertinently argues that these frictions are intrinsic to the SIVE, as the situational awareness and 'vision' of the border areas it generates are fragmented by both human and technological flaws: along this assemblage creeps take place, undermining the system's efficiency and its supposed ever-vigilant surveillance. Additionally, authorities directly involved in SIVE's operation have disclosed that its effectiveness in detecting migrant people is highly dependent on weather conditions (European Union Agency for Fundamental Rights 2013, 59). This reliance on environmental factors can render the system ineffective, while at the same time contributing to the dehumanization process connected with remote patrolling, further discussed in the next chapter. Indeed, under certain conditions such as wet weather, it is almost impossible for the personnel operating the SIVE to distinguish between a person, an animal, or a rock. For people working in control centres, a migrant person entering the land border area in Ceuta and Melilla by night would appear on the screen as a «black, pixelated shape that is still vaguely-humanoid» (Fisher 2018, 71).

Furthermore, the SIVE itself is heavily dependent on cooperation with third countries. Ethnographic research conducted by Fisher shows that the *Guardia Civil* relies significantly on Moroccan authorities for border control and on-the-ground support complementary to the SIVE. The *Guardia Civil* officers operating the SIVE depend in fact on the «clean up» operations of people on the move conducted by Moroccan counterparts – «otherwise we'd be completely overrun with *them*» (Fisher 2018, 72). This highlights the role of the SIVE as a measure of last resort and a 'rear-guard' within Spain's broader border control strategy, where neighbouring countries bear much of the burden.

There is also evidence that when the SIVE detects a migrant boat, the alarm is sent not only to the *Guardia Civil* and the *Salvamento Marítimo* in charge of rescue operations but also to Moroccan patrol boats. If the vessel is in Spanish waters, a rescue operation occurs only in case of distress; if in Moroccan waters, migrant people are intercepted and returned, regardless of distress conditions. Simply put, the boat is pulled back. Notably, the number of interceptions by Moroccan authorities oscillates closely in line with the political relations between the EU and Morocco. In addition, there are indications that Moroccan coastguards sometimes operate in Spanish waters, with reports of the Guardia Civil delaying intervention and blocking vessels until Moroccan patrols arrive (Fisher 2018, 73). In such cases, speed is crucial to prevent Spain from being compelled to disembark people at a Spanish port, and it is enhanced by SIVE's digitalised patrols, which enable the early coordination of operations.

Fisher's ethnography also reveals that while SIVE's technology can detect vessels even in Moroccan waters, the officials in the control centres often do not monitor these areas closely: verifying any possible alarm issued by the SIVE would require more staff (and a lot of work). Consequently, vessels are typically detected only in international waters, where rescue operations are less frequent (Fisher 2018, 73).

3.4. Drones buzzing around the SIVE?

Determining whether the fixed radar and camera systems that form the backbone of the SIVE are currently complemented by the deployment of drones remains challenging, as has been the case studying the Greek context. However, evidence suggests that Spain is increasingly using UAVs for various purposes along its borders, and it is reasonable to assume that such operations might be integrated into the SIVE to enhance its effectiveness.

In fact, Spain has extensively used the drones provided by the European Maritime Safety Agency primarily for pollution control, search and rescue operations, and maritime surveillance purposes. These functions partially overlap with the objectives of the SIVE, suggesting a potential convergence of efforts (European Maritime Safety Agency 2019; 2022). Additionally, an infographic produced by the *Guardia Civil* and made public by Maribel Casas-Cortes, Sebastian Cobarrubias, and John Pickles (2016, 7) indicates that UAVs were deployed under the SIVE framework as early as 2008. However, specific details about the number of drones, their areas of deployment, and how they were integrated into the system remain unclear.

Spain's involvement in several EU-funded drone projects under the 7th Framework Programme for Research further highlights the influence of EU funding and research schemes on national border policies. Notable here is the CLOSEYE project, which ended in 2017, aimed at fostering cooperation between Guardia Civil and Frontex personnel in this area[9]. The project involved

[9] Collaborative evaluation of border surveillance technologies in maritime environment by pre-operational validation of innovative solutions (CLOSEYE), Grant agreement ID: 313184. 1 April 2013 – 28 February 2017.

extensive UAV testing to monitor European maritime borders, strengthen the SIVE, and improve its integration into the European Border Surveillance System (Marin 2017; Statewatch 2013).

Attempts have also been made to deploy drones over the Spanish enclaves of Ceuta and Melilla. Already in 2017, drones were in fact integrated into an artificial intelligence surveillance system called *Surveiron*. However, this initiative was quickly abandoned due to environmental factors, particularly the strong Levante wind, which made drone operations in the area impractical (Andres 2021; Testa 2017). Despite this setback, the *Guardia Civil* expressed renewed interest in integrating drones into the SIVE network in 2020. In February 2022, the *Guardia Civil* made an emergency purchase of four UAVs to enhance border surveillance in Ceuta and Melilla, aiming to detect crossing attempts at an earlier stage while mitigating risks for human personnel in cases of violent «border assaults» (Infodron.es 2022). Interestingly, this purchase was made under an emergency tendering model used during the Covid-19 pandemic, regulated by Article 120 of Law 9/2017 on Public Sector Contracts, which allows for rapid procurement in situations affecting national defence[10].

At approximately the same time, Morocco strengthened its border monitoring capabilities in Ceuta and Melilla with the acquisition of 12 military drones from Türkiye (Drusila Castro 2022). Not surprisingly, the Spanish government responded positively, emphasizing that border enforcement decisions are a matter of State sovereignty on which no interferences should take place, and reaffirming its commitment to cooperating with Morocco for mutual benefit in this area.

These developments reflect a broader trend towards the integration of dual-use unmanned aircraft in border surveillance, with Spain taking a leading role. Indeed, Madrid is also spearheading the Next Generation Small RPAS project under the EU's Permanent Structured Cooperation (PESCO), which aims to develop Remotely Piloted Aircraft Systems to enhance military cooperation among EU Member States (PESCO 2021). These multi-purpose RPAS are expected to support not only military operations but also law enforcement and disaster or emergency response agencies. The possibility of equipping these drones with less-than-lethal effectors for police use indicates potential implications for future border patrol strategies (Statewatch 2021). While it is premature to draw definitive conclusions about the impact of these developments on border patrols, Spain's growing leadership in drone technology should not be overlooked.

3.5. The legal framework: between pushbacks, the SIVE, and drones

Once again, analysing the legal framework surrounding the *Sistema Integrado de Vigilancia Exterior* and the deployment of drones under its umbrella is a complex challenge. This complexity arises primarily from the lack of a specific

[10] Law no. 9/2017, Contracts of the Public Sector, 8 November 2017.

legal basis for the SIVE, which can only be traced back to the general mandate of the *Guardia Civil* (Ranger Project 2018). Thus, it is crucial to broadly explore the main concerns related to both access to international protection and border control in Spain, focusing on large-scale pushbacks as a particularly alarming and compelling phenomenon. Pushbacks and interceptions, just as the attempts to give them legal legitimacy, can in fact be facilitated by the SIVE, marking a point of concern in the overall digitalisation of border patrols.

To set the scene, over the past decade, Spain has transitioned from being one of the European countries with the lowest number of international protection applications to one of the Member States hosting the largest number of asylum seekers, partly due to the Dublin Regulation (Regulation 604/2013) (Oso, López-Sala, and Muñoz-Comet 2021)[11]. However, this increase has not translated into easier access to international protection for people on the move arriving via Spain's southern border. Scholars have here identified a phenomenon of «territorial deviation», whereby the majority of asylum applications are submitted 'within' Spain's territory rather than 'at the border' (López-Sala and Moreno-Amador 2020). Furthermore, while the securitisation and militarization of borders are significant factors, political narratives have also played a role in framing people on the move arriving at the southern border primarily as economic migrants. This racialised and largely neocolonial discourse casts them as 'bogus' asylum seekers who should be deterred or repelled. Consequently, people on the move from African countries face substantial, systemic obstacles in reaching Spanish borders and accessing protection (BVMN 2021, 5).

In this context, a landmark development in Spanish migration and border policies occurred during the 2008 economic crisis, described as a pivotal moment in consolidating privatisation, outsourcing, remote control, and technologisation of border control patterns (Godenau and López-Sala 2016; López-Sala and Godenau 2020; Oso, López-Sala, and Muñoz-Comet 2021). These processes have been coupled with overt 'migratory containment' strategies followed, in 2009, by the introduction of accelerated asylum procedures at the southern border. These procedures, which take place in closed centres, have been criticised for leading to selective immobilisation of people, thus violating the principle of equal treatment while lowering procedural and substantial guarantees, therefore producing an «infrastructural vacuum of access to refugee status» (López-Sala and Moreno-Amador 2020, 12). Similarly, the institutionalisation of Temporary Stay Centres for Foreigners (*Centros de Atención Temporal de Extranjeros*) – fenced buildings or secured areas within ports where migrant people are held for up to 72 hours while police procedures are carried out – further jeopardises

[11] Regulation no. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (Dublin Regulation), 26 June 2013.

access to a fair examination of individual claims. Overall, these centres have, in fact, proven efficient in acting as barriers to protection more than in expediting related procedures (Barbero 2021)[12].

Further barriers to international protection result from the harsh pushback operations documented at the borders, particularly around the fences of Ceuta and Melilla. One of the most tragic incidents that significantly shaped Spain's approach to border security was the 2005 '*Asalto Masivo*', where thousands of migrant people attempted to enter the enclaves. The ensuing violence, with police forces (Spanish or Moroccan, never conclusively determined) opening fire, resulted in at least 14 deaths (Carlotti 2022). This incident marked a critical moment in a 'defensive' turn in Spain's border policy, further reinforcing a narrative heavily skewed towards securitization and the externalization of migration management.

A particularly striking episode occurred in May 2021, when numerous sub-Saharan migrant people scaled the border fence in protest against the total closure of the borders, justified under the pandemic emergency. Spanish *Guardia Civil* agents, equipped with riot gear, quickly made their efforts futile. The threat of immediate repatriation was compounded by the use of tear gas and plastic bullets, aimed specifically at the hands and neck of people attempting to cross[13]. Notably, no one was allowed to claim protection.

According to monitoring organisations, border operations of this kind have increased both in violence and frequency over the past two years. These large-scale incidents, involving hundreds of people, are marked by their indiscriminate nature, affecting even unaccompanied minors (BVMN 2021, 19). A notable instance in this regard occurred in August 2021, when the Spanish government started returning children to Morocco under a contentious readmission agreement. This action constituted a blatant violation of Article 35 of Organic Law 4/2000 on the Rights and Freedoms of Foreigners in Spain, as well as European and international obligations[14]. Despite the Spanish human rights Ombudsperson's (Defensor del Pueblo 2021) objections, the repatriation of unaccompanied minors continued for months, until it was finally halted by a local court's intervention (Testa and Sánchez 2021).

Moreover, allegations of severe mistreatment by Spanish border guards within the enclaves have been extensively documented, with some cases making their way before the European Court of Human Rights. In April 2021, a letter from four UN Special Rapporteurs addressed to the Spanish government expressed concern over pushback practices towards Morocco, notably in the case of indis-

[12] See the Asylum Information Database (2021) for more information on these facilities and the related procedures in the centres.

[13] A visual documentation of this violent episode has been published by the Border Violence Monitoring Network: https://www.borderviolence.eu/wp-content/uploads/CEUTA1-general-and-shootings.mp4

[14] Organic Law no. 4/2000, On Rights and Freedoms of Foreigners in Spain and their social integration, 11 January.

criminate and summary expulsions at the border (UN Office of the High Commissioner for Human Rights 2021). Additionally, there are also reports of 'chain *refoulement'*, where individuals expelled from Spain are further deported from Morocco to Mauritania and beyond (BVMN 2021, 12). These practices, often amounting to 'hot returns' (*devoluciones en caliente*), are predominantly registered in Ceuta and Melilla (Costa Traba 2021).

Within the enclaves, foreign nationals intercepted by the *Guardia Civil* are in fact immediately handed over to Moroccan authorities, without any formal procedure. The Spanish government has attempted to legally justify these actions through the concept of the 'operational border' (*frontera operativa*), which suggests that the border is defined by the position of the *Guardia Civil* agents and not by the 'real' border, almost regardless of geographical considerations. This concept was first articulated in a report by the Deputy Operational Directorate of the *Guardia Civil*, submitted to the Ministry of the Interior and presented to the Congress of Deputies on 7 March 2014. The report asserts that «the internal fence materialises the line with which the State, in a free and sovereign decision, delimits, for the sole purposes of the aliens' regime, the national territory». According to this logic, migrant people only enter Spanish territory – and thus become subject to Spanish immigration laws – once they cross the internal fence (Martínez Escamilla and Sánchez Tomás 2019, 31). This interpretation effectively denies foreign nationals handed over to Moroccan authorities any protection afforded by Spanish law (Defensor del Pueblo 2005, 292). Of course, this rather imaginative approach is legally questionable, as the external fence separating Ceuta and Melilla from Morocco is largely situated on Spanish territory.

In 2015, the Spanish government further entrenched these practices by amending Organic Law no. 4/2000 (*Ley de Extranjeria*) with the introduction of the Tenth Additional Provision under the Law on Citizen Security (*Ley de Seguridad Ciudadana*). This provision allows for the routine expulsion of foreign nationals intercepted at the Ceuta and Melilla borders back to Morocco, citing a special regime referring to the substantial exceptionality of these cities. Furthermore, this provision mandates that applications for international protection must be submitted at designated border crossing points, where the Asylum Offices (*Oficinas de Asilo*) are located. While people of Moroccan, Algerian, and Syrian nationality can generally access these points, people on the move of sub-Saharan origin face significant barriers. The process involves in fact a dual triage by both Moroccan and Spanish authorities, based on nationality and deeply racializing procedures. In 2018, only six people from Burkina Faso, Guinea, and Mauritania were able to request asylum at the Melilla border crossing point, compared to the 290 who applied once inside Spanish territory (Costa Traba 2021). Consequently, sub-Saharan migrant people are often compelled to take extreme risks, such as scaling the border fence, to access Spanish territory (Amnesty International Spain 2016, 9–10; Commissioner for Human Rights 2015).

The adoption of the Tenth Additional Provision thus raised significant concerns, voiced also by the Council of Europe's Commissioner for Human Rights

(Muižnieks 2014). Although this provision stipulates that 'hot returns' must adhere to international human rights standards and protection laws, this requirement is fraught with controversy and contradictions, and no specific procedures are defined to ensure compliance.

Regrettably, the European Court of Human Rights' jurisprudence on this matter also remains contentious. Notably, the Court's ruling on the case of *N.D. and N.T. v. Spain* – initially decided on 3 October 2017 and later overturned by the Grand Chamber on 13 February 2020 – illustrates the deep tensions surrounding this issue[15]. In its 2017 decision, the Court found that the applicants, who had attempted to scale the fences in Melilla, were forcibly removed and returned to Morocco while under the exclusive and constant control of Spanish authorities. However, the Grand Chamber's 2020 ruling concluded that Spain had not violated the prohibition of collective expulsions, attributing the outcome of the operation to the applicants' «culpable conduct». This ruling provoked sharp criticism, as it appears to legitimise the indiscriminate pushback of migrant people if regular border crossing at specific points is made possible. However, the decision does not undertake a throughout examination of the *real* accessibility of such crossing points (Markard 2020). Concurrently, this approach risks endorsing *non-entrée* policies and effectively legitimising the establishment of a 'no man's land' around the enclaves (Sardo 2021).

These developments illuminate how political choices and legal interpretations are converging to mask the violence inherent in border enforcement. This convergence is also evident in the increasing digitalisation of border patrols, as exemplified by the SIVE, which can enhance pushbacks while simultaneously reducing their visibility.

As previously mentioned, the lack of a clear legal basis for the SIVE complicates any in-depth legal analysis. Additionally, according to data collected by the European Union Agency for Fundamental Rights in 2013, Spanish authorities claimed that the SIVE does not involve the collection or processing of personal data. However, as for the Greek case, in the absence of further evidence, this is not entirely reassuring. The Fundamental Rights Agency noted in fact that the ability of the SIVE to identify individuals depends on factors such as distance, lighting, and weather conditions, indicating that the processing of personal data remains technically feasible (European Union Agency for Fundamental Rights 2013). Thus, despite the absence of updated information regarding the data collected through radars, cameras, and data-sharing networks, it remains challenging to definitively determine whether personal data is processed by the Spanish surveillance system.

Furthermore, assuming that the SIVE can incorporate data from drones, it is essential to have a look at the national legislation governing the use of UAVs. Notably, Spain was one of the first European countries to introduce drone regulations, with the passage of Law 18/2014, which sought to address a significant gap in the

[15] ECtHR, *N.D. and N.T. v. Spain*, Applications nos. 8675/15 and 8697/15, 13 February 2020.

legal framework (Pauner Chulvi 2016)[16]. However, this law provided only partial and incomplete regulations, later addressed by the Royal Decree 1036/2017, which specifically covers drones within the broader framework of the Air Traffic Regulations (*Reglamento de Circulación Aérea*)[17]. The national regime was later replaced on 1 January 2021 by the provisions of EU Regulation 2019/947[18].

In terms of the professional and commercial use of drones, the 2014 Law permits a wide range of activities, including research and development, firefighting, aerial observation and surveillance, and search and rescue operations. Article 50 of Law 18/2014 stipulates that drone operators are responsible for all activities conducted with UAVs, including compliance with personal data protection obligations as outlined in Organic Law 1/1982 on the right to personal and family privacy and one's own image[19], Organic Law 15/1999 on data protection[20], and Organic Law 3/2019 on the protection of personal data with regards to digital rights[21]. Law 15/1999 defines personal data in accordance with the relevant European Directive, applying this definition to any images, sounds, or voices captured by drones.

Concerning the use of drones in public spaces by law enforcement agencies (*Fuerzas y Cuerpos de Seguridad*), Organic Law 4/1997 provides provisions for mobile video surveillance systems, although not explicitly mention drones[22]. It permits the use of these systems to prevent crimes and maintain public security, thus potentially applying in border settings. However, any use of drones by police forces must adhere to the principle of proportionality, both in terms of appropriateness and minimal intervention (Article 6, Law 18/2014) (Pauner Chulvi 2016, 97). Moreover, the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, AEPD) (2019b) has repeatedly emphasized the importance of conducting risk and data protection assessments before deploying drones, although there is no binding obligation in this sense. Notably, there is still no evidence suggesting that risk analyses are routinely performed before digital patrolling operations are initiated.

Ultimately, the use of drones by State surveillance forces must not subordinate individual rights to the principle of security, as this could exert a deterrent

[16] Law no. 18/2014, On the approval of urgent measures for growth, competitiveness and efficiency, 15 October 2014.

[17] Royal Decree no. 1036/2017, Governing the civil use of remotely piloted aircraft, 15 December 2017.

[18] Commission Implementing Regulation no. 2019/947 on the rules and procedures for the operation of unmanned aircraft, 24 May 2019.

[19] Organic Law no. 1/1982, On the Civil Protection of the Right to Honour, Personal Privacy and Self-Image, 5 May 1982.

[20] Organic Law no. 15/1999, On Protection of Personal Data, 13 December 1999.

[21] Organic Law no. 3/2018, On Protection of Personal Data and Guarantee of Digital Rights, 5 December 2018.

[22] Organic Law no. 4/1997, Regulating the Use of Video Cameras by Security Forces and Units in Public Spaces, 4 August 1997.

effect that undermines the full enjoyment of these rights – a concern highlighted in chapter 1 regarding the disciplinary effects of surveillance. However, this deterrent outcome is precisely the aim of the deployment of drones and systems such as the SIVE for border control.

Regarding the collection of data via drones, the AEPD labels drone operations into three categories: those not involving personal data processing (typically recreational or domestic use), those with a risk of inadvertent data processing, and those specifically intended for data processing (Spanish Data Protection Agency 2019a). Border surveillance activities likely fall within the two latter groups, which are thus subject to both the General Data Protection Regulation and Organic Law 15/1999. The AEPD also advocates for the implementation of privacy-by-design features and adhering to the guidelines for video surveillance, regardless of whether the systems are fixed, as with the SIVE, or mobile, as with drones (Spanish Data Protection Agency 2019c). This is particularly pertinent concerning the southern *frontera inteligente*, where the use of facial recognition technologies is explicitly considered. The AEPD has also underscored the necessity of applying existing legislation not only to data collection but throughout all stages of data processing. Any drone-related activity must thus comply with relevant laws, including video surveillance regulations and fundamental rights legislation (Spanish Data Protection Agency 2019d). Of course, these rights encompass not only data protection but also the right to claim asylum and the prohibition of *refoulement*.

In conclusion, the digitalisation of border patrols in Spain is being integrated into a regulatory and political framework that is frequently hostile to people on the move, often leading to discriminatory outcomes. Furthermore, the rapid evolution and integration of border surveillance technologies – facilitated by cooperation with third countries – has not been paralleled by a corresponding development of protection frameworks. The current legal framework governing the use of drones remains ambiguous and underdeveloped, particularly in the context of border enforcement, also due to the scarcity of information on the data thus collected.

Despite the high maintenance costs, the SIVE has not replaced traditional patrolling methods but rather seems to *facilitate* them, also in cases of externalisation agreements and violent pushback operations. Moreover, the limited contributions of the SIVE to sea rescue operations do not mitigate the System's role in endangering migratory routes and enabling *push* and *pullbacks* in coordination with Moroccan authorities, often marked by discriminatory stances. Today, the journey across the 'inviolable sea' of the Pillars of Hercules thus remains particularly perilous.

CHAPTER 4

Navigating national, supranational, and international spheres: between digital patrolling and fundamental rights

4.1. From the eastern to the western route: a comparative analysis of digital patrolling

By focusing on the case studies of Greece and Spain, this research has attempted to undertake a comprehensive analysis of the factual realities and legal frameworks surrounding the digitalisation of border patrols. These cases are significant due to their political, geographical, and legal dimensions, where remarkable technological experimentation in border areas is embedded, thereby enabling a comparative analysis of the strategies employed by EU Member States along the eastern and western migratory routes to Europe. Such a comparative approach is particularly effective in revealing processes, patterns, and concerns that extend beyond the specific cases of Greece and Spain, potentially applying – at least in part – to other settings and sites around the EU.

This chapter extends the comparative analysis to explore the wider ramifications of digital border patrolling, from local to national, EU, and international levels. Specifically, it critically examines issues surrounding human dignity and the right to international protection, particularly concerning the principle of *non-refoulement*, alongside the right to privacy and data protection. These discussions are framed within the context of recent developments on the regulation of interoperability and Artificial Intelligence. Additionally, the chapter addresses how the principle of non-discrimination is increasingly challenged by the digitalisation of patrolling, eventually raising further questions on accountability and jurisdictional matters.

To navigate these multiple layers, a 'topographical approach' is employed in order to read through and interrogate the most significant fallouts of digital pa-

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

trolling in Greece and Spain. As articulated by Nikolas Feith Tan and Thomas Gammeltoft-Hansen (2020), this perspective advocates for a bird's-eye view across various legal regimes, overlapping frameworks of liability, and geographical contexts. The overarching aim is thus to draw on the different border segments analysed to derive interpretive insights that shed light on the pervasive and rapidly evolving dynamics around digital patrolling. By comparing the two case studies, this section reflects on the significance of the specific contexts in which digitalisation processes unfold, the consequences of the general lack of transparency in border management, and the risks posed to people on the move by the inadequacy of current safeguards in digital border patrolling practices.

4.1.1. Untangling digital patrolling from the ground

Given their pivotal roles along the eastern and western migration routes and their shared land borders with non-EU countries, Greece and Spain hold highly strategic significance in the European framework of border control and migration management. Both countries have over the years prioritised deterrence against unauthorised or unsolicited migration, frequently employing practices that infringe upon fundamental rights. However, this 'deterrence approach' has proven more effective in rerouting migration through more perilous channels rather than overall reducing arrivals. Notwithstanding this, there has been persistent investment in advanced technological measures designed to prevent undetected entry into Europe. This effort consistently receives robust and growing support from the European Union and Frontex, also through financial allocations targeted at perceived crises and emergencies, notably under the Borders Emergency Assistance Fund. Moreover, both States actively engage in cooperation arrangements with neighbouring countries – Türkiye for Greece, and Morocco, along with Algeria, Senegal, and Mauritania for Spain – taking part in broader borders externalisation efforts in which digitalisation is entrenched.

The violence marking the land and sea borders in Greece and Spain remains a significant part of this picture, as frequent pushback operations and indiscriminate rejections abide stark, while increasingly mediated by advanced technologies. However, despite the growing deployment of drones and remote surveillance technologies, walls, barbed wire, and patrol dogs continue to dominate the EU's external borders. Concurrently, the increasing reliance on advanced surveillance technologies cannot be seen primarily as a means of protecting people on their journey to Europe. Instead, it is rooted in an environment increasingly hostile and restrictive for migration and international protection, often involving legislative measures that curtail fundamental rights. Greek Law 4636/2019[1], amended by Law 4686/2020[2], exemplifies this regression, while

[1] Law no. 4636/2019, On international protection and other provisions, 1 November 2019.

[2] Law no. 4686/2020, Improvement of the migration legislation, amendment of Law 4636/2019, 4375/2016, 4251/2014 and other provisions, 12 May 2020.

Spain's projects under the *frontera inteligente* model in Ceuta and Melilla hint at further tightening of borders, raising concerns about the consequences of criminalisation and discrimination in this area.

Overall, the analysis of digital patrolling in Greece and Spain reveals a clear trajectory in chasing enhanced situational awareness, detection, and tracking capabilities far beyond the EU's external borders. Whether using drones, thermal cameras, and pulse radars in Greece, or relying on integrated surveillance systems in Spain, this trend is marked by a pronounced militarization of border control. The latter, often cloaked in multi-purpose missions, humanitarian rhetoric, or efforts to dismantle trafficking networks, largely aims to make borders unreachable through a combination of technical, legal, and policy blocks and filters.

With the digitalisation of patrolling, gathering comprehensive data and information on what is happening before the borders becomes a key priority. This process culminates in the analysis, storage, and processing of the collected information to assess 'risks' at the external borders, straddling two seemingly opposing strategies: the standardisation of patrolling operations, which indiscriminately facilitates the containment and expulsion of people on the move regardless of their circumstances, and the targeted collection of extensive data – including personal and sensitive information – on those approaching the border and pre-frontier areas. Maximally standardised and simultaneously targeted patrols thus seem to coexist: the balance between these strategies shifts according to the security and strategic imperatives of each border area, remaining largely insulated from public scrutiny.

From here, the consolidation of situational awareness standards appears to reach unprecedented levels, whose full implications remain partially undefined or under-explored. Simultaneously, the capability to detect and track people and activities beyond the borders, and to make decisions based on advanced risk analyses that integrate information from various sources, is also advancing. This shift indicates a transformation in the nature of patrolling that goes beyond simply embedding advanced technologies in the sociotechnical assemblage of borders, as it further challenges the already floating concept of the border, intertwining surveillance, migration policy, and fundamental rights into a complex and inseparable matrix.

However, it is noteworthy that the deployment of advanced technological systems – as seen in the Evros region and along the Atlantic route – does not always lead to enhanced reaction capabilities and overall operational effectiveness. In practice, (techno-solutionist) expectations of effectiveness are often tempered and marked by paradoxes. The maintenance costs of these systems, instances of sabotage and resistance such as those against Spain's SIVE radars, and the continued reliance on traditional patrols alongside digital surveillance reveal another side of the story. Similarly, the mutable relations with neighbouring States, not rarely resulting in the cruel instrumentalization of people on the move for political leverage, significantly impact data harvesting activities that undergird digital patrolling. Digitalisation processes in border management in fact do not occur in a vacuum; they are deeply entrenched in and bent by specific contextual realities – and need to be considered accordingly.

Acknowledging such dialectics, the discourse on digitalisation should not be reduced to a binary debate between 'enthusiasts' and 'pessimists'. Instead, it is crucial to consider how the narrative of technological neutrality risks obscuring the inherent conflicts and struggles for recognition that define the migratory experience, flattening inequalities, and exacerbating vulnerabilities. Indeed, as evidenced by the bordering practices in Ceuta, Melilla, and the Aegean, context *shapes* technology to a considerable extent.

Moreover, the 'context' is a substantial factor influencing the deployment of patrolling technologies. Today, the digitalisation of patrols is foremost aimed at more pervasive surveillance and the dismantling of irregular migration routes – still the primary option for individuals kept at the margins of legal pathways, whether fleeing conflict, insecurity, environmental crises, or economic hardship in the attempt to reach Europe. This perpetuates global North-South asymmetries, which only privileged 'trusted travellers', the few 'facilitated' in their mobility by smart borders, can bypass. Additionally, as largely discussed, digitalisation is embedded within broader processes of externalisation, privatisation, and securitisation of border enforcement, which inject a military bias into migration policies. Consequently, far from being neutral, technological experimentation and innovation in this context replicate power hierarchies while raising transparency concerns, rendering security issues even more opaque, and diminishing public awareness[3]. Furthermore, digitalisation in border security exacerbates the differentiation of rights between citizens and non-citizens, a cleavage that invariably has profound social and political complications (De Genova 2002, 419; Molnar 2019, 306).

Both in Greece and in Spain, the analysis of on-the-ground developments and relevant legislation reveals to which extent border and migration issues remain largely opaque and subject to discretionary power, with State sovereignty and national security often being invoked to blankly justify the testing and use of new technologies. The militarized zone along the Evros border and the barriers around Ceuta and Melilla, where attempts at territorial deviation and systematic discrimination play a visible role, plastically exemplify this trend. Moreover, the veil of secrecy surrounding the details of patrolling technologies – both drones and integrated surveillance systems – has proven particularly challenging to lift. The little information available on the use of these tools often leaks from procurement contracts, media reports, and civil society organisations' witnesses rather than official sources.

In line with the findings discussed in the literature on the role of secrecy in border areas (see Pallister-Wilkins, Goede, and Bosma 2020), it is evident that

[3] It is crucial to highlight that transparency issues surrounding high levels of surveillance – often difficult to reconcile with democratic principles – are becoming increasingly prevalent, not only in Greece and Spain but across many European countries. According to the European Digital Rights (EDRi) (2020), at least fifteen European countries have, in recent years, engaged in trials involving highly invasive facial and biometric recognition technologies aimed at mass surveillance.

remote surveillance systems and AI-driven screenings are closely tied to national security concerns, resulting in classified data collection and processing methods (Molnar and Gill 2018, 18). The same applies to the algorithms and data used in systems like EUROSUR or SIVE, with alerts and risk assessments visualised on operational interfaces that reflect opaque objectives and rationales.

4.1.2. The legal landscape of digital patrolling: concealment, black holes, and regulatory attempts

The dynamic of 'concealment' in the realm of digital patrolling extends alarmingly to the legal sphere, where regulatory attempts often appear loose and fuzzy. This opacity has led experts to argue that States are actively evading international legal responsibilities through digitalisation efforts, particularly regarding access to asylum and international protection (Wallis 2022). A further concern in this context is the diffusion and dispersion of responsibilities for potential violations among various actors, possibly resulting in the widening of accountability gaps. The increasing reliance on national and European agencies, such as Frontex and EMSA, with border enforcement support mandates is also part of this picture, a phenomenon that Petra Molnar (2019, 306) has effectively described as a form of «agency laundering».

Despite some recent, and in some cases *very* recent, regulatory efforts in Greece and Spain, 'legal black holes' where migrant people can be abandoned persist. In the literature, the concept of legal black holes describes spaces and contested sites where individuals face severe *rightlessness* due to limited or suspended legal protections (Tan and Gammeltoft-Hansen 2020), thus depicting particularly well the case at hand. Here, State duties remain ungrounded, and technological experimentation thrives. Consequently, the absence of clear rules and a regulatory system, that often seems disconnected from basic rule of law principles, makes it challenging to prove and contest infringements related to digital patrolling.

Specifically, the regulation of drones and similar surveillance systems in Greece is still in its early stages. Competencies for the deployment of UAVs for surveillance purposes were only officially granted to the Hellenic Police by Presidential Decree 98/2019[4], which still lacks specifics on data storage and processing activities. The Hellenic Data Protection Authority played a central role during the legislative process, prompting several amendments to clarify the regulatory framework, eventually leading to the adoption of Presidential Decree 75/2020[5]. However, the current legal framework remains rapidly evolving, sometimes labyrinthine, and still fails to address all the grey areas associated with the digitalisation of patrolling. In contrast, Spain introduced a technical regulation on

[4] Presidential Decree no. 98/2019, Organisation and structure of the Drone Service, Establishment of Procurement Directorates and History of the Hellenic Police and Unmanned Aircraft Service, 21 March 2017.

[5] Presidential Decree no. 75/2020, Use of surveillance systems obtaining or documenting sound and pictures in public places, 10 September 2020.

drones as early as 2014 (Law 18/2014)[6], marking a significant milestone at the European level. Nonetheless, the overall regulatory framework remains vague, as exemplified by the absence of a specific legal basis for the use of the SIVE by the *Guardia Civil*. In both countries, moreover, the competencies of the authorities responsible for digital patrol systems and the modalities of cooperation with other security forces and European agencies seem rather oblique.

Both Greece and Spain have regulations stipulating that the deployment of new technologies at external borders, particularly those capable of collecting personal data and involving AI systems, must be accompanied by an impact assessment to evaluate their effects on the rights of the people concerned. However, various authorities, agencies, and organisations have reported that the actual implementation of these assessments is often defective and largely fails to meet the expected standards.

4.2. Technology and the law: rights at stake in digital patrolling operations

The digitalisation of patrolling profoundly affects the rights of people in patrolled areas and challenges the law's ability to provide an adequate bulwark of protection against potential violations pouring from legal black holes, secrecy imperatives, and the difficulties in regulating rapidly evolving systems. Attempting to assess the implications of these developments in border surveillance on people's lives and fundamental rights is a complex endeavour, but one of significant interest and importance.

As discussed, new technologies can introduce new risks, inequalities, and unforeseen consequences that turn oversight attempts concerning both their deployment and the use of the data thus collected into a complex endeavour (Dijstelbloem, Meijer, and Besters 2011, 15). This directly impacts human dignity and raises significant concerns regarding equality, data protection, and access to justice, especially when dealing with systems based on AI and with varying degrees of automation (European Union Agency for Fundamental Rights 2020). Currently, there is a notable absence or inadequacy of regulatory frameworks specifically addressing automation in the context of borders and migration management, notably concerning accountability schemes and protection mechanisms.

Given these challenges, it is helpful to embrace a framework that integrates and patches various legal regimes from a comparative (and bird's-eye) perspective, moving from a fundamental rights-centred approach. The goal is thus to go beyond the specific considerations introduced in earlier chapters on Greece and Spain, adopting a more holistic human rights protection strategy when addressing the rights of people on the move at the EU's external borders (see Beduschi 2022).

[6] Law no. 18/2014, On the approval of urgent measures for growth, competitiveness and efficiency, 15 October 2014.

To this end, zooming out from national case studies to examine International Human Rights Law (IHRL) perspectives, European fundamental rights regimes, and migration law insights can be promising. This analysis will focus on four 'pillars' – both human rights and core principles – of the fundamental rights system: human dignity, access to protection and asylum, privacy and data protection, and equality and non-discrimination. As emerged from the Greek and Spanish case studies, these areas are particularly ductile to digital patrolling.

4.3. Human dignity in times of de-humanised surveillance

According to Özgün E. Topak (2021, 796), border violence should be broadly understood as «the entire set of processes whereby migrants' somatic and mental capacities are repressed or destroyed at and beyond the territorial border». Building on a similar understanding, Claudia Aradau and Lucrezia Canzutti (2022) introduce the concept of «technologies of cruelty» to describe the processes of objectification and dehumanization crystallized in asylum politics when driven by the assumption that people seeking protection are inherently 'bogus'. These governing strategies are mirrored also in digital border spaces, in a shift that threatens the full respect of human dignity, a principle that can be described as underpinning all considerations on fundamental rights.

In recent years, legal scholars have engaged in various debates about the definition and scope of the concept of human dignity. This renewed interest stems from the recognition that, due to its interpretative versatility, human dignity can be a solid yet flexible framework for addressing emerging and complex socio-legal challenges (see Fernández Burgueño 2016). Without delving into the details of this often thorny debate, it should be noted that many scholars view human dignity as a «mother-right» (Barak 2015) that serves as a foundational 'framework right'.

In International Law, human dignity has been embedded in key human rights treaties since the 1948 Universal Declaration of Human Rights (UDHR)[7].

[7] UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III), 10 December 1948. In particular, reference to human dignity is present in the International Convention on the Elimination of all Forms of Racial Discrimination (UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination*, United Nations, Treaty Series, vol. 660, 21 December 1965), the International Covenant on Economic, Social and Cultural Rights (UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, United Nations, Treaty Series, vol. 993, 16 December 1966), the International Covenant on Civil and Political Rights (UN General Assembly, *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, 16 December 1966), the Convention on the Elimination of All Forms of Discrimination against Women (UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, United Nations, Treaty Series, vol. 1249, 18 December 1979), the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment (UN General Assembly, *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, United Nations, Treaty Series, vol. 1465, 10 December 1984), the Convention on the Rights of the Child (UN General Assembly, *Convention on the Rights of the Child*, United Nations, Treaty Series, vol. 1577, 20 November 1989), the International Convention on the Protection of the Rights of All Migrant Workers and Members of

However, the interpretation and application of human dignity vary significantly across different international jurisdictions, making it challenging (and not particularly desirable) to unify these diverse approaches[8]. Accordingly, the notion of human dignity has been integrated into national and regional legislation in a highly differentiated way.

In Europe, Article 1 of the European Convention on Human Rights (ECHR) enshrines human dignity as the inviolable foundation of fundamental rights. The Court of Justice of the European Union has also repeatedly affirmed that human dignity is an integral part and parcel of EU law[9].

Hans Jörg Sandkühler (2015) argues that the notion of human dignity becomes particularly influential in times marked by processes of societal dehumanization. This perspective seems indeed relevant in the context of digital patrolling, as it re-centres the debate on people on the move. These considerations pave the way to a deeper understanding of the implications of digital patrolling so far discussed, suggesting that a focus on human dignity could help to address some of the regulatory gaps that emerge with the *smartening* of borders.

As discussed, one of the most concerning aspects of digital patrolling is the shift in how surveillance is conducted. Patrolling personnel are increasingly removed from borderlines, operating from screens-cluttered coordination centres, while digital patrolling equipment is deployed closer to the people being monitored, also in international waters and third countries' territory.

Through the deployment of UAVs and the use of advanced surveillance systems, the avoidance and the impossibility of a direct 'encounter' between migrant people and actors engaged in patrol activities is often used to justify evading international obligations, notably in cases of distress at sea. Moreover, by preventing people on the move from reaching borders, States distance themselves from the responsibility of assessing asylum and international protection claims (Laursen 2022). The Commissioner for Human Rights of the Council of Europe (2021), Dunja Mijatović, recently pointed out the shift to aerial surveillance, especially in the Central Mediterranean, as evidence of European States' unwillingness to establish adequate protection systems.

Moreover, the digitalisation of patrolling shifts the discourse around border security towards a more impersonal and abstract direction, characterised by one-way interactions that reduce migrant people to 'security objects' to be 'managed' through advanced technological tools. This produces a deliberate distancing of people attempting to reach the external borders, leading to a de-

Their Families (UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, A/RES/45/158, 18 December 1990), and the Convention on the Rights of Persons with Disabilities (UN General Assembly, *Convention on the Rights of Persons with Disabilities*, A/RES/61/106, 24 January 2007).

[8] See Klein and Kretzmer (2002) for an in-depth study of the development of the concept of human dignity between International Human Rights Law and international jurisprudence.

[9] See CJEU, *Netherlands v. European Parliament and Council*, C-377/98, 9 October 2001, §70-77.

humanisation of border security that closely parallels the dynamics observed in the deployment of automated systems in warfare (Wall and Monahan 2011).

While it is sometimes argued that digital patrolling could make border control more 'humane' and less prone to arbitrary violence, this claim is contestable for several reasons. First, advanced surveillance systems rarely replace physical barriers but often complement them. This is evident, for example, both in the Evros region, along the wall remotely surveilled, and in Ceuta, where the triple fence is reinforced by the *frontera inteligente*. Secondly, in the crevices between the dehumanisation of patrolling and the objectification of people attempting to reach European borders, violence has been shown to even be more likely (Molnar 2020).

Moreover, as observed in both Greece and Spain, digital patrolling often compels people to take more dangerous routes. On this note, a particularly striking example comes from the other side of the Atlantic, where the Biden Administration has opted for new technologically advanced (and ostensibly more 'humane') monitoring strategies at the border with Mexico, aiming to take a distance from the brutality of the wall vehemently advocated during the Trump Presidency. However, it has been shown that this more politically palatable approach – which has led to the construction of Integrated Fixed Towers and the deployment of robotic patrol dogs – has driven migration routes through the Arizona desert, resulting in the tripling of deaths at the border (Chambers et al. 2021).

Overall, the coexistence of digital patrolling with increased direct and indirect border violence can be deemed well-established. Moreover, the use of digital tools in border patrolling is often justified by their effectiveness in performing "3D-tasks" – those considered 'dull, dirty, and dangerous' and thus particularly challenging and unpleasant. However, deploying drones for these purposes often leads to increased 'recklessness' in patrolling activities (Val Garijo 2020, 138), driven by the assumption that what is technically feasible is also legally, socially, and ethically acceptable.

In an influential article, Luisa Marin (2017) traced the dehumanization of border surveillance through drones and other digital patrolling systems to two main issues. The first concerns the ability of drones deployed in *dull* and *dangerous* settings to differentiate between scenarios requiring different legal responses. In theory, drones could in fact detect boats in distress, potentially triggering adequate interventions and reporting cases where medical assistance is needed. In this direction, Mark Coeckelbergh (2013) argues that advanced surveillance technologies might bridge the epistemic gap caused by the 'remoteness' of drone patrols, at least partially balancing the dehumanization of surveillance by enabling more targeted human interventions. In practice, however, it is rather unclear whether current surveillance systems, including those using UAVs, are designed to detect and collect data on distress circumstances or the conditions of vulnerability among people approaching the borders. Moreover, while the fascinating debate surrounding this issue lies well beyond the scope of this study, critical scholars working on data and AI have expressed doubts about the capacity of automated systems embedded in border patrols to fully (or better) 'comprehend' situations that prompt international obligations (see Hildebrandt 2020).

The second issue raised by Marin's analysis – in line with the study of bordering practices in Greece and Spain – further shows that the narrative of digitalisation as a humanitarian measure, ostensibly aimed at saving lives, has little empirical support. Instead, the latter suggests that digital surveillance aligns with securitarian and preventive priorities rather than protection. This discrepancy underscores a key point here: increased situational awareness through digital means simply does not necessarily lead to better assistance for migrant people in distress.

As mentioned, another dynamic fostered by the digitalisation of patrolling is the growing standardization of decision-making processes across various operational levels, from risk assessment to interception operations, reducing the space for individual case analysis. As it has been discussed, while standardization might limit discretionary and arbitrary decisions[10], it also challenges the international protection system, which is fundamentally based on the assessment of particular cases and individual conditions (Dijstelbloem, Meijer, and Besters 2011, 15). These circumstances raise an inevitable question: can human dignity, with all its complexities, be fully accounted for within an increasingly standardized framework?

In conclusion, the dynamics of digitalisation in patrolling – resulting in dehumanization, dilated distances, and the objectification of migrant people as «indistinct, pixelated, and vaguely humanoid shapes»[11]– risk creating conditions that severely limit the recognition of human dignity for those attempting to reach European borders (and pre-border areas). However, this is not definitive. Future developments, ideally also grounded in legal advancements rather than merely technological ones, could potentially address some of these challenges – at least partially – in the (now, quite unlikely) event that the EU border landscape undergoes significant change.

4.4. The right to seek protection: *non-refoulement* between access to asylum and border surveillance

As discussed, the digitalisation of patrolling, when embedded in migration containment and deterrence strategies, often manifests in violent border control measures designed to prevent access to European borders. As explored in chapters

[10] From this perspective, it is worth noting that the UN Global Compact for Safe, Orderly, and Regular Migration (GCM) has contributed to advancing, or at least facilitating, the adoption of unified and standardised approaches to migration management. These approaches include, among other aspects, the establishment of frameworks for efficient border crossings, with a pronounced emphasis on the integration of information technologies, pre-screening measures, and data collection on individuals involved. This trend toward the standardisation of migration management has prompted various concerns, particularly surrounding the endorsement of extensive data collection practices. These concerns are well-founded, given the disparate levels of data protection among States, which are far from *standardised*. For a nuanced discussion of these issues, see Kuşkonmaz (2021).

[11] See chapter 3.

2 and 3, the convergence of advanced patrolling technologies, securitizing policies, and vague legal frameworks raises significant human rights concerns, notably regarding the obligations stemming from the principle of *non-refoulement* and the right to seek asylum (Val Garijo 2020). Pushback operations, a widespread and alarming practice at the EU's external borders, exemplify these concerns[12]. Pushbacks not only have immediate and severe consequences for potential asylum seekers but also often result in the perpetration of extremely violent operations against people on the move, regardless of their intentions to seek protection. Although the primary concern here is the inability to access asylum, it is essential to avoid reinforcing the often biased and oppositional distinction that Rebecca Hamlin (2021) refers to as the «migrant/refugee binary». If the boundaries of this binary are frequently contested and marked by arbitrariness, yet at and before the border, such divisions tend to fade into irrelevance.

As already discussed, the indiscriminate prevention of access to protection in Europe is not exclusive to the digitalisation of patrolling, but a glaring outcome of border policies centred on externalization, containment, and pushback (or pullback) operations. Moving forward, this section presents a brief overview of the legal framework designed to counteract the barriers preventing the lodging of protection applications.

At the international level, the right to seek and enjoy asylum is enshrined in Article 14 of the UDHR and further regulated by the 1951 Refugee Convention and its 1967 Optional Protocol[13]. The right to seek asylum is obviously dependent on the principle of *non-refoulement*, which ensures that no individual is rejected without a thorough analysis of their situation. As anticipated in the previous chapters*, non-refoulement*, as established by the 1951 Convention (Article 33), prohibits States from removing, expelling, or extraditing individuals to a country where they risk facing the death penalty, torture, or other inhuman or degrading treatment. Thomas Gammeltoft-Hansen (2013, 44) describes it as the «strongest commitment» that the international community has made to protect those who are no longer able to avail themselves of the protection of their own State. Recognized as *ius cogens* and a peremptory norm of international law, *non-refoulement* is thus the primary obligation that States have to fulfil with regards to people in need of protection and the cornerstone of the whole international asylum regime – which would otherwise result in being empty and futile (Giuffré and Moreno-Lax 2019; Simeon 2019; Trevisanut 2014).

The *non-refoulement* principle is sanctioned by several other key international conventions, including the 1984 Convention against Torture (CAT, Article 3) and the 1966 International Covenant on Civil and Political Rights (ICCPR), deriving from the right to life (Article 6) and the prohibition of torture (Article

[12] Among the reports documenting violations at European borders, Human Rights 360° (2020) is particularly relevent.

[13] UN General Assembly, *Convention Relating to the Status of Refugees*, United Nations, Treaty Series, vol. 189, 28 July 1951 and UN General Assembly, *Protocol Relating to the Status of Refugees*, United Nations, Treaty Series, vol. 606, 31 January 1967.

7)[14]. At the European Union level, the right to seek asylum is guaranteed *inter alia* by Article 18 of the EU Charter of Fundamental Rights (CFR)[15], while *non-refoulement* and the prohibition of collective expulsions are codified in Article 19 of the CFR and Article 4 of Protocol No. 4 of the ECHR. Furthermore, several EU Directives and Regulations, such as the Qualification Directive[16], the Asylum Procedure Directive[17], the Return Directive[18], and the Schengen Borders Code[19], mirror these international human rights obligations.

Moreover, under the ECHR, *non-refoulement* is an absolute obligation[20], directly linked to the prohibition of arbitrary deprivation of life (Article 2) and the prohibition of torture (Article 3). The European Court of Human Rights has upheld the applicability of *non-refoulement* in cases of pushbacks, non-admissions, and rejections both at sea and at territorial borders, as seen in landmark cases such as *Soering v. UK*[21], *Hirsi Jamaa v. Italy*[22], and *N.D. and N.T. v. Spain*[23].

[14] The ICCPR does not explicitly prohibit the removal of individuals to States that practice or tolerate human rights violations. However, the UN Human Rights Committee has interpreted Articles 2, 6, and 7 of the Covenant to prevent extradition, deportation, expulsion, or any form of removal when there are well-founded fears of a real risk of irreparable harm, both in the country of expulsion and in any other country to which the individual might subsequently be sent (*chain refoulement*). Additionally, the principle of *non-refoulement* is reinforced by other international and regional instruments, such as the 1967 United Nations Declaration on Territorial Asylum, the 1969 Organization of African Unity (OAU) Convention Governing the Specific Aspects of Refugee Problems in Africa, the 1984 Cartagena Declaration on Refugees, and the 1966 Bangkok Principles on the Status and Treatment of Refugees. For a deeper analysis of these instruments, see James C. Simeon (2019).

[15] At the European Union level, the right to asylum is moreover enshrined in the Qualification Directive (2011/95/EU, Articles 2, 13, 18), the Asylum Procedures Directive (2013/32/EU, Preamble paras. 12, 15-18 and Articles 1, 2, 10), the Reception Conditions Directive (2013/33/EU, Preamble paras. 26, Articles 3, 6), the Schengen Borders Code (Regulation EU 2016/399), and the Dublin Regulation (604/2013).

[16] Qualification Directive 2011/95/EU, Article 21.

[17] Asylum Procedures Directive 213/32/EU, Articles 9, 28, 35, 38, 39, 41 and Annex I.

[18] Return Directive 2008/115/EC, Articles 4, 5 and 9.

[19] Schengen Borders Code Regulation (EU) No. 2016/399, Article 4.

[20] See ECtHR, *Saadi v. Italy*, Application no. 37201/06, 28 February 2008.

[21] In *Soering v. United Kingdom*, Application no. 14038/88, 7 July 1989, the European Court of Human Rights clarified that the principle of *non-refoulement* is supported by a *par ricochet* protection. The Court also established that, under certain circumstances, the responsibility of a State can arise due to the actions undertaken by another State.

[22] This pivotal ruling has, in fact, marked the transition from *push*back operations between Italy and Libya to *pull*back operations, in coordination between Italian and Libyan authorities. These operations, while characterised by a greater degree of externalisation, are no less severe in terms of the violations of the fundamental rights of the individuals involved.

[23] ECtHR, *Hirsi Jamaa and Others v. Italy*, Application no. 27765/09, 23 February 2012; and ECtHR, *N.D. and N.T. v. Spain*, Applications nos. 8675/15 and 8697/15, 13 February 2020. At §185, the Court provides a definition of the term 'expulsion', described as any forcible removal of aliens from a State's territory, irrespective of the lawfulness of the stay, the length of time they spent in the territory, the location in which they were apprehended, and their status as migrants or asylum-seekers.

These rulings emphasize the centrality of the rights of individuals in the protection system and reject the creation of «areas outside the law» in border zones[24].

Despite this comprehensive legal framework, violations of *non-refoulement* continue to be a major concern at the EU's borders, often involving violent push-backs or forms of 'cooperative deterrence' with third States, described in the literature as cases of «neo-*refoulement*» (Hathaway and Gammeltoft-Hansen 2014; Hyndman and Mountz 2008). As discussed, agreements with Türkiye and Morocco have often resulted in practices that effectively deny access to protection. Additionally, the preventive approach of smart borders tends to facilitate instances of «data-banned populations», as coined by Didier Bigo (2014), where individuals are denied entry to a European State based on data-driven profiling and categorisation, rather than individual assessment. Information gathered through digital patrolling can in fact lead to targeted policing operations that further entrench these exclusionary practices.

This opens the way to data-sharing practices with third States or non-State actors resulting in the denial of access to protection or, more broadly, in the limitation of mobility possibilities. These forms of cooperation, which could be described as forms of «digital refoulement», are difficult to document and challenge, yet their consequences can be severe from a human rights perspective (Fill 2021).

In addition to these fundamental provisions on the right to seek protection and the *non-refoulement* obligation, several international and European norms closely connected to the right to life apply to border surveillance operations and digital patrolling activities[25].

At the international level, particularly regarding maritime frontiers, relevant legal frameworks emerge from the law of the sea, as defined by the UN Convention on the Law of the Sea (UNCLOS)[26], the Safety of Life at Sea Convention (SOLAS)[27], and the Search and Rescue Convention (SAR)[28]. While a detailed discussion of these Conventions is beyond the scope of this analy-

[24] See ECtHR, *Hirsi Jamaa and Others v. Italy*, Application no. 27765/09, 23 February 2012, §178.

[25] Border surveillance provisions within the EU have already been discussed before. Suffices here to recall that the legal framework for border surveillance is established by Article 12 of the Schengen Borders Code and Article 12 of the EUROSUR Regulation. The former emphasises that the primary objective of border surveillance is to prevent unauthorised border crossings, counter cross-border criminality, and take action against those who have crossed the border illegally. The latter mandates the common application of surveillance tools, thus creating the context in which Frontex's coordination and support role can be fully realised. Frontex, indeed, plays a central role in the border enforcement framework through operations and interventions that frequently raise accountability and transparency concerns. On this issue, see Lena Karamanidou and Bernd Kasparek (2020).

[26] UN General Assembly, Convention on the Law of the Sea, 10 December 1982.

[27] International Maritime Organization, *International Convention for the Safety of Life at Sea*, 1 November 1974.

[28] International Maritime Organization, *International Convention on Maritime Search and Rescue*, 27 April 1979.

sis, it is essential to acknowledge that they form the fundamental regulatory background for border surveillance[29]. Notably, a recent report by the United Nations Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions reaffirms that UNCLOS, SOLAS, and SAR intend to establish a system to rescue all vessels in distress, without discrimination based on nationality, status, or circumstances in which a person is found (General Assembly of the United Nations 2017, para. 61). These principles were further reinforced in the Views adopted by the Human Rights Committee (2021) regarding the *A.S., D.I., O.I., and G.D. v. Italy and Malta* case, which addressed responsibility for failure to rescue at sea also emphasizing the obligation of conducting rescue operations seriously, even in situations involving concurrent jurisdiction among States.

However, the analysis of the case studies raises concerns about the actual enforcement of these frameworks in the context of digital patrolling. As discussed, the enhanced surveillance capabilities at and before borders are not necessarily correlated with more effective rescue operations and easier access to protection: while the occurrence of undetected shipwrecks should become increasingly rare or even exceptional, tragedies at sea and in pre-frontier areas continue to occur. This seems indicative of the underlying priorities driving digital patrolling operations. Despite the claimed full situational awareness, the persistence of such incidents highlights a troubling disconnect between the technological capabilities of surveillance systems and human rights obligations.

4.5. Data protection and privacy rights: the grey area of border zones

As highlighted in the analysis of the border areas in Greece and Spain, the digitalisation of patrolling raises significant concerns regarding data protection and privacy rights for individuals subjected to such surveillance. In fact, data collection at external borders often resembles indiscriminate trawling rather than targeted interventions. Given the uncertainty surrounding the type and volume of data collected and processed, it is essential to explore the legal questions arising from international and European obligations, which could potentially limit indiscriminate data harvesting practices at the borders.

4.5.1. International law considerations

First and foremost, it is important to clarify that the right to respect private life and the protection of personal data are distinct, self-standing rights. Internationally, the right to privacy is recognized as a human right, deeply rooted in the democratic principles of dignity and autonomy (Molnar 2021, 143). States must indeed respect, protect, and fulfil the rights to private life, home, and correspondence for individuals under their jurisdiction, as established by the Uni-

[29] For a deeper analysis of border surveillance under International Law, see Luisa Marin (2017).

versal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17).

While essential to the free development of an individual's personality and identity, the right to privacy is a qualified, not absolute, right. This means that State interferences can be deemed legitimate if they adhere to a four-fold test (Kuşkonmaz 2021), established in IHRL through UN Human Rights Committee decisions and general comments[30], and reports by UN Special Rapporteurs (OHCHR 2009; 2013). This test stipulates that interference cannot be arbitrary, must be provided for by domestic law in accordance with the principle of legality (OHCHR 2009, para. 17), must pursue a purpose necessary in a democratic society, and must aim to achieve a legitimate objective such as national security, public safety, public order, public health and morals, or the protection of others' rights and freedoms[31]. Additionally, the measures undertaken must be proportionate to the threat or risk they aim to address. A similar understanding of the principles of legality, necessity, proportionality, and pursuit of a legitimate aim is also established in the jurisprudence of different regional human rights regimes[32].

In terms of defining a 'legitimate aim', the UDHR and the ICCPR provide broad categories, such as protecting public order, which can potentially justify extensive policing activities and expand the scope of legitimate limitations to privacy rights (Murray 2020, 160). The principles of necessity and proportionality are more clearly defined and emphasized in various UN documents. For instance, General Comment No. 31 of the UN Human Rights Committee highlights the need for proportionate measures pursuing legitimate aims to ensure the protection of rights under the ICCPR (OHCHR 2004, para. 6). Moreover, in 2017, the Special Rapporteur on the Right to Privacy proposed a more comprehensive interpretation of the principle of necessity, arguing that it should be understood in light of the close connection between the ICCPR and the ECHR, particularly concerning Article 8 of the latter – thus aligning the principle of necessity in a democratic society (OHCHR 2019, para. 11).

To ensure compliance with these principles, the OHCHR has repeatedly advocated for independent supervision at the national level to prevent arbitrary data collection and processing (OHCHR 2014, para. 38). Moreover, States must provide remedies for violations of privacy rights. This includes making remedies accessible and known to individuals who may be involved in data collection practices,

[30] See HRC, *Van Hulst v. Netherlands*, Communication 903/1999, UN Doc. A/60/40, Vol. II, 1 November 2004 and HRC, *NK v. Netherlands*, Communication 2326/2013, UN Doc. CCPR/C/120/D/2326/2013/Rev.1, 18 July 2017

[31] The UN Special Rapporteur on the Right to Privacy (OHCHR 2019, para. 18) elaborated on this concept by applying the legitimate aims outlined in the limitation clause of Article 22 of the ICCPR, which pertains to freedom of assembly, to the grounds on which interference under Article 17 may be justified.

[32] See, for instance, IACHR, *Escher et al. v. Brazil*, Series C No. 193, 6 July 2009, §116, and ECHR, *Big Brother Watch and Others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, §304.

conducting prompt investigations into alleged violations (OHCHR 2014, para. 40), and defining by law the rights related to notification procedures and access to personal data (OHCHR 1988, para. 10). Of course, when considering access to remedies and obligations related to notification and data access in digital patrolling activities, ensuring an acceptable level of protection is far from guaranteed.

The rapid advancement and increasing use of surveillance technologies, often without public oversight, have thus raised international concerns about the effectiveness of privacy rights and data protection measures. An example of this concern is the appointment of a Special Rapporteur on the right to privacy in 2015 (Human Rights Council 2015), whose mandate highlights the risks posed by inadequately regulated technological progress to the right to privacy. Moreover, in 2016, a resolution on privacy in the digital age was adopted by the Third Committee of the General Assembly on Social, Humanitarian, and Cultural Issues, emphasizing the importance of respecting international commitments to privacy, particularly in relation to new technologies (Third Committee of the General Assembly of the United Nations 2016). The Resolution underscores that any legitimate security concerns States may have must be addressed consistently with their obligations under IHRL and that adequate remedies for violations must be ensured (Brown 2016).

Similarly, the UN General Assembly's Resolution 68/167 rights (2014) expressed concern about the human rights implications of surveillance technologies and mandated the High Commissioner for Human Rights to study the right to privacy in the digital age. The resulting reports have consistently highlighted the risks posed by advanced surveillance systems on individual rights, particularly the disproportionate impacts of technologies like remote real-time biometric recognition on certain groups (Human Rights Council 2021b). These concerns directly align with criticisms regarding the collection of biometric data through drones or other surveillance systems in the context of border patrolling.

Also the OHCHR has repeatedly expressed concerns about the normalization of mass surveillance technologies «as a dangerous habit, rather than an exceptional measure» (OHCHR 2014, para. 3), noting its potential to interfere with a range of human rights, including freedom of expression, peaceful assembly, and the right to family life (para. 20). Moreover, according to the Commissioner, the very existence of mass surveillance programs represents an interference with the right to privacy. Most of the digital patrol systems examined in this study, given their extensive monitoring capabilities, are likely to fall into the category of mass surveillance technologies.

In conclusion, while international law offers an overall robust framework for the protection of privacy rights and the regulation of data protection, these safeguards often remain unimplemented or ineffective in border zones, particularly in the context of digital border patrolling. This persistent gap is not merely the result of oversight but is frequently justified in the name of security imperatives, thereby pushing the boundaries of what constitutes legitimate and proportionate measures. As a result, privacy rights are increasingly undermined by the unchecked use of advanced surveillance technologies, which disproportionately affect people on the move at the EU's margins.

4.5.2. The European model: setting standards on digital patrolling?

At the European level, particularly regarding new technologies, a more comprehensive regulatory framework can be expected. The European Union has in fact emerged as a front-runner in efforts to regulate privacy and data protection, paying special attention to these rights. However, the application of these guarantees in border areas and within digital patrolling frameworks remains problematic.

The European Convention on Human Rights enshrines the right to respect for private and family life as a fundamental right in Article 8. Additionally, the Charter of Fundamental Rights of the EU establishes this right in Article 7 and the protection of personal data in Article 8, specifying that personal data must be processed fairly, for specified purposes, and based on the consent of the person concerned or on another legitimate basis provided by law. These provisions apply throughout the EU, without distinction of nationality, origin, religion, or status, covering both EU citizens and third-country nationals.

The conditions under which the right to respect for private and family life can be limited are outlined in Article 8, paragraph 2, of the ECHR. Interference by public authorities is permissible only when it is in accordance with the law and is necessary for a democratic society, pursuing legitimate aims such as national security, public safety, economic well-being, prevention of disorder or crime, protection of health or morals, or the protection of the rights and freedoms of others[33]. In line with the CJEU case law[34], any interference must thus be compatible with the principles of proportionality and subsidiarity, seeking a balance between competing interests in specific contexts (see Brouwer 2011, 151; Murray 2020, 159; Napieralski 2019, 6). Similarly, the rights set out in Articles 7 and 8 of the CFR may be subject to limitations under Article 52, paragraph 1[35], which also adheres to the necessity and proportionality tests applicable to the non-core aspects of the rights involved. The CJEU has also consistently emphasized the importance of the necessity test, particularly concerning data processing activities[36].

[33] On limitations, see European Court of Human Rights (2021, 25).

[34] Reference should be made to the CJEU decision in the *Joined Cases Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, 8 April 2014. In this ruling, the Court underscored the importance of the principle of proportionality within the EU law-making process, emphasising that legislative measures must not be more intrusive than necessary in order to achieve a lawful and specific purpose. The Court also urged the adoption of clearer and more precise rules concerning data collection, retention, and processing.

[35] The Article states that any limitation on fundamental rights must be prescribed by law, genuinely pursue objectives of general interest recognised by the Union or protect the rights and freedoms of others, must respect the essence of the right, and be necessary and proportionate.

[36] See CJEU, *Joined Cases Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, 8 April 2014; and CJEU, *Schrems v. Data Protection Commissioner*, C-362/14, 6 October 2015. See also European Data Protection Supervisor (2017, 21).

As established at the international level and repeatedly affirmed by the European Court of Human Rights, interferences with the right to privacy and personal data must be regulated by law, in line with the legality principle. The ECtHR (2021, 26) has found violations of Article 8 where domestic legislation lacked sufficient precision in specifying the extent and manner of limitations imposed by authorities[37]. The Court has also expressed concern in cases involving public order and security issues, where the legal basis for collecting personal data was excessively ambiguous or imprecise[38]. The principle of legality must, of course, extend to the realm of digital patrolling: the authority and powers of implementing bodies should be clearly, predictably, and accessibly delineated by legislation, with robust safeguards in place to prevent potential misuse by law enforcement authorities. Reflecting this requirement, the ECtHR has stipulated that legislation governing data processing should unambiguously specify the authorities responsible for data collection and retention, the types of data involved, and the categories of individuals subject to surveillance (see Brouwer 2011). Yet, as discussed, the realities on the ground in Greece and Spain indicate a significant departure from these established standards. However, the recent engagement of the ECtHR in cases concerning the right to privacy vis-à-vis intelligence services marks a promising development. Although a thorough examination of the Court's reasoning exceeds the scope of this discussion, this evolving case law could hold relevance for militarized zones and *no-go* zones in border areas, potentially expanding human rights protections and applying proportionality and necessity standards along these blurred legal regimes[39].

Beyond the CFR and the ECHR, privacy and data protection rights are also enshrined in a dense network of secondary legislation. Notably, concerning data processing activities, it is essential to mention the General Data Protection Regulation (GDPR) 2016/679 and the EU Law Enforcement Directive on protecting personal data processed for the purpose of criminal law enforcement (Directive 2016/680)[40].

The GDPR is today considered one of the most advanced data protection frameworks in the world. It specifically covers all automated personal data processing within the European Economic Area as well as other methods that are

[37] See ECtHR, *Dimitrov-Kazakov v. Bulgaria*, Application no. 11379/03, 10 February 2011, § 70, and ECtHR, *Shimovolos v. Russia*, Application no. 30194/09, 21 June 2011, § 33.

[38] See ECtHR, *Catt v. United Kingdom*, Application no. 43514/15, 24 January 2019, § 105.

[39] See ECtHR, *Centrum för Rättvisa v. Sweden*, Application no. 35252/08, 19 June 2018 and ECtHR, *Big Brother Watch and Others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.

[40] Regulation no. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 27 April 2016 and Directive no. 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive), 27 April 2016.

part of filing systems (European Union Agency for Fundamental Rights 2020, 58). However, it does not apply to data processing activities related to national security, which means it largely fails to protect people on the move, undocumented individuals, and non-EU citizens in border areas[41]. This creates a profound disparity between the level of protection guaranteed within the EU and at its external borders[42].

The Law Enforcement Directive, on the other hand, provides specific safeguards for how law enforcement authorities should apply the main data protection principles outlined by the GDPR. This Directive is particularly relevant with regard to the lawfulness, fairness, and transparency of personal data processing. Recital 26 clarifies that this obligation does not prevent law enforcement authorities from conducting activities such as criminal investigations or surveillance, but these actions must be legally regulated and constitute necessary and proportionate means in a democratic society, considering the legitimate interests of the individuals concerned.

The European Court of Human Rights (2021) has further refined its stance on data protection, elaborating three crucial tests for evaluating data-related activities: lawfulness, necessity[43], and the pursuit of a legitimate aim. These principles must always be adhered to in data processing. The ECtHR has also emphasized the importance of transparency in data processing, though this requirement becomes less stringent when national security interests are involved[44].

Under the GDPR, Article 35 mandates a Data Protection Impact Assessment (DPIA) for data processing activities that may pose a high risk to the rights and freedoms of the individuals involved. This requirement reflects a broader trend towards incorporating risk-based assessments into technological regulations, aiming for a more protective approach. However, the specificities of conducting DPIAs under the GDPR are still hotly debated within academia and beyond, with the scope of these assessments remaining largely vague (Quinn and Malgieri 2021, 1602).

In close connection with the concept of risks posed to individual rights, the notion of sensitive data is also evolving rapidly, both *de facto* and *de jure*. Sensi-

[41] Without delving into the specifics, the Entry/Exit System Regulation, referenced in chapter 1, should be recalled. In Recital 36, it stipulates that the EES Regulation is to be regarded as *lex specialis* in relation to the GDPR. Consequently, in the event of any conflict, the data protection provisions are not applicable. This relationship between the regulations is particularly revealing of the actual priorities that are intended to be safeguarded.

[42] At the national level, a notable development occurred in 2016, when the United Kingdom enacted data protection legislation that applied to every individual within its jurisdiction. This legislation, therefore, also potentially covered migrant people at the external borders.

[43] According to the ECtHR, to be considered necessary, an interference must happen in light of a «genuine, objective, and sufficiently important need». See ECtHR, *Handyside v. United Kingdom*, Application no. 5493/72, 7 December 1976, § 48 and ECtHR, *Sunday Times v. United Kingdom*, Application no. 13166/87, 26 November 1991, § 62.

[44] See ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, 6 June 2009; and ECtHR, *Dalea v. France (dec.)*, Application no. 964/07, 2 February 2010.

tive data, which includes different types of information that, if processed, could pose significant dangers to individuals, is expected to trigger stronger guarantees and a *sui generis* protection. The GDPR explicitly addresses sensitive data, with norms aimed at preventing unlawful and arbitrary discrimination against vulnerable groups, safeguarding human dignity, physical integrity, and the presumption of innocence (Quinn and Malgieri 2021). As mentioned, Article 9, paragraph 1 of the GDPR, lists categories of sensitive data, including biometric data and information revealing ethnic or racial origin and religious beliefs. The ECtHR has consistently recognized both data revealing racial and ethnic origin and biometric data – including fingerprints[45], palm prints[46], and voice samples[47] – as sensitive. As discussed, while these types of data could technically be collected by drones and other surveillance technologies, transparency in these practices is often lacking when it comes to digital patrolling.

Two main approaches to identifying sensitive data have emerged in the literature: the contextual approach and the purposeful approach. The contextual approach assesses whether data is sensitive based on the background of its collection or processing, while the purposeful approach considers the intentions behind data use. In practice, these approaches often blend into a hybrid model (Quinn and Malgieri 2021). The contextual approach is particularly useful in adapting to technological changes, as it is less restrictive than the purposeful approach. The purposeful approach allows for a more nuanced assessment of data sensitivity based on actual processing practices, rather than assuming sensitivity *a priori*. However, identifying the intentions behind data collection practices, especially in the complex intersections between migration and security policies, remains a significant challenge. Anyway, this ongoing debate is compelling and resonates with the importance of context in digital patrolling, coupled with the difficulties in discerning the multiple purposes behind data collection at external borders.

Additionally, both the GDPR (Article 22) and the Law Enforcement Directive (Article 11) generally prohibit automated decision-making, defined as de-

[45] See ECtHR, *McVeigh, O'Neill and Evans v. United Kingdom*, Applications nos. 8022/77, 8025/77 and 8027/77, 18 March 1981; ECtHR, *Kinnunen v. Finland*, Application no. 24950/94, 15 May 1996; ECtHR, *S. and Marper v. United Kingdom*, Application no. 30562/04 and 30566/04, 4 December 2008; ECtHR, *Dimitrov-Kazakov v. Bulgaria*, Application no. 11379/03, 10 February 2011; ECtHR, *M.K. v. France*, Application no. 19522/09, 18 April 2013; ECtHR, *Suprunenko v. Russia*, Application no. 8630/11, 19 June 2018; ECtHR, *Gaughran v. United Kingdom*, Application no. 45245/15, 13 February 2020; ECtHR, *P.N. v. Germany*, Application no. 74440/17, 11 June 2020; and ECtHR, *Willems v. Netherlands*, Application no. 57294/16, 9 November 2021.

[46] ECtHR, *P.N. v. Germany*, Application no. 74440/17, 11 June 2020.

[47] ECtHR, *P.G. and J.H. v. United Kingdom*, Application no. 44787/98, 25 September 2001; ECtHR, *Allan v. United Kingdom*, Application no. 48539/99, 5 November 2002; ECtHR, *Doerga v. Netherlands*, Application no. 50210/99, 27 April 2004; ECtHR, *Vetter v. France*, Application no. 59842/00, 31 May 2005; ECtHR, *Wisse v. France*, Application no 71611/01, 20 December 2005.

cisions made through automated processing, including profiling, that produce legal effects or significantly affect individuals (see Lagioia, Sartor, and Simoncini 2021). However, digital patrolling systems often result in risk calculations and flags or alerts that influence policing actions: while not being 'decisions' *stricto sensu*, they can have major consequences. These 'semi-decisions' do not fall under the prohibition of automated decision-making and are almost impossible for individuals to contest in a court or other *fora*[48]. This situation appears in contrast with Article 47 of the CFR of the EU and Article 13 of the ECHR, from which it can be derived that a victim of human rights violations caused by the deployment of an AI system by a public or private body should always have access to a national authority for redress.

Other important principles relevant to this analysis, partially discussed in chapters 2 and 3, are found in the Data Protection Directive 95/46 and the Framework Decision 2008/977/JHA on the protection of personal data processed in the context of police and judicial cooperation in criminal matters[49]. Key is here the purpose limitation principle, which should align with the data minimization principle, meaning that personal data processing should not exceed what is strictly necessary. The ECtHR has repeatedly scrutinized whether data processing activities were relevant or excessive in relation to their purposes, stressing the importance of minimizing data quantities and limiting collection purposes to what is deemed necessary[50].

The principles enshrined in Article 6(1)(b) of Directive 95/46 establish that personal data must be collected for specific, explicit, and legitimate purposes and should not be further processed in ways that are incompatible with those purposes. Additionally, data should not be retained longer than necessary for its intended purpose, and individuals involved in data processing must be informed beforehand that their data is being stored, as reaffirmed by the ECtHR[51]. This implies the prohibition of collecting personal data for unspecified or unknown

[48] For a deeper analysis of the access to justice on AI issues, see European Union Agency for Fundamental Rights (2020).

[49] Directive no. 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

[50] On the minimization of data quantities, see ECtHR, *L.L. v. France*, Application no. 7509/02, 11 April 2006, §§ 45-46; ECtHR, *Vicent Del Campo v. Spain*, Application no. 25527/13, 6 November 2018, § 51; ECtHR, *Khadija Ismayilova v. Azerbaijan*, Applications nos. 65286/13 and 57270/14, 10 January 2019, § 147; ECtHR, *Kruglov and Others v. Russia*, Applications nos. 11264/04 and 15 others, 4 February 2020, § 132. On the limitation of collection purposes, see for instance ECtHR, *Karabeyoglu v. Turkey*, Application no. 30083/10, 7 June 2016 and ECtHR, *K.H. and Others v. Slovakia*, Application no. 32881/04, 28 April 2009. See ECtHR, *Leander v. Sweden*, Application no. 9248/81, 26 March 1987; ECtHR, *Z. v. Finland*, Application no. 9/1996/627/811, 25 February 1997; and ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, 6 June 2009.

[51] See ECtHR, *Leander v. Sweden*, Application no. 9248/81, 26 March 1987; ECtHR, *Z. v. Finland*, Application no. 9/1996/627/811, 25 February 1997; and ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, 6 June 2009.

purposes. However, these standards are rarely met in the context of drone surveillance or other forms of remote and digitalized patrolling, where the purposes of data collection are often vague, and individuals remain uninformed about the extent of the data practices they are subjected to. The case studies have in fact revealed a concerning trend in digital patrolling that contradicts these principles, favouring the diffusion of multi-purpose frameworks, operations, and technologies over strict adherence to specified purposes.

The legal landscape surrounding digital patrolling activities is further complicated by the challenges of categorizing similar data collection within existing legal frameworks. Traditional distinctions in data protection, such as those between data collected for administrative, informational, or statistical purposes, are in fact extremely blurred in this context (Brouwer 2011).

Article 7 of Directive 95/46 also stipulates that all data processing activities must be legitimate, which means that they must be necessary for performing a task in the public interest or as part of a public law duty imposed on the agency responsible for the processing[52]. In an Opinion, the Article 29 Data Protection Working Party (2015, 12), an advisory body on data protection replaced in 2018 by the European Data Protection Board (EDPB), noted that these provisions could serve as the legal basis for 'security-related uses' also in border areas. It could in fact be argued that data are processed in order to fulfil legal obligations incumbent on border authorities. However, the Working Party stressed that the use of technologies like drones must be strictly necessary and proportionate, emphasizing the need to limit the 'chilling effect' on civil liberties and rights[53]. This is particularly important given the rapid pace of technological innovation, which often outstrips the capacity of European regulations to remain relevant and effective[54].

The Opinion also highlighted concerns about the large-scale integration of drones and sensor technologies in European airspace, identifying emerging risks to data protection and fundamental rights more broadly (Article 29 Data Protection Working Party 2015, 3). One significant risk is the potential for 'function creep', where data initially collected for one reason is used for entirely different,

[52] According to Article 7 of the Directive, to be regarded as legitimate, data processing must: be carried out after freely given, specific, and informed consent is obtained; be necessary for the performance of a contract to which the data subject is a party; be necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; be necessary in order to protect the vital interests of the data subject; and be necessary for the purposes of a legitimate interest.

[53] See chapter 1.

[54] In Europe, legislation on the use of drones mainly derives from the Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems and the Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft. Issues related to the use of drones are also addressed by the Frontex Regulation, which at Article 7 lays the basis for the Agency to buy the necessary technical assets and to collect and use the information acquired through drones and satellite.

and often incompatible, purposes. The Opinion also acknowledged that drone-based data processing is peculiar, marked by reduced transparency and increased privacy intrusion compared to other data collection methods, making it difficult to fairly balance the rights and interests involved. The covert nature of drone surveillance means in fact that data subjects are often unaware that their data is being processed, or for what purpose, leading to major intrusions into their privacy and personal lives. According to the Working Party, this risk is particularly acute when drones are operated by law enforcement agencies, as these activities could violate fundamental rights if they go beyond the limitations set by Article 52(1) of the Charter of Fundamental Rights and Article 8(2) of the ECHR. In fact, the Opinion stresses that law enforcement authorities do not always operate drones in accordance with a valid legal basis for personal data processing activities and concludes that the use of drones «should be restricted to cases where the processing is necessary in order to protect the vital interests of the data subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed» (Article 29 Data Protection Working Party 2015, 11).

On untargeted collection, retention, and use of data and personal data as part of border patrolling and border control procedures, the ECtHR's ruling in *S. and Marper v. the UK* (2008) is particularly relevant[55]. The Court found a violation of Article 8 of the ECHR in the UK's indefinite retention of personal data, such as fingerprints and DNA samples, of individuals who were found innocent at the end of a criminal proceeding. The Court expressed concern over the stigmatization caused by laws that allowed the police to keep such data. It emphasized the need to balance the utility of AI-assisted surveillance for crime prevention with the risks of stigmatization and privacy infringements (Murray 2020, 159). The Court concluded that States using digital identity platforms and other data collection systems must not turn them into tools of digital surveillance, especially when they affect particularly vulnerable populations (Beduschi 2019; Hu 2017).

In *S. and Marper v. the UK*, the Court also acknowledged the challenges posed by technological advancements to data protection, urging States to «strike the right balance» between protecting fundamental rights and embracing innovation[56]. This interpretation of Article 8 suggests that indiscriminate collection, retention, and processing of personal data in border monitoring activities should be excluded (Kuşkonmaz 2021, 217). Following this reasoning, it can be argued that being present in a border-crossing area should not automatically trigger criminal suspicion, as this approach would encourage discrimination, stigmatization, and criminalization[57]. This view also aligns with the CJEU's

[55] ECtHR, *S. and Marper v. United Kingdom*, Application no. 30562/04 and 30566/04, 4 December 2008.

[56] ECtHR, *S. and Marper v. United Kingdom*, Application no. 30562/04 and 30566/04, 4 December 2008, § 47.

[57] On the criminalisation of migrant populations through borders and databases, see Nina Amelung (2021).

stance that data-related activities cannot involve massive and indiscriminate data retention[58]. Conversely, a more restrictive interpretation could allow for broader margins of appreciation in border surveillance, giving Member States more leeway in controlling entry into their territory[59]. Although many scholars argue that the ECtHR jurisprudence leans towards outlawing mass and untargeted data regimes, it thus remains unclear whether this development will apply to surveillance practices in pre-frontier areas.

Despite the challenges and current shortcomings, some promising developments could lead to more positive outcomes in the future. Two areas of encouraging progress stand out: the increasing focus on human rights impact assessments for new technologies and the growing calls to adhere to the principles of purpose limitation, data minimization, proportionality, necessity, and lawfulness. While courts and other legal bodies may face difficulties in directly addressing cases related to digital patrolling, they could play a more significant role in ensuring broader compliance. The effective implementation of impact assessments and the adherence to these principles are in fact still far from satisfactory. The rights of data subjects are thus at risk of being rendered ineffective, with significant implications for the rule of law in border contexts (Finn and Wright 2012; Kuman 2020; Marin and Krajčíková 2016).

To conclude, the digitalisation of patrolling has largely led to the indiscriminate collection and processing of data, including personal and sensitive data. Evidence from Greece and Spain suggests that border monitoring activities are at risk of evolving into mass or 'bulk' surveillance. Moreover, surveillance practices underlined by risk analysis and suspicion criteria, which aim to link individuals approaching the border with potential security threats, frequently target third-country nationals. As argued by the Office of the United Nations High Commissioner for Human Rights (OHCHR 2014, para. 25), such activities can thus be deemed arbitrary, even when they serve a legitimate aim or are conducted on the basis of a legal regime. This often results in privacy violations, as well as discriminatory, stigmatizing, and criminalizing behaviours at external borders (see PICUM 2020).

4.6. Moving forward: data rights between interoperability and AI

Before concluding the discussion on privacy and data protection, it is crucial to touch upon two areas currently at the forefront of debates and poised to become increasingly significant: the growing interoperability among EU IT systems and the regulation of Artificial Intelligence systems.

[58] See CJEU, *Joined Cases Tele2 Sverige AB and Watson*, C-203/15 and C-698/15, 21 December 2016.

[59] A similar reasoning was advanced by the Court in earlier cases: ECtHR, *Leander v. Sweden*, Application no. 9248/81, 26 March 1987, § 59; and ECtHR, *Dalea v. France*, Application no. 54/1996/773/974, 19 February 1998.

Considerations on the increasing role of interoperability between EU large-scale databases might seem peripheral to digital patrolling. However, recent developments clearly indicate a trend towards greater integration of patrolling technologies and data collection systems at the external borders, making a brief exploration of interoperability timely.

The interoperability framework, which aims to facilitate identity checks of non-EU nationals, is regulated by Regulation 2019/817 on information systems in migration and border control and by Regulation 2019/818 on police and judicial cooperation, asylum, and migration[60]. This framework allows national authorities to cross-check information on individuals across various EU databases, including VIS, SIS II, EURODAC (briefly introduced in chapter 1), and the European Criminal Records Information System-Third Country Nationals (ECRIS-TCN)[61], which collects information on criminal convictions of non-EU citizens (see Brouwer 2020).

The main concerns surrounding the growing interoperability among different EU information systems, especially within the management of EU-Lisa, revolve around the semi-automated decisions triggered by 'risk flags', the overall inconsistency of interoperability with data protection standard[62], and potentially discriminatory outcomes based on nationality or ethnic grounds (Giannakou 2021). According to Evelien Brouwer (2020, 92), the non-discrimination principle and the essence of data protection provisions have been compromised for non-EU citizens whose data is collected through these interoperable databases. Moreover, the results of cross-database research are often considered influenced by 'automated digital bias', *i.e.* the tendency of the human operators to trust alerts and other semi-decisions without questioning the suggested outcomes. Taken together, these circumstances could lead to further erosion of safeguards for vulnerable groups of third-country nationals.

The next phase of the interoperability process is being pursued through the «enhanced interoperability paradigm» (European Commission 2016; see also Hanke and Vitiello 2019). This initiative aims to improve existing databases while closing information gaps, *de facto* blurring regulatory boundaries among different branches of EU policies, such as the Common Security and Defence Policy (CSDP) and the Area of Freedom, Security and Justice (AFSJ). The initiative also expands the scope of different databases for law enforcement and border management purposes.

[60] Regulation no. 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa, 20 May 2019, and Regulation no. 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, 20 May 2019.

[61] Regulation 2019/816, adopted in April 2019.

[62] It is often argued that the Regulations on interoperability do not provide any specific protection for the processing of biometric templates – *i.e.* digital representations of biometric samples – stored in the sBMS. On the issue, see among others Cristina Blasi Casagran (2021, 450).

Practically, large-scale European databases are now merged and cross-checked thanks to four new components: the European Search Portal (ESP), the Shared Biometric Matching Service (sBMS), the Multiple-Identity Detector (MID), and the Common Identity Repository (CIR). The ESP enables users to search multiple information systems at the same time, the sBMS allows them to compare biometric data, and the MID helps in detecting multiple identities connected to the same biometric data. The CIR, storing biographical and biometric data, is expected to significantly impact digital patrolling operations by requiring the collection and storage of biometric data, such as fingerprints and facial images, of any person crossing the EU's external borders[63]. This direct and indiscriminate integration of biometric data in border control activities suggests an even more explicit merging of border surveillance practices and data collection activities targeting people on the move. This process warrants close attention, as future developments here are likely to have significant long-term consequences on the digitalisation of patrols.

Moreover, scholars and human rights organizations have often argued that interoperability rarely meets the proportionality and necessity requirements, nor the provisions on purpose limitation, fairness, and transparency. They conclude that general considerations on public security should not suffice to limit fundamental rights related to privacy to this extent (Blasi Casagran 2021, 443; Statewatch and PICUM 2019). The New Pact on Migration and Asylum also emphasizes enhanced interoperability (European Commission 2020b), but leaves little room for respecting principles such as proportionality, data minimization, and purpose limitation. This raises further doubts about whether it should truly be considered a «fresh restart», as suggested by President Ursula von der Leyen (European Commission 2020a).

These considerations are particularly relevant in light of the ongoing debate around the Artificial Intelligence Act Proposal, presented by the European Commission on 21 April 2021 (European Commission 2020c). For the purposes of this analysis, suffice it to mention that the Proposal adopts a risk-based approach to AI regulation, aiming to distinguish between different kinds of AI systems[64]. The regulatory framework defines four levels of risk, corresponding to precise requirements and obligations: minimal or no risk, limited risk, high risk, and unacceptable risk.

[63] This development aligns with the introduction of two types of biometric identifiers – four fingerprints and a facial image – under the Entry/Exit Regulation. The Regulation has provided for the use of facial recognition technology for verification purposes at the border. On the issue, read Niovi Vavoula (2021, 475).

[64] In particular, Annex I of the Proposal distinguishes between: (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.

In this classification, AI systems applied in migration, asylum, and border control are considered high-risk technologies (Article 60). The discussions surrounding the list of high-risk AI systems have been marked by intense lobbying and contentious negotiations. Critics argue that these discussions are hindered by a lack of attention to the specific contexts in which AI systems are deployed, particularly in sensitive and liminal areas like border zones. Scholars have pointed out that the distinction between AI systems considered 'unacceptable risk' (and thus banned, such as predictive policing in criminal justice) and those deemed 'high risk' (allowed under strict safeguards) is not based on clear, objective criteria but rather on political compromises and arbitrary considerations (Edwards 2022). Despite these criticisms, the identification of high-risk technologies does introduce some (limited) accountability measures, such as the obligation to inform individuals affected by high-risk AI systems and the introduction of specific registration duties for public authorities. However, these measures do not result in corresponding individual rights, such as mechanisms for complaint or redress against the use of AI by public authorities, that are not mentioned by the Proposal (EDRI et al. 2021; EDRI 2022). This significantly lowers the scope of the protection thus afforded.

Given the rapid development and deployment of new AI systems, especially in the surveillance domain, several civil society organizations are advocating for a more 'future-proof' approach to the categorisation of risks. They argue that the current procedures for updating risk lists are too slow and inflexible to be able to keep pace with technological innovation (see EDRI et al. 2021). On a more positive note, the draft report published in April 2022 by the European Parliament's Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs has been praised for shifting towards a more people-centred approach to risk-based regulation, also making the update process more participatory, ensuring greater involvement from civil society (European Parliament 2021).

However, at the time of writing, debates on the AI Act continue to grapple with unresolved issues, particularly the harmful use of AI in migration and asylum contexts. Despite evidence that AI systems can contribute to discriminatory practices at and before borders, the draft fails to address these concerns adequately (Bircan and Korkmaz 2021; EDRI 2022). In support of these arguments, a significant concern is the exclusion of large-scale EU IT systems from the AI Proposal, as specified in Article 83(1). This exclusion raises serious human rights concerns, especially within the interoperability framework.

Although the Proposal frequently references fundamental rights as a criterion for assessing AI uses, it does not mandate comprehensive *ex-ante* fundamental rights-based impact assessments. This gap means there are no robust safeguards integrated by design into the development of AI systems. While certification for 'essential requirements' is required for high-risk systems, many civil society organizations, human rights agencies, and also Member States argue that a more comprehensive assessment should be mandatory to ensure accountability for AI-related harm (EDRI et al. 2022; European Union Agency for Fundamental Rights 2020).

AI systems that handle biometric data require special attention. At this stage, the Proposal classifies these systems as high-risk when used for identifying and categorizing individuals in contexts such as migration, asylum, border control, law enforcement, and emotion recognition. The 2020 European Commission White Paper on Artificial Intelligence allows the use of AI for remote biometric identification if the operation is «duly justified, proportionate and subject to adequate safeguards» (European Commission 2020e, 20). Despite ongoing discussions, the use of remote biometric identification systems is not yet prohibited under the Proposal, although there are indications that the European Parliament may advocate for banning such systems in publicly accessible spaces (EDRI 2022). However, even if such a ban were implemented, it would likely not extend to militarized areas like the Evros region or the enclaves of Ceuta and Melilla.

Moreover, the deployment of AI systems in border areas raises specific concerns about public transparency. The 'black box' problem, which refers to the difficulty of understanding how AI systems generate their outputs, is particularly troubling when it involves risk-based alerts used in surveillance systems like EUROSUR or the SIVE[65].

In conclusion, while the EU's efforts to regulate AI «assert and reinvent its artificial intelligence as anchored in the checks and balances of the rule of law» (Hildebrandt 2020), many questions about the use of digital patrolling systems remain unresolved. These legal provisions, in fact, do not provide sufficient protection for individuals in border areas, where the risks of fundamental rights violations are well known. Once again, digital patrolling – straddling the line between border control and migration management – seems to evade the most protective legislative and jurisprudential developments, potentially sidelining also the key principles enshrined by the European AI framework such as transparency, non-discrimination, and fairness (European Commission 2020d).

4.7. The right to non-discrimination: differentiated treatment and protected grounds

After examining human dignity, rights related to access to international protection, and the contentious issues surrounding privacy and data protection, this section explores another crucial human rights concern in the context of digital patrolling: the right to non-discrimination.

Discrimination is in fact a central issue in the realm of remote surveillance and digitalized patrolling, as these technologies inherently involve the categorization, filtering, and classification of human mobility. As previously discussed, the primary function of smart borders is to discriminate in the etymological sense of the term – differentiating between those who may pass and those who may not. However, as noted by Tendayi Achiume, UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, modern borders often discriminate in a normatively preju-

[65] For a critical perspective on the 'black box' phenomenon, see Frank Pasquale (2015).

dicial way. This form of discrimination allocates fundamental human rights differently based on race, gender, class, national origin, sexual orientation, and disability status, among other factors (Achiume 2021, 333). Thus, it is imperative to critically assess how the digitalisation of border patrols might exacerbate discrimination on various grounds, potentially leading to differential compliance with fundamental rights.

Internationally, the right to freedom from discrimination and the principle of equality are enshrined in a vast network of legal norms, deeply embedded in the international legal order. These rights are in fact protected by several key international instruments, including the UDHR (Articles 7 and 10), the International Covenant on Economic, Social and Cultural Rights (ICESCR, Articles 2 and 10), the ICCPR (Articles 4, 24, and 26), the Convention on the Elimination of Racial Discrimination (CERD), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Convention on the Rights of Persons with Disabilities (CRPD, Articles 3 and 5), the United Nations Convention on the Rights of the Child (CRC, Article 2), and the Refugee Convention (Article 3). These provisions prohibit both direct and indirect discrimination based on various grounds, including race, sex, religion, political beliefs, and national or social origin. Indirect discrimination occurs when ostensibly neutral policies or practices disproportionately affect certain individuals or groups, leading to less favourable treatment[66]. As discussed earlier, the motif of neutrality can often mask exclusionary practices and perpetuate power imbalances, making it a crucial theoretical juncture in the study of digital patrolling. It is in fact plausible that digital patrolling technologies may produce discriminatory outcomes related to protected characteristics, such as race and gender (Molnar 2021).

The 2021 report by the Human Rights Council on racial and xenophobic discrimination in the context of digital technologies in border and immigration enforcement is particularly insightful on this issue (Human Rights Council 2021a)[67]. The report highlights the lack of a cohesive global governance

[66] The Committee on the Elimination of Racial Discrimination (2008, para. 10), interpreting the Convention, provided a useful definition of forms of indirect discrimination, finding that «indirect – or *de facto* – discrimination occurs where an apparently neutral provision, criterion or practice would put persons of a particular racial, ethnic or national origin at a disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary».

[67] See also chapter 1. Among the issues addressed, the Report proposes a detailed examination of how borders enforcement technologies may facilitate or exacerbate racial discrimination. It highlights the role of online platforms, particularly social media, which can be a breeding ground for discrimination and xenophobic hatred; it scrutinises racial profiling systems linked to the deployment of new technological tools and AI in security, border control, and social services as aggravating forms of racism, racial discrimination, and xenophobia; it discusses the implications of mandatory biometric data collection and identification systems, which are believed to result in direct and indirect discrimination based on race, ethnicity, national origin,

framework to regulate the use of automated and digital technologies in border enforcement. It thus calls for a moratorium on surveillance technologies until robust human rights safeguards are established. These safeguards should include due diligence in line with IHRL standards, independent oversight, and full transparency regarding the use of surveillance systems that could lead to racial and other forms of discrimination (Human Rights Council 2021a, para. 66). Similarly, legal scholars have argued that considerations of non-discrimination should be integrated by design and from the outset in digitalisation processes to prevent fundamental rights violations (Beduschi 2019). However, as with broader human rights assessments, the tendency is to conduct these evaluations *ex-post* often undermining their role.

In the European context, the principle of non-discrimination is well-established in EU law, enshrined in the Treaty on European Union (Article 2), the Treaty on the Functioning of the European Union (Article 10), and the Charter of Fundamental Rights (Articles 20 and 21, which address equality before the law and non-discrimination). Additionally, the ECHR prohibits discrimination in Article 14, while Protocol 12 (Article 1) provides a general prohibition on discrimination, not limited to the rights protected by the Convention itself. Furthermore, the Schengen Border Code specifically requires border guards to perform their duties without discrimination based on gender, race, ethnic origin, religion, belief, disability, age, or sexuality[68].

As emerged in this chapter, two main axes of discrimination emerge in the context of digital patrolling. The first involves the targeting of non-EU nationals by border surveillance systems. The European Court of Human Rights has acknowledged that the protected position of EU citizens does not justify *a priori* differential treatment of non-EU nationals (see Brouwer 2011, 156)[69]. Such targeted surveillance may be inherently discriminatory against migrant people, particularly when border surveillance is intertwined with security objectives. This approach effectively singles out a well-defined population of non-EU people on the move as a high-risk group, often accompanied by stigmatizing and punitive attitudes (see Bigo, Ewert, and Kuşkonmaz 2020; Molnar 2021, 134; Statewatch and PICUM 2019). Various organizations have criticized the bias inherent in many surveillance systems at external borders, which often operate on the

descent, and religion, notably as migrant people and asylum seekers often lack control over the personal data they provide; it examines language recognition systems, such as those used by the German Federal Office for Migration and Refugees, which analyse an applicant's spoken language sample to assess the plausibility of their claimed nationality; and finally addresses mobile data extraction and social media intelligence practices specifically targeting migrant and refugee populations. These practices are widespread in several countries, including Austria, Belgium, Denmark, Germany, Norway, and the United Kingdom.

[68] Regulation no. 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), 9 March 2016.

[69] ECtHR, *Gaygusuz v. Austria*, Application no. 17371/90, 16 September 1996; and ECtHR, *Mamatkulov and Abdurasulovic v. Turkey*, Applications nos. 46827/99 and 46951/99, 6 February 2003.

flawed assumption that migration is closely linked to criminal justice, fostering an equivalence between migration and serious transnational crimes, such as terrorism. Alarmingly, the scope of those deemed 'risky' continues to expand, increasingly encompassing migrant people in international waters or transit countries.

The second axis of discrimination relates to protected grounds under international and European law, such as ethnicity, race, gender, and religion. As discussed, it is extremely challenging to fully understand how the algorithms processing the data collected by drones or other digital patrolling systems work in practice. A notable example is the situation at the borders of Ceuta and Melilla, where overt discrimination against sub-Saharan migrant people is likely supported by the digital surveillance systems employed in the *frontera inteligente*. On a more speculative level, it can be assumed that UAV patrols may allow for the identification of a person's origin, gender, and, in the case of visible religious symbols, their beliefs. Whether this information is then used to implement discriminatory policies based on risk assessments is difficult to prove or disprove with the information publicly available.

4.8. Keeping States accountable? Sketched considerations on jurisdiction

The analysis of the digitalisation of patrolling and, more broadly, the integration of new technologies into border surveillance reveals that these developments occur within highly dense and articulated regulatory frameworks. However, these often fail to adequately address the loopholes opened up by digitalisation. This creates a serious challenge where violations of rights are difficult to establish due to the lack of clear rules governing the use of these new technologies.

At the national level, existing accountability mechanisms frequently prove ineffective, even when they involve independent authorities, a concern repeatedly raised by the EU Fundamental Rights Agency[70]. Consequently, there is an urgent need for oversight mechanisms tailored to the specific contexts in which these technologies are deployed. Such mechanisms are essential to prevent the unchecked experimental use of new technologies in border control. Here, the question of jurisdiction regarding fundamental rights is particularly relevant, as it may provide a framework for developing accountability mechanisms and a valuable angle to further develop this study. The deployment of digital patrolling systems extends in fact the scope of externalisation and outsourcing policies to extreme and otherwise unimaginable levels. This contributes to the dilution of liability, accountability, and responsibility among actors, deliberately dispersing and shifting them among third States, European agencies, and private actors. Such practices raise complex jurisdictional issues.

[70] As recalled by the EU Fundamental Rights Agency (2020, 9), States have in fact a positive obligation to put in place effective monitoring and enforcement mechanisms in order to secure people's rights and freedoms, also when it comes to regulate digitalisation processes and the deployment of Artificial Intelligence systems.

The core question – which is here left completely open – concerns whether the various functions of digital patrolling, such as situational awareness, detection, tracking, information management, and risk analysis, constitute an exercise of jurisdiction over people on the move. This issue inevitably intersects with the broader and highly complex debate on the extraterritorial exercise of jurisdiction, which extends well beyond the scope of this book.

From the perspective of IHRL, the debate on the extraterritorial application of human rights conventions is relatively recent and limited. IHRL itself is grounded in the recognition of States' legal orders and features relatively weak enforcement mechanisms. As Nehal Bhuta (2016) vividly describes, the extraterritorial application of human rights mirrors the fracture lines of the Westphalian system, suggesting that as State activities extend beyond their borders and disconnect from traditional notions of territorial and political unity, human rights law must evolve to keep pace. The challenge of extraterritoriality is fundamental to the future of human rights in this area: while an increased focus on extraterritorial obligations could lead to higher standards of protection, a conservative interpretation of the territorial scope of State's positive and negative obligations could significantly weaken IHRL norms.

To tackle this challenge, various human rights courts and treaty bodies have developed a 'factual control' test to expand the scope of territorial jurisdiction, applying it to both the control of territory and individuals (see Committee Against Torture 2008, para. 7; International Court of Justice 2004, paras 109–110; OHCHR 2004). The ECtHR has also made strides in this direction, increasingly adopting a 'functional approach' to the applicability of fundamental rights in cases involving extraterritorial policies and practices (Carrera and Cortinovis 2019). The Court's jurisprudence recognizes in fact a jurisdictional link between individuals affected by external border control measures and the State responsible for those measures, whether through *de jure* or *de facto* control over the territory where the violation occurs or over the individual affected[71].

[71] The ECtHR jurisprudence has evolved through fundamental cases that are worth mentioning. Ruling on *Loizidou v. Turkey* (Application no. 15318/1989, 23 February 1995) and on *Ilaşcu and Others v. Moldova and Russia* (Application no. 48787/99, 8 July 2004), the Court recognized the responsibility for violations carried out outside the territory of the State, according to the criterion of 'effective control of the territory' where the violation takes place. In 2004, with the judgment on *Issa v. Turkey* (Application no. 3821/1991, 16 June 2004), this test has been extended through a functional approach to the 'effective control over the person' who suffers the violation by means of operating agents of the State: the Court has indeed stated at §71 that Article 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory. Moreover, with the definition of the so-called 'Hirsi test' (ECtHR, *Hirsi Jamaa and Others v. Italy,* Application no. 27765/09, 23 February 2012), the Court referred to the continuous or exclusive control *de jure* and *de facto* as the main benchmark or criterion. According to the Court, ruling on Hirsi, even though the pullback operation took place in high sea, Italy had exercised continuous and exclusive *de jure* and *de facto* control over the applicants as they were embarked on a military boat. Similarly, in Medvedyev (ECtHR, *Medvedyev and Others v. France,* Application no.

Some scholars, such as Fernando Val Garijo (2020, 148), argue that applying this test could be sufficient to trigger jurisdiction in cases where pullback operations are supported by drones and other remote-controlled systems. However, extending this interpretation to fully cover digital patrolling remains a particularly ambitious and underexplored proposition.

Border controls that are increasingly digitalized, externalized, and privatized pose a significant concern in legal scholarship. Valsamis Mitsilegas (2015, 21) highlights the resulting issues as a critical challenge to the rule of law and human rights, emphasizing the urgent need for a paradigm shift that centres individuals – not States – in border control legislation and practice. Such a shift would be crucial to ensure that individual rights do not fade into the background, overshadowed by security considerations and other priorities.

The issue of jurisdiction, particularly its extraterritorial expansion, and its implications for digitalisation, thus remains central in the effort to strengthen an accountability framework that considers human dignity, access to international protection, privacy and data protection, and non-discrimination in the context of digital patrolling. In conclusion, the debate on jurisdiction and accountability remains open and critically important as we continue to grapple with the legal and political implications of digitalized border control.

3394/03, 29 March 2010), the Court concluded that France was exercising at least *de facto* full and effective control over a boat during an interception operation in high seas, adopting a functional approach to extraterritorial operations. Furthermore, in *Al-Skeini* and in *Jaloud* (*Al-Skeini and Others v. United Kingdom*, Application no. 55721/07, 7 July 2011; *Jaloud v. Netherlands*, Application no. 47708/08, 20 November 2014), the ECtHR adopted a more functional conceptualisation of jurisdiction, establishing that the latter emerges where the State exercises forms of public power normally to be exercised by a sovereign government – for instance, the maintenance of security – and consequently brings people under its authority and control.

Concluding remarks and pathways forward

Discussing the digitalisation of patrolling is akin to navigating the sharpest edges of sovereignty, tackling surfacing issues and patterns that extend well beyond the scope of digital patrolling itself. The urgency of exploring this field stems from the recognition that, with the partial exception of highly skilled and seasonal workers, the current legal pathways for migration and access to international protection in Europe remain profoundly unjust and inadequate. Consequently, much unfolds at these outer edges where, for many people seeking entry into Europe, the stark confrontation with the violence of external borders is an unavoidable reality. Grounded in this understanding, the study of digital border patrolling reaffirms the enduring centrality of border zones, which are imbued with profound political, social, and legal significance. Indeed, the act of patrolling not only reconfigures terrains, routes, and norms but also opens spaces for contestation and resistance.

Through the lens of patrolling, the book has aimed to chart the processes of digitalisation at the European Union's external borders, exploring how emerging technological advancements take shape on the ground and critically analysing their consequences – both potential and actual – on the rights of individuals subjected to these developments. It has also interrogated the broader trajectories of migration law within which the digitalisation of patrolling is embedded, revealing the complex interplay between technology and human rights in the borderland scape.

In addressing the first research question, which centres on the conceptualisation of digital patrolling, these pages contribute to the debate by offering an

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

analysis of the capability areas that constitute the 'smart' borderwork. The technologies and functionalities at the core of digital patrolling have been identified, categorised according to a taxonomy based on these capability areas, and simultaneously charted following their proliferation across Europe. What has emerged is a complex intertwining of new and old methods of patrolling that blends remote surveillance, externalisation strategies, AI-driven risk analysis, and pushback operations.

The book has also reconstructed the debates and logics underpinning the spread of high-tech border and migration management tools, revealing tensions between a rhetoric centred on the efficiency of surveillance through advanced technologies and a discourse framing the digitalisation of borders as a humanitarian endeavour. The second rationale, encapsulated in the «care-and-control continuum» (Pallister-Wilkins 2015) and resulting from the merger of migration and border security policies, appears increasingly tenuous when subjected to scrutiny. The practices of digital patrolling – ranging from data trawling and risk assessment criteria to the policing interventions they provoke – demonstrate clearly defined priorities, which are far from humanitarian.

Ultimately, if we assumed that saving lives in perilous situations through state-of-the-art technological innovations is one of the key objectives of border control, it would become difficult to reconcile this intent with the fact that Europe continues to enforce some of the world's deadliest borders.

The analysis of the various capability areas has also revealed that the shift towards digital patrolling is far from merely a matter of «doing the same job better and faster» (Broeders and Dijstelbloem 2016, 242). Instead, it entails profound transformations that mark a paradigm shift demanding further enquiry.

Without reducing these considerations to cost-benefit evaluations on digital patrolling, the advent of new, partially automated patrolling systems significantly alters both the modalities of border surveillance and the strategies employed by those seeking to circumvent such control. What surfaces are contradictions and tensions shaping spaces of oppression and resistance that, while colliding, remain partially obscured by technical considerations that largely bypass the rights of the people involved.

In fact, beneath the façade of legitimacy granted to border violence by cutting-edge situational awareness tools, the effects of digital patrols are as tangible and pervasive as ever for people on the move who are deemed unwelcome at Europe's borders. As discussed, the employment of deterrence mechanisms bolstered by digitally mediated and generalised surveillance reshapes the migratory routes, making these journeys even more perilous and deadly – yet still failing to prevent departures and crossing attempts. Paradoxically, despite significant investments, the effectiveness of digital patrol systems often falters, troubled by errors and breakdowns. In many instances, these failures bring a sense of relief, as the non-functioning of digital patrol tools can sometimes constitute a reprieve.

As explored, the partial invisibility of digital patrolling methods also fundamentally alters the nature of border control. The removal of these technologies from public scrutiny, coupled with the intensity of previously inconceivable surveillance, risks producing – or more accurately, is designed to produce – a 'chilling effect' that can result in the normalisation of human rights violations.

The study has also underscored the non-neutrality of digital patrolling, highlighting its structural entanglement with the socio-political contexts in which advanced surveillance technologies are deployed. This contextualisation reveals a troubling experimentalism, largely unbounded by national, European, or international law. As Claudia Aradau (2020) has observed, technological experimentation at borders becomes a «mode of governing without protocols» that exacerbates the disparity between the rights of European citizens and those afforded to people on the move at the EU's external borders.

Moreover, the geographic scope of these stringent surveillance regimes is expanding. At the same time, within such extended border zones, the 'rights cleavage' – based on categories of perceived risk and trust – is also widening. Surveillance, from the outset, takes on a punitive function, disproportionately affecting minority groups in precarious conditions. The digitisation of border patrols appears to amplify what Étienne Balibar (2002) refers to as the «heterogeneity» of borders, further intensifying their uneven effects on different individuals. In this context of growing distance and remoteness, a divisive discourse of 'us' versus 'them' easily takes root, permeating from border management into migration policies and binding the two ever more tightly (see Molnar 2022). Yet it would be misleading to think that experimentalism at the border is confined to these zones. The encroachment of highly intrusive surveillance technologies from so-called irregular migrants to asylum seekers, refugees, and even humanitarian organisations highlights the permeability of security policies across different contexts. Border technologies very rarely remain on the border. The same drones patrolling the Evros region have already been deployed in various European countries to monitor protests and demonstrations, reminding us that similar forms of unchecked surveillance raise profound questions not only about migration policies but also about the health of our democracies (EDRI 2020).

Indeed, alongside this experimentalism lies a distinct form of solutionism that can be described as «techno-solutionism» (Morozov 2013), fostering a self-perpetuating cycle. As noted earlier, the problems, errors, and shortcomings associated with advanced surveillance systems are presented primarily as technological challenges, which, it is argued, can be resolved by further increasing surveillance capabilities and deploying even more advanced systems. This approach completely fails to engage with the multifaceted nature of migration and provides a technological answer to a political (and legal) question, suggesting that dilemmas around borders can be addressed through claims of objectivity or technological neutrality. The tensions arising from drone patrols or surveillance systems like SIVE or EUROSUR are thus rarely framed in their legal, socio-political, ethical, or anthropological dimensions, which are nevertheless crucial to grasping the inherent complexity of migration and human mobility.

In line with the second research question, the book has adopted a topographical approach to examine the impact of digital patrolling by conducting a comparative study of its patterns at the EU's external borders. The result is an in-depth analysis of the phenomenon in Greece and Spain, from both legal and technological perspectives, with a particular focus on the most strategic and surveillance-prioritised border sections. The research has thus exposed how dense and often impenetrable the veil of secrecy surrounding the deployment of new technologies in border control can be. In such an opaque information environment, it becomes particularly challenging to disentangle the multi-purpose claims associated with new surveillance tools, with the constant risk of errors and misinterpretations looming large throughout the research process. Remarkably, the lack of transparency undermines public interest in the democratic oversight of surveillance technology development, leading to accountability gaps that are both hard to identify and challenging to address.[1] Nonetheless, through meticulous research involving primary and secondary sources and reference to the substantial work of various on-the-ground organisations, it has been possible to navigate (at least partially) the restrictions of militarized border areas, offering grounded hypotheses and shedding light on the 'common secrets' around digital patrolling.

The case studies have further illuminated the distinct forms of border violence that unfold in Europe's periphery, revealing how digital patrolling, far from mitigating these dynamics, is enmeshed within them. Moreover, the convergence of militarization, criminalisation, and externalisation in border governance and migration policies exacerbates the objectification and dehumanisation of non-pre-vetted travellers attempting to cross the EU's external borders. By reducing individuals to mere objects of surveillance, digital patrolling raises profound concerns about the preservation of human dignity.

This drift is mirrored by the growing tension between the standardisation of patrol practices and the increasing targeted deployment of surveillance mechanisms. As discussed, targeted surveillance fosters expansive processes of identification and categorisation, well before individuals even reach European borders. While the categorisation of people on the move – whether refugees, asylum seekers, or irregular migrants – *before* the EU's borders is inherently problematic and largely arbitrary, digital patrolling often simplifies the task by creating a binary distinction between people who are deemed trustworthy and those who are considered risky. Moreover, as the case studies from Greece and Spain have illustrated, the digitalisation of patrols fails to curb the arbitrary discretion and unpredictability that characterise border control policies. In this context, standardisation does not equate to respect for the rule of law but it functions as a mechanism that overlooks the specific individual circumstances, undermining the broader system of protection.

Accordingly, the legal frameworks in place in Greece and Spain reveal the inadequacy of current legislation to provide effective safeguards for individuals subjected to digital patrolling. Firstly, the regulatory environment is convolut-

[1] On this note, mention should be made of *CJEU, Breyer v. Commission*, Case T-158/19, 15 March 2019.

ed, riddled with grey zones, referrals to specialised agencies or references to operational regulations that are often not publicly accessible. This opacity favours the framing of migration as a border security issue. Secondly, the lack or ineffective application of impact assessments and mechanisms for redress makes it extremely difficult to challenge the consequences of digital patrolling in court. A glaring disproportionality emerges between the impact of digital patrolling on the rights of individuals and the limited avenues available for seeking justice and obtaining substantive and procedural protection. Courts, which could potentially play a crucial role, seem currently constrained by the complexities of adjudicating on digital patrolling and by a general reluctance to extend judicial scrutiny to surveillance and data regimes in security contexts, particularly in pre-frontier areas. As accountability and oversight mechanisms remain loose, harmful forms of digital patrolling are largely insulated from judicial and political contestation.

The decoupling of rights from the procedures intended to safeguard them is not simply the product of regulatory challenges in rapidly evolving techonological fields, though these difficulties are indeed real. Rather, it reflects a deliberate orientation that is taking root across various domains of migration law at both the national and supranational levels. As the debates surrounding the European Union's proposed New Pact on Migration and Asylum demonstrate, the digitalisation of borders often accompanies accelerated procedures aimed at efficiency and speed in migration management, even at the expense of the rights of the people affected. In evaluating the digitalisation of patrolling, it is clear that what the Council of Europe's Commissioner for Human Rights (2021) has identified as a «widespread unwillingness of European States to set up an adequate system of protection» is at play.

Building on all these considerations, the final section of the book has examined the implications of the digitalisation of border patrols on the rights of people on the move, across European and international legal frameworks. Specifically, this analysis has focused on the impact of digitalisation on rights related to access to protection and asylum, privacy and data protection, as well as equality and non-discrimination, thereby addressing the third and final research question. What emerges as particularly alarming is the stark contrast between the principles that should guide the digitalisation of patrols – such as proportionality, necessity, legality, and data minimization – and the strategies that underpin the digitalisation process. This discrepancy becomes particularly evident in the developments within the interoperability framework and in the attempts to regulate AI applications in migration and asylum contexts.

Concerning the increasing automation of surveillance systems, it has been shown how these technologies largely operate within a zone of legal uncertainty, where efforts to adopt a truly 'future-proof' approach to technological development fall short, struggling to balance competing interests between security and human rights. While fully automated decision-making or surveillance systems today are not integrated into the EU's borders, this research highlights that ongoing experiments are moving in that direction, raising serious concerns. Several obligations – and notably the prohibition of introducing automated decision-making as outlined in the GDPR and the Law Enforcement Directive –

risk becoming unenforceable in practice. Even now, semi-automated decisions generated by surveillance systems through mechanisms like flags and risk alerts significantly influence patrolling activities. Furthermore, the opaque nature of the data collection and processing involved makes it almost impossible to apply the legal safeguards available at both European and international levels.

Another concerning aspect of digital patrolling is its discriminatory dimension. These systems are, in fact, designed to specifically target non-EU nationals, and in doing so, they often gather sensitive data that may lead to discrimination – particularly on ethnic and religious grounds. This reinforces exclusionary practices and oppressive power dynamics, further marginalising individuals who are already forced into a liminal existence marked by unpredictability and violence and thus replicating forms of «vulnerabilisation» (Scudieri 2020, 199).

Within this context, the EU and its Member States appear overall ill-equipped to provide adequate protection, with digital patrolling largely slipping through existing legislative frameworks, even those aimed at regulating digitalisation and AI. The gap between legal norms and potential violations on the ground is widening, exacerbated by jurisdictional challenges that are unable to fully address actions increasingly dispersed across different actors and territories. Substantial European and national investments and research projects aimed at enhancing the automation of surveillance are not only accelerating the digitalisation of patrols but are also shaping the future of border and migration policies in a way that prioritises containment and exclusion.

There is, however, potential for change. This could for instance come from the integration of fundamental rights assessments prior to the deployment of new technologies at the EU's external borders, ensuring compliance with essential principles of data governance, transparency, non-discrimination, and fairness. National, supranational, and international jurisprudence may also play a role in ensuring that digital patrolling is brought under closer scrutiny. However, for this to happen, border surveillance policies must be rendered more transparent, allowing for a critical examination that could lead to their radical re-evaluation.

In conclusion, by addressing these issues, the book aims to contribute to a critical and multidimensional understanding of a process that is often framed as inevitable and neutral. That said, digital patrolling should not be demonised outright, as it holds the potential – at least in theory – to yield positive outcomes also from a fundamental rights perspective. While significant challenges would remain, the possibility of a radically different use of patrolling systems can still be imagined. However, as long as digital patrolling continues to reinforce policies focused on migration containment and pushbacks, its consequences will inevitably be severe and insidious.

Building on this, the study suggests numerous avenues for future research. It would be especially valuable to investigate these dynamics through extensive fieldwork, employing a broader range of socio-legal methodologies. Additionally, exploring whether and how constitutional law could offer a higher level of protection would delineate a significant area of inquiry. Furthermore, a comprehensive analysis of accountability mechanisms extending to agencies, third countries, and private actors involved in digital patrolling would be of great importance. This would deepen the examination along the lines of border externalisation and cooperation frameworks.

Ultimately, if borders and patrolling practices are changing – and they undoubtedly are –, approaches to the protection of the rights of people on the move must evolve accordingly. Law and policy cannot afford to continually lag behind. It is crucial to critically examine the violence inherent in bordering practices, including digital ones, to illuminate and dismantle them. At the same time, however, we must envision spaces for a more humane and rights-respecting future. In the wise words of Ruha Benjamin (2019), «remember to imagine and craft the worlds you cannot live without, just as you dismantle the ones you cannot live within».

List of cases, international legal instruments, and legislation

List of cases

CJEU, *Netherlands v. European Parliament and Council,* C-377/98, 9 October 2001

CJEU, *Joined Cases Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* C-293/12 and C-594/12, 8 April 2014

CJEU, *Schrems v. Data Protection Commissioner,* C-362/14, 6 October 2015

CJEU, *Joined Cases Tele2 Sverige AB and Watson,* C-203/15 and C-698/15, 21 December 2016

CJEU, *Breyer v. Commission,* Case T-158/19, 15 March 2019

ECtHR, *Handyside v. United Kingdom,* Application no. 5493/72, 7 December 1976

ECtHR, *McVeigh, O'Neill and Evans v. United Kingdom,* Applications nos. 8022/77, 8025/77 and 8027/77, 18 March 1981

ECtHR, *Leander v. Sweden,* Application no. 9248/81, 26 March 1987

ECtHR, *Soering v. United Kingdom,* Application no. 14038/88, 7 July 1989

ECtHR, *Sunday Times v. United Kingdom,* Application no. 13166/87, 26 November 1991

ECtHR, *Loizidou v. Turkey,* Application no. 15318/1989, 23 February 1995

ECtHR, *Kinnunen v. Finland,* Application no. 24950/94, 15 May 1996

ECtHR, *Gaygusuz v. Austria,* Application no. 17371/90, 16 September 1996

Alice Fill, École Normale Supérieure (ENS-PSL), France, alice.fill@ens.psl.eu, 0009-0004-7750-3578

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

ECtHR, *Z. v. Finland*, Application no. 9/1996/627/811, 25 February 1997

ECtHR, *Dalea v. France*, Application no. 54/1996/773/974, 19 February 1998

ECtHR, *P.G. and J.H. v. United Kingdom*, Application no. 44787/98, 25 September 2001

ECtHR, *Allan v. United Kingdom*, Application no. 48539/99, 5 November 2002

ECtHR, *Mamatkulov and Abdurasulovic v. Turkey*, Applications nos. 46827/99 and 46951/99, 6 February 2003

ECtHR, *Doerga v. Netherlands*, Application no. 50210/99, 27 April 2004

ECtHR, *Issa v. Turkey*, Application no. 3821/1991, 16 June 2004

ECtHR, *Ilaşcu and Others v. Moldova and Russia*, Application no. 48787/99, 8 July 2004

ECtHR, *Vetter v. France*, Application no. 59842/00, 31 May 2005

ECtHR, *Wisse v. France*, Application no 71611/01, 20 December 2005

ECtHR, *L.L. v. France*, Application no. 7509/02, 11 April 2006

ECtHR, *Saadi v. Italy*, Application no. 37201/06, 28 February 2008

ECtHR, *S. and Marper v. United Kingdom*, Applications nos. 30562/04 and 30566/04, 4 December 2008

ECtHR, *K.H. and Others v. Slovakia*, Application no. 32881/04, 28 April 2009

ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, 6 June 2009

ECtHR, *Dalea v. France*, Application no. 964/07, 2 February 2010

ECtHR, *Medvedyev and Others v. France*, Application no. 3394/03, 29 March 2010

ECtHR, *Dimitrov-Kazakov v. Bulgaria*, Application no. 11379/03, 10 February 2011

ECtHR, *Shimovolos v. Russia*, Application no. 30194/09, 21 June 2011

ECtHR, *Al-Skeini and Others v. United Kingdom*, Application no. 55721/07, 7 July 2011

ECtHR, *Hirsi Jamaa and Others v. Italy*, Application no. 27765/09, 23 February 2012

ECtHR, *M.K. v. France*, Application no. 19522/09, 18 April 2013

ECtHR, *Jaloud v. Netherlands*, Application no. 47708/08, 20 November 2014

ECtHR, *Karabeyoglu v. Turkey*, Application no. 30083/10, 7 June 2016

ECtHR, *Centrum för Rättvisa v. Sweden*, Application no. 35252/08, 19 June 2018

ECtHR, *Suprunenko v. Russia*, Application no. 8630/11, 19 June 2018

ECtHR, *Vicent Del Campo v. Spain*, Application no. 25527/13, 6 November 2018

ECtHR, *Khadija Ismayilova v. Azerbaijan*, Applications nos. 65286/13 and 57270/14, 10 January 2019

ECtHR, *Catt v. United Kingdom*, Application no. 43514/15, 24 January 2019

ECtHR, *Kruglov and Others v. Russia*, Applications nos. 11264/04 and 15 others, 4 February 2020

ECtHR, *Gaughran v. United Kingdom*, Application no. 45245/15, 13 February 2020

ECtHR, *N.D. and N.T. v. Spain*, Applications nos. 8675/15 and 8697/15, 13 February 2020

ECtHR, *L.A. and Others v. Greece and A.A. v. Greece*, Applications nos. 12237/20 and 12736/20, 5 March 2020 and 7 March 2020

ECtHR, *P.N. v. Germany,* Application no. 74440/17, 11 June 2020
ECtHR, *Big Brother Watch and Others v. United Kingdom,* Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021
ECtHR, *Willems v. Netherlands,* Application no. 57294/16, 9 November 2021

HRC, *Van Hulst v. Netherlands,* Communication 903/1999, UN Doc. A/60/40, Vol. II, 1 November 2004
HRC, *NK v. Netherlands,* Communication 2326/2013, UN Doc. CCPR/C/120/D/2326/2013/Rev.1, 18 July 2017

IACHR, *Escher et al. v. Brazil,* Series C No. 193, 6 July 2009

International legal instruments and other documents

UN General Assembly, *Universal Declaration of Human Rights,* 217 A (III), 10 December 1948
UN General Assembly, *Convention Relating to the Status of Refugees,* United Nations, Treaty Series, vol. 189, 28 July 1951
UN General Assembly, *International Convention on the Elimination of All Forms of Racial Discrimination,* United Nations, Treaty Series, vol. 660, 21 December 1965
UN General Assembly, *International Covenant on Economic, Social and Cultural Rights,* United Nations, Treaty Series, vol. 993, 16 December 1966
UN General Assembly, *International Covenant on Civil and Political Rights,* United Nations, Treaty Series, vol. 999, 16 December 1966
UN General Assembly, *Protocol Relating to the Status of Refugees,* United Nations, Treaty Series, vol. 606, 31 January 1967
UN General Assembly, *Convention on the Law of the Sea,* 10 December 1982 International Maritime Organization, *International Convention for the Safety of Life At Sea,* 1 November 1974
International Maritime Organization, *International Convention on Maritime Search and Rescue,* 27 April 1979
UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women,* United Nations, Treaty Series, vol. 1249, 18 December 1979
UN General Assembly, *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,* United Nations, Treaty Series, vol. 1465, 10 December 1984
UN General Assembly, *Convention on the Rights of the Child,* United Nations, Treaty Series, vol. 1577, 20 November 1989
UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families,* A/RES/45/158, 18 December 1990
UN General Assembly, *Convention on the Rights of Persons with Disabilities,* A/RES/61/106, 24 January 2007

European Union legislation

Directive no. 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995

Regulation no. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 26 October 2004 (no longer in force)

Directive no. 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications (Data Retention Directive), 15 March 2006 (no longer in force)

Regulation no. 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), 20 December 2006

Regulation no. 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), 9 July 2008

Regulation no. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 25 October 2011

Regulation no. 1168/2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 25 October 2011 (no longer in force)

Directive no. 2013/32 on common procedures for granting and withdrawing international protection (Asylum Procedures Directive), 26 June 2013

Regulation no. 603/2013 on the establishment of Eurodac for the comparison of fingerprints, 26 June 2013

Regulation no. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (Dublin Regulation), 26 June 2013

Regulation no. 1052/2013 establishing the European Border Surveillance System (Eurosur), 22 October 2013

Regulation no. 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), 9 March 2016

Directive no. 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law Enforcement Directive), 27 April 2016

Directive no. 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 27 April 2016

Regulation no. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 27 April 2016

Regulation no. 2016/1624 on the European Border and Coast Guard, 14 September 2016 (no longer in force)

Regulation no. 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, 30 November 2017

Regulation no. 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS), 12 September 2018

Regulation no. 2018/1241 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), 12 September 2018

Regulation no. 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) no. 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) no. 1077/2011, 14 November 2018

Regulation no. 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals, 28 November 2018

Regulation no. 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, 28 November 2018

Regulation no. 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, 28 November 2018

Regulation no. 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa, 20 May 2019

Regulation no. 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, 20 May 2019

Commission Implementing Regulation no. 2019/947 on the rules and procedures for the operation of unmanned aircraft, 24 May 2019

Regulation no. 2019/1896 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, 13 November 2019

National legislation

Greece

Law no. 3838/2010, On Current Provisions related to Greek Nationality and the Political Participation of Expatriates and Legally Residing Immigrants, 24 March 2010

Law no. 3917/2011, Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the obtaining or recording of sound or image at public areas and relative provisions, 21 February 2011

Law no. 4249/2014, Reorganization of Greek Police, Fire Brigade and the General Secretariat for Civil Protection, upgrade of the Services of the Ministry of Public Order and Citizen Protection and regulation of other matters concerning the Ministry of Public Order and Citizen Protection, 24 March 2014

Law no. 4332/2015, Amendment of the provisions of the Greek Nationality Code – Amendment of Law 4521/2014, 9 July 2015

Law no. 4375/2016, On the organization and operation of the Asylum Service, the Appeals Authority, the Reception and Identification Service, the establishment of the General Secretariat for Reception, the transposition into Greek legislation of the provisions of Directive 2013/32/EC, 3 April 2016

Greek Civil Airport Service, Decision D/IPA/21860/1422, 30 September 2016

Presidential Decree no. 98/2019, Organisation and structure of the Drone Service, Establishment of Procurement Directorates and History of the Hellenic Police and Unmanned Aircraft Service, 21 March 2017

Law no. 4624/2019, On the Hellenic Data Protection Authority, the implementation of Regulation 2016/679 and the transposition of Directive 2016/680, 29 August 2019

Law no. 4636/2019, On international protection and other provisions, 1 November 2019

Law no. 4650/2019, Regulations of issues of the Ministry of National Defence and other provisions, 17 December 2019

Law no. 4686/2020, Improvement of the migration legislation, amendment of Law 4636/2019, 4375/2016, 4251/2014 and other provisions, 12 May 2020

Presidential Decree no. 75/2020, Use of surveillance systems obtaining or documenting sound and pictures in public places, 10 September 2020

Law no. 4825/2021, Reform of deportation and return procedures of third country nationals, attracting investors and digital nomads, issues of residence permits and procedures for granting international protection, provisions within the competence of the Ministry of Migration and Asylum and the Ministry of Citizen Protection and other emergency provisions, 4 September 2021

Morocco

Law no. 02/03, Entry and stay of foreigners into the Kingdom of Morocco, irregular emigration and immigration, 20 November 2003

Spain

Organic Law no. 15/1999, On Protection of Personal Data, 13 December 1999

Organic Law no. 1/1982, On the Civil Protection of the Right to Honour, Personal Privacy and Self-Image, 5 May 1982

Organic Law no. 4/1997, Regulating the Use of Video Cameras by Security Forces and Units in Public Spaces, 4 August 1997

Organic Law no. 4/2000, On Rights and Freedoms of Foreigners in Spain and their social integration, 11 January

Law no. 18/2014, On the approval of urgent measures for growth, competitiveness and efficiency, 15 October 2014

Law no. 9/2017, Contracts of the Public Sector, 8 November 2017

Royal Decree no. 1036/2017, Governing the civil use of remotely piloted aircraft, 15 December 2017

Organic Law no. 3/2018, On Protection of Personal Data and Guarantee of Digital Rights, 5 December 201

References

Achiume, E. Tendayi. 2021. 'Digital Racial Borders'. *AJIL Unbound* 115: 333–38. https://doi.org/10.1017/aju.2021.52

Agier, Michel. 2008. *Gérer Les Indésirables: Des Camps de Réfugiés Au Gouvernement Humanitaire*. Paris: Flammarion (Bibliothèque Des Savoirs).

Aizeki, Mizue, Geoffrey Boyce, Todd Miller, Joseph Nevins, and Miriam Ticktin. 2021. 'Smart Borders or a Humane World?'. Immigrant Defense Project's Surveillance, Tech & Immigration Policing Project, and the Transnational Institute.

Akkerman, Mark. 2021. 'Border Wars. The Arms Players Frofiting from Europe's Refugee Crisis'. In *The Militarization of the European Union*, edited by Kees van der Pijl. Newcastle: Cambridge Scholars Publishing. https://doi.org/10.13140/RG.2.2.23015.47527

Alarm Phone Sahara. 2021. 'Civilian Patrol in the Desert beyond a Snag'. https://alarmephonesahara.info/en/blog/posts/civilian-patrol-in-the-desert-beyond-a-snag. 10 June 2021 (2024-09-01).

Alarm Phone, Borderline Europe, Mediterranea Saving Humans, and Sea-Watch. 2020. 'Remote Control: The EU-Libya Collaboration in Mass Interceptions of Migrants in the Central Mediterranean'.

Alscher, Stefan. 2005. 'Knocking at the Doors of "Fortress Europe": Migration and Border Control in Southern Spain and Eastern Poland'. *San Diego: Center for Comparative Immigration Studies*.

Amelung, Nina, Rafaela Granja, and Helena Machado. 2021. *Modes of Bio-Bordering The Hidden (Dis)Integration of Europe*. Singapore: Palgrave Pivot. https://doi.org/10.1007/978-981-15-8183-0

Amelung, Nina. 2021. '"Crimmigration Control" across Borders: The Convergence of Migration and Crime Control through Transnational Biometric Databases'. *Historical Social Research* 46 (3). https://doi.org/10.12759/hsr.46.2021.3.151-177

Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. 'Questioning Security Devices: Performativity, Resistance, Politics'. *Security Dialogue* 46 (4): 293–306. https://doi.org/10.1177/0967010615586964

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

Amnesty International Spain. 2016. 'En Tierra de Nadie. La Situación de Las Personas Refugiadas y Migrantes En Ceuta y Melilla'.

Amnesty International. 2021. 'Greece: Freedom of Assembly at Risk and Unlawful Use of Force in the Era of Covid-19'.

Amoore, Louise. 2006. 'Biometric Borders: Governing Mobilities in the War on Terror'. *Political Geography* 25 (3): 336–51. https://doi.org/10.1016/j.polgeo.2006.02.001

Amoore, Louise. 2013. *The Politics of Possibility: Risk and Security beyond Probability*. Durham: Duke University Press.

Amoore, Louise. 2021. 'The Deep Border'. *Political Geography,* 109. https://doi.org/10.1016/j.polgeo.2021.102547

Amoore, Louise. 2023. 'Machine Learning Political Orders'. *Review of International Studies* 49 (1): 20–36. https://doi.org/10.1017/S0260210522000031

Andersson, Ruben. 2014. 'Hunter and Prey: Patrolling Clandestine Migration in the Euro-African Borderlands'. *Anthropological Quarterly* 87 (1): 119–49. https://doi.org/10.1353/anq.2014.0002

Andres, Jacqueline. 2021. 'EU Border Regime. Profiteering from Dehumanisation and Mythologised Technologies'. Brussels: The Left in the European Parliament.

Aradau, Claudia, and Lucrezia Canzutti. 2022. 'Asylum, Borders, and the Politics of Violence: From Suspicion to Cruelty'. *Global Studies Quarterly* 2 (2).

Aradau, Claudia. 2020. 'Experimentality, Surplus Data and the Politics of Debilitation in Borderzones'. *Geopolitics* 27(1)*:* 1–21. https://doi.org/10.1080/14650045.2020.1853103

Article 29 Data Protection Working Party. 2015. 'Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones - 01673/15/EN WP 231'.

Asociación Pro Derechos Humanos de Andalucía. 2021. 'Derechos Humanos En La Frontera Sur 2021'.

Asociación Pro Derechos Humanos de Andalucía. 2022. 'Balance Migratorio Frontera Sur 2021'.

Asylum Information Database. 2021. 'Country Report: Spain - 2020 Update'. https://asylumineurope.org/wp-content/uploads/2021/03/AIDA-ES_2020update.pdf (2024-09-01).

Bachiller López, Covadonga. 2022. 'Border Policing at Sea: Tactics, Routines, and the Law in a Frontex Patrol Boat'. *The British Journal of Criminology* 63 (1), 1–17. https://doi.org/10.1093/bjc/azac009

Balibar, Étienne. 2002. Politics and the Other Scene. Translated by Christine Jones, James Swenson, and Chris Turner. London Brooklyn, New York: Verso.

Balibar, Etienne. 2009. 'Europe as Borderland'. *Environment and Planning D: Society and Space* 27 (2): 190–215. https://doi.org/10.1068/d13008

Barak, Aharon. 2015. 'Human Dignity as a Framework Right (Mother-Right)'. In *Human Dignity: The Constitutional Value and the Constitutional Right,* 156–69. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781316106327.013

Barbero, Iker, and Giacomo Donadio. 2019. 'La Externalización Interna de Las Fronteras En El Control Migratorio En La UE'. *Revista CIDOB d'Afers Internacionals,* 122, 137–62. https://doi.org/10.24241/rcai.2019.122.2.137

Barbero, Iker. 2021. 'Los Centros de Atención Temporal de Extranjeros Como Nuevo Modelo de Control Migratorio: Situación Actual, (Des)Regulación Jurídica y Mecanismos de Control de Derechos y Garantías'. *Derechos y Libertades: Revista de Filosofía Del Derecho y Derechos Humanos,* 45, 267-302. https://doi.org/10.20318/dyl.2021.6108

Bathke, Benjamin. 2021. 'Greece to Fortify Border to Stop Migrants, Seeks EU Funds', InfoMigrants. https://www.infomigrants.net/en/post/37355/greece-to-fortify-border-to-stop-migrants-seeks-eu-funds. 22 December 2021 (2024-09-01).

Beduschi, Ana. 2019. 'Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights'. *Big Data & Society* 6 (2). https://doi.org/10.1177/2053951719855091

Beduschi, Ana. 2022. 'Governance of Digital Technologies and Human Rights', *Geneva Graduate Institute* 11 (Global challenges).

Bellanova, Rocco, and Denis Duez. 2016. 'The Making (Sense) of EUROSUR: How to Control the Sea Borders?' In *EU Borders and Shifting Internal Security*, edited by Raphael Bossong and Helena Carrapico, 23–44. Cham: Springer International Publishing.

Bellingcat. 2020. 'Frontex at Fault: European Border Force Complicit in "Illegal" Pushbacks'. https://www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks. 23 October 2020 (2024-09-01).

Bhuta, Nehal. 2016. 'The Frontiers of Extraterritoriality - Human Rights Law as Global Law'. In *The Frontiers of Human Rights*, edited by Nehal Bhuta, 1–20. Oxford: Oxford University Press.

Bigo, Didier, and Elspeth Guild, eds. 2005. *Controlling Frontiers: Free Movement into and within Europe*. Burlington: Ashgate.

Bigo, Didier, Lina Ewert, and Elif Mendos Kuşkonmaz. 2020. 'The Interoperability Controversy or How to Fail Successfully: Lessons from Europe'. *International Journal of Migration and Border Studies* 6 (1): 93-114. https://doi.org/10.1504/IJMBS.2020.108687

Bigo, Didier. 2006. 'Internal and External Aspects of Security'. *European Security* 15 (4): 385–404. https://doi.org/10.1080/09662830701305831

Bigo, Didier. 2014. 'The (in)Securitization Practices of the Three Universes of EU Border Control: Military/Navy – Border Guards/Police – Database Analysts'. *Security Dialogue* 45 (3): 209–25. https://doi.org/10.1177/0967010614530459

Bigo, Didier. 2022. 'The Digitalisation of Border Controls and Their Corporate Actors'. In *Privatising Border Control*, edited by Mary Bosworth and Lucia Zedner, Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780192857163.003.0013

Bircan, Tuba, and Emre Eren Korkmaz. 2021. 'Big Data for Whose Sake? Governing Migration through Artificial Intelligence'. *Humanities and Social Sciences Communications* 8 (1). https://doi.org/10.1057/s41599-021-00910-x

Blasi Casagran, Cristina. 2021. 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU'. *Human Rights Law Review* 21 (2): 433–57. https://doi.org/10.1093/hrlr/ngaa057

Bonnevalle, Pierre. 2022. 'L'État Français et La Gestion de La Présence Des Personnes Exilées Dans La Frontière Franco-Britannique : Harceler, Expulser et Disperser. Rapport d'enquête Sur 30 Ans de Fabrique Politique de La Dissuasion'. Plateforme des Soutiens aux Migrant.e.s and CERAPS.

Bosworth, Mary. 2008. 'Border Control and the Limits of the Sovereign State'. *Social & Legal Studies* 17 (2): 199–215. https://doi.org/10.1177/0964663908089611

Bourne, Mike, Heather Johnson, and Debbie Lisle. 2015. 'Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies'. *Security Dialogue* 46 (4): 307–25. https://doi.org/10.1177/0967010615578399

Broeders, Dennis, and Huub Dijstelbloem. 2016. 'Digitizing Identities: Doing Identity in a Networked World'. In *Digitizing Identities: Doing Identity in a Networked World*, edited by Irma van der Ploeg and Jason Pridmore. New York: Routledge, Taylor & Francis Group.

Broeders, Dennis. 2007. 'The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants'. *International Sociology* 22 (1): 71–92. https://doi.org/10.1177/0268580907070126

Brouwer, Evelien. 2011. 'Legal Boundaries and the Use of Migration Technology'. In *Migration and the New Technological Borders of Europe*, edited by Huub Dijstelbloem and Albert Meijer, 134–69. New York: Palgrave Macmillan.

Brouwer, Evelien.2020. 'Large-Scale Databases and Interoperability in Migration and Border Policies'. *European Public Law* 26 (1): 71–92. https://doi.org/10.54648/euro2020005

Burgess, J. Peter, and Dariusz Kloza. 2021. *Border Control And New Technologies: Addressing Integrated Impact Assessment*. Brussel: VUB Press.

Burt, Peter, and Jo Frew. 2020. 'Crossing A Line. The Use of Drones to Control Borders'. *Drone Wars UK*. https://dronewars.net/wp-content/uploads/2020/12/DW-Crossing-a-Line-WEB.pdf. 1 December 2020 (2024-09-01).

BVMN. 2019. 'I Told Them: Stop! You're Hurting Me. I Cannot Breathe'. https://www.borderviolence.eu/violence-reports/august-5-2019-1500-near-sturlic-bih/. 8 May 2019 (2024-09-01).

BVMN. 2020. 'If We Had Known, We Would Not Have Come to Thessaloniki. But I Thought We Have Papers, We Have UNHCR Documents, Nothing Will Happen to Us!' https://www.borderviolence.eu/violence-reports/august-27-2020-0900-thessaloniki-greece/. 27 August 2020 (2024-09-01).

BVMN. 2021. 'Systematic Human Rights Violations: Border Violence, Pushbacks and Containment in Ceuta and Melilla'. https://www.borderviolence.eu/wp-content/uploads/special-report-on-ceuta-and-melilla.pdf. (2024-09-01).

Candidatu, Laura, Koen Leurs, and Sandra Ponzanesi. 2019. 'Digital Diasporas: Beyond the Buzzword: Toward a Relational Understanding of Mobility and Connectivity'. In *The Handbook of Diasporas, Media, and Culture*, edited by Jessica Retis and Roza Tsagarousianou. Medford: Wiley Blackwell. https://doi.org/10.1002/9781119236771.ch3

Carling, Jørgen. 2007. 'The Merits and Limitations of Spain's High-Tech Border Control'. *The Online Journal of the Migration Policy Institute*.

Carlotti, Sebastian. 2022. 'Prove Di Esternalizzazione Dei Confini in Africa Occidentale: Una Breve Storia Del Controllo Remoto Delle Migrazioni Nella Regione', 18 February 2022, *ASGI* .

Carrasco, Benjamín. 2022. 'La Guardia Civil Invertirá 25,7 Millones En Su Sistema de Detección de Pateras y Narcolanchas En El Estrecho'. *InfoDefensa. https://www.infodefensa.com/texto-diario/mostrar/3515613/guardia-civil-invertira-257-millones-sistema-deteccion-pateras-narcolanchas-estrecho.* 31 March 2022 (2024-09-01).

Carrera, Sergio, and Elspeth Guild. 2010. ''Joint Operation RABIT 2010': FRONTEX Assistance to Greece's Border with Turkey: Revealing the Deficiencies of Europe's Dublin Asylum System'. *CEPS Paper in Liberty and Security in Europe*. Brussels: Centre for European Policy Studies.

Carrera, Sergio, and Roberto Cortinovis. 2019. 'Search and Rescue, Disembarkation and Relocation Arrangements in the Mediterranean. Sailing Away from Responsibility?'. *CEPS Paper in Liberty and Security in Europe*. Brussels: Centre for European Policy Studies.

Casas-Cortes, Maribel, Sebastian Cobarrubias, and John Pickles. 2016. '"Good Neighbours Make Good Fences": Seahorse Operations, Border Externalization and Extra-Territoriality'. *European Urban and Regional Studies* 23 (3): 231–51. https://doi.org/10.1177/0969776414541136

Catalán, Nacho. 2014. 'Funcionamiento Del Sistema Integrado de Vigilancia Exterior (SIVE)'. *El País*, 13 August 2014.

Chambers, Samuel Norton, Geoffrey Alan Boyce, Sarah Launius, and Alicia Dinsmore. 2021. 'Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence'. *Journal of Borderlands Studies* 36 (3): 443–68. https://doi.org/10.1080/08865655.2019.1570861

Chelioudakis, Eleftherios. 2020. 'Greece: Technology-Led Policing Awakens', *European Voices on Surveillance*. https://aboutintel.eu/greece-policing-border-surveillance/. 29 June 2020 (2024-09-01).

Christides, Giorgos, Bashar Deeb, Klaas van Dijken, Alexander Epp, Steffen Lüdke, Andrei Popoviciu, Lamia Šabić, Jack Sapoch, Phevos Simeonidis, and Nicole Vögele. 2021. 'Europe's Violent Shadow Army Unmasked', *Spiegel International*. https://www.spiegel.de/international/europe/greece-and-croatia-the-shadow-army-that-beats-up-refugees-at-the-eu-border-a-a4409e54-2986-4f9d-934f-02efcebd89a7. 1 October 2021 (2024-09-01).

Cockerell, Isobel. 2021. 'Greece Aims Long-Range Sound Cannons at Migrants across Its Border', *Coda Media*. https://www.codastory.com/authoritarian-tech/sound-cannons-greece/. 28 July 2021 (2024-09-01).

Coeckelbergh, Mark. 2013. 'Drones, Information Technology, and Distance: Mapping the Moral Epistemology of Remote Fighting'. *Ethics and Information Technology* 15 (2): 87–98. https://doi.org/10.1007/s10676-013-9313-6

Commissioner for Human Rights and Council of Europe. 2021. 'A Distress Call for Human Rights The Widening Gap in Migrant Protection in the Mediterranean - Follow-up Report to the 2019 Recommendation by the Council of Europe Commissioner for Human Rights'.

Commissioner for Human Rights. 2015. 'Spain: Legislation and Practice on Immigration and Asylum Must Adhere to Human Rights Standards - Ref. CommDH 001 (2015)'.

Commissioner for Human Rights. 2021a. 'Greece's Parliament Should Align the Deportations and Return Bill with Human Rights Standards'.

Commissioner for Human Rights. 2021b. 'Greek Authorities Should Investigate Allegations of Pushbacks and Ill-Treatment of Migrants, Ensure an Enabling Environment for NGOs and Improve Reception Conditions'.

Committee Against Torture. 2008. 'General Comment 2, Implementation of Article 2 by States Parties - CAT/C/GC/2'.

Committee on the Elimination of Racial Discrimination. 2008. 'Consideration of Reports Submitted by State Parties under Article 9 of the Convention: Concluding Observations, United States of America - CERD/C/USA/CO/6'.

Costa Traba, Tania. 2021. 'Devoluciones En Caliente de Migrantes En La Frontera Sur de Europa'. *AULA Revista De Humanidades Y Ciencias Sociales* 67(2): 39–47. https://doi.org/10.33413/aulahcs.2021.67i2.177

Council of the European Union. 2018. 'Frontex Annual Activity Report 2017 - 10525/18'.

Csernatoni, Raluca. 2018. 'Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management'. *European Security* 27 (2): 175–200. https://doi.org/10.1080/09662839.2018.1481396

Defensor del Pueblo. 2005. 'Informe Anual 2005 y Debates En Las Cortes Generales'.

Defensor del Pueblo. 2021. 'Devolución Sin Procedimiento de Menores Extranjeros No Acompañados En Ceuta'.

Degli Esposti, Sara. 2014. 'When Big Data Meets Dataveillance: The Hidden Side of Analytics'. *Surveillance & Society* 12 (2): 209–25. https://doi.org/10.24908/ss.v12i2.5113

Dijstelbloem, Huub, Albert Meijer, and Michiel Besters. 2011. 'The Migration Machine'. In *Migration and the New Technological Borders of Europe*, edited by Huub Dijstelbloem and Albert Meijer. New York: Palgrave Macmillan.

Dijstelbloem, Huub, and Dennis Broeders. 2016. 'The Datafication of Mobility and Migration Management. The Mediating State and Its Consequences'. In *Digitizing Identities: Doing Identity in a Networked World*, edited by Irma van der Ploeg and Jason Pridmore. New York: Routledge.

Dijstelbloem, Huub, Rogier van Reekum, and Willem Schinkel. 2017. 'Surveillance at Sea: The Transactional Politics of Border Control in the Aegean'. *Security Dialogue* 48 (3): 224–40. https://doi.org/10.1177/0967010617695714

Dijstelbloem, Huub. 2021. *Borders as Infrastructure: The Technopolitics of Border Control*. Cambridge, Massachusetts: The MIT Press.

Dokos, Thanos P. 2021. 'Thanos Dokos: Greek National Security: An Assessment and Challenges'. *Ekathimerini*. https://www.ekathimerini.com/opinion/261588/thanos-dokos-greek-national-security-an-assessment-and-challenges/. 25 January 2021 (2024-09-01).

Drusila Castro, Livia. 2022b. 'Madrid Justifica La Decisión de Rabat de Desplegar Dronesarmados En La Frontera Con Ceuta y Melilla', *Infodron.es*. https://www.infodron.es/texto-diario/mostrar/3529196/madrid-justifica-decision-rabat-desplegar-drones-armados-frontera-ceuta-melilla. 11 February 2022 (2024-09-01).

e-evros.gr. 2020. 'Evros: With Drones, Thermal Cameras & Armored Jeeps They Are Fortifying the Borders (Translated from Greek)'. https://www.e-evros.gr/gr/eidhseis/3/ebros-me-drones-8ermikes-kameres-8wrakismena-tzip-oxyrwnoyn-ta-synora/post41202. 7 September 2020 (2024-09-01).

e-evros.gr. 2021a. 'Evros Fence: Four Local and 2 Regional Operation Centers Will Be Put into Operation (Translated from Greek)'. https://www.e-evros.gr/gr/eidhseis/3/fraxths-ebroy-tessera-topika-2-perifereiaka-epixeirhsiaka-kentra-ths-el-as-8a-te8oyn-se-leitoyrgia/post42826. 23 February 2021 (2024-09-01).

e-evros.gr. 2021b. 'Evros: We Have a Fence, the Turks Have Drones (Translated from Greek)'. https://www.e-evros.gr/gr/eidhseis/3/ebros-fraxth-emeis-drones-oi-toyrkoi/post42763. 17 February 2021 (2024-09-01).

EDRI, European Disability Forum, Bits of Freedom, Fair Trails, Access Now, Panoptycon Foundation, PICUM, Epicenter.Works, Algorithm Watch, and ANEC. 2021. 'An EU Artificial Intelligence Act for Fundamental Rights - A Civil Society Statement'. 30 November 2021.

EDRI, European Disability Forum, Bits of Freedom, Fair Trails, Access Now, Panoptycon Foundation, PICUM, Epicenter.Works, Algorithm Watch, and ANEC. 2022. 'Civil Society Reacts to EP AI Act Draft Report'. 4 May 2022.

EDRI. 2020. 'Ban Biometric Mass Surveillance!'. 13 May 2020.

EDRI. 2022. 'The European Parliament Must Go Further to Empower People in the AI Act'. 21 April 2022.

Edwards, Lilian. 2022. 'Regulating AI in Europe: Four Problems and Four Solutions'. *Ada Lovelace Institute*. 1 March 2022.

El Día. 2009. 'La Delegada Del Gobierno En Canarias Admite Que El Sive No Detectó La Patera Naufragada En Lanzarote'. https://www.eldia.es/canarias/2009-02-16/7-delegada-Gobierno-Canarias-admite-Sive-detecto-patera-naufragada-Lanzarote.htm. 16 February 2009 (2024-09-01).

Ellebrecht, Sabrina. 2020. *Mediated Bordering: Eurosur, the Refugee Boat, and the Construction of an External EU Border*. Bielefeld: Transcript.

Emmanouilidou, Lydia, and Katy Fallon. 2021. 'With Drones and Thermal Cameras, Greek Officials Monitor Refugees'. *Al Jazeera*. https://www.aljazeera.com/news/2021/12/24/greece-pilots-high-tech-surveillance-system-in-refugee-camps. 24 December 2021 (2024-09-01).

Euro-Med Monitor. 2021. 'EU Use of Hi-Tech to Deter Asylum Seekers Is Condemnable and Dangerous', 3 June 2021.

European Commission. 2014a. 'Communication from the Commission to the European Parliament and the Council: Better Situational Awareness by Enhanced Cooperation across Maritime Surveillance Authorities: Next Steps within the Common Information Sharing Environment for the EU Maritime Domain – COM/2014/0451 Final'.

European Commission. 2014b. 'Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Ex-Post Evaluation of the External Borders Fund for the Period 2007-2010 (Report Submitted in Accordance with Article 52(3)(c) of Decision No 574/2007/EC of the European Parliament and of the Council of 23 May 2007) - COM(2014) 235 Final'.

European Commission. 2015. 'Annex to the Commission Recommendation Adopting the Practical Handbook for Implementing and Managing the European Border Surveillance System (EUROSUR Handbook) - C(2015) 9206 Final'.

European Commission. 2016a. 'Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security – COM/2016/0205 Final'.

European Commission. 2016b. 'Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) 2016/399 as Regards the Use of the Entry/Exit System – COM(2016) 196 Final'.

European Commission. 2016c. 'Proposal for a Regulation of the European Parliament and of the Council Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third Country Nationals Crossing the External Borders of the Member States of the European Union and Determining the Conditions for Access to the EES for Law Enforcement Purposes and Amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 – COM(2016) 194 Final'.

European Commission. 2020a. 'A Fresh Start on Migration: Building Confidence and Striking a New Balance between Responsibility and Solidarity – Press Relese'.

European Commission. 2020b. 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum – COM/2020/609 Final'.

European Commission. 2020c. 'Migration and Home Affaires – Funding Contacts'.

European Commission. 2020d. 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts - COM/2021/206 Final'.

European Commission. 2020e. 'Remarks by President von Der Leyen at the Joint Press Conference with Kyriakos Mitsotakis, Prime Minister of Greece, Andrej Plenković, Prime Minister of Croatia, President Sassoli and President Michel'.

European Commission. 2020f. 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics – COM(2020) 64 Final'.

European Commission. 2020g. 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust – COM(2020) 65 Final'.

European Commission. 2021a. 'Cordis – NESTOR, an Enhanced Pre-Frontier Intelligence Picture to Safeguard rhe European Borders'.

European Commission. 2021b. 'Horizon Europe, the EU Research and Innovation Programme 2021-2027 General Overview'.

European Commission. 2021c. 'Internal Security Fund – Lead DG: HOME'.

European Commission. 2021d. 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts - COM(2021) 206 Final'.

European Commission. 2022. 'Proposal for a Council Implementig Decision Setting out a Recommendation on Addressing the Deficiencies Identified in the 2021 Evaluation of Greece on the Application of the Schengen Acquis in the Field of Management of the External Borders – COM(2022) 99 Final'.

European Council on Refugees and Exiles. 2021. 'Greece: EU Funded Securitisation of Camps, Legal Action Against Frontex Before CJEU as Greek PM and Leggeri Exchange Mutual Praise on Reduction of Arrivals'. https://ecre.org/greece-eu-funded-securitisation-of-camps-legal-action-against-frontex-before-cjeu-as-greek-pm-and-leggeri-exchange-mutual-praise-on-reduction-of-arrivals/. 28 May 2021 (2024-09-01).

European Court of Human Rights. 2021. 'Guide on Case-Law of the Convention: Data Protection'.

European Data Protection Suprevisor. 2017. 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit'.

European Digital Rights. 2021. 'European Court Supports Transparency in Risky EU Border Tech Experiments'. https://edri.org/our-work/european-court-supports-transparency-in-risky-eu-border-tech-experiments/. 16 December 2021 (2024-09-01).

European Maritime Safety Agency. 2019. 'RPAS Drone Flights Get Underway in Spain to Assist SASEMAR in Its Search and Rescue and Pollution Monitoring Operations'. http://www.emsa.europa.eu/newsroom/press-releases/download/5527/3452/23.html. 6 February 2019 (2024-09-01).

European Maritime Safety Agency. 2022. 'EMSA Outlook 2022'.

European Maritime Safety Agency. 2022. 'RPAS Operations'. http://www.emsa.europa.eu/rpas-operations.html. 1 January 2022 (2024-09-01).

European Parliament. 2021a. 'Artificial Intelligence in Criminal Law and Its Use by the Police and Judicial Authorities in Criminal Matters P9_TA(2021)0405'.

European Parliament. 2021b. 'Working Document – Report on the Fact-Finding Investigation on Frontex Concerning Alleged Fundamental Rights Violations'.

European Union Agency for Fundamental Rights. 2013. 'Fundamental Rights at Europe's Southern Sea Borders'. https://doi.org/10.2811/26971

European Union Agency for Fundamental Rights. 2020. 'Getting the Future Right: Artificial Intelligence and Fundamental Rights'. https://doi.org/10.2811/452644

European Union. 2021. 'Technical Specification Issue – Supply of Systems for Smart Policing of the ISF (Translated from Greek)'. https://s3.documentcloud.org/documents/20448704/smart-policing-elas-teukhos-tekhnikon-prodiagraphon.pdf (2024-09-01).

Everuss, Luis. 2021. 'AI, Smart Borders and Migration'. In *The Routledge Social Science Handbook of AI*, edited by Anthony Elliott, 339–57. New York: Routledge.

External Borders Fund. 2007. 'Annex 1-Multi Annual Programme'. http://www.astynomia.gr/images/stories/3101SOLID-MAP-EBF-%20ELannex1.pdf. (2024-09-01).

Fallon, Katy. 2020. ‘UN Warns of Impact of Smart Borders on Refugees: “Data Collection Isn't Apolitical”’, The Guardian. 11 November 2020 (2024-09-01).

Favilli, Chiara. 2018. ‘L'Unione Che Protegge e l'Unione Che Respinge. Progressi, Contraddizioni e Paradossi Del Sistema Europeo Di Asilo’. *Questione Giustizia* 2:28–43.

Fernández Burgueño, Borja. 2016. ‘The Uselfulness of the Legal Concept of Dignity in the Human Rights Discourse: Literature Review’. *Oxímora Revista Internacional de Ética y Política*, 8: 9–19. https://doi.org/10.1344/oxi.2016.i8.15472

Fernández Jurado, José Antonio, and Sebastián Sabariego Rivero. 2006. ‘Servicio Integral de Vigilancia Exterior (S.I.V.E.). Consecuencias de Su Implantación’. *Boletín Criminológico* 12 (89). https://doi.org/10.24310/Boletin-criminologico.2006.v12i.8772

Ferraris, Valeria. 2020. ‘Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere?’ In *Big data processi decisionali: strumenti per l'analisi delle decisioni giuridiche, politiche, economiche e sociali*, edited by Simona Gozzo, Carlo Pennisi, Vincenzo Asero, and Rossana Sampugnaro. Milano: Egea.

Fill, Alice. 2021. ‘Le politiche migratorie europee tra esternalizzazione e violazione dell'obbligo di non-refoulement: pushback, pullback e backscattering’. *Studi sulla questione criminale* 3: 83–106. https://doi.org/10.7383/103020

Finn, Rachel L., and David Wright. 2012. ‘Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications’. *Computer Law & Security Review* 28 (2): 184–94. https://doi.org/10.1016/j.clsr.2012.01.005

Fisher, Daniel X.O. 2018. ‘Situating Border Control: Unpacking Spain's SIVE Border Surveillance Assemblage’. *Political Geography* 65:67–76. https://doi.org/10.1016/j.polgeo.2018.04.005

Follis, Karolina S. 2017. ‘Vision and Transterritory: The Borders of Europe’. *Science, Technology, & Human Values* 42 (6): 1003–30. https://doi.org/10.1177/0162243917715106

Fritsch, Stefan. 2011. ‘Technology and Global Affairs: Technology and Global Affairs’. *International Studies Perspectives* 12 (1): 27–45. https://doi.org/10.1111/j.1528-3585.2010.00417.x

Frontera Digitales. 2022. ‘La Implantación de La Inteligencia Artificial En Frontera y La Vulneración de Derechos’. https://www.idhc.org/es/noticias/la-implantacion-de-la-inteligencia-artificial-en-frontera-y-la-vulneracion-de-derechos/. 12 January 2022 (2024-09-01).

Frontex, EMSA, and EFCA. 2018. ‘Pilot Project “Creation of a European Coastguard Function” – Final Report’.

Frontex. 2012. ‘Frontex Signs a Memorandum of Understanding with Turkey’.

Frontex. 2015. ‘Africa-Frontex Intelligence Community Joint Report’.

Frontex. 2020a. ‘Answer to the Written Question E-003553/2019’.

Frontex. 2020b. ‘Management Board Meeting, 10 November Agenda Item: Rapid Border Intervention in Greece’.

Frontex. 2020c. ‘Written Question P-2306/20: Blocking Real-Time Position Display for Frontex Assets’.

Frontex. 2021a. ‘Artificial Intelligence-Based Capabilities for the European Border and Coast Guard Final Report’.

Frontex. 2021b. ‘Frontex Continues Its Support for Spain’. https://frontex.europa.eu/media-centre/news/news-release/frontex-continues-its-support-for-spain-nOvbKi.

Frontex. 2021c. ‘Main Operations’. https://frontex.europa.eu/we-support/main-operations/operation-poseidon-greece-/. 29 January 2022 (2024-09-01).

Gammeltoft-Hansen, Thomas. 2013. *Access to Asylum: International Refugee Law and the Globalisation of Migration Control*. Cambridge: Cambridge University Press.

Gatopoulos, Derek, and Costas Kantouris. 2021. 'In Post-Pandemic Europe, Migrants Will Face Digital Fortress'. *AP News*. https://apnews.com/article/middle-east-europe-migration-technology-health-c23251bec65ba45205a0851fab07e9b6. 31 May 2021 (2024-09-01).

Geese, Alexandra, and Erik Marquardt. 2021. 'Letter to the Commission on the Surveillance Technology Centaur, Hyperion and RAE Used in the MPRIC on the Greek Islands and Their Funding Though the RRF'. https://alexandrageese.eu/wp-content/uploads/Letter-on-MRPIC-and-Surveillance.pdf. 26 November 2021 (2024-09-01).

General Assembly of the United Nations. 2014. 'Resolution 68/167 Adopted by the General Assembly on 18 December 2013, The Right to Privacy in the Digital Age - A/RES/68/167'.

General Assembly of the United Nations. 2017. 'Report of the Special Rapporteur of the Human Rights Council on Extrajudicial, Summary or Arbitrary Executions. Unlawful Death of Refugees and Migrants - A/72/335'.

Giannakou, Eleni. 2021. 'Migrants' Human Rights Facing Surveillance Technologies in Immigration Enforcement'. https://jmce.gr/portal/wp-content/uploads/2021/11/Giannakou-Migrants.pdf. September 2021 (2024-09-01).

Giuffré, Mariagiulia, and Violeta Moreno-Lax. 2019. 'The Rise of Consensual Containment: From Contactless Control to Contactless Responsibility for Migratory Flows'. In *Research Handbook on International Refugee Law*, by Satvinder Juss, 82–108. Cheltenham: Edward Elgar Publishing.

Glouftsios, Georgios, and Loukinas Panagiotis. 2022. 'Perceiving and Controlling Maritime Flows. Technology, Kinopolitics, and the Governmentalisation of Vision'. *International Political Sociology* 16 (3). https://doi.org/10.1093/ips/olac010

Glouftsios, Georgios. 2021a. *Engineering Digitised Borders: Designing and Managing the Visa Information System*. Singapore: Palgrave Macmillan.

Glouftsios, Georgios. 2021b. 'Governing Border Security Infrastructures: Maintaining Large-Scale Information Systems'. *Security Dialogue* 52 (5): 452–70. https://doi.org/10.1177/0967010620957230

Godenau, Dirk, and Ana López-Sala. 2016. 'Multi-Layered Migration Deterrence and Technology in Spanish Maritime Border Management'. *Journal of Borderlands Studies* 31(2): 151–169. https://doi.org/10.1080/08865655.2016.1174602

Godin, Marie, and Giorgia Donà. 2021. 'Rethinking Transit Zones: Migrant Trajectories and Transnational Networks in "Techno-Borderscapes"'. *Journal of Ethnic and Migration Studies* 47 (14): 3276–92. https://doi.org/10.1080/1369183X.2020.1804193

González, Alexis. 2018. 'La Guardia Civil Declara "Información Reservada" Los Fallos de Los Radares Para Detectar Pateras En Canarias'. *Canariasahora*. https://www.eldiario.es/canariasahora/sociedad/guardia-civil-informacion-sive-canarias_1_2821571.html. 27 January 2018 (2024-09-01).

Graeber, David. 2012. 'Dead Zones of the Imagination: On Violence, Bureaucracy, and Interpretive Labor: The Malinowski Memorial Lecture, 2006'. *Journal of Ethnographic Theory* 2 (2): 105–28. https://doi.org/10.14318/hau2.2.007

Greek National Commission for Human Rights. 2020. 'GNCHR's Observations on Draft Law of Ministry for Migration and Asylum "Improvement of Migration Legislation, Amendments of Provisions of Laws 4636/2019, 4375/2016, 4251/2014 and Other Provisions"'.

Greek National Commission for Human Rights. 2021. 'Contribution by the Greek National Commission for Human Rights (GNCHR) to the UN Special Rapporteur on the Human Rights of Migrants in Reply to the Questionnaire on Pushback Practices and Their Impact on the Human Rights of Migrants'.

Guardia Civil. 2010. 'Sistema Integrado de Vigilancia Exterior (SIVE) - Nota de Prensa'. https://www.guardiacivil.es/es/prensa/especiales/sive/funciones.html. (2024-09-01).

Guerra, Giorgia. 2018. 'An Interdisciplinary Approach for Comparative Lawyers: Insights from the Fast-Moving Field of Law and Technology'. *German Law Journal* 19 (3): 579–612. https://doi.org/10.1017/S2071832200022793

Gurierrez, Peter. 2022. 'Putting Unmanned Systems on Task Over the Mediterranean'. *Inside Unmanned Systems*. https://insideunmannedsystems.com/putting-unmanned-systems-on-task-over-the-mediterranean/. 3 November 2022 (2024-09-01).

Kuşkonmaz, Elif Mendos. 2021. 'Border Management and Technology: A Challenge to the Right to Privacy'. In Migration, Security, and Resistance, by Graham Hudson and Idil Atak, 205–23. London: Routledge.

Habib, Adil. 2021. 'The Ongoing Digitisation of Europe's Borders', *Digital Freedom Fund*. https://digitalfreedomfund.org/the-ongoing-digitisation-of-europes-borders/. 18 June 2021 (2024-09-01).

Hamlin, Rebecca. 2021. *Crossing: How We Label and React to People on the Move*. Stanford: Stanford University Press.

Hanke, Philip, and Daniela Vitiello. 2019. 'High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability"'. In *Use and Misuse of New Technologies*, edited by Elena Carpanelli and Nicole Lazzerini, 3–35. Cham: Springer International Publishing.

Hathaway, James C., and Thomas Gammeltoft-Hansen. 2014. 'Non-Refoulement in a World of Cooperative Deterrence'. *Columbia Journal of Transnational Law* 53 (2): 235–84. https://doi.org/10.2139/ssrn.2479511

Hellenic Data Protection Authority. 2018. 'Decision 65/2018 - File No: G/E/8187/16-10-2018. List of Types of Processing Operations Subject to the Requirement to Carry out an Audit of the Processing Operations Related to the Provision of Data Pursuant to Article 35 Par. 4 of the GDPR'.

Hellenic Data Protection Authority. 2020. 'Opinion 3 /2020 - Original No: G/E/2566-1/29-06-2020'.

Hellenic Data Protection Authority. 2021. 'Annual Report 2019'. https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2019. (2024-09-01).

Hellenic Ministry of Citizen Protection. 2015. 'National Programme ISF - Identification of the Designated Authorities'.

Hellenic Ministry of Digital Governance. 2021. 'Ref: 90026'. https://diavgeia.gov.gr/doc/%CE%A9%CE%A33%CE%A846%CE%9C%CE%A4%CE%9B%CE%A1-%CE%9C%CE%976?inline=true. (2024-09-01).

Hellenic Republic Ministry of Civil Protection. 2020. 'A/A E.S.E.I.S.: 90188'. http://www.astynomia.gr/images/stories/2020/prokirikseis20/18062020diakiriksi11-20.pdf. (2024-09-01).

Herrera, Geoffrey Lucas. 2006. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany: State University of New York Press.

Herz, John H. 1976. *The Nation-State and the Crisis of World Politics: Essays on International Politics in the Twentieth Century*. New York: D. McKay.

Hildebrandt, Mireille. 2020. 'The Artificial Intelligence of European Union Law'. *German Law Journal* 21 (1): 74–79. https://doi.org/10.1017/glj.2019.99

Hirschl, Ran. 2014. *Comparative Matters: The Renaissance of Comparative Constitutional Law*. Oxford: Oxford University Press.

Holmes, Oliver. 2022. 'US Tests of Robotic Patrol Dogs on Mexican Border Prompt Outcry'. *The Guardian*, 4 February 2022.

Homo Digitalis, Reporters United, and The Press Project. 2021. 'Report – Notification of an Infringement of the Provisions of Decree 75/2020 by the Hellenic Republic and Request for the Exercise of the Powers of the Defendant (Translated from Greek)'. https://www.homodigitalis.gr/wp-content/uploads/2021/05/Γνωστοποίηση-Παράβασης-των-διατάξεων-του-ΠΔ752020-και-αίτημα-άσκησης-των-σχετικών-εξουσιών.pdf. 12 May2024 (2024-09-01).

Homo Digitalis. 2020a. 'Covid-19 & Digital Rights in Greece (Translated from Greek)'. https://www.homodigitalis.gr/wp-content/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf. 22 April 2020 (2024-09-01).

Homo Digitalis. 2020b. 'COVID-Tech: COVID-19 Opens the Way for the Use of Police Drones in Greece', *European Digital Rights (EDRI)*, 24 June 2020.

Homo Digitalis. 2020c. 'Facial Recognition: Homo Digitalis Calls on Greek DPA to Speak Up'. https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/. 1 April 2020 (2024-09-01).

Homo Digitalis. 2020d. 'Homo Digitalis' Input to the UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Ms. E. Tendayi Achiume, for Her 2020 Thematic Report to the General Assembly Related to Race, Borders, and Digital Technologies'. https://homodigitalis.gr/en/posts/8253/. 11 November 2020 (2024-09-01).

Homo Digitalis. 2020e. 'Open Letter - Information Regarding the Use of Unmanned Aerial Vehicles (Drones) by Law Enforcement Authorities in Greece (Translated from Greek)'. https://homodigitalis.gr/posts/6579/. 30 April 2020 (2024-09-01).

Howden, Daniel, Fotiadis Apostolis, and Antony Loewenstein. 2019. 'Once Migrants on Mediterranean Were Saved by Naval Patrols. Now They Have to Watch as Drones Fly Over', *The Guardian*, 4 August 2019.

Hu, Margaret. 2017. 'Biometric Surveillance and Big Data Governance'. In *The Cambridge Handbook of Surveillance Law*, edited by David Gray and Stephen E. Henderson, 121–49. Cambridge: Cambridge University Press.

Human Rights 360°. 2020. 'Defending Human Rights in Times of Border Militarization, May 2020-September 2020'. https://www.humanrights360.org/wp-content/uploads/2020/10/Evros-Report-19.10.pdf. 1 October 2020 (2024-09-01).

Human Rights Committee. 2021. 'Views Adopted by the Committee under Article 5 (4) of the Optional Protocol, Concerning Communication No. 3042/2017 - CCPR/C/130/D/3042/2017'.

Human Rights Council. 2015. 'Resolution Adopted by the Human Rights Council 28/16, The Right to Privacy in the Digital Age - A/HRC/RES/28/16'.

Human Rights Council. 2021a. 'Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement - A/HRC/48/76'.

Human Rights Council. 2021b. 'The Right to Privacy in the Digital Age, Report of the United Nations High Commissioner for Human Rights - A/HRC/48/31'.

Human Rights Council. 2022. 'Greece: New Biometrics Policing Program Undermines Rights Risk of Illegal Racial Profiling and Other Abuses'.

Human Rights Watch. 2020. 'Greece/EU: Allow New Arrivals to Claim Asylum'. https://www.hrw.org/news/2020/03/10/greece/eu-allow-new-arrivals-claim-asylum. 10 March 2020 (2024-09-01).

Hyndman, Jennifer, and Alison Mountz. 2008. 'Another Brick in the Wall? Neo-Refoulement and the Externalization of Asylum by Australia and Europe'. *Government and Opposition* 43 (2): 249–69. https://doi.org/10.1111/j.1477-7053.2007.00251.x

Ilias, Aggelos, Nadina Leivaditi, Evangelia Papatzani, and Electra Petracou. 2019. 'Border Management and Migration Controls in Greece - Greece Country Report'. Working Papers Global Migration: Consequences and Responses, Paper 2019/22.

Infodron.es. 2022. 'La Guardia Civil Compra de Urgencia Drones Para Detectar Asaltos a Las Vallas de Ceuta y Melilla'. https://www.infodron.es/id/2022/02/15/noticia-8203la-guardia-civil-compra-urgencia-drones-detectar-asaltos-vallas-ceuta.html. 15 February 2022 (2024-09-01).

International Court of Justice. 2004. 'Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion'.

Intracom Telecom. 2019. 'Intracom Telecom Undertakes a "Smart Policing" Project'. https://www.intracom-telecom.com/en/news/press/press2019/2019_07_02.htm. 2 July 2019 (2024-09-01).

İşleyen, Beste. 2021. 'Technology and Territorial Change in Conflict Settings: Migration Control in the Aegean Sea'. *International Studies Quarterly* 65 (4): 1087–96. https://doi.org/10.1093/isq/sqab046

Jeandesboz, Julien. 2016. 'Smartening Border Security in the European Union: An Associational Inquiry'. *Security Dialogue* 47 (4): 292–309. https://doi.org/10.1177/0967010616650226

Jeandesboz, Julien. 2017. 'European Border Policing: EUROSUR, Knowledge, Calculation'. *Global Crime* 18 (3): 256–85. https://doi.org/10.1080/17440572.2017.1347043

Joly, Josephine, and Alasdair Sandford. 2021. 'Poland's Senate Approves €350 Million Wall along Belarus Border'. *Euronews*. https://www.euronews.com/2021/10/29/poland-s-senate-to-vote-on-350-million-wall-along-belarus-border. 29 October 2021 (2024-09-01).

Jumbert, Maria Gabrielsen. 2018. 'Control or Rescue at Sea? Aims and Limits of Border Surveillance Technologies in the Mediterranean Sea'. *Disasters* 42 (4): 674–96. https://doi.org/10.1111/disa.12286

Karamanidou, Lena, and Bernd Kasparek. 2020. 'Fundamental Rights, Accountability and Transparency in European Governance of Migration: The Case of the European Border and Coast Guard Agency FRONTEX'. RESPOND Working Papers Global Migration: Consequences and Responses - Paper 2020/59.

Klein, Eckart, and David Kretzmer. 2002. *The Concept of Human Dignity in Human Rights Discourse*. Leiden: Brill | Nijhoff. https://doi.org/10.1163/9789004478190

Koca, Burcu Toğral. 2020. 'Bordering Processes through the Use of Technology: The Turkish Case'. *Journal of Ethnic and Migration Studies* 48(8), 1909–1926. https://doi.org/10.1080/1369183X.2020.1796272

Koslowski, Rey, and Marcus Schulzke. 2018. 'Drones Along Borders: Border Security UAVs in the United States and the European Union'. *International Studies Perspectives* 19 (4): 305–24. https://doi.org/10.1093/isp/eky002

Kuman, Richa. 2020. 'The Role of Security and Defence Companies in EU Migration and Border Control and the Impact on the Protection of the Rights of Refugees, Migrants and Asylum Seekers'. *OHCHR Submission*.

Kuşkonmaz, Elif Mendos. 2021. 'Border Management and Technology: A Challenge to the Right to Privacy'. In *Migration, Security, and Resistance*, by Graham Hudson and Idil Atak, 205–23. London: Routledge.

Lagioia, Francesca, Giovanni Sartor, and Andrea Simoncini. 2021. 'Articolo 22 - Processo Decisionale Automatizzato Relativo Alle Persone Fisiche, Compresa La

Profilazione'. In *Codice Della Privacy e Data Protection*, edited by Roberto D'Orazio, 378–90. Milano: Giuffrè Francis Lefebvre.

Lagos, Ioannis. 2019. 'Question for Written Answer E-004115/19 to the Commission Ioannis Lagos (NI)'.

Latonero, Mark, and Paula Kift. 2018. 'On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control'. *Social Media + Society* 4 (1). https://doi.org/10.1177/2056305118764432

Laursen, Lucas. 2022. 'Europe Expands Virtual Borders to Thwart Migrants', *IEEE Spectrum*, 4 February 2022.

Leese, Matthias, Simon Noori, and Stephan Scheel. 2021. 'Data Matters: The Politics and Practices of Digital Border and Migration Management'. *Geopolitics* 27(1), 5–25. https://doi.org/10.1080/14650045.2021.1940538

Leese, Matthias. 2016. 'Exploring the Security/Facilitation Nexus: Foucault at the "Smart" Border'. *Global Society* 30 (3): 412–29. https://doi.org/10.1080/14650045.2021.1940538

Lemberg-Pedersen, Martin. 2013. 'Private Security Companies and the European Borderscapes'. In *The Migration Industry and the Commercialization of International Migration*, edited by Thomas Gammeltoft-Hansen and Ninna Nyberg Sørensen. London: Routledge.

Leurs, Koen, and Kevin Smets. 2018. 'Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe'. *Social Media + Society* 4 (1). https://doi.org/10.1177/2056305118764425

Leurs, Koen, and Tamara Shepherd. 2017. 'Datafication & Discrimination'. In *The Datafied Society*, edited by Mirko Tobias Schäfer and Karin van Es, 211–32. Amsterdam: Amsterdam University Press.

López-Sala, Ana, and Dirk Godenau. 2020. 'In Private Hands? The Markets of Migration Control and the Politics of Outsourcing'. *Journal of Ethnic and Migration Studies*, 48(7), 1610–1628. https://doi.org/10.1080/1369183X.2020.1857229

López-Sala, Ana, and Gracia Moreno-Amador. 2020. 'En Busca de Protección a Las Puertas de Europa: Refugiados, Etiquetado y Prácticas Disuasorias En La Frontera Sur Española'. *Estudios Fronterizos* 21. https://doi.org/10.21670/ref.2006048

Loukinas, Panagiotis. 2017. 'Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy'. *Surveillance & Society* 15 (3/4): 439–46. https://doi.org/10.24908/ss.v15i3/4.6613

Loukinas, Panagiotis. 2021. 'Drones for Border Surveillance: Multipurpose Use, Uncertainty and Challenges at EU Borders'. *Geopolitics* 27(1), 89–112. https://doi.org/10.1080/14650045.2021.1929182

Marin, Luisa, and Kamila Krajčíková. 2016. 'Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights'. In *Drones and Unmanned Aerial Systems*, edited by Aleš Završnik, 101–27. Cham: Springer International Publishing.

Marin, Luisa. 2011. 'Is Europe Turning into a "Technological Fortress"? Innovation and Technology for the Management of EU's External Borders: Reflections on FRONTEX and EUROSUR'. In *Regulating Technological Innovation*, edited by Michiel A. Heldeweg and Evisa Kica, 131–51. London: Palgrave Macmillan.

Marin, Luisa. 2016. 'The Humanitarian Drone and the Borders: Unveiling the Rationales Underlying the Deployment of Drones in Border Surveillance'. In *The Future of Drone Use*, edited by Bart Custers, 115–32. The Hague: T.M.C. Asser Press.

Marin, Luisa. 2017a. 'The Deployment of Drone Technology in Border Surveillance. Between Techno-Securitization and Challenges to Privacy and Data Protection'.

In *Surveillance, Privacy and Security: Citizens' Perspectives*, edited by Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova, and Walter Peissl. Abingdon, New York: Routledge.

Marin, Luisa. 2017b. 'The "Metamorphosis" of the Drone: The Governance Challenges of Drone Technology and Border Surveillance'. In *Embedding New Technologies into Society*, edited by Diana M. Bowman, Elen Stokes, and Arie Rip, 299–333. Singapore: Jenny Stanford Publishing.

Marin, Luisa. 2020. 'The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions'. *European Public Law 26(1):* 157-80. https://doi.org/10.54648/euro2020009

Markard, Nora. 2016. 'The Right to Leave by Sea: Legal Limits on EU Migration Control by Third Countries'. *European Journal of International Law* 27 (3): 591–616. https://doi.org/10.1093/ejil/chw034

Markard, Nora. 2020. 'A Hole of Unclear Dimensions: Reading ND and NT v. Spain'. *EU Immigration and Asylum Law and Policy. https://eumigrationlawblog.eu/a-hole-of-unclear-dimensions-reading-nd-and-nt-v-spain/.* 01 April 2020 (2024-09-01).

Martín, María, and Miguel González. 2021. 'España Prepara Un Nuevo Modelo Fronterizo Para Ceuta y Melilla'. *El País*. https://elpais.com/espana/2021-12-13/espana-prepara-un-nuevo-modelo-fronterizo-para-ceuta-y-melilla.html. 13 December 2021 (2024-09-01).

Martín, María. 2021. 'El Año Más Letal En La Ruta Migratoria Hacia España'. *El País*. https://elpais.com/espana/2021-09-28/espana-una-ruta-migratoria-mortal.html. 28 September 2021 (2024-09-01).

Martínez Escamilla, Margarita, and José Miguel Sánchez Tomás. 2019. 'La Vulneración de Derechos En La Frontera Sur: De Las Devoluciones En Caliente al Rechazo En Frontera', *Critica Penal y Poder* 18:28-39.

Mazzeo, Antonio. 2021. 'Border Surveillance, Drones and Militarisation of the Mediterranean', *Statewatch*. https://www.statewatch.org/analyses/2021/border-surveillance-drones-and-militarisation-of-the-mediterranean/. 6 May 2021 (2024-09-01).

McNabb, Miriam. 2021. 'Unmanned Helicopters: Alpha 900 Flying with Greek Navy', *DroneLife*. https://dronelife.com/2021/11/23/unmanned-helicopters-alpha-900-flying-with-greek-navy/. 23 November 2021 (2024-09-01).

Mezzadra, Sandro, and Brett Neilson. 2013. *Border as Method, or, the Multiplication of Labor*. Durham: Duke University Press.

Milivojevic, Sanja. 2016. 'Re-Bordering the Peripheral Global North and Global South: Game of Drones, Immobilising Mobile Bodies and Decentring Perspectives on Drones in Border Policing'. In *Drones and Unmanned Aerial Systems*, edited by Aleš Završnik, 83–100. Cham: Springer International Publishing.

Mitsilegas, Valsamis. 2015. 'The Law of the Border and the Borders of Law. Rethinking Border Control from the Perspective of the Individual'. In *Rethinking Border Control for a Globalizing World: A Preferred Future*, edited by Leanne Weber, 15–31. New York: Routledge.

Molnar, Petra. 2019. 'Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective'. *Cambridge International Law Journal* 8 (2): 305–30. https://doi.org/10.4337/cilj.2019.02.07

Molnar, Petra. 2021. 'Robots and Refugees: The Human Rights Impacts of Artificial Intelligence and Automated Decision-Making in Migration'. In *Research Handbook* *on International Migration and Digital Technology*, edited by Marie McAuliffe. Cheltenham: Edward Elgar Publishing.

Molnar, Petra. 2022a. 'Surveillance Sovereignty: Migration Management Technologies and the Politics of Privatization'. In *Migration, Security, and Resistance: Global and Local Perspectives*, edited by Graham Hudson and Idil Atak. New York: Routledge.

Molnar, Petra. 2022b. 'Territorial and Digital Borders and Migrant Vulnerability Under a Pandemic Crisis'. In *Migration and Pandemics*, edited by Anna Triandafyllidou, 45–64. Cham: Springer International Publishing.

Monroy, Matthias. 2020. 'Drones for Frontex: Unmanned Migration Control at Europe's Borders'. *Statewatch*. https://www.statewatch.org/analyses/2020/drones-for-frontex-unmanned-migration-control-at-europe-s-borders/. 27 February 2020 (2024-09-01).

Monroy, Matthias. 2021. 'Border Drones (Part 1): Unmanned Surveillance of the EU's External Borders by Frontex'. *Security Architectures and Police Collaboration in the EU* (blog). 22 July 2021.

Monroy, Matthias. 2022a. 'Demands from EU Member States: Greece to Upgrade Borders with Helicopters, Drones, Police Dogs'. *Security Architectures and Police Collaboration in the EU* (blog). 3 March 2022.

Morozov, Evgeny. 2013. To Save Everything, Click Here: The Folly of Technological Solutionism. New York: PublicAffairs.

Monroy, Matthias. 2022b. 'Frontex Has Air Superiority'. Security Architectures and Police Collaboration in the EU (blog). 9 February 2022.

Mountz, Alison. 2020. *The Death of Asylum: Hidden Geographies of the Enforcement Archipelago*. Minneapolis: University of Minnesota Press.

Muižnieks, Nils. 2014. 'España No Puede Legalizar Lo Que Es Ilegal', Huffington Post. https://www.huffingtonpost.es/nils-muiznieks/espana-no-puede-legalizar_b_6294882.html. 10 December 2014 (2024-09-01).

Muller, Benjamin J. 2011. 'Risking It All at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation'. *Geopolitics* 16 (1): 91–106. https://doi.org/10.1080/14650045.2010.493775

Murray, Daragh. 2020. 'Using Human Rights Law to Inform States' Decisions to Deploy AI'. *AJIL Unbound* 114:158–62. https://doi.org/10.1017/aju.2020.30

Nagore Casas, María. 2019. 'The Instruments of Pre-Border Control in the EU: A New Source of Vulnerability for Asylum Seekers?' *Paix et Securite Internationales* 7, 161–98. https://doi.org/10.25267/Paix_secur_int.2019.i7.05

Napieralski, Antoni. 2019. 'Collecting Data at EU Smart Borders: Data Protection Challenges of the New Entry/Exit System'. *Zeitschrift für kritik - recht - gesellschaft* 1 (2): 199. https://doi.org/10.33196/juridikum201902019901

OHCHR. 1988. 'CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation'.

OHCHR. 2004. 'General Comment No. 31 The Nature of the General Legal Obligation Imposed on States Parties to the Covenant - CCPR/C/21/Rev.1/Add. 13'.

OHCHR. 2009. 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism - A/HRC/13/37'.

OHCHR. 2013. 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression - A/HRC/23/40'.

OHCHR. 2014. 'Report of the Office of the United Nations High Commissioner for Human Rights The Right to Privacy in the Digital Age - A/HRC/27/37'.B273

OHCHR. 2019. 'Report of the Special Rapporteur on the Right to Privacy - UN Doc A/HRC/40/63'.

Oliveira Martins, Bruno, and Maria Gabrielsen Jumbert. 2020. 'EU Border Technologies and the Co-Production of Security "Problems" and "Solutions"'. *Journal of Ethnic and Migration Studies* 48(6), 1430–1447. https://doi.org/10.1080/1369183X.2020.1851470

Ombudsman. 2021. 'Alleged Returns to Turkey of Aliens Who Had Entered Greece Seeking International Protection (Translated from Greek)'. https://www.synigoros.gr/?i=human-rights.el.files.791636. (2024-09-01).

Oso, Laura, Ana López-Sala, and Jacobo Muñoz-Comet. 2021. 'Migration Policies, Participation and the Political Construction of Migration in Spain'. *Migraciones. Publicación Del Instituto Universitario de Estudios Sobre Migraciones* 51:1–29. https://doi.org/10.14422/mig.i51y2021.001

Pagoudis, Georges. 2022. 'Complaints to the Supreme Court about Refoulements (Translated from Greek)'. *Efsyn*. https://www.efsyn.gr/ellada/dikaiosyni/332993_ston-areio-pago-kataggelies-gia-epanaproothiseis. 21 February 2022 (2024-09-01).

Pallister-Wilkins, Polly, Marieke de Goede, and Esme' Bosma, eds. 2020. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Abingdon; New York: Routledge.

Pallister-Wilkins, Polly. 2015. 'The Humanitarian Politics of European Border Policing: Frontex and Border Police in Evros'. *International Political Sociology* 9 (1): 53–69. https://doi.org/10.1111/ips.12076

Pannia, Paola, Federico Veronica, Andrea Terlizzi, and Silvia D'Amato. 2018. 'Comparative Report: Legal And Policy Framework Of Migration Governance'. *RESPOND Working Paper Series*. https://doi.org/10.5281/zenodo.1458945

Papatzani, Evangelia, Nadina Leivaditi, Aggelos Ilias, and Electra Petracou. 2020. 'Conflicting Conceptualisations of Europeanisation Greece Country Report'. *RESPOND Working Paper Series*. https://doi.org/10.5281/zenodo.4244374

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pauner Chulvi, Cristina. 2016. 'El Uso Emergente de Drones Civiles En España. Estatuto Jurídico e Impacto En El Derecho a La Protección de Datos'. *Revista de Derecho Político* 95: 83–115. https://doi.org/10.5944/rdp.95.2016.16233

Peoples, Columba, and Nick Vaughan-Williams. 2010. *Critical Security Studies: An Introduction*. Abingdon; New York: Routledge.

PESCO. 2021. 'PESCO Projects - Next Generation Small RPAS (NGSR)'. https://www.pesco.europa.eu/project/next-generation-small-rpas-ngsr/ (2024-09-01).

Petracou, Electra, Nadina Leivaditi, Giorgos Maris, Maria Margariti, Paraskevi Tsitsaraki, and Ilias Angelos. 2018. 'Greece Country Report: Legal & Policy Framework of Migration Governance'. *RESPOND Working Paper Series*. https://doi.org/10.5281/zenodo.1418569

Petridi, Corina. 2021. 'Greek Camps for Asylum Seekers to Introduce Partly Automated Surveillance Systems'. Algorithm Watch. https://algorithmwatch.org/en/greek-camps-surveillance/. 27 April 2021 (2024-09-01).

PICUM. 2020. 'How Do the New EU Regulations on Interoperability Lead to Discriminatory Policing?'. https://picum.org/wp-content/uploads/2020/04/

INFOGRAPHIC.-Interoperability-Systems-and-Access-to-Data_WEB_RGB.pdf. 1 June 2020 (2024-09-01).

Podkowik, Jan, Robert Rybski, and Marek Zubik. 2021. 'Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?' *International Journal of Constitutional Law* 19 (5): 1597–1631. https://doi.org/10.1093/icon/moab132

PorCausa. 2020a. 'Industra Del Control Migratorio'. https://porcausa.org/somos-lo-que-hacemos/industria-del-control-migratorio/. 1 June 2020 (2024-09-01).

PorCausa. 2020b. 'Migration Control Industry - Who Are the Paymasters?' https://porcausa.org/wp-content/uploads/2020/07/Migration-Control-Industry-1-Who-are-the-paymasters.pdf. 1 January 2020 (2024-09-01).

Prakken d'Oliveira Human Rights Lawyers. 2021. 'EU Agency Frontex Charged with Illegal Pushbacks'. https://www.prakkendoliveira.nl/en/news/news-2021/eu-agency-frontex-charged-with-illegal-pushbacks. 20 October 2021 (2024-09-01).

ProAsyl. 2013. 'Pushed Back - Systematic Human Rights Violations against Refugees in the Aegean Sea and at the Greek-Turkish Land Border'. https://www.proasyl.de/en/material/pushed-back-systematic-human-rights-violations-against-refugees-in-the-aegean-sea-and-the-greek-turkish-land-border/. 1 November 2013 (2024-09-01).

Quinn, Paul, and Gianclaudio Malgieri. 2021. 'The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework'. *German Law Journal* 22 (8): 1583–1612. https://doi.org/10.1017/glj.2021.79

Ranger Project. 2018. 'Ranger H2020-700478 - The Legal Framework of Maritime Surveillance'. https://www.ranger-project.eu/wp-content/uploads/2018/03/D3.3.pdf. 5 June 2017 (2024-09-01).

Reece, Jones, and Johnson Corey. 2016. 'Border Militarisation and the Re-articulation of Sovereignty'. *Transactions of the Institute of British Geographers* 41 (2): 187–200. https://doi.org/10.1111/tran.12115

Reekum, Rogier van. 2019. 'Patrols, Records and Pictures: Demonstrations of Europe in the Midst of Migration's Crisis'. *Environment and Planning D: Society and Space* 37 (4): 625–43. https://doi.org/10.1177/0263775818792269

Region of Western Greece. 2020. 'Drones and Other Modern Equipment in the Security Forces from the Region of Western Greece' (translated from Greek). https://www.pde.gov.gr/gr/enimerosi/deltia-tupou/item/13763-drones-kai-allos-sugxronos-exoplismos-sta-somata-asfaleias-apo-tin-perifereia-dytikis-elladas-epixeirisiakos-kombos-politikis-prostasias-to-aerodromio-toy-epitalioy.html. 18 June 2020 (2024-09-01).

ROBORDER. 2021. 'Roborder - Aims & Objectives'. https://roborder.eu/the-project/aims-objectives/. 1 January 2021 (2024-09-01).

Rumford, Chris. 2008. 'Introduction: Citizens and Borderwork in Europe'. *Space and Polity* 12 (1): 1–12. https://doi.org/10.1080/13562570801969333

Sandberg, Marie, Luca Rossi, Vasilis Galis, and Martin Bak Jørgensen, eds. 2022. *Research Methodologies and Ethical Challenges in Digital Migration Studies: Caring for (Big) Data?*. Cham: Palgrave Macmillan.

Sandkühler, Hans Jörg. 2015. 'La Dignité Humaine et La Transformation Des Droits Moraux En Droit Positif'. In *Le Respect de La Dignité Humaine*, edited by Antônio Augusto Cançado Trindade and César Barros Leal, 67–102. Fortaleza: Expressão Gráfica e Editora.

Sardo, Alessio. 2021. 'Border Walls, Pushbacks, and the Prohibition of Collective Expulsions: The Case of N.D. and N.T. v. Spain'. *European Journal of Migration and Law* 23 (3): 308–31. https://doi.org/10.1163/15718166-12340104

Scarciglia, Roberto. 2015. 'Comparative Methodology and Pluralism in Legal Comparison in a Global Age'. *Beijing Law Review* 6 (1): 42–48. https://doi.org/10.4236/blr.2015.61006

Scheel, Stephan, Evelyn Ruppert, and Funda Ustek-Spilda. 2019a. 'Enacting Migration through Data Practices'. *Environment and Planning D: Society and Space* 37 (4): 579–88. https://doi.org/10.1177/0263775819865791

Scheel, Stephan. 2019. *Autonomy of Migration? Appropriating Mobility within Biometric Border Regimes*. London; New York: Routledge.

Schweller, Randall L. 2014. *Maxwell's Demon and the Golden Apple: Global Discord in the New Millennium*. Baltimore: The Johns Hopkins University Press.

Scudieri, Laura. 2020. 'Migranti e Cyber-Soluzionismo: Le Nuove Rotte Del Digital Divide'. In *I Soggetti Vulnerabili Nei Processi Migratori: La Protezione Internazionale Tra Teoria e Prassi*, edited by Isabel Fanlo Cortés and Daniele Ferrari. Torino: G. Giappichelli.

SESAR. 2016. 'European Drones Outlook Study Unlocking the Value for Europe'. https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf. 1 November 2016 (2024-09-01).

Simeon, James C. 2019. 'What Is the Future of Non-Refoulement in International Refugee Law?' In *Research Handbook on International Refugee Law*, edited by Satvinder Juss, 183–206. Cheltenham: Edward Elgar Publishing.

Słomczyńska, Irma, and Paweł Frankowski. 2016. 'Patrolling Power Europe: The Role of Satellite Observation in EU Border Management'. In *EU Borders and Shifting Internal Security*, edited by Raphael Bossong and Helena Carrapico, 65–80. Cham: Springer International Publishing.

Spanish Data Protection Agency. 2019a. 'Drones and Data Protection'. https://www.aepd.es/guides/drones-and-data-protection.pdf. 1 January 2019 (2024-09-01).

Spanish Data Protection Agency. 2019b. 'Gestión Del Riesgo y Evaluación de Impacto En Tratamientos de Datos Personales'. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf. 1 January 2019 (2024-09-01).

Spanish Data Protection Agency. 2019c. 'Guía Sobre El Uso de Videocámaras Para Seguridad y Otras Finalidades'.https://www.aepd.es/guias/guia-videovigilancia.pdf. 1 January 2019 (2024-09-01).

Spanish Data Protection Agency. 2019d. 'Informe Juridico RGPD y Drones'. https://www.aepd.es/documento/informe-juridico-rgpd-drones.pdf. 1 January 2019 (2024-09-01).

Spanish Ministry of the Interior. 2012. 'Ex-Post Evaluation Report on the Results and Impacts of Actions Co-Financed by the External Borders Fund Annual Programmes 2007 to 2010 (Report Set out in Article 52(2) (B) of Decision No 574/2007/Ec)'.

Spanish Ministry of the Interior. 2013. 'Decisión de La Comisión Por La Que Se Aprueba, Para España, El Programa Anual 2013 Del Fondo Para Las Fronteras Exteriores y La Cofinanciación Para 2013 Con Cargo a Dicho Fondo - Programa Anual 2013'.

Spanish Refugee Aid Commission. 2017. 'Refugees and Migrants in Spain: The Invisible Walls behind the Southern Border'. https://www.cear.es/wp-content/uploads/2018/03/REPORT-MUROS-FRONTERA-SUR.pdf. 1 January 2017 (2024-09-01).

Spanish Refugee Aid Commission. 2021. 'Informe 2021: Las Personas Refugiadas En España y Europa'. https://www.cear.es/wp-content/uploads/2021/06/Informe-Anual-CEAR-2021.pdf. 1 December 2021 (2024-09-01).

Spanish State Secretariat for Security. 2018. 'Lista de Proyectos Presentados En La Cuenta Financiera 2018 Del FSI'.

Spanish State Secretariat for Security. 2019. 'Lista de Proyectos Presentados En La Cuenta Financiera Del FSI 2019'.

Spanish State Secretariat for Security. 2020. 'Lista de Proyectos Presentados En La Cuenta Financiera Del FSI 2020'.

Statewatch and PICUM. 2019. 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status'. https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf. 14 November 2019 (2024-09-01).

Statewatch. 2013. 'EU: Field Testing: CLOSEYE Project Puts Drones over the Mediterranean'. https://www.statewatch.org/news/2013/may/eu-field-testing-closeye-project-puts-drones-over-the-mediterranean/. 10 May 2013 (2024-09-01).

Statewatch. 2019. 'Aid, Border Security and EU-Morocco Cooperation on Migration Control'. https://www.statewatch.org/media/documents/analyses/no-347-eu-morocco-aid-border-security.pdf. 1 November 2019 (2024-09-01).

Statewatch. 2021a. 'Greece: The New Hotspots and the Prevention of "Primary Flows": A Human Rights Disaster'. https://www.statewatch.org/analyses/2021/greece-the-new-hotspots-and-the-prevention-of-primary-flows-a-human-rights-disaster/. 13 December 2021 (2024-09-01).

Statewatch. 2021b. '"Next Generation" Armed Drone with Police Potential Tipped for EU Financial Backing'. https://www.statewatch.org/news/2021/october/next-generation-armed-drone-with-police-potential-tipped-for-eu-financial-backing/. 4 October 2021 (2024-09-01).

Stierl, Maurice, and Deanna Dadusc. 2021. 'The "Covid Excuse": EUropean Border Violence in the Mediterranean Sea'. *Ethnic and Racial Studies* 45(8), 1453–1474. https://doi.org/10.1080/01419870.2021.1977367.

Suchman, Lucy, Karolina Follis, and Jutta Weber. 2017. 'Tracking and Targeting: Sociotechnologies of (In)Security'. *Science, Technology, & Human Values* 42 (6): 983–1002. https://doi.org/10.1177/0162243917731524

Tan, Nikolas Feith, and Thomas Gammeltoft-Hansen. 2020. 'A Topographical Approach to Accountability for Human Rights Violations in Migration Control'. *German Law Journal* 21 (3): 335–54. https://doi.org/10.1017/glj.2020.31

Tazzioli, Martina, and William Walters. 2016. 'The Sight of Migration: Governmentality, Visibility and Europe's Contested Borders'. *Global Society* 30 (3): 445–64. https://doi.org/10.1080/13600826.2016.1173018.

Tazzioli, Martina. 2018. 'Spy, Track and Archive: The Temporality of Visibility in Eurosur and Jora'. *Security Dialogue* 49 (4): 272–88. https://doi.org/10.1177/0967010618769812

Tazzioli, Martina. 2021. '"Choking without Killing": Opacity and the Grey Area of Migration Governmentality'. *Political Geography* 89. https://doi.org/10.1016/j.polgeo.2021.102412.

Testa, Gonzalo, and Gabriela Sánchez. 2021. 'La Justicia Frena La Devolución Desde Ceuta de Nueve Menores Marroquíes', *El Diario.es*. https://www.eldiario.es/desalambre/solicitan-nuevo-juzgado-paralizacion-devoluciones-menores-ceuta-interior-ejecuta-cuarta_1_8222823.html. 16 August 2021 (2024-09-01).

Testa, Gonzalo. 2017. 'Así Funcionan Los Drones Que El Gobierno Planea Usar Para Vigilar La Frontera Española'. *El Diario.Es*. https://www.eldiario.es/desalambre/gobierno-utilizar-drones-vigilar-ceuta_1_3566296.html. 24 February 2017 (2024-09-01).

Third Committee of the General Assembly of the United Nations. 2016. 'Third Committee Agenda Item 68 (b) Promotion and Protection of Human Rights:

Human Rights Questions, Including Alternative Approaches for Improving the Effective Enjoyment of Human Rights and Fundamental Freedoms. The Right to Privacy in the Digital Age - A/C.3/71/L.39/Rev.1'.

Tholen, Berry. 2010. 'The Changing Border: Developments and Risks in Border Control Management of Western Countries'. *International Review of Administrative Sciences* 76 (2): 259–78. https://doi.org/10.1177/0020852309365673

Topak, Özgün E, and Luna Vives. 2018. 'A Comparative Analysis of Migration Control Strategies along the Western and Eastern Mediterranean Routes: Sovereign Interventions through Militarization and Deportation'. *Migration Studies*, 8 (1): 66–89. https://doi.org/10.1093/migration/mny029

Topak, Özgün E. 2014. 'The Biopolitical Border in Practice: Surveillance and Death at the Greece-Turkey Borderzones'. *Environment and Planning D: Society and Space* 32 (5): 815–33. https://doi.org/10.1068/d13031p

Topak, Özgün E. 2021. 'Border Violence and Migrant Subjectivities'. *Geopolitics* 26 (3): 791–816. https://doi.org/10.1080/14650045.2019.1626828

Trevisanut, Seline. 2014. 'The Principle of Non-Refoulement and the De-Territorialization of Border Control at Sea'. *Leiden Journal of International Law* 27 (3): 661–75. https://doi.org/10.1017/S0922156514000259

UN Office of the High Commissioner for Human Rights. 2012. 'UN Special Rapporteur on the Human Rights of Migrants Concludes the Fourth and Last Country Visit in His Regional Study on the Human Rights of Migrants at the Borders of the European Union: Greece'.

UN Office of the High Commissioner for Human Rights. 2021. 'Información Recibida En Relación Con Presuntas Devoluciones En Frontera o "Pushbacks" de Personas Migrantes, Incluyendo Adolescentes Migrantes, En Las Fronteras de España Con Marruecos En Melilla. ESP 3/2021'.

UNHCR. 2019. 'UNHCR Urges Greece to Strengthen Safeguards in Draft Asylum Law'. https://www.unhcr.org/gr/en/13170-unhcr-urges-greece-to-strengthen-safeguards-in-draft-asylum-law.html. 24 October 2019 (2024-09-01).

Val Garijo, Fernando. 2020. 'Drones, Border Surveillance and the Protection of Human Rights in the European Union'. *Public Security and Public Order* 25. https://doi.org/10.13165/PSPO-20-25-09

Vavoula, Niovi. 2021. 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism'. *European Journal of Migration and Law* 23 (4): 457–84.

Wall, Tyler, and Torin Monahan. 2011. 'Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes'. *Theoretical Criminology* 15 (3): 239–54. https://doi.org/10.1177/1362480610396650

Wallis, Emma. 2022. 'Digital Borders: EU Increases Use of Technology to Monitor Migration'. *InfoMigrants*. https://www.infomigrants.net/en/post/38478/digital-borders-eu-increases-use-of-technology-to-monitor-migration. 18 February 2022 (2024-09-01).

Walters, William. 2016. 'Live Governance, Borders, and the Time–Space of the Situation: EUROSUR and the Genealogy of Bordering in Europe'. *Comparative European Politics* 15 (5): 794–817. https://doi.org/10.1057/s41295-016-0083-5

Weber, Leanne. 2006. 'The Shifting Frontiers of Migration Control'. In *Borders, Mobility and Technologies of Control*, edited by Sharon Pickering and Leanne Weber, 21–43. Dordrecht: Springer Netherlands.

Index of Names

Achiume T. 114-115
Akkerman M. 20, 70
Amoore L. 14, 16, 25, 52
Andersson R. 38
Aradau C. 14, 40, 93, 123
Bachiller López C. 65
Balibar É. 12, 123
Barak A. 93
Beduschi A. 92, 109, 116
Benjamin R. 127
Bigo D. 14-15, 20, 25, 32, 99, 116
Broeders D. 14, 16, 122
Brouwer E. 103-104, 108, 111, 116
Carling J. 68, 70, 74-76
Carrera S. 46, 118
Casas-Cortes M. 71, 78
Covadonga B. 65
Csernatoni R. 14-15, 28, 33, 38, 40
De Genova N. 90
Dijstelbloem H. 14-16, 27-28, 31-32, 53, 92, 96, 122
Ellebrecht S. 74
Favilli C. 49
Fisher D. 77-78
Follis K. 12, 15, 29, 32-36
Gammeltoft-Hansen T. 88, 91, 97, 99
Giuffré M. 14, 97
Glouftsios G. 8, 15-16, 27, 29, 34, 36-37, 39
Hamlin R. 97
Hildebrandt M. 96, 114
Jeandesboz J. 14, 31, 38
Johansson Y. 63
Jumbert M. G. 21, 35-36, 74
Koca B. T. 48-49
Latonero M. 25, 28, 39
Leese M. 11, 14
Lemberg-Pedersen M. 43
Leurs K. 14, 16
Loukinas P. 28, 33-36, 38-40, 53
Malgieri G. 105-106
Marin L. 14-15, 32-36, 38, 55, 79, 95-96, 100, 110
Mezzadra S. 23
Mijatović D. 63, 94
Mitsilegas V. 119
Molnar P. 18, 45-46, 48, 90-91, 95, 100, 115-116, 123
Monroy M. 11, 32-33, 37, 48, 52-54
Moreno-Lax V. 14, 97
Neilson B. 23
Oliveira Martins B. 21, 35
Pallister-Wilkins P. 17, 90, 122

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, © 2025 Author(s), CC BY 4.0, published by Firenze University Press, ISBN 979-12-215-0577-1, DOI 10.36253/979-12-215-0577-1

Quinn P. 105-106
Scheel S. 11, 14, 16, 25
Scudieri L. 126
Simeon J. C. 97-98
Tazzioli M. 16, 18, 29, 31-32, 38-39
Topak Ö. 13, 19, 47-48, 52, 65, 93
Trevisanut S. 97
Vavoula N. 112
von der Leyen U. 46, 112
Walters W. 16, 28, 31-32, 38-40

PREMIO CESARE ALFIERI «CUM LAUDE»

TITOLI PUBBLICATI

1. Antonio Sparacino, *Considerazioni sul credito di ultima istanza all'indomani della crisi. Le città europee, evoluzione e futuro*, 2013
2. Chiara Dara, *Gross violationsdei diritti delle donne in Messico. la risposta del diritto internazionale*, 2014
3. Giulia Mannucci, *Il conflitto di giurisdizione tra Italia e India nel casoEnrica lexie: quale ruolo per il diritto internazionale?*, 2014
4. Marzio Di Feo, *Automi, realtà virtuale e formiche. Un'analisi della complessità del fenomeno bellico spaziale*, 2016
5. Francesca Pannozzo, *Dal Terzo al Primo Mondo. Singapore: un esperimento di successo*, 2018
6. Michele Gerli, *Beyond Nuclear Ambiguity. The Iranian Nuclear Crisis and the Joint Comprehensive Plan of Action*, 2019
7. Karina Galytska, *European-Russian Energy Relations: from Dependence to Interdependence*, 2021
8. Guido Panzano, *Ethnic Domination in Deeply Divided Places. The Hegemonic State in Israel and Estonia*, 2021
9. Andrea Cellai, *La traiettoria storica dell'Etiopia di Meles Zenawi. Fra democrazia rivoluzionaria, federalismo etnico e Stato sviluppista*, 2022
10. Alessandro Ravasio, *The Lay Preacher. Il laburismo di Tony Blair*, 2023
11. Alice Fill, *Digital Patrolling. Emerging Bordering Practices around Europe*, 2025

PREMIO CESARE ALFIERI CUM LAUDE

The digitalisation of border security is reshaping migration governance across Europe and beyond, transforming border areas through the deployment of advanced surveillance technologies. Greece and Spain, as critical gateways, have become testing grounds for drones and remote monitoring systems designed to enforce borders from afar. In a walk down extreme border zones, this book delves into the rise of digital patrolling, a key facet of this transformation, offering a multidisciplinary analysis grounded in human rights law, comparative migration law, and critical migration studies. By exploring how digital patrolling impacts the ‘filtering’ of human mobility, it uncovers the legal and societal fallouts of Europe’s shifting borders, highlighting the tension between security measures and fundamental rights.

ALICE FILL is a PhD student in International Relations and International Law at the École Normale Supérieure (Chair in Geopolitics of Risk) in Paris, and at the University of Roma Tre (Department of Law). She is also a fellow at the Institut Convergences Migrations (CNRS).

ISSN 2612-8063 (print)
ISSN 2704-5730 (online)
ISBN 979-12-215-0576-4 (Print)
ISBN 979-12-215-0577-1 (PDF)
ISBN 979-12-215-0578-8 (ePUB)
ISBN 979-12-215-0579-5 (XML)
DOI 10.36253/979-12-215-0577-1
www.fupress.com