Morocco's Governance of Cities and Borders: AI-Enhanced Surveillance, Facial Recognition, and Human Rights

Bergh, S.I.; Cherrat, I.; Colin, F.; Wagner, B.; Matulionyte, R.; Zalnieriute, M.

19

Morocco's Governance of Cities and Borders

AI-Enhanced Surveillance, Facial Recognition, and Human Rights

Sylvia I. Bergh, Issam Cherrat, Francesco Colin, Katharina Natter, and Ben Wagner

19.1 INTRODUCTION*

Owing to advances around artificial intelligence (AI), such as computer vision and facial recognition, digital surveillance technologies are becoming cheaper and easier to use as everyday tools of governance worldwide.[1] Typically developed by companies and governments in the Global North and tested in the Global South or on the 'periphery' of powerful actors,[2] they are becoming key tools of governance in both democratic and authoritarian contexts.[3] As the AI Global Surveillance Index

* We are grateful to the former Centre of Expertise on Global Governance at The Hague University of Applied Sciences and the Institute of Security and Global Affairs at Leiden University for the seed grant that made this research possible.

1 Louise Eley and Ben Rampton, 'Everyday surveillance, Goffman, and unfocused interaction' (2020) 18 *Surveillance & Society* 199–215, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13346; David Lyon, *Theorizing Surveillance: The Panopticon and Beyond* (William Publishing, 2006); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001); Rocco Bellanova, Kristina Irion, Katja Lindskov Jacobsen, Francesco Ragazzi, Rune Saugmann, Lucy Suchman, Jesus Benito-Picazo, Enrique Domínguez, Esteban J. Palomo, and Ezequiel López-Rubio, 'Toward a critique of algorithmic violence' (2021) 15 *International Political Sociology* 121–150. https://academic.oup.com/ips/article/15/1/121/6170592; Jesus Benito-Picazo et al., 'Deep learning-based video surveillance system managed by low cost hardware and panoramic cameras' (2020) 27 *Integrated Computer-Aided Engineering* 373–387, www.medra.org/servlet/aliasResolver?alias=iospress&doi=10.3233/ICA-200632; Eley and Rampton, 'Everyday surveillance'; Francesco Ragazzi, 'Security Vision: The algorithmic security politics of computer vision' (2021), www.securityvision.io/.

2 Jozef Andraško, Matúš Mesarčík, and Ondrej Hamuľák, 'The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU Legal Framework' (2021) 36 *AI & SOCIETY* 623–636, https://link.springer.com/10.1007/s00146-020-01125-5; Steve Gold, 'Military biometrics on the frontline' (2010) 2010(10) *Biometric Technology Today* 7–9, https://linkinghub.elsevier.com/retrieve/pii/S0969476510702071; Josh Chin and Clément Bürge, 'Twelve days in Xinjiang: How China's surveillance state overwhelms daily life' (20 December 2017), *Wall Street Journal*, www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

3 Taylor C. Boas, 'Weaving the authoritarian web: The control of internet use in nondemocratic regimes' in John Zysman and Abraham Newman (eds.), *How Revolutionary Was the Digital*

shows,[4] countries with authoritarian systems and low levels of political rights are investing particularly heavily in AI surveillance techniques such as advanced analytic systems, facial recognition cameras, and sophisticated monitoring capabilities.[5]

AI surveillance offers governments two major capabilities. First, it allows regimes to automate many tracking and monitoring functions formerly delegated to human operators. This brings cost efficiencies, decreases reliance on security forces, and over-rides potential principal–agent loyalty problems.[6] Second, as AI systems never tire or fatigue, AI technology can cast a much wider surveillance net than traditional control methods. As Feldstein points out, 'this creates a substantial "chilling effect" even without resorting to physical violence as citizens never know if an automated bot is monitoring their text messages, reading their social media posts, or geotracking their movements around town'.[7]

Some scholars have observed the radical interdependence of the global AI development ecosystem, as only a few countries can afford to build their own local AI ecosystems.[8] For example, China is a major supplier of AI surveillance, with Huawei

Revolution? National Responses, Market Transitions, and Global Technology (Stanford University Press, 2006), pp. 373–390; Bert Hoffmann, 'Civil society in the digital age: How the internet changes state–society relations in authoritarian regimes. The case of Cuba' in Francesco Cavatorta (ed.), *Civil Society Activism under Authoritarian Rule: A Comparative Perspective* (Routledge, 2012), pp. 219–244; Lydia Khalil, 'Digital authoritarianism, China and COVID' (2 November 2020), Lowy Institute, www.lowyinstitute.org/publications/digital-authoritarianism-china-covid; Justin Sherman, 'Digital authoritarianism and implications for US national security' (2021) 6(1) *The Cyber Defense Review* 107–118, www.jstor.org/stable/2699411; Ben Wagner, 'Whose politics? Whose rights? Transparency, capture and dual-use export controls' (2021) 31 *Security and Human Rights* 35–46, https://brill.com/view/journals/shrs/31/1-4/article-p35_35.xml.

4 Steven Feldstein, 'The global expansion of AI surveillance' (17 September 2019), Carnegie Endowment for International Peace, Paper, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

5 See ibid., pp. 18–19, for details on the technologies themselves. Suffice it to state here that facial recognition 'is a biometric technology that uses cameras – both video or still images – to match stored or live footage of individuals with images from a database. […] They can scan distinctive facial features in order to create detailed biometric maps of individuals without obtaining consent. Often facial recognition surveillance cameras are mobile and concealable.' However, advanced video surveillance and facial recognition cameras could not function without cloud computing capabilities. If video surveillance is the 'eyes' then cloud services are the 'brains' that connect cameras and hardware to the cloud computing models via 5G networks. However, as cloud computing in isolation is not inherently oriented toward surveillance, these secondary technologies are categorised as 'enabling technologies': ibid., p. 21.

6 Ibid.

7 Ibid., p. 13.

8 Roxana Akhmetova and Erin Harris, 'Politics of technology: The use of artificial intelligence by US and Canadian immigration agencies and their impacts on human rights' in Emre E. Korkmaz (ed.), *Digital Identity, Virtual Borders and Social Media* (Edward Elgar Publishing, 2021), pp. 52–72, www.elgaronline.com/view/edcoll/9781789909142/9781789909142.00008.xml; Ausma Bernot, 'Transnational state-corporate symbiosis of public security: China's exports of surveillance technologies' (2021) 10(2) *International Journal for Crime, Justice and Social Democracy* 159–173, www.crimejusticejournal.com/article/view/1908; Peter Dauvergne, 'The globalization of artificial intelligence: Consequences for the politics of environmentalism' (2021) 18 *Globalizations* 285–299. www.tandfonline.com/doi/full/10.1080/14747731.2020.1785670; Orabile Mudongo, 'Africa's expansion of AI surveillance – Regional gaps and key trends' (26 February 2021), Briefing Paper, Africa Portal, www.africaportal.org/publications/africas-expansion-ai-surveillance-regional-gaps-and-key-trends/; Ben

alone providing technology to at least fifty countries. France, Germany, Japan, and the United States are also major players in this sector.[9] As a consequence, the governance challenges around AI-enhanced technologies are inherently trans-national.

Indeed, the rise of AI accentuates several existing challenges for human rights law around (digital) technology. For example, such technology obscures the identity of the violator and makes violations themselves more invisible. This makes it much harder for citizens to hold duty bearers accountable.[10] It is also becoming much less clear whom citizens should try to hold to account in the first place. The current framework for addressing human rights harms inflicted by business entities is built on the distinction between public authority exercised by the state (which gives rise to a binding obligation to respect and protect rights) and private authority exercised by a company (which gives rise to a moral responsibility to respect rights). However, the distinction between the public and private spheres is becoming increasingly blurred, and as a result, it is less clear how human rights law is applicable.[11] Instead, citizens must rely on states to take seriously their duty to protect individuals from harms by non-state actors, such as requiring private companies to institutionalise the practice of technology risk and impact assessments.[12] It is clear that this is a formidable challenge in liberal democratic countries, let alone in authoritarian ones such as Morocco.

In this chapter, we focus on the role played by AI-enhanced surveillance tools in Morocco's governance of cities and borders. We ask to what extent AI technologies are deployed in Morocco, and how they could reshape existing modes of public governance. We address these questions in two areas: urban surveillance and the control of migration at the Moroccan–Spanish border. We focus on the use of facial recognition technologies (FRT) in AI-enhanced cameras in particular, but we also address other technologies and other uses of AI, following a pragmatic approach that investigated where it was possible to access data. Indeed, AI surveillance is not a stand-alone instrument of repression, but complements existing forms of repression. As Feldstein observes, 'it forms part of a suite of digital repression tools – information and communications technologies used to surveil, intimidate, coerce, and harass opponents in order to inflict a penalty on a target and deter specific activities or beliefs that challenge the state'.[13]

Wagner, 'After the Arab spring: New paths for human rights and the internet in European foreign policy' (July 2012), Briefing Paper, European Parliament: Directorate-General for External Policies, European Union, www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT%282012%29457102_EN.pdf; Ben Wagner, 'Push-button-autocracy in Tunisia: Analysing the role of internet infrastructure, institutions and international markets in creating a Tunisian censorship regime' (2012) 36(6) *Telecommunications Policy* 484–492, https://linkinghub.elsevier.com/retrieve/pii/S0308596112000675.

[9] Feldstein, 'The global expansion of AI surveillance', p. 8.

[10] Molly K. Land and Jay D. Aronson, 'Human rights and technology: New challenges for justice and accountability' (2020) 16(1) *Annual Review of Law and Social Science* 223–240, www.annualreviews.org/doi/10.1146/annurev-lawsocsci-060220-081955.

[11] Ibid., p. 226.

[12] Ibid., pp. 226, 235.

[13] Feldstein, 'The global expansion of AI surveillance', p. 16.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

The chapter is structured as follows. First, we outline the legal framework and governance context around Morocco's use of AI technologies for urban and border surveillance. We then discuss our methodological approach, including some of the key limitations we faced during the research, before sharing our findings with respect to the use of FRT in the governance of cities and borders, respectively. Subsequently, we discuss AI-enhanced surveillance as an intrinsically transnational challenge in which private interests of economic gain and public interests of national security collide with citizens' human rights across the Global North/Global South divide. We also reflect on the challenges and opportunities of monitoring human rights in the face of increasing deployment of AI-enhanced technologies in authoritarian governance.

19.2 THE LEGAL FRAMEWORK AND GOVERNANCE CONTEXT IN MOROCCO

The Moroccan governance system has been described as 'an entrenched neo-authoritarian system'.[14] Over the past decades, the monarchy has repeatedly weakened the political opposition by co-opting major parties into government. Human rights violations, lack of press freedom, and the harassment of human rights non-governmental organisations (NGOs) persist. However, while these deficiencies have attracted the attention of human rights organisations and press freedom watchdogs, they have not been properly taken up by inter-governmental actors. Quite the contrary: in the wider regional context, Morocco's political stability has been viewed as an asset and is likely to become even more valuable (to the EU and United States), further insulating the regime from critiques of its civil and human rights records.[15]

At the same time, Morocco is one of the highest performers in e-governance in Africa.[16] Morocco has more than 27 million internet users, or 75 per cent of its population,[17] and ranks high in the UN's 2016 E-Government Survey in terms of e-participation, e-consultation and online service delivery as well as in its E-Government Development Index, a composite indicator used to measure the willingness and capacity of national administrations to use information and communications technologies to deliver public services. Indeed, Morocco's new development model focusses on consolidating technological added value, and public administrations are increasingly making use of algorithms in online public services.[18] The combination of authoritarian rule and advanced use of e-government

[14] Bertelsmann Stiftung, 'BTI 2022 country report – Morocco' (2022), p. 38.
[15] Ibid.
[16] Privacy International, 'State of privacy Morocco' (26 January 2019), https://privacyinternational.org/state-privacy/1007/state-privacy-morocco.
[17] Mounir Bensalah, 'Toward an ethical code of AI and human rights in Morocco' (2021) 1(2) *Arribat – International Journal of Human Rights* 187–203.
[18] Ibid.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

makes Morocco a particularly interesting case to study the role of AI in technologies in public governance.

At first glance, Morocco's legal framework around privacy seems robust. The constitution contains an explicit protection of the right to privacy (Art. 24), there is a data protection law (Law n° 09-08, promulgated in February 2009), and a data protection agency, the *Commission nationale de contrôle de la protection des données à caractère personnel* (CNDP). In addition, Morocco is a signatory of a number of treaties with privacy implications, including the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* and its additional Protocols.[19] Furthermore, in 2018, Morocco joined the Open Government Partnership, an inter-governmental organisation promoting government transparency and citizen participation, and in 2021 it submitted its second two-year action plan, including twenty-two commitments that span a wide range of participatory, accountable, and transparent governance areas.[20] Since 2010, the security sector has also been put on a clearer legal footing: private security was regulated, state security services were given statutes and mandated to better respect human rights, thanks in no small measure to the efforts of human rights organisations.[21]

Yet, as Hagmann[22] points out, some laws still lack implementation decrees. In addition, clientelist and political interests continue to influence whether and how penal provisions are implemented, human rights abuses investigated and reprimanded, or demonstrations and NGOs authorised and banned. Indeed, Privacy International notes that 'there remains vast grey areas regarding the discretionary powers offered to judges and intelligence agencies' when it comes to rules around legitimate breaches of individual privacy.[23] This situation is worsened by the fact that the judiciary is not independent and that public scrutiny and democratic oversight over the work of intelligence services is lacking. In addition, the law on the protection of personal data (09–08) does not cover those data collected in the interest of national defence or the interior or exterior security of the state.[24]

Against the backdrop of this legal framework, technological tools are already integrated in everyday authoritarian governance and surveillance, especially at urban level. Traditionally based on a wide network of informants (car guards, local shop owners, informal vendors and beggars, etc.), mass surveillance is evolving through

[19] Privacy International, 'State of privacy Morocco'.

[20] See www.opengovpartnership.org/members/morocco/.

[21] Jonas Hagmann, 'Globalizing control research: The politics of urban security in and beyond the Alaouite kingdom of Morocco' (2021) 6(4) *Journal of Global Security Studies* 1–23, https://academic.oup.com/jogss/article/doi/10.1093/jogss/ogab004/6208882; Privacy International, 'State of privacy Morocco'.

[22] Hagmann, 'Globalizing control research'.

[23] Privacy International, 'State of privacy Morocco'.

[24] Anaïs Lefébure and Mehdi Mahmoud, 'De la "smart" à la "safe" city, au détriment de nos vies privées?' (2 July 2021), *Tel Quel*, https://telquel.ma/2021/07/02/de-la-smart-a-la-safe-city-au-detriment-de-nos-vies-privees_1727757.

the use of technology. Phone tapping is common for listening to conversations, and more refined tools for surveillance have also been employed. For example, during the regional and local elections of September 2015, 30,000 mobile phone lines of candidates and regional or provincial party officials, in addition to local government officials and others, were reportedly tapped at the request of the Ministry of Interior.[25] Another example is the Moroccan government's use, at least since October 2017, of Pegasus spyware produced by the Israeli firm NSO Group, to surveil and attack human rights defenders.[26] The general impression is that these technologies have allowed the bringing about of a more 'surgical' approach to the repression of dissent, one that systematically targets key figures,[27] instead of the population as a whole.

Israeli companies are not the only provider of surveillance technology to Moroccan authorities. In 2015, there was a leak confirming that Morocco had bought the technology of Italian spyware company Hacking Team.[28] In June 2017, an investigation by BBC Arabic and the Danish newspaper *Dagbladet* revealed that UK defence firm BAE Systems had sold mass surveillance technologies – called Evident – through its Danish subsidiary ETI to six Middle Eastern governments, including Morocco.[29] There are also concerns that the European Neighbourhood Instrument may have been used to fund the training of Moroccan authorities in 'telephone tapping and video recordings' and 'special investigation techniques for electronic surveillance'.[30] More recently, there have been plausible but unconfirmed reports that the Moroccan police used COVID-19 mobile passport application check-ins to

[25] Privacy International, 'State of privacy Morocco'.

[26] Amnesty International, 'Morocco: Human rights defenders targeted with NSO Group's spyware' (10 October 2019), www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/; Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, 'HIDE AND SEEK: Tracking NSO Group's Pegasus spyware to operations in 45 countries' (18 September 2018), The Citizen Lab, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Bethan McKernan, 'Emmanuel Macron "pushes for Israeli inquiry" into NSO spyware concerns' (25 July 2021), *The Guardian*, www.theguardian.com/world/2021/jul/25/emmanuel-macron-pushes-for-israeli-inquiry-into-nso-spyware-concerns. 'Once installed on a phone, the [Pegasus] software can extract all of the data that is already on the device, such as text messages, contacts, GPS location, email and browser history. It can additionally create new data by using the phone's microphone and camera to record the user's surroundings and ambient sounds.' N. Hopkins and D. Sabbagh, 'WhatsApp spyware attack was attempt to hack human rights data, says lawyer' (14 May 2019), *The Guardian*, www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate, cited in Land and Aronson, 'Human rights and technology', p. 228.

[27] Such as Mâati Monjib, Hicham Mansouri, Taoufik Bouachrine, Souleiman Raissouni, and Omar Radi, *Marruecos y el cambio de ciclo: en busca de un nuevo pacto social y de nuevas legitimidades*, ed. Alfonso Casani and Beatriz Tomé-Alonso (Fundacionalternativas, 2021), p. 11, https://.org/wp-content/uploads/2022/07/115f8026034f62907a4d1382c8788886.pdf.

[28] Privacy International, 'Eight things we know so far from the Hacking Team hack' (9 July 2015), https://privacyinternational.org/news-analysis/1395/eight-things-we-know-so-far-hacking-team-hack.

[29] Privacy International, 'State of privacy Morocco'.

[30] Parliamentary question dated 19 November 2019 (E-003890/2019/rev.1) to the Commission, Rule 138, Pierfrancesco Majorino (S&D), www.europarl.europa.eu/doceo/document/E-9-2019-003890_EN.html.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

track the movements of citizens and identify those who disobeyed the rules of the state of emergency linked to COVID-19 measures.[31]

In terms of surveillance in public spaces, protests still see a heavy deployment of security forces. Violence and arrests of demonstrators are still common and recent research shows how the strategic use of violence to clamp down on protest events can serve as a tool for regime survival.[32] However, whether and to what extent AI-enhanced technologies are used to respond to and control these events remains unclear. So far, most information on the use of AI-enhanced surveillance of public spaces has come from news reporting on the business arrangements and calls for tenders – either leaked or public – concerning the development of these technologies. This includes a series of articles detailing the deployment of video-surveillance technologies in Al Hoceïma, Agadir, Casablanca, Marrakech, and Meknes.[33] In July 2022, the weekly magazine *TelQuel* also published an interview with a high-level police officer about the potential improvement achieved by the use of drones and AI in Casablanca, which is the only example of a public statement by a government official on the matter.[34]

With regard to border control, AI-enhanced technologies have been introduced by countries around the world not only to deter or stop irregular migration by surveilling borders, but also to serve as systems for tracking, controlling, and accelerating cross-border mobility more generally. In Morocco, for instance, this has resulted in the mounting of facial recognition cameras or procurement of thermal imaging cameras at its borders with the two Spanish enclave cities Ceuta and Melilla, largely funded by the EU.[35] These borders are regularly mediatised as the main entry points for Sub-Saharan African migrants into Spain (and thus the EU), but they also experience a high daily flow of visitors and cross-border workers throughout the year.

[31] Antónia do Carmo Barriga, Ana Filipa Martins, Maria João Simões, and Délcio Faustino, 'The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?' (2020) 2(1) *Social Sciences & Humanities Open* 1–5, https://linkinghub.elsevier.com/retrieve/pii/S2590291120300851.

[32] Chantal E. Berman, 'Policing the organizational threat in Morocco: Protest and public violence in liberal autocracies' (2021) 65(3) *American Journal of Political Science* 733–754.

[33] *TelQuel* dedicated an entire issue to the use of high-tech surveillance in Moroccan cities, available at the following link: https://telquel.ma/sommaire/securite-nos-villes-sous-haute-surveillance; Kenza Filali, 'Le Maroc parmi les importateurs de materies d'espionnage Britannique' (11 March 2018), Le Desk, https://ledesk.ma/encontinu/le-maroc-parmi-les-importateurs-de-materiel-despionnage-britannique/; Kenza Filali, 'El Mahdi El Majidi s'allie au Francais Cerbair specialiste des solutions anti-drones' (9 June 2021), Le Desk, https://ledesk.ma/enoff/el-mahdi-el-majidi-sallie-au-francais-cerbair-specialiste-des-solutions-anti-drones/; *Africa Intelligence*, 'National police to expand all-seeing eye on Casablanca' (21 April 2021), www.africaintelligence.com/north-africa/2021/04/21/national-police-to-expand-all-seeing-eye-on-casablanca,109659676-art.

[34] Yassine Majdi, 'Fathi Hassan (DGSN): Nous planchons sur le recours aux drones et a l'intelligence artificielle' (July 2022), *Tel Quel*, https://telquel.ma/sponsors/fathi-hassan-dgsn-nous-planchons-sur-le-recours-aux-drones-et-a-lintelligence-artificielle_1774312.

[35] *Africa Intelligence*, 'Spain and EU to supply border surveillance equipment to Morocco' (14 June 2022), www.africaintelligence.com/north-africa/2022/06/14/spain-and-eu-to-supply-border-surveillance-equipment-to-morocco,109791869-art.

For Spain, controlling and preventing irregular migration into Ceuta and Melilla has been a hot topic since the 1990s, while Morocco considers Ceuta and Melilla as cities colonised by Spain, and they are therefore a regular cause of diplomatic crisis between the Moroccan and Spanish governments.[36] Spanish media regularly accuse Morocco of attempts to put pressure on Spain by not effectively controlling borders, while Morocco invokes its unwillingness to play a gendarme role and calls for an integrated and participative approach to deal with the issue, including financial support from the EU.[37]

Managing the Spanish–Moroccan border is certainly big business given the considerable budgets allocated by the EU to 'fight' irregular migration and to 'protect' Ceuta and Melilla.[38] For example, Indra Sistemas, a Spanish information technology and defence systems company, received at least 26.6 million euros across forty public contracts (twenty-eight without public tender), mostly from the Spanish Ministries of the Interior and Defence, for migratory control tasks including: the maintenance of the Integrated External Surveillance System (SIVE) of the Civil Guard, the installation of radars on the southern border and facial recognition at border posts, or the integration of the new 'intelligent borders' system.[39] The French technology giant Atos also obtained at least twenty-six contracts from the Spanish Ministry of the Interior from 2014 to 2019, totalling more than 18.7 million euros, in order to repair and supply equipment for the SIVE. Similarly, from 2014 to 2019, the Government of Spain awarded French company Thales at least eleven migration control contracts (3.8 million euros in total), most of them to supply night vision systems and their respective maintenance services.[40] The most recent deal over 4.8 million euros on the procurement of thermal surveillance cameras for the Moroccan Ministry of Interior has been concluded between the Spanish defence equipment company Etel 88 and the Spanish development agency FIIAPP.[41]

In co-operation with mostly European tech companies, both Moroccan cities as well as Morocco's northern border with Spain have thus seen the increasing

[36] K. Natter, 'The formation of Morocco's policy towards irregular migration (2000–2007): Political rationale and policy processes' (2014) 52 *International Migration* 15–28, https://doi.org/10.1111/imig.12114; R. Andersson. 'Hardwiring the frontier? The politics of security technology in Europe's "fight against illegal migration"'. (2016) 47(1) *Security Dialogue* 22–39, https://doi.org/10.1177/0967010615606044.

[37] Público, 'Diez multinacionales se embolsan el 65% del dinero que España destina a frenar la migración' (1 July 2020), El control de la migración, un oscuro negocio, https://temas.publico.es/control-migracion-oscuro-negocio/2020/07/01/diez-multinacionales-se-embolsan-el-65-del-dinero-que-espana-destina-a-frenar-la-migracion/.

[38] R. Andersson, *Illegality, Inc.: Clandestine Migration and the Business of Bordering Europe* (University of California Press, 2014); El Confidencial and Fundación PorCausa, 'Fronteras SA: la industria del control migratorio' (n.d.), www.elconfidencial.com/espana/2022-07-15/fronteras-industria-control-migratorio_34602287/.

[39] Público, 'Interior Implantará Un Sistema de Reconocimiento Facial En La Frontera de Melilla' (27 July 2015), www.publico.es/politica/interior-implantara-sistema-reconocimiento-facial.html.

[40] Fundación Por Causa, 'Industria Del Control Migratorio 2: Quién Se Lleva El Dinero?' (2020), https://porcausa.org/somos-lo-que-hacemos/industria-del-control-migratorio/

[41] *Africa Intelligence*, 'Spain and EU to supply border surveillance equipment'.

deployment of and reliance on AI-enhanced technologies as governance tools. While Morocco's legal framework around privacy and data protection has also been upgraded over the last decade, its limited implementation and the vast leverage of security and legal actors in interpreting the law, however, raise a host of challenges on the intersection between AI technologies and human rights. In the next section, we outline how we methodologically approached our research on urban and border surveillance, as well as some of the key limitations we faced.

19.3 METHODOLOGY

Francesco Colin and Issam Cherrat conducted the fieldwork for the urban and border surveillance cases, respectively, during the period March to August 2022. The fieldwork relied on extensive desk reviews, including various published and unpublished publications on the use of technology in urban and border governance, academic studies, grey literature from NGOs and state institutions, as well as the available press in French and English.

The other main component of the fieldwork was a set of nine semi-structured interviews on urban surveillance and twenty interviews on border surveillance with key stakeholders. Given the scarcity of information on the topic of the research, as well as the difficulty in accessing knowledgeable actors, we relied on snowball sampling. The interviewees included scholars, journalists, public officials, police officers, and civil society actors. Great care was taken during the research process to ensure the safety and anonymity of the interviewees and researchers. All interviewees were informed orally about the scope of the research and gave their consent prior to the interviews. Only two interviewees in the urban use case granted their permission to be recorded, while all of them asked to be quoted anonymously in the research outputs. Six interviewees contacted for the case study on border governance declined to have their interview mentioned in the study.

The study was severely limited by the broader security context in which the research was carried out. The sensitive nature of the topic – related to matters of national security and territorial integrity – as well as its relatively novel application in the Moroccan context made it complicated to access information and interviewees. All data revolving around surveillance practices is perceived to be the exclusive competence of Morocco's security apparatus, and thus represents a subject on which one simply cannot ask too many questions. The limited information on the use of these technologies was extracted from calls for tender (CFT), to the extent that they were in the public domain. Such documents are accessible only when they get leaked by the press or in the case of privileged sources. In addition, many of these calls were still ongoing (or had been re-issued) at the time of writing. Finally, it was not possible to acquire first-hand information on the actual functioning of these technologies. Our attempts to establish direct contact with the staff of the

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

intelligence services have been unsuccessful, and none of the interviewees had a direct knowledge of how these technologies are employed on the ground.

In addition to the issue of access, the overall general climate of repression (and associated fears of reprisals for speaking out) limited the fieldwork on both urban and border surveillance. Despite the precautions taken by the researchers, such as the exclusive use of secure platforms for communication, interviewees measured their words carefully when speaking about surveillance technologies. Representatives of private companies engaged in the deployment of these technologies were unwilling to participate in the research, saying that they did not want to jeopardise the relationship with the General Directorate for National Security (DGSN), the national police force, in the event of future tenders. In the case of border controls, several stakeholders refused to be interviewed once they learned about the topic, and access to information from government institutions was denied.

19.4 AI-ENHANCED TECHNOLOGIES IN MOROCCAN CITIES

Across Moroccan cities, pilot experiences with AI-enhanced technologies are being developed for a plethora of applications – such as traffic management, monitoring of air quality, and energy efficiency, but also irrigation and waste collection.[42] However, generally speaking, in Morocco 'there is still very little actual AI in smart cities'.[43] As we noted earlier, most of the available data on the procurement of AI-enhanced technology such as facial recognition cameras is based on CFT documents, but information on its actual deployment, functioning, and use is extremely scarce.

Based on the desk review, it was possible to develop Table 19.1, which provides a schematic summary of the technology deployed in the urban context in Morocco.

Although Table 19.1 shows an impressive deployment of technology, especially for the city of Casablanca, these numbers still pale in comparison with other countries: while in Casablanca there are 'only' 0.74 cameras per 1,000 people, in the ten most surveilled cities of the world this ratio ranges from 62.52 to 8.77 cameras.[44] Moreover, although the absolute lack of transparency surrounding these projects does not allow us to trace a clear timeline, we know that the deployment of high-tech surveillance technology has accelerated after the 2011 bombing at the Café Argana in Marrakech – as the attacked area was supposed to be covered by video surveillance, but apparently cameras were not working.[45] Furthermore, Table 19.1 shows that the current wave

[42] Interviewee 8, 18 July 2022. Due to security and ethical concerns, it is not possible to provide further details about interviewees.

[43] Interviewee 3, 10 June 2022.

[44] This data is available at: www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[45] Interviewee 6, 29 June 2022. See also France Media Agency, 'À Marrakech, 38 caméras sur la place Jamaa el Fna' (4 May 2012), *La Presse*, www.lapresse.ca/voyage/destinations/afrique/maroc/201205/04/01-4522102-a-marrakech-38-cameras-sur-la-place-jamaa-el-fna.php.

TABLE 19.1 *Review of video-surveillance technologies in Moroccan cities*[a]

City	Technology deployment	Main stakeholders involved
Al Hoceïma	Existing installation: no cameras installed. Future projects: 60 cameras in 'strategic areas' of the city.	Tender managed by the *Agence pour la promotion et développement du Nord* (SDL).
Agadir	Existing installation: no cameras installed. Future projects: 220 video-surveillance cameras to be installed and a new HQ to manage them.	Tender launched by the *Agadir Souss Massa Aménagement* (SDL). It has been awarded to *TPF Ingénierie* (France). The separate tender for the HQ has yet to be awarded.
Casablanca	Existing installation: 60 cameras deployed in 2015; 500 cameras deployed in 2016; 150 cameras deployed in 2017. Future projects: 577 new cameras currently under CFT; 2 drones; new HQ to control operations.	Tender co-ordinated by *CasaTransport* (SDL), on behalf of the DGSN. The companies *Tactys* and *CeRyX* (France) developed the technical elements, and the tender has been unsuccessful in early 2022.
Fez	Existing installation: exact number unclear, sources report 'a hundred cameras in the main arteries of the city'[b] Future projects: no information on future projects.	Project co-ordinated by the DGSN. Cameras installed by *Sphinx Electric* (Morocco) in 2018.
Marrakech	Existing installation: no information available. Future projects: 223 new cameras in the old medina and a new data centre to be installed in Jamaâ el Fna square.	Tender co-ordinated by Al Omrane, which has been awarded to *Sphinx Electric* (Morocco) in February 2022.
Meknes	Existing installation: no cameras installed. Future projects: new video surveillance system (2021).	Project launched by the municipality.
Rabat	Existing installation: no information available. Future projects: video-surveillance of the forest ring road surrounding the city ('*Ceinture verte*').	Tenders are managed by *Rabat Région Aménagement*. The new project has yet to be launched officially.
Tangier	Existing installation: 200 cameras installed. Future projects: no information on future projects.	Project co-ordinated by the DGSN. Cameras deployed by *Cires Technology* (France).

[a] Last updated: 19 August 2022.

[b] Anaïs Lefébure and Mehdi Mahmoud, 'Casablanca, Marrakech, Dakhla … Nos villes sous haute surveillance?' (2 July 2021), *Tel Quel*, https://telquel.ma/2021/07/02/casablanca-marrakech-dakhla-nos-villes-bientot-sous-haute-surveillance_1727723.

Source: Compilation by Francesco Colin from multiple sources.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

of projects represents an extension of past deployments in some cities (Casablanca, Marrakech, Rabat) and the creation of new installations in others (Al Hoceïma, Agadir, Menkes). In any case, interviewees generally agree that these projects only represent the beginning, rather than the end, of such endeavours.[46]

However, there is no information available on the concrete way in which AI is employed in the analysis of images captured through these cameras. As one interviewee put it, 'we know there is a computer at the central police station in Rabat, but god knows what goes on there'.[47] CFT documents provide some useful information here: the CFT for the expansion of the surveillance system in the city of Casablanca runs to 389 pages and outlines the type of technology that needs to be provided, as well as its potential. It specifies that the cameras must be able to perform facial recognition tasks, that is, to be able to identify a target against a picture or a recorded photo, either in real time and on recorded footage (p.12 CFT's Annex).[48] The CFT for the new video surveillance project in the city of Al Hoceïma provides more details in terms of cameras' (desired) capabilities: to compare the data collected via video surveillance against existing databases of pictures, to easily add pictures to databases based on live video feed, and to search for a specific person through an image added to the system.[49] The capacity to identify a target on the basis of an image is the central function of face recognition systems in these contexts.[50] However, the role of central security agents on the ground is still substantial: they would need to perform dynamic search functions (based on video metadata and on visual inputs), compile reports based on different data types and sources, and ensure co-ordination with police intervention on the ground.

In line with discursive shifts in the global surveillance trade,[51] the massive investment by Moroccan cities in AI-enhanced surveillance technology is presented as a shift from the 'smart' to the 'safe' city. Official discourse stresses the physical security purposes of the systems, such as catching accidents and thefts on camera. However, a small but increasing number of Moroccan civil society actors are raising concerns about the consequences of mass transmission of personal data to government entities in terms of privacy and individual liberties.[52] In addition, our study found that

[46] Interviewee 2, 31 May 2022; interviewee 5, 24 June 2022; interviewee 8, 18 July 2022.

[47] Interviewee 5, 24 June 2022.

[48] Casa Transports SA, 'Cahier Des Clauses Techniques Particulières (CCTP) – Préstations de Réalisation de La 2ème Phase Du Poste Central de La Gestion de La Circulation et de La Vidéoprotection de Casablanca' (2021) [unpublished].

[49] The system deployed in Al Hoceïma also needs to allow the future integration of other 'intelligent analytics', such as intrusion detection, people's count, gatherings, etc. (p. 43).

[50] Interviewee 8, 18 July 2022.

[51] Privacy International, 'From smart cities to safe cities: Normalising the police state?' (15 August 2018), https://privacyinternational.org/long-read/2231/smart-cities-safe-cities-normalising-police-state.

[52] Lefébure and Mahmoud, 'De la "smart" à la "safe" city'; Lefébure and Mahmoud, 'Casablanca, Marrakech, Dakhla'; see also Hagmann, 'Globalizing control research', for a case study of the surveillance system in place in Marrakech. Interviewee 9, 22 July 2022.

the legal framework attributes all control of local security issues to the local representatives of the Ministry of the Interior, rather than to elected local governments, limiting public oversight and accountability.

19.5 AI-ENHANCED TECHNOLOGIES AT MOROCCAN BORDERS

Unlike the unclear situation with regard to urban surveillance, it is known that the borders between Morocco and the two Spanish enclaves Ceuta and Melilla are progressively being transformed into 'smart' borders through the increasing deployment of AI-enhanced cameras and FRT. Yet, border control management is surrounded by secrecy in Morocco. Topics related to national security are treated with suspicion, and only fragmentary pieces of information are leaked to the press. It is almost impossible to know which firm or company has won a tender to install cameras or such equipment on the borders between Morocco and Spain, including the use of FRT cameras in its airports.[53] In the words of an interviewee who did not want to be listed, 'as a police officer, we do not ask about these things, I guess we do not have the right even, we are simply trained to use new technologies when they are deployed'. Therefore, for this section on the use of FRT at the Moroccan–Spanish border, we are relying on information from the Spanish side.

According to the Spanish Minister of Interior's declaration in March 2022, Spain has modernised its entire technological systems at the border posts in Beni Enzar, Melilla, and in El Tarajal, Ceuta.[54] This modernisation consists of the implementation of a fast-track system for cross-border workers, the installation of fifty-two posts for greater agility in the passage of people, and sixteen registration kiosks featuring the control and collection of biometric data. Furthermore, currently up to thirty-five cameras equipped with facial recognition systems are being installed between the entry and exit points of the borders of Ceuta and Melilla. The project is based on an entry control system with FRT, in which, in addition to the thirty-five cameras, there are four micro-domes,[55] and a software platform to host the Live Face Identification System for the control of the closed-circuit television system. It is implemented by the company *Gunnebo Iberia*, a subsidiary of the Swedish world leader in security products, and *Thales Spain*, a subsidiary of the technological multi-national dedicated to the development of information systems for the aerospace, defence, and security markets.

Overall, the use of AI-enhanced cameras at the Ceuta and Melilla borders aims to shorten border control processing, enhance security at the crossings, and increase control over people and goods entering and exiting the border. The main problem at

[53] Ayoub Khattabi, 'La reconnaissance faciale bientôt à l'aéroport de Rabat-Salé' (4 August 2022), le360, https://fr.le360.ma/economie/la-reconnaissance-faciale-bientot-a-laeroport-de-rabat-sale-264740.

[54] Senado, 'Diario de Sesiones Senado 22 Marzo 2022' (2022), www.senado.es/legis14/publicaciones/pdf/senado/ds/DS_P_14_83.PDF.

[55] Wide-angle dome cameras with a small form factor (i.e., building them as small as possible).

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

the Tarajal entry gate (Ceuta), for example, was that the poor existing infrastructures made it impossible to control the waiting line and to systematically track who enters and leaves through this passage. The poor infrastructure allowed for the smuggling of illegal goods and made it difficult to track whether minors entered Ceuta irregularly. The main objective of the deployment of new technologies is thus to monitor the number of people who enter and leave and to detect the number of people who do not return after a period of time. The technology used allows for flexible mobile facial scanning, that is, the inspection of people inside cars, trucks, buses, and on motorcycles or bicycles.[56] It will also allow the implementation of 'black lists' during the passage of border control, showing personal information of the individual transiting through the border if they are registered on such a list. Deploying this technology, it is expected that some 40,000 facial readings per day can be carried out in Ceuta and 85,000 in Melilla.

Civil society actors have already drawn attention to the risks inherent to the use of those technologies at the Ceuta and Melilla borders: more than forty Spanish organisations and associations signed a statement rejecting the 'smart borders' project.[57] They emphasised that the project's ambition to 'exercise greater security control through the use of artificial intelligence, by collecting biometrics, such as facial recognition, fingerprints, […] poses a risk of violating human rights'.[58] They particularly highlighted that 'the collection of biometric data for people who do not have a European passport is not in accordance with the principle of proportionality'.[59] Indeed, as another civil society association highlighted, the Spanish–Moroccan borders risk being turned 'into a laboratory for security practices'. They argue that with regards to the right to data privacy, 'this will not happen at other borders such as Barajas-Madrid airport and will not happen with European citizens, but will happen at the borders where migrants cross in a state of extreme poverty, and it will happen with populations suffering from racism'.[60]

In terms of migration control, the deployment of FRT at the Moroccan–Spanish border is probably effective in controlling regular migration, for instance by facilitating and speeding up the circulation of individuals and cars, but less so when it comes to attempts at irregular migration. While it will inevitably make it harder for those migrants who need to reach Spanish territory in order to claim their rights to protection, that is, asylum seekers and unaccompanied minors, FRTs cannot

[56] Fundación por Causa, 'Industria Del Control Migratorio 2: Quién Se Lleva El Dinero?'.

[57] Amal Kennin, 'Munẓmāt Isbānya Tantqad Mašrwaʿ "Ālḥudwd Ālḏakya" Fy Sbta Wa Mlylya [Spanish organizations criticize the "smart borders" project in Ceuta and Melilla]' (14 January 2022), Hespress, www.hespress.com/930243-الذ-الحدود-مشروع-تنتقد-إسبانية-منظمات.html.

[58] Ibid.

[59] Ibid.

[60] Mohammad Okba, 'Paula Guerra Cáceres: "La Inteligencia Artificial Es Una Amenaza Para Los Migrantes y Es Una Forma de Control Migratorio"' [Paula Guerra Cáceres: Artificial intelligence is a menace for migrants and a form of migratory control] (14 June 2022), Bayana, https://baynana.es/es/paula-guerra-caceres-la-inteligencia-artificial-es-una-amenaza-para-los-migrantes-y-es-una-forma-de-control-migratorio/.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

predict when migrants will attempt to pass the fences of Ceuta and Melilla and are ineffective when thousands gather and decide to climb the fence simultaneously, such as the 2022 attempts in Melilla that caused the death of thirty-seven migrants.[61] Moreover, migrants adapt their border crossing strategies according to the technologies in place, for example in Fnideq,[62] where irregular migrants reach Ceuta's shore by swimming when it is foggy and cameras cannot detect them. Lastly, the installation of 'smart borders' in the north of Morocco has (once again) redirected irregular migrants towards the longer, more costly and deadly migratory routes in the south of Morocco, where one can reach the (Spanish) Canary Islands through a perilous journey by boat.[63]

Despite Spain's massive investment in these technologies, it remains unclear what the actual effects and outcomes of FRT used are on Moroccan–Spanish border dynamics since no official reports have been released yet. The impression from the field is that the new 'smart' border has slightly improved the quality of daily tasks, but that border crossings are still overwhelmed during periods of intense flux (during summer and national holidays). Furthermore, irregular migration dynamics seem to not have been affected by the use of new technologies, as migrants have adapted their strategies to cross the border.

19.6 DISCUSSION

Despite the rapidly increasing use of FRT in Moroccan urban and border surveillance, public debate around these issues is still lacking in Morocco. In both cases, authorities justify the use of AI-enhanced technologies by the will to improve users' experience and security.[64] Between the high sensitivity of the data that is captured through these technologies and the generalised opacity with which it is treated, there are grounds to be concerned for the respect of citizens' right to privacy.

From the two cases analysed, two cross-cutting issues emerge. The first one is the involvement of external actors, such as international donors, multi-national companies and foreign states, which makes AI-enhanced surveillance an inherently transnational issue. External actors play a key role in the development and financing of FRTs, in their installation on the ground, but also in the (limited) monitoring of human rights protection frameworks. International donors provide funding for urban and border surveillance projects for instance, but they could also play a more active role in enforcing mechanisms for transparency in using such surveillance

[61] Aurélie Collas and Sandrine Morel, 'Au Maroc, Dans l'enclave de Melilla, Une Tentative d'entrée de Migrants Tourne Au Drame' (27 June 2022), *Le Monde*, www.lemonde.fr/afrique/article/2022/06/27/a-melilla-une-tentative-d-entree-de-migrants-tourne-au-drame_6132174_3212.html.

[62] A Moroccan city neighbouring Ceuta.

[63] Andersson, *Illegality, Inc.*; El Confidencial and Fundación PorCausa, 'Fronteras SA: la industria del control migratorio'.

[64] Khattabi, 'La reconnaissance faciale'.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

infrastructures. Yet, this is not always the case. For Casablanca's first video surveillance projects (2015 and 2017), part of the funding came from a World Bank loan through a project to improve urban transportation. Although the World Bank raised concerns about the use of its funds, and demanded an audit that concluded the video surveillance system was not eligible for funding in the framework of their project, the project was still financed.[65] Recently, the World Bank even approved an increase of 100 million dollars (in addition to the already committed 200 million dollars) to finance further development projects by the city of Casablanca.[66]

Similarly, the EU is extensively funding border control and surveillance technologies in Morocco, with little transparency concerning their use and few requirements in terms of associated human rights protection. For instance, the Moroccan DGSN acquired spying software from the Swedish firm MSAB and the US company *Oxygen Forensic* with funding from the Africa Emergency Fund, set up by the EU in 2015 for its 'fight against irregular migration'.[67] While this technology transfer project was implemented in the context of migration co-operation, the EU has no effective mechanism in place to prevent the misuse of such technologies for other repressive activities. More generally, although the EU has timidly tried to regulate the export of high-risk surveillance,[68] it faces resistance from Members States.[69] Additional rules were put in place in the revision of the EU's Export Control Framework under EU Regulation 2021/821. But although export controls in the EU are becoming increasingly strict, EU Member States still often find ways to export these technologies that are deemed relevant for reasons of national security.[70]

The second cross-cutting issue that emerges from the analysis is that Morocco's existing legal framework through which these projects are launched and implemented provides important obstacles to any kind of public oversight. Most of the tenders that accompany the development of these projects are circulated behind

[65] Interviewee 6, 29 June 2022.

[66] World Bank, 'World Bank supports additional financing for the Casablanca Municipal Support Program-for-results', World Bank, Press Release (22 June 2022), www.worldbank.org/en/news/press-release/2022/06/22/world-bank-supports-additional-financing-for-the-casablanca-municipal-support-program-for-results.

[67] Lorenzo D'Agostino, Zach Campbell, and Maximilian Popp, 'Wie die EU Marokkos Überwachungsapparat aufrüstet' [How the EU is arming Morocco's surveillance apparatus] (25 July 2022), Der Spiegel, www.spiegel.de/ausland/marokko-wie-die-eu-rabats-ueberwachungsapparat-aufruestet-a-d3f4c00e-4d39-41ba-be6c-e4f4ba650351.

[68] See Ot L. van Daalen, Joris V.J. van Hoboken, and Melinda Rucz, 'Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control' (2022) 48 *Computer Law & Security Review* 105789; European Parliament, 'Draft Report by the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware' (2022), www.sophieintveld.eu/nl/pega-draft-report.

[69] See Sabrina Winter, 'Spähsoftware für Autokraten – Wie die Europäische Union ihre Kontrollen aufweichte – und Deutschland half' (5 October 2023), FragDenStaat, https://fragdenstaat.de/blog/2023/10/05/wie-die-europaische-union-ihre-kontrollen-aufweichte-und-deutschland-half/.

[70] Wagner, 'Whose politics? Whose rights?'.

https://doi.org/10.1017/9781009321211.022 Published online by Cambridge University Press

closed doors and not made public. Occasional leaks to the press are the main way in which these projects come to public knowledge. However, when tenders are unsuccessful, Moroccan law authorises the contracting authority to proceed through 'over-the-counter' contracts – which do not require any kind of publicity.[71] In other words, the companies that will implement these projects are selected directly by the contracting authority without a public tendering process, raising important questions in terms of transparency of the use of public funds. This will be the case for the 720 million Moroccan Dirhams project that will set up the new video surveillance system in the city of Casablanca.[72] Some interviewees also noted that when these tenders escape public scrutiny, they tend to be attributed to companies that have close ties to the regime.[73]

While the leaked CFTs provide some insights into which cameras are installed and how many, they leave Moroccan citizens and civil society in the dark as to how they will actually be used. Companies deploying these technologies argue that they have no control over their end-use. For instance, a source working for Huawei in Morocco highlighted: 'if Huawei sells video surveillance products, it does not have access to what the final clients do with them, and does not participate in their installation'.[74] Similarly, European companies seem impervious to ethical concerns for the eventual misuse of the technology provided. In the framework of these projects, they 'do what they are asked to without too much resistance'.[75]

Other state institutions that should monitor the ethical implications of the use of AI-enabled surveillance technologies are not raising any concerns either. In its position paper on the digital transition, the Moroccan *Conseil Économique, Social et Environmental* defines AI development as a 'national priority', but it does not touch upon the use of AI in urban video surveillance. Similarly, the *Conseil National des Droits Humains* recently organised an international colloquium to discuss ethical implications of uses of AI, but it dealt with this topic from a purely academic perspective and avoided raising the issue of FRT-based surveillance by state authorities.[76] Lastly, while raising the issue of the storage and analysis of personal data through facial recognition by private actors, the *Commission nationale de contrôle de la protection des données à caractère personnel* seemed untroubled by the use of the same technologies by security services and the exponential increase in the collection of personal data. In short, video surveillance is treated as the sole prerogative of the security apparatus, and so far public monitoring actors have avoided to engage directly with the topic. It seems that, implicitly and explicitly, public security should not be the public's concern.

[71] Interviewee 6, 29 June 2022.
[72] Equivalent to roughly 69 million euros.
[73] Interviewee 5, 24 June 2022; interviewee 6, 29 June 2022.
[74] Lefébure and Mahmoud, 'Casablanca, Marrakech, Dakhla'.
[75] Interviewee 6, 29 June 2022.
[76] A press release of the event is available at http://cndh.org.ma/an/taxonomy/term/447.

19.7 CONCLUSION

Our analysis shows that the umbrella argument of public security is applied not only to the use of AI-enhanced technologies in Moroccan urban spaces and at the Moroccan-Spanish border, but also to their deployment, oversight, and monitoring. As a result, the information on whether (and eventually how) high-tech surveillance technology is used is confidential, national security agencies are seemingly exempt from the monitoring of other state institutions, and independent actors are expected to trust that these institutions are acting in citizens' best interest. This makes effective public oversight impossible, and amplifies the potential for it to be used for 'surgical' repression.

The lack of oversight is also nurtured by the absence of a public debate – and ostensibly of public interest – on the matter. An exemplary anecdote is that among the inhabitants of Casablanca, many think that the cameras around the city do not work, and are put there only to bring about an improvement in public behaviour.[77] Kindling a public discussion on the securitisation of public spaces through high-tech surveillance was one of the ambitions of the *TelQuel* issue of July 2021, but so far this debate is still lacking.[78] On the contrary, interviewees perceived Moroccans as being quite ill-informed about related issues of personal data protection.[79]

However, if the future plans inventoried in this chapter are indeed implemented, Morocco is rapidly advancing towards the implementation of AI-enabled technologies in urban and border surveillance, including FRT. It is clear that state institutions plan to use these technologies extensively, and the lack of (trans)national institutional oversight and public debate on the matter should raise concerns about the extent to which such implementation will affect citizens' rights. Until the topic is picked up in public debate and diplomatic relations and reforms in the way this technologies are purchased and governed, Moroccan authorities will continue to conduct widespread AI-enabled surveillance without any oversight or accountability.[80]

[77] Interviewee 8, 18 July 2022.

[78] 'Vidéosurveillance: au doigt et à l'œil' (2 July 2021), *TelQuel*, https://telquel.ma/2021/07/02/videosurveillance-au-doigt-et-a-loeil_1727702.

[79] Interviewee 2, 31 May 2022; interviewee 5, 24 June 2022; interviewee 8, 18 July 2022.

[80] Interviewee 8, 18 July 2022.