

The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management

Giray SADIK

Assoc. Prof. Dr., Yıldırım Beyazıt University, Department of International Relations, Ankara

Ceren KAYA

Ph.D. Candidate, Yıldırım Beyazıt University, Department of International Relations, Ankara

To cite this article: Giray Sadik and Ceren Kaya, “The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management”, *Uluslararası İlişkiler*, Vol. 17, No. 68, 2020, pp. 145-160, DOI: [10.33458/uidergisi.856932](https://doi.org/10.33458/uidergisi.856932)

To link to this article: <https://dx.doi.org/10.33458/uidergisi.856932>

Submitted: 30 June 2020
Last Revision: 16 December 2020
Published Online: 04 January 2021
Printed Version: 18 February 2021

Uluslararası İlişkiler Konseyi Derneği | International Relations Council of Turkey
Uluslararası İlişkiler – Journal of International Relations

E-mail : bilgi@uidergisi.com.tr

All rights of this paper are reserved by the *International Relations Council of Turkey*. With the exception of academic quotations, no part of this publication may be reproduced, redistributed, sold or transmitted in any form and by any means for public usage without a prior permission from the copyright holder. Any opinions and views expressed in this publication are the author(s)'s and do not reflect those of the *Council*, editors of the journal, and other authors.

The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management

Giray SADIK

*Assoc. Prof. Dr., Yıldırım Beyazıt University, Department of International Relations, Ankara
E-mail: gsadik@ybu.edu.tr*

Ceren KAYA

*Ph.D. Candidate, Yıldırım Beyazıt University, Department of International Relations, Ankara
E-mail: ckaya@ybu.edu.tr*

ABSTRACT

This study offers critical analysis on the role of surveillance technologies in the securitization of migration policies and the impact of such practices on the EU's international identity. The EU member states have adopted various technological instruments that have serious consequences both for the course of the EU's migration policies and its normative international identity. The findings of this research suggest that by securitizing its migration policies through new surveillance technologies, the EU may risk violating its founding norms and principles. These violations are, in turn, likely to have serious political repercussions for the global image and credibility of the EU in the years to come.

Keywords: Surveillance Technologies, Securitization, Border Management, Normative Power, Migration Policy of the EU

AB Göç Politikalarının ve Sınır Yönetiminin Güvenikleştirilmesinde Gözetim Teknolojilerinin Rolü

ÖZET

Bu çalışma, gözetim teknolojilerinin göç politikalarının güvenikleştirilmesindeki rolü ve bu tür uygulamaların AB'nin uluslararası kimliği üzerindeki etkisi hakkında eleştirel bir analiz sunmaktadır. AB üye devletleri hem AB'nin göç politikaları hem de normatif uluslararası kimliği açısından ciddi sonuçları olan çeşitli teknolojik araçlar edinmiştir. Bu çalışmanın bulguları, AB'nin göç politikalarını yeni gözetim teknolojileri ile güvenikleştirmesinin kuruluş normlarını ve ilkelerini ihlal etme riski taşıyabileceğini düşündürmektedir. Bu ihlallerin önümüzdeki yıllarda AB'nin küresel imajı ve güvenilirliği açısından ciddi siyasi yansımaları olması muhtemeldir.

Anahtar Kelimeler: Gözetim Teknolojileri, Güvenikleştirme, Sınır Yönetimi, Normatif Güç, AB'nin Göç Politikası.

Introduction

One of the most challenging subjects occupying the EU's political and security agenda in recent years has been the large-scale movement of people, fleeing from political, social and economic crisis in their home countries, and the substantial rise of asylum-seekers waiting at the doors of European states. The unprecedented level of asylum applications has led to chaos among EU member states on how to handle the process, and this is recognized as a 'refugee crisis'. This has resulted either in new technology investments or the upgrading of various tools and means of migration and border management. Automated decision-making, artificial intelligence, biometric data collection, facial recognition, iris scanning, and fingerprinting are some of the tools used to enhance European border surveillance.

This study aims to examine the role of surveillance technologies in the securitization of the EU's border-management and migration policies. In light of these practices, this article critically evaluates the impact of these policies on the EU's normative international identity. The securitization of migration and normative power are issues that have thus far been studied separately, as there is limited understanding about their interaction in practice and policy development. To address this gap in the literature, we aim to explore their relationship by integrating their analyses, and critically reflecting on their implications for the global credibility and influence of the EU. Evidently, these implications are likely to be more far-reaching than merely affecting EU member states, and thus are expected to have significant repercussions for the wider European neighborhood, especially on the transit and source countries for refugees in the Middle East and North Africa (MENA).

The first section of the paper discusses the concept of securitization with reference to the EU's migration and border policies in theoretical and practical terms. In the following section, we assess the technologies of surveillance and control, particularly the EU's information technology (IT) systems—Schengen Information System (SIS), Visa Information System (VIS) and Eurodac—to exemplify the EU's securitizing practices. The third section discusses ethical concerns about the deployment of surveillance technologies, and the last section tries to describe the foreign policy behavior of the EU by looking at the goals, means and results of deploying the above-mentioned information technology systems. The study arrives at the conclusion that IT systems are securitizing migration and border management through their everyday practices, rather than exceptional or extraordinary means as expected by securitization theory, and that there is an essential need for impact assessment of the EU's surveillance technologies. Left unchecked, these technologies could lead to a systematic violation of basic human rights and the founding norms and principles of the Union, placing under controversy and even discrediting the EU's claim as a normative power in its relations with the non-EU world.

Securitization of Migration Policies

The Europeanization of migration policies—the convergence of member states' national migration policies at the European level—are primarily motivated by the internal security concerns of member states, particularly with the abolition of internal borders after the 1985 Schengen Agreement. This has mostly determined the course of EU migration policies. Since the 1980s, the direction of these policies has been predominantly determined by the security-oriented interests of EU member states and societies, indicated in the presentation of migrants as criminals, terrorists, troublemakers, or 'un-

able-to-assimilate' in political discourses and public debates.¹ According to Ceyhan and Tsoukala, this securitarian discourse has steadily increased the adoption of new control mechanisms by member states, such as external controls before and at the borders that include selective visa-granting systems, penalties for carriers of illegal migrants, creation of databases, cooperation with third countries on border management, and the deployment of law-enforcement agencies, military forces, and new technologies to strengthen border controls.²

The issue of the securitization of migration is usually treated within the Copenhagen School's theoretical framework, which basically defines securitization as the discursive construction of an issue as an imminent threat by the securitizing actors through speech acts.³ This is the most referenced theoretical perspective in security studies. Proponents of the Copenhagen School would argue that when the issue is declared an existential threat, extra-ordinary measures, not legal in normalcy, concerning the issue are deemed legitimate.⁴ As an alternative to this constructivist approach, the Paris School's sociological approach pioneered by Didier Bigo privileges practices over discourses. Although this study does not undermine the role of language and speech acts in the securitization of migration in Europe, it finds the argument of the second approach more promising in explaining securitization of migration in Europe.

How can the sociological approach, particularly as elaborated by Didier Bigo, explain the securitization of migration even in the absence of an explicit declaration of an issue as a security threat? This approach conceives bureaucratic routines, day-to-day practices (rather than extraordinary measures), policy tools, and technological developments as the major indicators of migration securitization.⁵ However, Bigo does not diminish the role of speech acts and the construction of myths by politicians regarding immigrants in the securitization process. For him, "the securitization of immigration (...) emerges from the correlation between some successful speech acts of political leaders (...), and the specific field of security professionals (...)." By criticizing the Copenhagen School's overemphasis on 'exceptionalization', Bigo stresses that "securitization works through everyday technologies, through the effects of power that are continuous rather than exceptional (...)", which shows how discourses work in practice.⁷ In this regard, the technological advancements in control and surveillance are causing, and are not caused by the securitization of migration. Bigo defines the securitization of migration as "a process that creates continuous unease and uncertainty" and links it to "computerization, risk profiling, visa policy, the remote control of borders, the creation of international or nonterritorial zones in airports", which are conducted by professional 'managers of unease' such as customs, intelligence services, police forces, border patrols and suppliers of surveillance technologies.⁸ Practitioners

1 Ayşe Ceyhan and Anastassia Tsoukala, "The Securitization of Migration in Western Societies: Ambivalent Discourses and Policies," *Alternatives*, Vol. 27, Special Issue, 2002, p. 21-39.

2 *Ibid.*, p.31.

3 Barry Buzan et al., *Security: A New Framework for Analysis*, London, Lynne Rienner, 1998.

4 *Ibid.*

5 Didier Bigo, "Security and Immigration: Toward a Critique of the Governmentality of Unease," *Alternatives*, Vol. 27, Special Issue, 2002, p. 63-92; Didier Bigo, "The (in)securitization practices of the three universes of EU border control: Military/ Navy – border guards/police – database analysts," *Security Dialogue*, Vol. 45, No 3, 2014, p. 209-225; Thierry Balzacq, "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies," *Journal of Common Market Studies*, Vol. 46, No 1, 2008, p. 75-100; Jef Huysmans, *The Politics of Insecurity*, New York, Routledge, 2006.

6 Bigo, *Security and Immigration*, p. 65.

7 *Ibid.*, p. 73.

8 *Ibid.*, p. 73,78.

of these offices are, by the nature of their duties, managers of what may be referred to as unease, that is the risk and fear that may emerge in the absence of their duties. According to Bigo, although these security professionals claim that they are just reacting to new threats that necessitate extraordinary measures, this is not the case in practice as they try to guarantee their immediate interests such as competition for budgets and missions. These professional ‘managers of risk and fear’ transfer the legitimacy that they have gained from their struggle against terrorists and criminals towards other targets such as transnational political activists or people crossing borders.⁹ Thus, professional managers of unease, who define threats and risks and claim that they are equipped with the necessary technologies to handle these threats, now target migrants and asylum seekers as experimental objects to test and utilize their technologies so that they will maintain their existence and authority in the management of migration.¹⁰

A deeper analysis on the securitization of migration requires going beyond the discourses of political leaders and looking at the practices and instruments that might “embody a specific threat image,” as suggested by Balzacq.¹¹ As emphasized by Huysmans, although asylum may not be spoken off as a threat, its inclusion in policy frameworks that focus on internal security and border policing, as in the case of the Schengen Agreement, renders asylum a security problem.¹² As seen from the main activities of Frontex, such as the coordination of joint surveillance and control operations at the external borders and operational assistance to member states in coordinating and organizing return operations, there is no need for discourses from political leaders to declare asylum-seekers a security threat, since the routinized practices, complex technologies, and military equipment deployed by the Frontex give the message that they are fighting against a security threat. This is because they are normally used to tackle traditional security threats such as terrorism or a military attack.¹³ It is this security rationality that integrates asylum and immigration in policy frameworks dealing with more traditional security issues such as terrorism, rather than an act of explicit threat definition of immigration as suggested by Huysmans.¹⁴

In a similar vein, Neal also goes beyond the language of exceptionalism and urgency in the securitization of migration and suggests that the establishment of Frontex was not the outcome of the EU and its institutions’ urgent response to the 9/11 terrorist attacks as expected by the classical logic of securitization theory of the Copenhagen School, but rather it appeared as a technocratic project, in a sense, that emerged as a logical continuation of integration processes and not an urgent or extraordinary measure.¹⁵ Although EU institutions overtly linked migration to terrorism and border security in their policy statements and extraordinary meetings as a response to 9/11, the language of exceptionalism was absent in the establishment of Frontex.¹⁶ However, the absence of exceptionalism does not necessarily mean that Frontex is not securitizing migration and border management. On the contrary,

9 Ibid., p. 63-64.

10 Bigo, *Security and Immigration*, p. 77.

11 Balzacq, *The Policy Tools of Securitization*, p. 76.

12 Huysmans, *The Politics of Insecurity*, p. 4.

13 Sarah Leonard, “EU border security and migration into the European Union: FRONTEX and securitization through practices”, *European Security*, Vol. 19, No 2, 2010, p. 231-254.

14 Huysmans, *The Politics of Insecurity*, p.4.

15 Andrew W. Neal, “Securitization and Risk at the EU Border: The Origins of FRONTEX”, *Journal of Common Market Studies*, Vol. 47, No 2, 2009, p. 333–356.

16 Ibid., p. 334, 343.

Frontex can be defined as a tool of securitization with its day-to-day activities such as risk analysis, but not as an outcome of the post-9/11 securitization of migration.¹⁷ In this regard, both Neal and Huysmans emphasize technocratic processes, institutional routines, and continuities in framing insecurity domains and advocate the ‘governmentality of unease’ approach of Bigo as a favorable alternative to securitization theory of Copenhagen School.

All these findings address the same point: the securitization of migration in Europe is more a result of specific routinized practices, technocratic processes, and everyday technologies that are deployed or produced by security professionals who create security problems and manage this unease. The deployment of control and surveillance technologies has led to a perception of people crossing borders as a source of unease. Although the role of language is undeniable in the securitization of migration, as many political leaders and the EU institutions openly linked and continue to link migration to security, the theoretical perspective of the Paris School offers a wider frame for understanding the securitization of migration in the case of Europe. For instance, political leaders do not always use securitizing discourses; on the contrary, most of the time they advocate inclusionary, humanitarian, and pro-migrant statements, and yet they cannot prevent the securitization of migration. This is because the securitization of migration is not exclusively caused by discourses but by policy tools and practices, as well as the advancement of new technologies and surveillance mechanisms.

The following section will illustrate how these technologies and their providers partaking in European external border management are contributing to the securitization of migration.

Surveillance Technologies in European External Border Management

This section tries to assess how surveillance technologies, namely SIS, VIS, and Eurodac, are securitizing migration and border management by looking at the dynamics and motivations behind these technologies in the light of the Paris School’s approach to securitization. The study tries to present an empirical analysis of the initial purposes assumed for these IT systems and their transformation and integration into counter-terrorism strategy. In this regard, two questions seem to be critical: for what purposes were these information technology systems devised and what are their areas of usage today?

SIS, VIS and Eurodac are large-scale centralized databases, storing personal and biometric data, that were established to manage borders, migration, and asylum. The comparison of the initial purposes of these databases with their presently pursued objectives is fundamental in understanding their transformation from immigration and asylum management to counter-terrorism and intelligence tools, and subsequently the securitization of migration policies. This research benefited from primary and secondary sources to accomplish such a comparison. EU regulations, decisions, conventions, and the European Commission’s proposals and communications that brought about establishment, operation, and use of these information technology systems are major primary sources in collecting data on surveillance technologies. As for the secondary sources, this study benefited from books, journal articles, working papers, dissertations, newspapers, and reports that support the data collected from primary sources. The secondary sources are also vital in revealing the real motivations of IT systems and exploring the security continuum they created.

¹⁷ Ibid., p. 346, 348.

The Schengen Information System (SIS) was established by the 1990 Convention Implementing the Schengen Agreement (CISA) of 1985 as a compensatory measure following the abolition of internal border controls among five member states (the three Benelux countries, France and Germany). It was designed as a joint information system to ‘maintain public policy and public security, and national security’, by collecting and exchanging data on persons, vehicles, and objects for which an alert has been issued and by allowing competent authorities to create or consult alerts for purposes of border, police, and customs control and, when necessary, denial of entry and residence to unwanted third-country nationals in the Schengen territory.¹⁸ After a while, the Schengen states decided to upgrade the SIS in both technical and functional terms, which resulted in extending its functions and later developing the second-generation SIS, called SIS II, which became operational in 2013.¹⁹ During the negotiations on the improvement of the SIS, counter-terrorism and access to SIS by internal security and intelligence services (Europol and Eurojust) were major concerns when system functions were extended.²⁰ Expanding the capacity of the system to accommodate new members of the Schengen area, benefiting from the new technology, combating terrorism, and having the technology to store biometrics were the major drivers behind developing SIS II.²¹ In this system, Brouwer explains that IT companies developing it were instructed to design it as a ‘flexible tool’ so that it would easily and efficiently adapt to new circumstances and requirements and perform new tasks whenever needed. Thus, technically SIS II was ready for new functions even in the absence of new political objectives that would later determine its functions.²² Concerning the technological devices deployed for border surveillance in general and the discussions on the development of SIS II in particular, Leonard stresses that technical solutions were devised before political objectives; that is to say, sometimes decisions were taken not because there were specific objectives to achieve but because “it is technologically feasible to do so.”²³

“Ensuring a high level of security within the area of freedom, security and justice (AFSJ) of the European Union” was added to the initial purposes of the system by the Regulation on the use of SIS II²⁴ along with the new functionalities such as inclusion of biometrics and interlinking of differ-

18 “Convention Implementing the Schengen Agreement of 1985”, Official Journal L 239, 22 September 2010, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922\(02\):en:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):en:HTML) (Accessed 12 May 2020), Article 92, 93; “Schengen Information System”, European Commission, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en (Accessed 15 May 2020).

19 Jorrit J. Rijpma, “Brave New Borders: The EU’s Use of New Technologies for the Management of Migration and Asylum”, Marise Cremona (ed.), *New Technologies and EU Law*, New York, Oxford University Press, 2017, p.197-241.

20 Evelien Brouwer, “Legal Boundaries and the Use of Migration Technology”, Huub Dijstelbloem and Albert Meijer (eds.), *Migration and the New Technological Borders of Europe*, London, Palgrave Macmillan, 2011 p. 134-169; Dennis Broeders, “A European ‘Border’ Surveillance System under Construction”, Huub Dijstelbloem and Albert Meijer (eds.), *Migration and the New Technological Borders of Europe*, London, Palgrave Macmillan, 2011, p. 40-67.

21 Benedita Menezes Queiroz, *Illegally Staying in the EU: An Analysis of Illegality in EU Migration Law*, Oxford, Hart Publishing, 2018.

22 Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden, Martinus Nijhoff Publishers, 2008, p. 88.

23 Sarah Leonard, “The ‘Securitization’ of Asylum and Migration in the European Union: Beyond the Copenhagen School’s Framework”, Paper presented at the SGIR Sixth Pan-European International Relations Conference, 12-15 September 2007, Turin, Italy.

24 “Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)”, Official Journal L 381, 28 December 2006, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006R1987> (Accessed 18 May 2020).

ent alerts.²⁵ In 2018, a new SIS package was agreed to make enhancements in the areas of biometrics, counter-terrorism, vulnerable persons, irregular migration, and access for EU agencies,²⁶ which would ensure the role of the SIS II as an identification and investigation tool. The purposes and areas of use of SIS have expanded and will apparently continue to expand in the near future with new technological developments and political objectives that focus in particular on security, counter-terrorism, and fighting illegal migration.

Eurodac, another IT system of the EU, was established in 2003 as an EU asylum fingerprint database in order to implement the Dublin regulation that determines the state responsible for processing asylum applications.²⁷ The major purpose of this system is to detect whether an individual has already submitted an application in one of the member states, which will be responsible for the application. Thus, it was designed to prevent asylum seekers from making multiple applications in different member states. In addition to managing asylum, Eurodac also functions as a tool for fighting against illegal migration by storing the fingerprints of migrants who crossed borders illegally.²⁸ In 2013, the Eurodac Regulation was amended following the revision of the Dublin Regulation. While the initial aim of Eurodac for collecting the fingerprints was to determine the state responsible for inspecting an asylum application, law enforcement authorities were later provided access to this database and then started using it as an investigative tool in combating crime, terrorism, and illegal migration.²⁹

The VIS, established in 2004, is another centralized database that aims to support the common EU visa policy by allowing Schengen states to exchange data on the short-stay visa applications of third country nationals.³⁰ The major purpose of the system is facilitating border checks by verifying the identity of an individual, preventing abuses and visa shopping, protecting travelers from identity theft, facilitating the application of the Dublin Regulation, and enhancing internal security by assisting in investigation, detection and prevention of terrorist and criminal offences.³¹ In addition to visa, border, immigration, and asylum authorities, the Council decided that the internal security and law enforcement authorities should also be given access to VIS to reinforce internal security and fight against terrorism.³² In 2007, the Justice and Home Affairs Council agreed to use “designated authori-

25 Brouwer, *Legal Boundaries*; Queiroz, *Illegally Staying in the EU*.

26 “Schengen Information System”, European Commission, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en (Accessed 20 May 2020).

27 “Identification of applicants (EURODAC)”, European Commission, https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en, (Accessed 19 May 2020).

28 Broeders, *A European ‘Border’ Surveillance*, p. 40-67.

29 “Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013”, Official Journal L180, 29 June 2013, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:EN:PDF> (Accessed 4 June 2020).

30 “Council Decision of 8 June 2004 establishing the Visa Information System (VIS)”, Official Journal L213, 15 June 2004, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0512&from=GA>, (Accessed 5 June 2020)

31 “Visa Information System (VIS)”, European Commission, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en, (Accessed 10 June 2020).

32 “Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences”, Commission of European Communities, 24 November 2005, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005PC0600&from=EN> (Accessed 18 June 2020).

ties of member states” instead of internal security agencies, which would come to mean that national governments would determine any agency as “designated,” and be given access to VIS.³³

After briefly introducing the major purposes of each database, it is now essential to discuss, in the light of the Paris School’s approach, the common features of these systems that contribute to the securitization of EU migration policies. Firstly, as aforementioned, the technical feasibility of Eurodac, VIS, and SIS II took precedence over the political decisions on the necessity of these systems. Furthermore, legal and political implementations of these databases, their expected efficiency, and their consequences for human rights were not taken into consideration properly in the decisions developing these databases.³⁴ Thus, it can be said that SIS II, VIS, and Eurodac were devised as solutions waiting for problems which would be determined by professional managers of unease, such as customs, intelligence services, or police, who target immigrants as new experimental objects for their technologies and projects and thus define immigration as a threat to internal security. Regarding the European level of cooperation on migration in the 1990s, Guiraudon stresses that “solutions had been devised before problems had been defined” and “the solution was police cooperation and reinforced controls.”³⁵ Today, these solutions are new technologies of surveillance and control designed as flexible tools to keep up with new developments and requirements. This flexibility would come to mean being ready for future functionalities, which brings us to the second common feature that led to securitization of migration.

SIS II, VIS, and Eurodac violated the principle of purpose limitation, which is the core principle of data protection law and basically refers to collection of data for specified, explicit, and justified purposes.³⁶ Instruments originally designed for the management of migration, asylum and borders are increasingly being used in the field of internal security and law enforcement.³⁷ Initially established as administrative files, databases started to function as intelligence tools, which collect as much data as possible, with the extension of their purposes and additional authorities given access to these systems.³⁸ For instance, while the initial purpose of SIS was to compensate for the abolition of internal borders by assisting border, police, and customs control and preventing illegal immigration on a hit or no-hit basis,³⁹ SIS II assumed more security-oriented and intelligence purposes like ensuring a high level of security in AFSJ and granting access to Europol and Eurojust. Similarly, Eurodac and VIS were designed as reporting tools managing migration and asylum—the former reporting asylum seekers making multiple applications and the latter reporting the ones whose visa expired—but the recent revisions on their use and extension of the authorities having access to them rendered them investigative and intelligence tools. Although Boswell argues that the terrorism threat following 9/11 did not affect

33 Brouwer, *Digital Borders and Real Rights*, p.132; “Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)”, OJ L 218, 13 August 2008, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008R0767>, (Accessed 18 June 2020)

34 Brouwer, *Digital Borders and Real Rights*.

35 Virginie Guiraudon, “The constitution of a European immigration policy domain: a political sociology approach”, *Journal of European Public Policy*, Vol. 10, No 2, 2003, p. 268.

36 Queiroz, *Illegally Staying in the EU*.

37 Rijpma, *Brave New Borders*, p. 207; Christina Boswell, “Migration Control in Europe After 9/11: Explaining the Absence of Securitization”, *Journal of Common Market Studies*, Vol. 45, No 3, 2007, p. 589–610.

38 Brouwer, *Digital Borders and Real Rights*; Brouwer, *Legal Boundaries*.

39 A ‘hit’ means wanted persons or objects are found thanks to the data stored in SIS and the system states what to do with that person or object.

political discourse and practice in Europe, which had emerged long before 9/11 and thus rejected the predominant view that 9/11 terrorist attacks led to the securitization of migration as expected by logic of exceptionalism, she acknowledges that law enforcement agencies utilized migration-control practices to support counter-terrorism strategy.⁴⁰

Contrary to Boswells' argument that the use of counter-terrorism tools for migration control did not happen after 9/11, this study suggests that the use of immigration and asylum data for combating terrorism and crime by internal security and intelligence agencies created a security continuum, which depicts every immigrant and asylum-seeker as potential security threats. This led to the interchangeable use of migration and counter-terrorism tools. Even if there is no explicit discourse that declares immigrants as threats to internal security, the use of these technologies in the management of migration and asylum, deployed to combat traditional security threats such as terrorism and cross-border crime, is also a securitizing practice. Today, supporting this view is the trend towards further militarization of border surveillance and migration control, especially the extended use of aircrafts, helicopters and unmanned aerial vehicles (UAVs) in border management and deployment of armed forces at borders.

The securitization of migration is fundamentally caused by the routinized practices of police, customs, and border guards, the digitalization of border controls, the technologies of surveillance, and the use of biometrics, which were originally devised to prevent unwanted entries into European territory. Following the 9/11 attacks, counter-terrorism measures, new monitoring technologies, and computerized migration databases gained prominence in the EU immigration law, which intensified the claims that the EU is becoming an "electronic fortress",⁴¹ "cyber-fortress",⁴² or a "technological fortress",⁴³ to name a few appellations. As suggested by Broeders, recent migration databases created digital borders.⁴⁴ They are not only present in European territory but also in non-EU countries, airports, and even in international waters. For instance, the very recent technology launched for identifying illegal migrants, terrorists, and criminals is artificial intelligence-based lie detectors that started to be tested in the airports of Hungary, Latvia and Greece, expanded security measures in airports. This new technology will monitor passengers' faces to detect whether they are lying while answering questions about their travel, and this facet of the technology is widely criticized by privacy-advocating groups.⁴⁵ While the use of technology in migration policy may reinforce the security of external borders and cut irregular arrivals, the consequences concerning fundamental rights raises some ethical concerns that will be discussed in the next section.

40 Boswell, *Migration Control in Europe After 9/11*, p. 590.

41 Queiroz, *Illegally Staying in the EU*.

42 Elspeth Guild, et al., "The Commission's New Border Package: Does It Take Us One Step Closer to a 'Cyber-Fortress Europe?'" CEPS Policy Brief No. 154, 5 March 2008, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334058, (Accessed 19 June 2020).

43 Luisa Marin, "Is Europe Turning into a Technological Fortress? Innovation and Technology for the Management of EU's External Borders: Reflections on FRONTEX and EUROSUR", Michiel A. Heldeweg and Evisa Kica (eds.), *Regulating Technological Innovation. A Multidisciplinary Approach*, UK, Palgrave Macmillan Ltd, 2011, p. 131-151.

44 Broeders, "A European 'Border' Surveillance.

45 Rob Picheta, "Passengers to face AI lie detector tests at EU airports", 2 November 2018, <https://edition.cnn.com/travel/article/ai-lie-detector-eu-airports-scli-intl/index.html>, (Accessed 20 June 2020).

Ethical Concerns in Deploying Surveillance Technologies

Even if the providers and users of these databases have reached their aims in cutting large-scale irregular and illegal movements of people to European territory and securing borders, the consequences of this enormous technology on the rights of migrants and the founding norms and principles of the EU should be considered when deploying such databases. In this regard, a lack of proper impact assessment of these surveillance technologies raises serious ethical concerns regarding individual rights such as the right to privacy and data protection or the right to asylum.

The storage of personal information and of biometric data of migrants and asylum seekers at an unprecedented level, with the stated aim of identifying and distinguishing the wanted and unwanted movements, is a highly delicate issue, especially with respect to the right to privacy. Designed as flexible tools to embrace new functions, the above-discussed databases failed to specify and even justify their purposes and do not have clear limits of purpose. Broader access given to authorities responsible for law enforcement, internal security, and intelligence has concomitantly changed the initial purposes of databases as discussed above. The consequences of this change on individual rights are sometimes not even a secondary concern for the designers of such databases and policy makers who are rather busy with internal security objectives and profits. However, the collection of personal data for multiple, technically feasible purposes may harm data protection and infringe upon the right to privacy and private life that is enshrined in the article 8 of European Convention on Human Rights. This can also result in politically unjustifiable data collection. The trends and regulations in using databases and biometrics do not comply with the standards set to protect private life, such as by storing information without informing individuals properly and by having too general, unspecified purposes, or transferring information to third parties.⁴⁶

Queiroz, for instance, discusses how recent technological developments in information systems facilitate “crimmigration”, that is the conflation of immigration and criminalization.⁴⁷ He emphasizes how three drivers of the criminalization of immigration interact negatively with the data extracted from these information systems; namely, failing to comply with the principle of purpose limitation, enhanced accessibility instead of proportionality, and the shift from immigration to an instrumental use of databases.⁴⁸ Extensive and authoritarian use of these databases might also prevent individuals from exercising the international right of seeking asylum, which is guaranteed by the article 18 of Charter of Fundamental Rights of the EU.⁴⁹ Brouwer warns that, in order to protect asylum seekers and their rights to data protection, the personal data of asylum seekers stored in Eurodac should not be given to the authorities of the asylum seeker’s country of origin and thus to law enforcement and security agencies.⁵⁰ However, Eurodac is currently accessible to law enforcement authorities, and recent proposals to revise it present safety risks for asylum seekers, including the sharing personal data with third countries via the agents in the countries of origin seeking to persecute, which may inflict serious harm on the individuals and their families in need of international protection.⁵¹ For Ceyhan

46 Brouwer, *Legal Boundaries*, p. 140.

47 Queiroz, *Illegally Staying in the EU*.

48 *Ibid.*, p. 120.

49 “Charter of Fundamental Rights of the European Union”, Official Journal C 364, 18 December 2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf, (Accessed 23 June 2020).

50 Brouwer, *Legal Boundaries*, p.164.

51 European Union Agency for Fundamental Rights, “The impact of the proposal for a revised Eurodac Regulation on fundamental rights: Opinion of the European Union Agency for Fundamental Rights”, Vienna, FRA, December 2016.

and Tsoukala, the criminalization of migration also weakened the distinction between migrants and asylum seekers as all migrants documented or undocumented were monitored with suspicion, which reduced the number of asylum seekers obtaining refugee status.⁵²

Dijstelbloem also emphasizes the undesirable effects and risks of technology such as unjust refusal of migrants due to errors in information files; biometry's violation of personal integrity; excessive demand for carrying out checks; and stigmatization and discrimination of people on the ground of race, color or religion.⁵³ In brief, ethical concerns associated with the use of these large-scale databases should be addressed by policy makers, if not by the companies designing the databases. Public scrutiny and control by independent supervisory authorities should be allowed. This might be a promising way to safeguard the fundamental rights of migrants. As suggested by Dijstelbloem, when migrants are treated as the subject—instead of the object—of migration policy, greater justice will be established in relation to their status.⁵⁴

It is also important to recall the founding norms and principles of the Union, including the rule of law, human rights, and anti-discrimination. These are also placed under risk with the recent trends in using the IT systems, which undermines the EU's normative foreign policy. The next section will discuss the repercussions of securitizing aspects of centralized databases on the normative power of the EU.

Reflections of Surveillance Technologies on the Normative Power of the EU

This section of the study discusses how the surveillance technologies of the EU -SIS, VIS, and Eurodac- contradict the main components of normative power and normative foreign policy of the EU. The concept of normative power is first briefly explained.⁵⁵

There are several studies that focus on the criteria of what constitutes a normative power and whether the EU can be defined as a normative actor in its external relations.⁵⁶ Some of these criteria will be discussed here in relation to the EU's foreign policy on border management and migration

52 Ceyhan and Tsoukala, *The Securitization of Migration*, p.28.

53 Huub Dijstelbloem, "Europe's new technological gatekeepers. Debating the deployment of technology in migration policy", *Amsterdam Law Forum*, Vol. 1, No 4, 2009, p. 13-14.

54 *Ibid.*, p.18.

55 Here in this study, the normative power of the EU is assessed within the context of its surveillance technologies or IT systems that are part of its migration and border management policies. To be more precise, this study does not look at all the components of the EU's migration and border management policies which for instance comprises externalization of migration policies to non-EU countries, militarization of borders, return and readmission policies etc. For a detailed analysis of the EU's normative power in the field of migration policy see Ceren Zengin, *Assessment of the European Union's Normative Power Within the Context of its Migration Policy*, Unpublished M.A. Thesis, Ankara, Middle East Technical University, Graduate School of Social Sciences, 2017.

56 Ian Manners, "Normative Power Europe: A Contradiction in terms?" *Journal of Common Market Studies*, Vol. 40, No 2, 2002, p. 235-258; Ian Manners, "The European Union as a Normative Power: A Response to Thomas Diez", *Millennium: Journal of International Studies*, Vol. 35, No 1, 2006, p. 167-180; Ian Manners, "The Normative Ethics of the European Union", *International Affairs*, Vol. 84, No 1, 2008, p. 45-60; Helene Sjursen, "The EU as a 'normative' power: how can this be?", *Journal of European Public Policy*, Vol.13, No 2, 2006, p.235-251; Thomas Diez, "Constructing the Self and Changing Others: Reconsidering 'Normative Power Europe'", *Journal of International Studies*, Vol. 33, No 3, 2005, p. 613-636; Federica Bicchi, "Our size fits all': normative power Europe and the Mediterranean", *Journal of European Public Policy*, Vol. 13, No 2, 2006, p. 286-303; Nathalie Tocci, "Profiling Normative Foreign Policy: The European Union and its Global Partners." CEPS Working Documents No. 279, 20 December 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1337974 (Accessed 15 June 2020).

policy. The ‘normative power Europe’ concept was first put forward by Ian Manners, who differentiated the normative power of the EU from the traditional classifications of the EU as a civilian or military power and emphasized the normative basis of the EU with reference to its founding norms and principles such as rule of law, human rights, democracy, anti-discrimination, and social solidarity that are specified under the EU treaties and declarations.⁵⁷ Manners suggests that the diffusion of such norms and principles to the outside world through several mechanisms is the *sine qua non* of the EU’s normative power because its normative power comes from “its ability to shape the conceptions of ‘normal’ in international relations.”⁵⁸ In other words, the EU is a normative power to the extent that it spreads its normative basis to non-EU countries and regions and ‘normalizes’ its norms in world politics. Manners defines this ability as the “the greatest power of all.”⁵⁹

There are several other studies suggesting a number of criteria for being a normative power. Sjørusen, for instance, emphasizes the consistency of EU norms with the international legal system, ‘self-binding’ through law (that is the EU binding itself, not only others, through international law) and transforming power politics through strengthening cosmopolitan law as distinguishing indicators of normative power.⁶⁰ Diez, on the other hand, gives importance to ‘self-reflexivity’ as a distinguishing feature of normative power. For him, the normative power discourse is a kind of practice that constructs the European identity and constructing identity through creating others as inferior may cause the EU to overlook its own shortcomings and thus risk its normative power.⁶¹ In this regard, only reflexive thinking can prevent the EU from violating international norms while creating its own identity and that of others and rescue the normative power that Europe claims.⁶²

In this study on the EU’s surveillance technologies, the EU’s normative power or foreign policy will be assessed using Nathalie Tocci’s proposed criteria for being a normative power.⁶³ For Tocci, normative foreign policy has three major components: normative goals, normative means, and normative impact. Inspired by Wolfer’s definition of milieu and possession goals,⁶⁴ Tocci defines normative goals as milieu goals that shape the environment by taking international legal arrangements, regimes, and law into consideration, thus binding all the actors concerned; normative means as instruments that are used within the boundaries of law, regardless of their being persuasive or coercive methods; and normative impact as the results that meet the normative objectives of the foreign policy actor. By looking at the goals, means, and impact of any foreign policy, Tocci defines four foreign policy types or actors: normative, realpolitik, imperial, and status quo. Table 1 illustrates how different combinations of goals, means, and impact produce different foreign policy outcomes.⁶⁵

57 Manners, Normative Power Europe, p. 235-258.

58 Ibid., p. 239.

59 Ibid., p. 253.

60 Sjørusen, The EU as a ‘normative’ power, p. 235-251.

61 Diez, Constructing the Self and Changing Others, p. 613-636.

62 Ibid., p. 632, 636.

63 This study uses Nathalie Tocci’s analysis on normative foreign policy for two reasons. Firstly, Tocci’s analysis addresses almost all of the normative power criteria suggested in the literature. Thus, it is a comprehensive one. Secondly, Tocci’s classification of foreign policy outcomes on the basis of the interplay of the goals, means, and impact provides an opportunity to compare different types of foreign policy and define the EU’s international identity on this basis.

64 While milieu goals refer to those that aim to shape the conditions of the environment (milieu), possession goals refer to maintenance or reinforcement of national possessions. See Tocci, Profiling Normative Foreign Policy, p. 4.

65 In Table 1, Tocci adds a new dimension, that is, ‘impact’ may be intended or unintended. Intended impact refers to harmony between the goals and the results and unintended impact is incompatible with the goals set at the beginning.

Table 1: Foreign Policy Outcomes

Type of actor	Normative		Realpolitik		Imperial		Status Quo	
	Intended	Unintended	Intended	Unintended	Intended	Unintended	Intended	Unintended
Goals								
Means								
Impact								



Non-normative



Normative

Source: Tocci, *Profiling Normative Foreign Policy*, p. 9.

In the light of the discussion above on normative power, it is now essential to discuss why the deployment of surveillance technologies through the EU’s centralized databases—SIS, VIS, and Eurodac—contradict the EU’s normative power or foreign policy. To be more precise and clear, this study analyses how the EU behaves like a realpolitik actor with its non-normative goals, means, and impact rather than as a normative actor (see below with Table 2). In stark contrast to the normative goals, the EU has non-normative and possession goals in deploying surveillance technologies. Rather than shaping its environment within the confines of law, the EU aims to secure its external borders, maintain the security of ‘area of freedom, security and justice’, and curtail irregular flows to the EU. None of these goals are normative, as they seek to enhance or maintain possessions of the EU instead of shaping the conditions beyond its borders.

The militarization and digitalization of surveillance at the borders, providing internal security and intelligence agencies and law enforcement authorities such as Europol and Eurojust with access to centralized databases and the collection of personal data for multiple, unspecified, and unjustifiable purposes, are the non-normative means of the EU in deploying surveillance technologies because neither of them meets the criteria of complying with domestic and international legal principles. As discussed in previous sections, the deployment of such centralized databases results in the securitization

of migration and therefore treating migrants or asylum seekers as if they are potentially responsible for organized crimes such as terrorism or cross-border crime. Sealing borders to unwanted migrants and asylum seekers is also another non-normative outcome of deploying SIS, VIS, and Eurodac. It causes people in need of international protection to find more dangerous migratory routes to reach European shores. Violation of the principles of non-refoulement and the respect for human rights, right to privacy, and right to asylum that are enshrined under European and international law illustrate the non-normative impact of the EU’s foreign policy, rendering the EU a realpolitik actor in external border management rather than a normative power as claimed by Ian Manners or the EU itself. Thus, the security concerns of EU member states outweigh their normative commitments in the case of migration and border security.

Table 2: The EU as a Realpolitik Actor⁶⁶

EU MIGRATION POLICY	Goals	Means	Impact	Type of actor
IT Systems SIS, VIS, Eurodac	Non-normative <ul style="list-style-type: none"> • Security of external borders • Maintaining the security of ‘area of freedom, security and justice’ of the EU • Curtailing irregular flows to the EU. 	Non-normative <ul style="list-style-type: none"> • Militarization and digitalization of surveillance at the borders • Giving access to internal security and intelligence agencies and law enforcement authorities- Europol and Eurojust • Collection of personal data for multiple, unspecified and unjustifiable purposes 	Non-normative <ul style="list-style-type: none"> • Securitization of migration and border management • Shifting responsibility for migration and asylum management to non-EU countries • Sealing borders to unwanted migrants • More dangerous migratory routes for refugees • Violation of international and European law (non-refoulement and respect for human rights, right to privacy and right to asylum) 	REAL POLITIK ACTOR

Source: Authors’ own construction

⁶⁶ Table 2 is the authors’ own construction inspired by two authors: Nathalie Tocci and Ceren Zengin. See Tocci, “Profiling Normative Foreign Policy,” p. 9, and Zengin, Assessment of the European Union’s Normative Power, p. 125.

In sum, in contrast to the claim of a ‘normative power Europe’, the findings of this study suggest that the EU behaves like a *realpolitik* actor on account of its migration policies and border management. Apart from the consequences of the EU’s non-normative foreign policy behavior on migrant rights, which led us to define the EU as a *realpolitik* political body, there might be a new set of implications of identifying the EU as a *realpolitik* actor in the field of migration and border management. On the one hand, the EU’s current practices are encouraging us to test the credibility of the EU’s normative power claim and reveal its shortcomings. On the other hand, identifying the EU as a *realpolitik* actor in its migration and border management policies and the EU’s possible acknowledgement of this non-normative identity might have some unfavorable effects on migrant rights and the leverage that human rights actors have on the EU. That is, if defining the EU as a *realpolitik* actor would better serve the naming and shaming strategies of human rights organizations in denouncing the EU’s human rights violations, such as its practices of pushbacks, forced return, border closures, denial of access to asylum seekers at EU borders, and encouraging the EU as a normative power to enforce its normative commitments, this might be constructive for migrant rights and the normative international identity of the EU. However, on the other hand, if identifying the EU as a *realpolitik* actor would come to mean for the EU an admission to this non-normative identity and further justification of its security-oriented migration and border management practices, then such a *realpolitik* identification might remove the leverage that human rights actors have on the EU. Indeed, the claim of ‘normative power Europe’ provides opportunities for several human rights organizations to criticize the security-oriented policies and practices of the EU and to encourage EU member states and institutions to practice what they preach. Hence, there is a need for further research on the implications of identifying the EU as a *realpolitik* actor in the field of migration and border management and its foreign policy behavior in the future.

Concluding Remarks

This study treated the role of surveillance technologies in the securitization of migration policies and the implications of such practices on the fundamental rights of migrants and the normative power of the EU. The first section looked at the securitization of migration with a particular emphasis on the theoretical framework of the Paris School, pioneered by Didier Bigo. The second section examined the initial and current purposes of the EU’s large-scale IT systems, namely, SIS, VIS, and Eurodac, in order to illustrate their securitizing practices. The third section discussed the ethical concerns associated with deploying surveillance technologies. The final section evaluated the consequences of surveillance technologies on the normative foreign policy of the EU.

This study sought to highlight several issues. The migration policy of the EU is fundamentally motivated by the security concerns of its member states. The arguments of the Paris School are more promising in explaining the securitization of migration in Europe and the role of surveillance technologies in this process. The objectives of the EU’s centralized databases are not only to manage asylum or migration at the borders anymore but now also to safeguard internal security, to counter terrorism, and to combat organized crime. The extensive use of surveillance technologies raises ethical concerns regarding the rights of individuals, which should be addressed by proper impact assessment and independent supervision of these technologies. The normative power concept expresses an ideational power rather than a physical power; it gives particular importance to the normative goals, means, and

impact of any external policy and prioritizes normative commitments that are free of strategic interests. Lastly, surveillance technologies cause the securitization of migration and border management, which undermines the credibility of the EU's normative foreign policy as well as its founding norms, and thus causes it to behave as a *realpolitik* actor rather than a normative power.

Evidently, the issues this research is exploring are likely to have critical implications for Europe and beyond. The drift of EU practices from a normative to a *realpolitik* orientation is likely to be more than just a failure of the EU to practice what it preaches, and therefore a mere change in the EU's discourse of admitting its *realpolitik* precautions may be necessary but insufficient. As a matter of fact, the EU's increasing reliance on surveillance technologies may rob it of one of its core competencies in human rights, the one of leading by example. As this scenario has appeared more and more vivid in recent years, the EU is likely to observe the growing trend of rising illiberal tendencies from within, such as populists in Hungary, Poland, etc. and from its already volatile neighborhood, such as in MENA and Central Asia. Therefore, the two-fold integrative analysis of this paper on the role of surveillance technologies on the EU's normative power is the beginning rather than the end for the EU's global standing, where it still struggles to develop a coherent strategy that can speak and act in tandem. In the absence of such consistency and in the presence of amassing refugees and shouting populists, the securitization trend is likely to lead down to a risky path that further militarizes EU border security. Reading these likely trends in light of debates about the planned EU battle groups, PESCO, Frontex, and EU border guards reveals the emergence of an Orwellian Fortress Europe rather than a Kantian peaceful Europa. Undoubtedly, international reactions are likely to be significantly different to those contrasting EU-images, and therefore these trends, along with their policy implications, offer diverse venues for multi-dimensional and multi-stakeholder future research concerning Europe and beyond.