German Law Journal (2024), **25**, pp. 935–955
doi:10.1017/glj.2024.52

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Special Issue: Strategic Litigation in EU Law

Climbing a Wall: Strategic Litigation Against Automated Systems in Migration and Asylum

Francesca Palmiotto[1] and Derya Ozkul[2]

[1]IE University, Madrid, Spain, and Hertie School, Berlin, Germany and [2]University of Warwick, Coventry, UK
Corresponding author: Derya Ozkul; Email: derya.ozkul@warwick.ac.uk

(Received 24 October 2024; accepted 19 November 2024)

Abstract
Strategic litigation plays a crucial role in advancing human rights in the digital age, particularly in cases where data subjects, such as migrants and protection seekers, experience significant power imbalances. In this Article, we consider strategic litigation as part of broader legal mobilization efforts. Although some emerging studies have examined contestation against digital rights and migrant rights separately using legal mobilization frameworks, scholarship on legal mobilization concerning the use of automated systems on migrants and asylum seekers is scarce. This Article aims to address this gap by investigating the extent to which EU law empowers strategic litigants working at the intersection of technology and migration. Through an analysis of five specific cases of contestation and in-depth interviews, we explore how EU data protection law is leveraged to protect the digital rights of migrants and asylum seekers. This analysis takes a socio-legal perspective, analyzing the opportunities presented by EU data protection law and how civil society organizations (CSOs) utilize them in practice. Our findings reveal that the pre-litigation phase is particularly onerous for strategic litigants in this field, requiring a considerable investment of resources and time before even reaching the litigation stage. We illustrate this phase as akin to "climbing a wall," characterized by numerous hurdles that CSOs face and the strategies they employ to overcome them.

Keywords: Automated systems; strategic litigation; legal mobilization; data protection; EU law; GDPR; migration; asylum

A. Introduction

Contesting automated systems is challenging due to the need for specific legal expertise, a comprehensive understanding of the system in place, and ample resources. One major barrier is the opaqueness surrounding algorithms, which makes it difficult for people who are subjected to them to detect their presence and understand their inner workings. Automated systems often operate in the shadows and are invisible to outsiders, so individuals may not even realize that their application has been subjected to automated assessment. Contesting automated systems also demands technical expertise and access to information, often protected by trade secrets or safeguarding national security, especially in the case of migration. Consequently, although individuals affected by these tools have initiated a few litigation efforts, likely due to a lack of resources and knowledge, civil society organizations (CSOs) have emerged as the primary actors contesting the use of automated systems.

Strategic litigation is vital to advancing human rights in the digital age, particularly where vulnerable data subjects, such as migrants and protection seekers, suffer significant power

imbalances. Acknowledging the importance of CSOs in protecting digital rights, the General Data Protection Regulation (GDPR) offers new legal opportunities for strategic litigation. For example, Article 80 of the GDPR explicitly allows non-profit organizations to bring complaints on behalf of data subjects. Moreover, regarding automated decision-making, EU law sets different safeguards for individual rights, most notably the right not to be subject to an automated decision, rights of access and transparency, and remedies for violating data protection law. The venues offered by EU data protection law complement other available remedies to challenge automated systems, deriving from international human rights law, EU primary law, public administrative law principles, and constitutional rights of EU Member States.

Considering the different legal venues available and the practical challenges in contesting automated systems highlighted above, in this Article, we investigate specifically how EU data protection law is mobilized to defend migrants' and asylum seekers' digital rights.[1] This question is important to study because migrants, including asylum seekers, are among the most vulnerable data subjects as they face the risk of being denied entry to a territory or being deported at any time with little power to contest. We address this question from a socio-legal perspective, showing not only what venues EU data protection law offers but also how CSOs use them in practice. By exploring the role of legal mobilization in addressing systemic issues faced by migrants and asylum seekers, our Article aims to contribute to a broader understanding of how legal mobilization can drive changes in law, policy, and implementation of automated systems.

In the next section, Section B, we establish our conceptual framework, locating "strategic litigation" within CSOs' broader efforts of "legal mobilization." Despite some emerging studies that use legal mobilization frameworks to examine contestation against digital rights and migrant rights separately, we point out the scarcity of scholarship in analyzing legal mobilization against the use of automated systems on migrants and asylum seekers. Our Article aims to fill this gap. After briefly outlining the affordances of EU law for contesting automated systems, we introduce our key research question—to what extent does EU law empower strategic litigants—and outline our approach to studying it. We explain the case studies we have selected, demonstrating various instances of CSOs working to contest automated systems used in migration and asylum contexts.

Moving on to Section C, we analyze the efforts of CSOs to overcome these barriers to litigation. We find that CSOs mobilize in three main ways. First, they utilize freedom of information (FOI) laws to demand transparency regarding the presence and functioning of the technologies they are concerned with. Second, they seek specialized legal and technical expertise by engaging technologists and legal advisers who are experts in data protection laws, as well as by forming coalitions with external actors when they lack this expertise in-house. Third, after gathering sufficient information and evidence on (potential) harms, they choose to submit their complaints to the relevant Data Protection Authorities (DPAs) in their countries or file their claims in courts, depending on the "legal opportunity structures" in the jurisdictions they operate and to what extent they can overcome the barriers.

In our concluding discussion, we combine our conceptual framework and findings and argue that the several barriers faced by CSOs hamper their possibility of even reaching the litigation stage and access to justice. We metaphorically illustrate the pre-litigation phase as a wall consisting of multiple hurdles that exemplify the barriers they encounter and the strategies they need to use to overcome them. Finally, we provide recommendations to dismantle this wall, thereby enabling strategic litigants to contribute to shaping a digital society in compliance with fundamental rights and democratic principles.

[1]In this Article, the term "automated systems" refers to any automated tools used to assist, support, inform, or complement human decision-makers in the field of migration and asylum.

B. Framing Strategic Litigation Against Automated Systems

I. Strategic Litigation as a Form of Legal Mobilization

The term "strategic litigation" lacks a universally accepted definition in the literature;[2] however, most studies agree that it involves a purposeful approach to litigation aimed at achieving structural change beyond individual benefit. In contrast to "common litigation," which focuses on defending individual interests, strategic litigation is intentionally pursued to achieve outcomes with broader societal implications. This approach leverages courts to drive reform at a structural level and challenges the distribution of legal, political, social, or economic goods in society.[3] Although common litigation may incidentally result in broader impacts, such outcomes are unplanned and unintended.

Moreover, strategic litigation is sometimes used interchangeably with "public interest litigation."[4] This refers to "civil rights advocacy seeking to restructure public agencies" or public policies.[5] In contrast to traditional litigation, which aims to settle "disputes between private parties about private rights,"[6] public interest litigation seeks to promote public welfare. The term "strategic litigation" is also sometimes used interchangeably with "test case litigation," but their objectives may differ. Test case litigation primarily aims to test arguments or legal principles, establishing precedents for the future. In contrast, strategic litigation not only seeks to establish precedents but also aims to influence the political agenda through litigation.[7]

The concept of "strategic litigation" also shares similarities with "legal mobilization," which involves "the use of law in an explicit, self-conscious way through the invocation of a formal institutional mechanism."[8] In one of the earlier works on legal mobilization, Zemans states that legal mobilization is intrinsically linked to the assertion of rights:

> Defining legal mobilization as the act of invoking legal norms to regulate behavior is purposively broad enough to include the earliest stage of legal activity; in its simplest case, a particular behavior is demanded by verbal appeal to the law. The law is thus mobilized when a desire or want is translated into a demand as an assertion of one's rights.[9]

The scholarship on legal mobilization refers to using the law to build, energize, or shape social movements, as well as political agendas.[10] This scholarship corrected the early social movement literature's lack of emphasis on using the law as a means of mobilization.[11] In that sense, the

[2]Michael Ramsden & Kris Gledhill, *Defining Strategic Litigation,* 4 Civ. Just. Q. 407, 409 (2019).

[3]Michael Ramsden, *Strategic Litigation Before the International Court of Justice: Evaluating Impact in the Campaign for Rohingya Rights*, 33 Eur. J. Int'l L. 442, 444 (2022) [hereinafter Ramsden, *Rohingya Rights*].

[4]Alan K. Chen & Scott Cummings, Public Interest Lawyering: A Contemporary Perspective (2014).

[5]Charles F. Sabel & William H. Simon, *Destabilization Rights: How Public Law Litigation Succeeds*, 117 Harv. L. Rev. 1016, 1016 (2004).

[6]Abram Chayes, *The Role of the Judge in Public Law Litigation*, 89 Harv. L. Rev. 1281, 1282 (1976).

[7]Michael Ramsden, *Strategic Litigation in English Judicial Review*, 28(4) Jud. Rev. 261, 263 (2023) [hereinafter Ramsden, *Strategic Litigation*].

[8]Emilio Lehoucq & Whitney K. Taylor, *Conceptualizing Legal Mobilization: How Should We Understand the Deployment of Legal Strategies?*, 45 L. & Soc. Inquiry 166, 168 (2020).

[9]Frances Kahn Zemans, *Legal Mobilization: The Neglected Role of the Law in the Political System*, 77 Am. Pol. Sci. Rev. 690, 700 (1983).

[10]*See generally* Paul Burstein, *Legal Mobilization as a Social Movement Tactic: The Struggle for Equal Employment Opportunity*, 96 Am. J. of Socio., 1201–25 (1991); Chris Hilson, *New Social Movements: The Role of Legal Opportunity*, 9 J. of Eur. Pub. Pol'y, 238–55 (2002); Charles R. Epp, The Rights Revolution: Lawyers, Activists, and Supreme Courts in Comparative Perspective (1998); Michael W. McCann, Rights at Work: Pay Equity Reform and the Politics of Legal Mobilization (1994); Leveraging the law: using the courts to achieve social change (D. A. Schultz ed., 1998).

[11]*See generally* Doug McAdam, Sidney Tarrow & Charles Tilly, Dynamics of Contention (2001) (displaying early research on social movement literature).

scholarship on legal mobilization has broadened the social movement field by looking at how actors shape a social movement through the use of law.[12] It also examines how actors interact with the law when there is no alternative way to perform their rights[13] on an everyday basis—through the attainment of legal consciousness over a period of time.[14] However, this consciousness can alter after the experience of litigation.[15] Analyzing how activists mobilized around disability, Lisa Vanhala defines the scope of the term as the following:

> Legal mobilization can include many different types of strategies and tactics, such as raising rights consciousness among particular communities or the public, delivering public legal education or specialized legal education, lobbying for law reform or changes in the levels of access to justice, providing summary legal advice and referral services, and undertaking strategic or test case litigation.[16]

The term "legal mobilization" connotes a wider range of activities to mobilize the law, compared with "strategic litigation," which is focused on litigation alone.

Drawing upon this scholarship, in this Article, we use the term "strategic litigation" to examine how various actors use litigation to pursue objectives beyond individual cases,[17] treating it as one of the forms of legal mobilization. We define "strategic litigation" as "*the intentional use of litigation to effect legal or policy change beyond individual cases*." To explore broader uses of the law, including alternative legal avenues for seeking justice, we use the term "legal mobilization." In the context of automated decision-making systems in migration and asylum, available legal routes include seeking information from public authorities through FOI laws, seeking grievances against violations of the data protection law through DPAs and providing witness evidence in court cases.

Overall, the scholarship analyzing the use of litigation for broader objectives has evolved in different strands. One strand of this scholarship focuses solely on the success of strategic litigation. Several studies have explored the effectiveness of litigation in terms of changing the law, using the law in a new way, or altering the implementation of existing laws. However, as Helen Duffy points out, the success of strategic litigation cannot always be understood by looking at the outcome of a court case alone but by the wider impacts that particular litigation has given rise to.[18] For example, looking at the impact of judicial activism on socioeconomic rights in Latin America, Rodriguez-Garavito finds that judicial decisions can lead to both direct and indirect material and symbolic impacts.[19] On the one hand, the direct material impact refers to the establishment of a legal precedent and changes in the implementation of the law. On the other hand, the indirect symbolic impact involves transforming public opinion.

This second strand of scholarship conceptualizes success more broadly in terms of changing political debates and public opinions about the issue at hand. This scholarship also takes a different epistemological approach to studying legal mobilization. Instead of taking only a causal

[12]*See generally* Research handbook on law, movements and social change (S. A. Boutcher, C.S. Shdaimah, M.W. Yarbrough eds., 2023); Lisa Vanhala, Making Rights a Reality?: Disability Rights Activists and Legal Mobilization (2010).

[13]Whitney K. Taylor, *Ambivalent Legal Mobilization: Perceptions of Justice and the Use of the Tutela in Colombia*, 52 L. & Soc'y Rev. 337, 367 (2018).

[14]Amy Blackstone, Christopher Uggen & Meather McLaughlin, *Legal Consciousness and Responses to Sexual Harassment*, 43 L. & Soc'y Rev. 631, 668 (2009); Shannon Gleeson, *Labor Rights for All? The Role of Undocumented Immigrant Status for Worker Claims Making*, 35 L. & Soc. Inquiry 561, 602 (2010).

[15]Mary Gallagher & Yujeong Yang, *Getting Schooled: Legal Mobilization as an Educative Process*, 42 L. & Soc. Inquiry 163, 194 (2017).

[16]Vanhala, *supra* note 12, at 6.

[17]Ramsden, *Rohingya Rights*, supra note 3 at 442.

[18]*See generally* Helen Duffy, Strategic human rights litigation: understanding and maximising impact (2018).

[19]Rodríguez-Garavito César, *Beyond the Courtroom: The Impact of Judicial Activism on Socioeconomic Rights in Latin America*, 89 Tex. L. Rev. 1669, 1698 (2011).

approach, such as what actions lead to what outcomes, they also incorporate a constructionist perspective to legal mobilization and look at how actors frame their cause and how that framing may change over time according to the "legal opportunity structures"[20] as well as the social and political contexts they are located in,[21] and the role of mobilizing actors.[22] Analyzing the framing around a cause matters not only to understand the success of litigation but also how it changes a social movement. For example, Lisa Vanhala's scholarship shows that the act of mobilizing rights can have both intended and unintended consequences for social movements themselves.[23] Her book on disability rights shows that strategic litigation may change not only the political discourse but also how the social movement around that particular topic itself is framed. This strand of scholarship tends to take a longitudinal approach to analyze the impact of legal mobilization over time, not just the short-term immediate impact of litigation.

The scholarship has also examined various topics of study, including mobilization around migration and migrant rights in the context of Europe.[24] One important area of study is identifying the actors involved in this field. For example, Passalacqua analyzed 291 rulings of the CJEU relating to migration to map out the actors that defend migrant rights at the European level.[25] Pijnenburg and van der Pas have mapped out existing strategic litigation cases against human rights violations that arise from migration controls in Europe.[26] This strand of literature also explores why some CSOs use EU law more frequently than others and what factors lead to this mobilization.[27] Another area of study is how litigation occurs in different levels of judicial fora and its impacts. The literature has explored how CSOs mobilize EU, international, and domestic legislation on discrimination to promote migrants' rights.[28] Specifically, this literature analyses how actors use legislation at the national level,[29] before the CJEU,[30] and compares the practice of intervention before the CJEU with its counterpart in Strasbourg, the European Court of Human Rights.[31] However, the scholarship also points out that immediate successes in litigation are not the end of the story. As Southerden has pointed out, executive reactions can subvert the outcomes

[20]For a broader use of this concept within the legal mobilization scholarship, *see generally* Gianluca De Fazio, *Legal Opportunity Structure and Social Movement Strategy in Northern Ireland and Southern United States*, 53 Int'l J. Compar. Socio. 3–22 (2012); Gesine Fuchs, *Strategic Litigation for Gender Equality in the Workplace and Legal Opportunity Structures in Four European Countries*, 28 Can. J. L. & Soc'y / Revue Canadienne Droit et Société 189–208 (2013); Ellen Ann Andersen, Out of the Closets and into the Courts (Univ. of Mich. Press) (2018); Lisa Vanhala, *Is Legal Mobilization for the Birds? Legal Opportunity Structures and Environmental Nongovernmental Organizations in the United Kingdom, France, Finland, and Italy*, 51 Compar. Pol. Stud. 380–412 (2018); Lisa Vanhala, *Legal Opportunity Structures and the Paradox of Legal Mobilization by the Environmental Movement in the UK*, 46 L. & Soc'y Rev. 523–56 (2012).

[21]Fuchs, *supra* note 20.

[22]Vanhala, *supra* note 20.

[23]Vanhala, *supra* note 12.

[24]*See generally* Leila Kawar, *Contesting Migration Governance through Legal Mobilization*, *in* Handbook on the Governance & Pols. of Migration 380 (2021).

[25]Virginia Passalacqua, *Who Mobilizes the Court? Migrant Rights Defenders Before the Court of Justice of the EU*, 15 L. & Dev. Rev. 381, 381 (2022).

[26]*See generally* Annick Pijnenburg & Kris Van Der Pas, *Strategic Litigation against European Migration Control Policies: The Legal Battleground of the Central Mediterranean Migration Route*, 24 Eur. J. Migration & L. 401–29 (2022).

[27]*See generally* Kris Van Der Pas, *All That Glitters Is Not Gold? Civil Society Organisations and the (non-)Mobilisation of European Union Law*, 62 J. Common Mkt. Stud. 525–45 (2024).

[28]*See generally* Venera Protopapa, *From Legal Mobilization to Effective Migrants' Rights: The Italian Case*, 26 Eur. Pub. L. 477–507 (2020).

[29]*See generally* Venera Protopapa, *Shaping Equality for Migrants. Legal Mobilisation in Italy and the Race Equality Directive*, J. Européen des Droits de l'Homme 3–32 (2019); Virginia Passalacqua, *El Dridi Upside Down: A Case of Legal Mobilization for Undocumented Migrants' Rights in Italy*, Tijdschrift voor bestuurswetenschappen en publiekrecht 215–25 (2016).

[30]Virginia Passalacqua, Legal Mobilization and the Judicial Construction of EU Migration Law (Feb. 17, 2020) (PhD dissertation, European University Institute) (on file with European University Institute).

[31]Jasper Krommendijk & Kris Van Der Pas, *To Intervene or Not to Intervene: Intervention Before the Court of Justice of the European Union in Environmental and Migration Law*, 26(8) Int'l J. of Hum. Rts. 1394 (2022).

of even successful litigation.[32] This underscores the need for a comprehensive and long-term analysis of the entire mobilization process beyond the immediate success of a particular case. Notably, none of this scholarship in migration and asylum fields has examined legal mobilization against the uses of automated systems.

With regards to strategic litigation against the use of algorithms or their unfair outcomes, the scholarship explores the use of litigation against algorithmic management in employment, including platform work,[33] and the use of strategic litigation in internet and data protection laws.[34] Additionally, there are opinion pieces[35] and reports[36] that examine what the EU law offers litigators and what specific strategies are available for litigators to challenge the use of automated systems in the public sector. Anne Kaun further explores litigation against a municipality's use of an automated system for welfare provision in Sweden and analyzes the negotiations and meaning-making around the definition of the system in use during contestation processes.[37] Her analysis shows that litigation also involves re-imagining what these technologies are and what they are capable of. However, none of this scholarship examines litigation or other forms of legal mobilization against the use of algorithms and their unfair outcomes in migration and asylum contexts.

Therefore, in this Article, we aim to fill this gap by investigating the relatively unexplored area of legal mobilization in challenging automated systems within migration and asylum contexts. We focus specifically on the actors involved and the structural opportunities and barriers they face. Despite the increasing prevalence of these technologies and mounting concerns about their impact on migrants and asylum seekers,[38] there remains a significant lack of studies examining legal mobilization around them. As we explain below, a number of CSOs have been involved in addressing these issues, yet there has been no analysis of their experiences with judicial and non-judicial avenues. Inspired by the constructionist strand of scholarship, we start our analysis by investigating the context in which CSOs operate. In the following section, we focus on the affordances of EU law and the barriers to strategic litigation.

II. The Role of EU Law in Contesting Automated Systems

Contesting automated systems is challenging. As scholars have long observed, individuals and CSOs encounter significant obstacles when contesting automated systems, which in turn hamper the right to an effective remedy and due process rights.[39] Despite these challenges, EU data

[32]Tom Southerden, "Lifting the Wire": Litigating for Migrants' Rights in the UK (Jan. 19, 2017) (Ph.D. dissertation, University of Sussex) (on file with the University of Sussex).

[33]Antonio Aloisi, *Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights*, 40 INT'L J. COMPAR. LAB. L. & INDUS. RELS. 37, 40 (2024); Giovanni Gaudio, *Litigating the Algorithmic Boss in the EU: A (Legally) Feasible and (Strategically) Attractive Option for Trade Unions?*, 40 INT'L J. COMPAR. LAB. L. & INDUS. RELS. 91, 91 (2023).

[34]COURTS, PRIVACY AND DATA PROTECTION IN THE DIGITAL ENVIRONMENT 10 (Maja Brkan & Evangelia Psychogiopúlu eds.) (2017); Sean McDonald, Impact-Orienting Digital Strategic Litigation (Jan. 1, 2020) (unpublished manuscript) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805834); Vera Strobel, *Strategic Litigation and International Internet Law*, *in* DIGITAL TRANSFORMATIONS IN PUBLIC INTERNATIONAL LAW 261, 274 (Angelo Jr. Golia et. al. eds., 2022).

[35]Nani Jansen Reventlow, *Making Accountability Real: Strategic Litigation*, DIGIT. FREEDOM FUND BLOG (Jan. 30, 2020), https://digitalfreedomfund.org/making-accountability-real-strategic-litigation/.

[36]*Litigating algorithms: Challenging government use of algorithmic decision systems*, AI NOW INSTITUTE (2018), https://ainowinstitute.org/wp-content/uploads/2023/04/litigatingalgorithms.pdf.

[37]Anne Kaun, *Suing the Algorithm: The Mundanization of Automated Decision-Making in Public Services through Litigation*, 25 INFO. COMMC'N & SOC'Y 2046, 2047 (2022).

[38]Derya Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe.*, REFUGEE STUD. CTR. (2023), https://www.rsc.ox.ac.uk/publications/automating-immigration-and-asylum-the-uses-of-new-technologies-in-migration-and-asylum-governance-in-europe.

[39]*See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. UNIV. L. REV. 1249, 1266 (2008); Andrea Aler Tubella, Andreas Theodorou, Virginia Digum & Loizos Michael, *Contestable Black Boxes, in* RULES AND REASONING 159, 159 (Víctor Gutiérrez-Basulto et al. eds., 2020); Madalina Busuioc, *Accountable Artificial Intelligence: Holding Algorithms to*

protection law offers crucial legal tools to challenge automated systems. The GDPR aims to protect the right to data protection, enshrined in Article 8 of the EU Charter of Fundamental Rights (CFR), by setting rights for data subjects and obligations for data controllers and processors. When considering automated systems, the GDPR in Article 22 importantly sets a prohibition of solely automated decisions, subject to exceptions, and conditions for their uses when allowed. Next to the prohibition of solely automated decisions, the Articles 12, 13, 14, and 15 of the GDPR grant data subjects individual rights, in particular transparency and access rights, to retain control over their personal data and be informed about data processing.

Additionally, the GDPR also provides remedies for violations of the Regulation. In case of a potential data protection infringement, individuals have access to judicial remedies, under Article 79 of the GDPR, or can choose to lodge a complaint with independent non-judicial authorities under Article 77 of the GDPR: the Data Protection Authority (DPA). The rationale behind creating extra-judicial remedies in the GDPR is to provide more easily accessible, quicker and less costly justice routes for data subjects, thus fostering an effective enforcement of data protection rights. Finally, the GDPR also enables CSOs to play an important bottom-up governance role in enforcing data protection rights.[40] To achieve effective protection of the right to data protection, Article 80 of GDPR allows CSOs acting in the public interest to make complaints and represent data subjects in front of DPAs or courts.[41] As pointed out in the literature, by including CSOs in the enforcement structure of data protection, the GDPR aims to foster a process of collective emancipation,[42] thus creating an "architecture of empowerment."[43]

Taken together, the GDPR provides an essential toolkit for strategic litigants challenging automated systems, granting standing and grounds for CSOs to contest technological practices, seek transparency, and access remedies to protect migrants' and asylum seekers' digital rights. At least, in theory. In practice, however, empirical research has identified critical GDPR enforcement issues, including inconsistencies in national practices and discrepancies in handling complaints by DPAs.[44] The recent and novel wave of litigation in this field is an occasion for scholars to test empirically whether EU data protection truly empowers strategic litigants.[45] The aim of this Article is precisely to analyze and assess the GDPR's legal potential in light of current litigation practices by CSOs in the understudied field of automated systems in migration and asylum. By exploring the role of strategic litigants in addressing systemic issues faced by migrants and asylum seekers, our Article seeks to contribute to a broader understanding of how legal mobilization can drive changes in law, policy, and the implementation of automated systems, and the role of EU law therein.

Account, PUB. ADMIN. REV. 825, 833 (2020). *See also* SIMONA DEMKOVA, AUTOMATED DECISION-MAKING AND EFFECTIVE REMEDIES: THE NEW DYNAMICS IN THE PROTECTION OF EU FUNDAMENTAL RIGHTS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE 47 (2023) (evaluating contesting automated systems in the specific context of migration and asylum); Dimitri Van Den Meerssche, *Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association*, 33 EUR. J. INT'L L. 171, 179 (2022).

[40]René Mahieu & Jef Ausloos, *Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access*, LAW ARCHIVE (Jul. 2, 2020), https://osf.io/preprints/lawarchive/b5dwm.

[41]*See Opinion of the Fundamental Rights Agency on the "Data Protection Reform Package,"* 2012 (2/2012) [hereinafter FRA Opinion].

[42]JAN PHILIPP ALBRECHT, HANDS OFF OUR DATA! (2015); Swee Leng, *Missed Opportunity for Digital Rights and Civil Society in the DSA & DMA–Learning the Wrong Lesson from GDPR*, 25(6) GERMAN L.J. (2024) (in this Issue) (describing potential problems with the current interpretation of Article 80 GDPR and its joint reading with the Consumer Class Action Directive).

[43]Mahieu & Ausloos, *supra* note 40, at 2.

[44]Gloria González Fuster, Jef Ausloos, Damian Bons, Lee Bygrave, Barbara de Rosa Lazarotto, Laura Drechsler, Olga Gkotopoulou, Christopher Hristov, Kristina Irion, Lina Jasmontaite, Charlotte Kroese, Orla Lynskey & Maria Magierska, *The Right to Lodge a Data Protection Complaint: Ok, but Then What?: An Empirical Study of Current Practices Under the GDPR* 1–65 (Eur. Univ. Institute, Working Paper 2022), https://cadmus.eui.eu/handle/1814/74899.

[45]Pola Cebulak, Marta Morvillo, and Stefan Salomon, *Strategic Litigation in EU Law: Who Does it Empower?*, 25(6) GERMAN L.J. (2024) (in this Issue) (defining empowerment in strategic litigation).

Table 1. List of selected technologies contested in migration and asylum contexts

Technology contested	CSO	Country
1) Mobile phone data analysis	Gesellschaft für Freiheitsrechte (GFF)	Germany
2) Mobile phone data analysis	Privacy International (PI)	UK
3) Electronic monitoring	Privacy International (PI)	UK
4) Surveillance systems in reception centers	Homo Digitalis	Greece
5) Social media monitoring system	Homo Digitalis	Greece

III. Does EU Law Empower Strategic Litigants? Our Approach and Methods

The potential emancipatory function of the GDPR is the core focus of our investigation. Although legal scholars have criticized the enforcement of the GDPR, both *de jure* and *de facto*,[46] we question whether EU data protection law empowers strategic litigants in the overlooked field of migration and asylum. Methodologically, we approach this question from a socio-legal perspective. This includes analyzing the tools offered by EU law for strategic litigants and evaluating how strategic litigants utilize EU law in practice. Drawing on legal mobilization literature, we focus on the objectives of strategic litigants, the obstacles they encounter, the venues and legal fora they engage with, and the role of EU law in these processes.

For our empirical study, we conducted a case study analysis and semi-structured interviews with CSOs involved in selected cases, as well as their external partners, an academic and a journalist. To select our cases, we used the Tech Litigation Database, GDPRHub, and the websites of civil society organizations across Europe. We also utilized data from the AFAR Project's comprehensive mapping study[47] to gather instances of FOI requests by CSOs and witness statements. Based on three specific criteria: (1) *the subject of litigation*, specifically automated systems; (2) *the actors involved*, specifically those pursuing a public interest; and (3) *the geographical scope*, specifically systems used by EU Member States authorities,[48] we have identified the following instances of contention (Table 1).

In many studies on strategic litigation, researchers examine how litigants present their legal arguments. However, these arguments may only offer a partial view of the strategic litigants' goals, especially when the litigation is part of a broader campaign, and the litigants take a long-term perspective to make an impact.[49] Therefore, following a thorough analysis of these cases, we conducted in-depth interviews with selected CSOs and or their partners.[50] Specifically, in May 2024, we interviewed the current Senior Lawyer and Legal Officer from Privacy International (PI) regarding their contestation against the use of mobile phone data and electronic monitoring in the UK. We also interviewed a collaborator of Homo Digitalis, Dr. Niovi Vavoula, regarding their contestation against the use of HYPERION and KENTAYROS systems designed to surveil asylum seekers in the camps in Greek islands. Finally, we interviewed Anna Biselli. Together with

[46]*See generally* Giulia Gentile & Orla Lynskey, *Deficient by design? The Transnational Enforcement of the GDPR*, 71 Int'l & Compar. L. Q. 799–830 (2022); Woojeong Jang & Abraham L. Newman, *Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation,** 60 J. Common Mkt. Stud. 283–300 (2022); Gloria González Fuster et al., *supra* note 44.

[47]Ozkul, *supra* note 38.

[48]Our analysis includes the UK, as EU law applied until 31 December 2020. After this date, it became part of UK domestic legislation. In particular, we focus on two cases brought by Privacy International under the UK GDPR and the Data Protection Act 2018, two legal acts that implement the EU GDPR into domestic law.

[49]Michael Ramsden, *Strategic Litigation, supra 7.*

[50]Research Ethics Review Approval, Ref No: HSSREC 187/23- 24 AM01, issued by the University of Warwick (constituting the approval the Authors received to conduct the interviews and further research for this Article).

Gesellschaft für Freiheitsrechte (GFF), Biselli conducted a study regarding their contestation of mobile phone data extraction in asylum procedures in Germany. These interviews complemented our analysis in understanding the intended objectives of choosing specific cases, the methods of contestation, and the obstacles faced in each case.

C. Emerging Contestation Methods

In this section, we present our analysis of the obstacles that actors involved with contesting automated systems in the context of migration and asylum encounter when they seek to challenge them. We explore the opportunities provided by EU law, the practical impediments they face, as well as the strategies they use when seeking transparency, gathering expertise, and obtaining remedies. Each sub-section starts with illustrative case studies that underscore the importance of each barrier.

I. Seeking Transparency

In 2021, the Greek Ministry of Immigration and Asylum unveiled in their annual action plan the installation of two technology systems in reception and accommodation centers for asylum seekers. Named after mythological Greek figures, Hyperion and Kentauros Systems have the potential to turn reception facilities into a panopticon of digital surveillance. By processing biometric data of asylum seekers, tracking and monitoring their movements with drones and cameras, and analyzing their behavior with Artificial Intelligence, these systems raise significant risks for the privacy and other fundamental rights of asylum seekers as well as of NGO members visiting the relevant centers and their employees. Despite the invasive nature of such projects, very little information was shared with the public. This is where the fight of Homo Digitalis, a Greek organization focused on the protection of digital rights, started. To work on their strategic litigation, they first needed more information about how the Greek Ministry of Immigration and Asylum would use them. In this section, we explore CSOs' efforts to overcome the barrier of seeking transparency, specific difficulties in the context of migration and asylum, and the mobilization of GDPR tools to obtain information about the technologies of concern.

When CSOs decide to work on contesting the use of a specific technology, the first obstacle they face is the lack of adequate technological information and its potential implications for data subjects. As automated systems are often products developed by private companies, access to information can be denied based on their commercial interest. Moreover, in the field of migration and asylum, national security interests are often presented as justification for withholding information. Without understanding the system's functionality, purpose, and operation, litigants cannot formulate a robust contestation strategy. Lack of transparency can also arise from the inherent opacity of algorithms, as highlighted by scholars like Pasquale and Burrell.[51] One of our interviewees shared the following frustration with us when they plan their strategies:

> The ability to obtain information [. . .] it's the main hurdle. Once we have the information, then it's relatively [easy]. We have all the resources and the means to get something to a challenge. We know how to do it, but obtaining the right information is really the most tricky part, and for technology, obviously, it's even harder than I think in any other field because unless you have your hands on the actual code of an algorithm or the actual physical thing that an authority uses, then you can't really figure out much. So that's really the key part.[52]

[51] *See generally* Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (2015); Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 Big Data & Soc'y 1, 1 (2016).

[52] Interview with Lucie Audibert, Senior Lawyer and Legal Officer, Privacy International (May 30, 2024).

Seeking transparency about the systems is the first and probably most important step for strategic litigants. For this purpose, EU data protection law can provide useful legal tools to obtain information about automated systems.

Transparency is a fundamental principle of EU data protection law and administrative decision-making. In the GDPR, the transparency principle epitomized in Article 5(1)(a) is developed into concrete individual rights for data subjects and duties for controllers throughout the regulation. Transparency of data processing takes the form of a duty to inform data subjects in Articles 12, 13, and 14, a right to access personal data in Article 15 and a right to receive meaningful explanations of automated decision-making in Article 22. The overarching aim of these provisions is to enable data subjects to have control over data processing and exercise their substantive rights.

Transparency rules in the GDPR govern information flows between the data subject and the controller. In this relationship, under Article 13 GDPR, data subjects must be informed of the purpose of the processing, the storage period and legal basis, the possibility of data transfer, as well as their rights as data subjects and information about the controller and the data protection officer. Such information must be given in a concise, transparent and easily accessible way per Article 12 GDPR. Additionally, data subjects under Articles 14 and 15 GDPR have the right to request information about their personal data and rights. Despite the individual dimension of transparency in the GDPR, access rights can be mobilized to achieve collective and social justice aims.[53] As shown by Mahieu and Ausloos, access rights are a crucial legal tool for investigating data infrastructures, working at best "when used collectively and is aimed at empowerment and transparency at a societal level."[54] Therefore, in theory, transparency rights represent an important tool for strategic litigants. By knowing what goes inside and what gets out, the black box of automated systems can be opened, and errors can be identified.

Transparency rights were crucial, for example, for Privacy International (PI) when they were investigating the details of electronic monitoring, specifically of "GPS ankle tags," that the UK Home Office introduced for immigration bail in 2021. Seeking transparency about the details of this technology, PI collaborated with migrants and their legal representatives to obtain "Data Subject Requests" (DSR). Our interview with them revealed that DSRs can be an important tool for understanding the details of a technology, including the frequency of data collection and the potential inaccuracies:

> Every case that has reached courts has started with a DSR usually. So, for example, in the electronic monitoring cases, the DSR is that clients were filing with the Home Office would produce Massive Excel spreadsheets of their location data over months and months and months. And through that, we were then able to assess a lot of how the system was working, how often location data was being collected, and then one really interesting use of that was in one specific client's case. We kind of sat down with them and looked through the spreadsheet of data and then checked with him every single location data point and said, 'OK, were you actually there? 'Were you actually there?'. And so that way, we were able to identify inaccuracies. And then the recording location data. So that was extremely useful.[55]

However, access rights are contingent on two conditions: The presence of a data subject whose data is being processed and the willingness to submit a data access request. In practical terms, it can be extremely challenging for migrants and asylum seekers to exercise these rights. Although recognized as "vulnerable" data subjects by the European Data Protection Supervisor (EDPS),

[53]*See* Vera Franz, Ben Hayes & Lucy Hannah, Civil Society Organizations and General Data Protection Regulation Compliance, 9 (2020). *See also* Mahieu & Ausloos, *supra* note 40.

[54]Mahieu & Ausloos, *supra* note 40.

[55]Audibert, *supra* note 52.

migrants, in general, face rigid legal frameworks that often work against their rights.[56] For many asylum seekers and refugees, data protection rights may not be a priority, due to a lack of information about available remedies and their immediate struggles in their daily lives. Asylum seekers awaiting the outcome of their application to seek protection may be afraid of speaking out against authorities. Scholars argue that this particular vulnerability has enabled state authorities to use migration contexts as a "testing ground"[57] by introducing various technologies in a trend often referred to as "techno solutionism"[58] in migration management, which may compromise fundamental rights standards and exacerbate the imbalance.

Migrants, including asylum seekers, may be afraid even to speak with journalists anonymously due to their fear of the authorities. For instance, journalist and computer scientist Anna Biselli collaborated with Gesellschaft für Freiheitsrechte (GFF) to uncover the German Federal Office for Migration and Refugee (BAMF)'s use of automated tools during the asylum procedure. In 2017, BAMF introduced the use of mobile phone data extraction in asylum procedures, along with other tools. Anna Biselli attempted to gather information from asylum seekers about how data extraction was working in practice, but she found it extremely difficult:

> While [asylum seekers] are still undergoing asylum procedure, they are incredibly vulnerable. So, they don't want to talk on the record, at least, and they don't want to be quoted. And they are afraid that, even if you give them some other name, they might be identified. [. . .] In other cases, they are [. . .] like usually it's easier to talk to people who are in a rather privileged situation, and they want to get this out [. . .] the injustice they face [. . .] but, they are safe.[59]

This situation makes seeking transparency about automated tools used in migration and asylum contexts particularly challenging. In other areas, it can be easier for CSOs to obtain information about the technology in use through DSRs. According to our interviewee from PI, DSRs can be a hugely helpful tool to obtain information about the technology in use:

> At PI, in our work in general, we very often file data subject access requests [DSR] and requests for explanations of automated decision making. And that's quite easy when we're researching a general commercial system where we, as staff, might be data subjects. In the migration context, it's much more complicated because the data subjects are often very vulnerable people who might not be in a place to help us directly or that we might not be able to support directly.[60]

It is, therefore, much harder for migrants to exercise this right due to their particularly vulnerable situation vis-a-vis the authorities.

Additionally, access rights are also limited as they do not grant technical information about the system itself. To obtain greater insights into automated systems, CSOs mobilize another tool offered by the GDPR: The Data Protection Impact Assessment (DPIA). Article 35 of the GDPR mandates controllers to conduct a DPIA whenever data processing is in operation, especially when those involving new technologies pose a high risk to individuals' rights and freedoms. Specific examples are provided in Article 35(3), such as extensive automated evaluations, large-scale processing of special categories of data, and systematic monitoring of public areas. In migration

[56]Claudia Mora & Jeff Handmaker, *Migrants' Citizenship and Rights: Limits and Potential for NGOs' Advocacy in Chile*, *in* Migration, Gender and Social Justice 281, 281 (Thanh-Dam Truong et al. eds., 2014).

[57]Petra Molnar, *Technological Testing Grounds: Border Tech Is Experimenting with People's Lives*, EDRi (Nov. 9, 2020), https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/.

[58]Niovi Vavoula, *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, 23 Eur. J. of Migration & L. 457 (Aug. 15, 2021).

[59]Interview with Anna Biselli, Editor-in-Chief, Netzpolitik (May 24, 2024).

[60]Audibert, *supra* note 52.

and asylum, where profiling or automated decision-making and processing of sensitive data of vulnerable data subjects are prevalent, DPIAs must theoretically be conducted whenever new technologies are employed.[61]

In line with GDPR's primary objective of safeguarding the right to personal data protection, DPIAs aim to ensure accountability, aiding controllers in complying and demonstrating that appropriate compliance measures are in place.[62] The GDPR specifies the minimum features of a DPIA in Article 35(7), including a description of the processing operations and purposes, an assessment of the necessity and proportionality of the processing, an evaluation of risks to data subjects' rights and freedoms, and measures to address these risks and demonstrate compliance. Despite the importance of DPIA, the GDPR does not explicitly require their publication. In the Guidelines on the DPIA by Article 29 Working Party, now European Data Protection Supervisor,[63] their publication is, however, encouraged. As a good practice, controllers should publish DPIAs, either fully or in summary, to promote transparency and accountability. DPIAs' publication is especially recommended when a public authority carries them out.[64]

However, in practice, especially in the migration context, it is difficult for CSOs and individuals to access DPIAs. Authorities do not always publish DPIAs publicly, and if they do, they may release only heavily redacted versions. As a result, it is challenging to review them or verify whether agencies have carried them out. One method of obtaining DPIAs is by submitting FOI requests.

FOI requests allow citizens to obtain access to public institution documents. They are a direct implementation of the right of access to public information, a human right recognized in international law under Article 19 UDHR and Article 10 ECHR, EU law in Article 42 CFR, Article 15 TFEU and in the Regulation 1049/2001 and by EU Member States. The advantage of FOI requests is that citizens can ask for any document held by public authorities without the need to adduce any justification to substantiate their request. For these reasons, FOI is a commonly used method by journalists and CSOs to promote transparency and support their investigations. Unlike access rights under data protection law, the right of access to public information allows individuals to seek transparency about the technical components of automated systems, such as source codes, contracts with the providers, training data or user manuals.

Although, in theory, FOI requests can be refused only exceptionally, in reality, not all requests are successful. Our interviewees shared that authorities reject providing DPIAs through FOI requests, release heavily redacted versions, ignore them, or respond only after a long delay. If requests are rejected, authorities may cite reasons such as national security, public interest, or commercial interests.[65] For instance, Lucie Audibert from PI highlighted the challenges of receiving a meaningful response to their FOI requests to the UK Home Office regarding their use of technology in the context of migration:

> In PI's experience over the years, the Home Office has always been the most difficult government entity to get information from, both from a procedural perspective and because they tend to massively delay their responses or simply forget to respond until we follow up

[61] *See Guidelines on Data Protection Impact* Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purpose of Regulation 2016/697, at 10 (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236 (discussing how, according to the Guidelines, the DPIA should be carried out for several use cases in migration, such as evaluation or scoring, ADM, sensitive data and data concerning vulnerable data subjects, including asylum seekers and any cases with power imbalance).

[62] *Id.* at 4.

[63] *Id.*

[64] *Id.* at 18.

[65] *See* Milka Sormunen & Davide Gnes, *Learning Through Rejection: Studying the Informalisation of EU Readmission Policy with Access to Documents Requests*, *in* (In)visible European Government 72, 72 (M. Hillebrandt, P. Leino-Sandberg & I. Koivisto eds., 2023) (showing that authorities may reject responses to FOI requests in other areas of migration too).

> with them. And then substantively, they'll really very often claim blanket exemptions. So, either national security and prevention of immigration offences, sometimes commercial interests, if there's a company involved. But even when there's no company involved, sometimes they'll claim their own commercial interests as in their negotiation interests as a commercial entity.[66]

Challenging such rejections requires additional resources, namely organizational time. For example, Anna Biselli informed us that BAMF rejected her request for DPIAs after a long wait, and they were unable to challenge this rejection due to time constraints: "What I really wanted to have but didn't get is data protection impact assessments because that is something I would be really interested in, and we requested it, and they rejected it. And then there were some organizational problems, and we didn't manage to file the claim in time." Receiving DPIAs in this context not only demands resources but also requires staff members on long-term contracts to handle specific cases over a prolonged period and to accommodate the fluctuating response schedules of authorities.

All these obstacles, including the time to wait for a response and then to challenge a rejection, may influence CSOs' decisions to proceed with their strategic litigation. For instance, one of our interviewees deliberated on whether to continue with a case, stating:

> I think of all the FOI requests that we've filed with the Home Office over the past few years. Each of them has taken almost or more than a year to get to a final kind of resolution, and even then, that might be more refusals, and then we take a decision as to whether we want to challenge the refusals or just let it go and that will be kind of an ad hoc decision based on the importance of the information and what we think is the quality of the argument for applying the exemptions.[67]

In other cases, CSOs' FOI requests may simply be ignored. For example, when Homo Digitalis sought information about the Greek Ministry of Immigration and Asylum's use of Hyperion and Kentavros Systems, their request for the DPIAs was disregarded:

> Some of the questions addressed to the Ministry were whether a DPIA has been conducted, whether the Ministry has communicated the results of such a DPIA to the Hellenic DPA, whether they have put together a privacy notice for the related envisaged data processing activities and what is the foreseen legal basis that the Ministry plans to use for the related data processing operations of biometric and biographic data. However, this request remained unanswered.[68]

This situation later prompted Homo Digitalis to approach the Hellenic DPA,[69] another method of contestation which we will explore in Section III below. For now, let us examine how CSOs seek to obtain expert knowledge about the details of these technologies and how they can challenge them.

II. Gathering Expertise

Contesting an automated tool in migration and asylum also requires expert knowledge to assess the capabilities and limitations of the specific technology. For example, in 2017, an amendment to

[66]Audibert, *supra* note 52.

[67]*Id.*

[68]Eleftherios Chelioudakis, *Unpacking AI-Enabled Border Management Technologies in Greece: To What Extent Their Development and Deployment Are Transparent and Respect Data Protection Rules?*, 53 COMP. L. & SEC. REV. 1, 6 (2024).

[69]*Id.*

the Asylum Act in Germany allowed the BAMF to analyze asylum seekers' mobile phone data to establish their identity and nationality.[70] This process involves scrutinizing data such as browsing history, addresses, and geodata stored on the mobile phone. Once the phone is unlocked to enable the so-called 'read-out', the device is linked to a computer, which then analyses the data and generates a report containing statistical information and country indicators.[71] The results of this automated analysis can then be used, with certain safeguards, to determine asylum seekers' country of origin. However, the exact method by which the technology converts the extensive data stored in phones into statistical indicators of nationality is not clear. What weight is given to a browning history or location data from photos and apps? What factors affect the final statistical percentage? What logic and criteria are used to produce an automated assessment of an individual's identity? This is where the fight of GFF, a Berlin-based non-profit organization focused on defending fundamental and human rights by legal means, started. In this section, we explore how CSOs overcome the barrier of obtaining expert knowledge about the details of the technologies they are concerned with and how they challenge these technologies by building coalitions.

When questions arise about the accuracy and technical capabilities of automated systems, there are two ways to answer them. One is to receive an explanation of the system's functionalities from its developers or deployers. The second is to have the expertise and access to technical information to review and interpret the system independently. The GDPR attempts to follow the first option by granting a higher level of transparency for data subjects when a decision is solely automated.[72] When subject to automated decision-making, data subjects have the right to obtain "meaningful information about the logic involved", or "right to an explanation",[73] as well as know the significance and the envisaged consequences of such processing under Articles 13(2)(f), Article 14(2)(g) and Article 15(1)(g) GDPR. Although the scope of this right to an explanation remains unclear, as the Court of Justice has still not clarified important aspects of these provisions, the legal requirement of "meaningful information about the logic involved" can potentially help litigants in interpreting the system they aim to challenge.

In practice, our research shows that contesting the use of a technology based on the right to an explanation has not been effective. Authorities are reluctant to consider their decision-making systems "solely automated," claiming that a human caseworker makes the final decision. They may also refrain from acknowledging the use of an automated system when challenged by CSOs. For example, in the case of contestation against electronic monitoring, when PI attempted to challenge the use of an automated tool that recommends whether a migrant should be electronically monitored, the UK Home Office denied its use:

> In terms of automated decision-making, it has come up a lot in the electronic monitoring cases because there's this tool, the Electronic Monitoring Review tool, which is supposed to be an algorithm that kind of helps decision makers make decisions as to whether someone should be kept on a tag or moved to what they call it a less invasive tag like the non-fitted tags [. . .] Through the cases that have gone through the courts for now, the Home Office has denied using this tool for these specific cases even though we know it exists and it has been

[70] *See* Asylgesetz [AsylG] [Asylum Act] Jun. 26, 1992, BGBl § 15a (Ger.); Aufenthaltsgesetz [AufenthG] [Residence Act] Feb. 17, 2020, BGBl § 48a (Ger.).

[71] Anna Biselli & Lea Beckmann, *Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe* 18 (Gesellschaft Für Freiheitsrechte e.V.) [GFF, Society for Civil Rights] (Ger.) (2020), https://freiheitsrechte.org/uploads/publications/Digital/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control-Gesellschaft_fuer_Freiheitsrechte_2019.pdf.

[72] On the scope and definition of Article 22 GDPR, *see* Francesca Palmiotto, *When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis*, 25 GERMAN. L.J. 210, 214–15 (2024).

[73] *See* Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7 INT'L DATA PRIV. L. 243, 248 (2017) (contending with the term "right to an explanation").

> used and is used in other cases. So, for now, we haven't been able to get any disclosure on that, but it's an argument that we have brought forward multiple times to say if this tool is being used, then individuals are entitled to an explanation of how it works. And very often, they'll refuse to provide a full answer, but they'll draw our attention to their immigration bail policy, which has, like, a table. That sets out the variables that are fed into the algorithm. So, the different levels of risk and harm that someone may pose. How that impacts the decision [. . .] but it's really basic information, and it does not actually give us information as to the weights that are applied to the different factors. So yeah, for now, it's been really, really basic information, but probably try and use those rights, but I mean [. . .] the right not to be subject to automated decision-making, for now, hasn't been fruitful but might be in the future.[74]

In the lack of effective legal tools to understand how automated systems work, CSOs have resorted to coalition building as a means of gathering expert knowledge. Through coalition building, CSOs join forces, pooling their resources, time and technical expertise to strategize ways to advance their cause. This collaboration often involves organizations, academic researchers, journalists, and computer scientists who share a common interest in challenging the use of automated systems.

One aspect of coalition building involves sharing available information to combine resources effectively. For example, organizations may deliberately make their FOI requests on open platforms, such as whatdotheyknow.com in the UK and FragDenStaat.de in Germany, enabling others to track and access the responses from authorities.[75] They may also maintain close communication with each other to share the information they uncover. For example, in their contestation against electronic monitoring, PI used the responses to FOI requests made by other organizations, such as the Bail for Immigration Detainees (BID) and the Public Law Project (PLP), as a basis for their subsequent claim to the UK DPA, Information Commissioner's Office (ICO).

Another aspect of coalition building involves seeking technological expertise to understand the possible limitations of the technologies in use. Migrant or digital rights experts may lack detailed technical knowledge about how specific systems operate. If they can afford it, CSOs may either have in-house technical staff members or collaborate with external partners. For example, PI, a relatively large organization focused on new technologies, has its own team of technologists. The collaboration between the technological and the legal teams was crucial for PI to provide their third-party intervention for the UK Home Office's use of mobile phone data extraction and their witness statement for electronic monitoring:

> At PI, we have a team of technologists who are really wonderful from very diverse technical backgrounds. So [for] most of the technical issues we cover, someone in that team is going to be able to cover it. [. . .] So, for example we did this big piece of research into the tags themselves, so the kind of physical makeup of the tags. You know what they were. [. . .] what components were instrumental in collecting location data, et cetera. And then with that, basically, we got some tags from the open market and then our technologists tested them over the course of a few months, and then they were quite instrumental at kind of identifying all the failings and all the potential incompatibilities and inaccuracies between their experience of wearing the tag and what the data was showing.[76]

[74]Audibert, *supra* note 52.

[75]For an analysis of digital platforms as an empowering tool, *see* Julia Trautendorfer, *Empowering Citizens for Transparency: Using Independent Digital Platforms for Freedom of Information*, HERTIE SCHOOL (Jun. 6, 2024), https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/empowering-citizens-for-transparency-using-independent-digital-platforms-for-freedom-of-information.

[76]Audibert, *supra* note 52.

Similarly, in their pre-litigation research, GFF collaborated with computer scientist and journalist Anna Biselli, who had already submitted many FOI requests to BAMF, to uncover the technical limitations of this practice. This collaboration helped both parties to understand the details of this practice and eventually challenge it at the DPA and in court. Biselli shared, "I have exchanged information with GFF, and so it was quite logical to do it together because I had the expertise from all those FOI requests, and from the IT perspective, and the GFF had the legal perspective, which I don't have because I'm not a lawyer."[77]

Finally, another aspect of coalition building involves combining different types of expertise for research, strategy, and claim-making. For example, in their opposition to the Hyperion and Kentauros systems, Homo Digitalis worked with European Digital Rights (EDRi) to gather information about the technical details, as well as envisaged data processing activities.[78] When their requests went unanswered, Homo Digitalis collaborated with other Greek organizations, namely the Hellenic League for Human Rights and HIAS Greece, as well as Dr Niovi Vavoula, a lecturer at Queen Mary University of London at the time, and together they decided to file a complaint with the Hellenic DPA to investigate the deployment of these systems.[79] The academic who participated in this collaboration provided a legal analysis of the practice in question. Given Dr Vavoula's expertise in the intersection of migration and technology, she helped the CSOs draft their complaint to the DPA by highlighting the missing points from a data protection perspective:

> I was involved in the stage of preparing the claim before the Greek DPA and strategising as to which arguments to make in our claim. [. . .] in order to make a claim that would be as scientifically sound and complete as possible, and due to my expertise at the intersection of migration and technology, I was asked to provide input on the arguments to make. [. . . .] I was given information about the process, so where we stand.[. . .] the fact that we didn't have the legal basis and impact assessment, we knew that these already were breaches of data protection law, we identified some more, and then we submitted the claim.[80]

These collaborations are indicative of a common challenge in this field: the significant difficulty in comprehending the workings of automated systems and their impact on data subjects, and the substantial resources needed for this task. It was only through these collaborations that CSOs were able to overcome these obstacles and move forward to the next stage, which involves obtaining remedies.

III. Obtaining Remedies

After seeking transparency and gathering expert knowledge, the next step is choosing and obtaining remedies. In this section, we explore how CSOs attempt to obtain remedies by choosing the appropriate legal forum. We show that they base this decision on the existing "legal opportunity structures," that is, the presence or absence of legal institutions that they can turn to, as well as the potential to collaborate with a litigant.

As a general principle of EU law and a fundamental right under Article 47 CFR, individuals have the right to an effective remedy before a Court when their rights are violated. Member States have a duty to provide remedies that are sufficient to ensure effective legal protection of individuals according to Article 19(1) TFEU. Although, in theory, a remedy may be available under the law, several barriers may render a remedy ineffective in practice. Before the GDPR was

[77]Biselli, *supra* note 59.

[78]Chelioudakis, *supra* note 68.

[79]*The Hellenic DPA is Requested to Take Action Again the Deployment of ICT systems IPERION & KENTAUROS in Facilities Hosting Asylum Seekers in Greece*, Homo Digitalis (Feb. 6, 2020), https://homodigitalis.gr/en/posts/10874/.

[80]Interview with Dr. Niovi Vovoula, Assoc. Professor in Cyber Pol'y, Univ. of Luxembourg (May 20, 2024).

proposed, the European Commission's impact assessment underlined that litigation obstacles, such as cost of court proceedings, delays and lack of awareness, were particularly affecting the area of data protection.[81] The Fundamental Rights Agency, in their opinion on the legislative proposal, also highlighted that the reluctance of data subjects to access court seemed to be linked to formalities and strict procedural requirements.[82] The proposed GDPR was then the right occasion to revert this trend. Following the experience with national equality bodies in the field of EU non-discrimination, the GDPR introduces a new form of redress mechanism: The DPA as a non-judicial dispute mechanism. Under the GDPR, data subjects can bring a complaint before a Court in Article 79 GDPR or to a DPA in Article 77 GDPR, which is an optional dispute mechanism in addition to traditional remedies available under EU or national law. Additionally, the GDPR broadens legal standing rules for CSOs, allowing public interest actions to be brought before DPAs in Article 80 GDPR. Originally conceived as "the preferred point of access to data protection breaches,"[83] DPAs would have decreased costs, delays and formalities that were hampering access to justice for data subjects and CSOs acting in the public interest.

In four of the five cases we examined, CSOs resorted to DPAs. Homo Digitalis contested against Hyperion and Kentauros Systems, as well as the AI-enabled social media monitoring tool to profile individuals and predict migration flows towards Greece.[84] GFF contested against mobile phone data extraction during the asylum procedure, and Privacy International contested against electronic monitoring by filing a complaint with their relevant DPAs in the countries where they operated. GFF and PI also went to Court, while Homo Digitalis kept their complaint with the DPA level.

Our findings show that CSOs resort to DPAs for two main reasons. First, when pursuing legal action in court is not feasible and when the data protection issues are considered serious enough to warrant a DPA investigation. For example, when Homo Digitalis did not receive responses to their FOI requests regarding their questions on data protection in the case of surveillance systems used in reception centers, they chose to file a complaint with the Hellenic DPA, in collaboration with the Hellenic League for Human Rights, HIAS Greece, and Dr Niovi Vavoula, as it was the only available legal recourse for them. The technologies in question, Hyperion and Kentauros Systems, which are designed to surveil asylum seekers in the camps in Greek islands, posed significant challenges in finding a litigant to bring to court due to asylum seekers being essentially detained within these centers and facing imminent expulsion upon failed asylum claims.[85] Nevertheless, as they strongly believed in their claim, "because the data protection breaches were so glaring that it would be very difficult for a DPA to ignore,"[86] they decided to file a complaint with the Hellenic DPA. In this case, the Hellenic DPA decided to investigate the claim promptly and ultimately imposed an administrative fine of €175,000 on the Ministry of Migration and Asylum due to breaches related to a lack of cooperation as the data controller, incomplete DPIAs and other shortcomings with compliance with GDPR.[87] Similarly, Homo Digitalis submitted another

[81] *See Commission Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council to Improve the Working Conditions in Platform Work in the European Union*, at ¶ 10.10.1, 396 final/2 (Oct. 12, 2021) https://op.europa.eu/en/publication-detail/-/publication/48491c8f-59bb-11ec-91ac-01aa75ed71a1.

[82] FRA Opinion, *supra* note 41, at 30.

[83] *Id.*

[84] *See* Chelioudakis, *supra* note 68.

[85] Vovoula, *supra* note 80.

[86] *Id.*

[87] Press Release, Hellenic Data Protection Authority, Ministry of Migration and Asylum Receives Administrative Fine and GDPR Compliance Order Following an Own-Initiative Investigation by the Hellenic Data Protection Authority (Mar. 4, 2024) (on file with author).

request to the Hellenic DPA to investigate the use of a social media monitoring system by the Coast Guard. This request was made in collaboration with the Hellenic League for Human Rights, HIAS Greece, Privacy International, and the researcher Phoebus Simeonidis, and the Hellenic DPA recently reported to them that it will soon conclude its assessment.[88]

In a similar vein, when PI wanted to challenge electronic monitoring, they decided to file a complaint with the UK DPA, the Information Commissioner's Office (ICO). They took this course of action because they believed that challenging the practice through litigation was impractical, and they also held firm in their belief that the Home Office's GPS tagging practice violated the UK GDPR and intruded upon individuals' privacy rights. PI also provided witness testimony in support of claimants in two cases, ADL & others v SSHD, and Nelson v SSHD, for judicial review,[89] but found it impossible to systematically contest the practice through litigation. Our participant explained that when they began their technical research on the GPS tags, several individual judicial review cases were filed, but none of these cases progressed to court as the Home Office promptly removed the tag upon case filing.[90] Due to this evasive maneuver, PI chose to lodge a complaint with the ICO to escalate the matter to a quasi-judicial body.[91] Subsequently, the submission to the ICO was successful, resulting in the issuance of an Enforcement Notice and a formal warning to the Home Office on March 1, 2024, citing widespread violations of data protection law in its GPS tagging of migrants.[92]

Second, CSOs may choose both to file a complaint with a DPA and take legal action in court as part of their strategic litigation. For example, the organization GFF challenged the use of mobile phone data extraction by initiating legal proceedings in the Administrative Courts of Hanover, Berlin, and Stuttgart with three different litigants. In June 2021, the Berlin Administrative Court ruled in favor of GFF's complaint and allowed a direct appeal to the Federal Administrative Court. As a result, GFF suspended the other court cases. This was followed by the German Federal Administrative Court (BVerwG) issuing a landmark ruling on February 16, 2023 stating that the Federal Office for Migration and Refugees (BAMF)'s practice of regularly analyzing mobile phones was unlawful (BVerwG 1 C 19.21).[93] Additionally, several months before the Berlin Administrative Court's ruling, in February 2021, GFF lodged a complaint with the German DPA, Federal Commissioner for Data Protection, thus adding another dimension to their strategic litigation process.

Nonetheless, contrary to the original expectations under GDPR, our empirical research reveals that filing a complaint with DPAs also comes with challenges. The main obstacle reported by our participants is that DPAs are often under-resourced, which may lead to delays in investigating a

[88] *See* Chelioudakis, *supra* note 68.

[89] *See UK Migrant GPS Tracking Challenges*, PRIVACY INT'L (last visited Jun. 20, 2024) https://privacyinternational.org/legal-action/uk-migrant-gps-tracking-challenges. *See also* ADL & Ors v. Sec'y of State for the Home Dep't [2022] QB (Eng.) (Statement of Lucie Audibert in support of Claimants application for Judicial review on behalf of Privacy International); Nelson v. Sec'y of State for the Home Dep't [2024] AC (Eng.) (First witness statement of Jonah Mendelsohn in support of the Applicant's application for judicial review on behalf of Privacy International) (appeal taken from First-Tier Tribunal (Immigration and Asylum)).

[90] Audibert, *supra* note 52.

[91] *Id.*

[92] Press Release, Privacy International, GPS Tagging of Migrants UNLAWFUL, UK Authority Finds After PI complaint (Feb. 29, 2024), available at http://privacyinternational.org/news-analysis/5261/gps-tagging-migrants-unlawful-uk-authority-finds-after-pi-complaint; *ICO Enforcement Notice*, ICO (Feb. 28, 2024), https://ico.org.uk/media/action-weve-taken/enforcement-notices/4028870/ho-migrant-tagging-20240228-en.pdf; *ICO Warning Letter*, ICO (Feb. 28, 2024), https://ico.org.uk/media/action-weve-taken/4028872/ho-migrant-tagging-20240228-warning.pdf.

[93] *See* Francesca Palmiotto & Derya Ozkul, "*Like Handing My Whole Life Over*": *The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures*, VERFASSUNGSBLOG (Feb. 28, 2023), https://verfassungsblog.de/like-handing-my-whole-life-over/ (analyzing the ruling).

complaint, or they may even choose not to investigate it at all. For example, in the complaint filed with the Hellenic DPA regarding Hyperion and Kentauros Systems, even though the Hellenic DPA made their decision to investigate the complaint rather promptly, their final decision came only after more than two years of the claim that was submitted, which prompted one of our participants to reflect that "it's not just a lack of resources that even if the resources are allocated, it still takes a lot of time".[94] This finding broadly aligns with existing studies on DPAs in other fields.[95] As a result, CSOs need to carefully consider whether to file a complaint with a DPA, as it requires an investment of time without a guarantee of an investigation. Nevertheless, in cases where contesting through litigation is not viable, DPAs can still play a vital role in curbing the use of automated tools in migration and asylum.

D. Conclusion

Access to remedies is a fundamental principle of EU law and is a human right. Strategic litigation in the public interest becomes crucial when automated systems are employed, given the systemic impact these systems may have on individuals. Within the enforcement architecture of the GDPR, CSOs are considered key actors in pursuing public interest actions and providing effective protection to individuals. In this Article, we have analyzed how CSOs pursue strategic litigation against automated systems in migration and asylum and the role of EU law therein. Prompted by the lack of research in this field, despite its growing relevance, we have questioned whether EU data protection law truly empowers strategic litigants. We have addressed this question from a socio-legal perspective, considering not only the legal tools offered by the GDPR, but also whether CSOs use them in practice. Our analysis shows that CSOs attempt to mobilize GDPR legal tools, although two main issues risk rendering them ineffective.

The first issue relates to the specific context of our investigation, where asylum seekers and migrants are the data subjects. As vulnerable individuals, they fear repercussions for exercising their access rights or contesting authorities' use of automated systems. For CSOs, this represents an obstacle to obtaining information as well as finding a litigant to bring a strategic case. In this context, CSOs have resorted to DPAs, prompting them to investigate the case or bring complaints before them. However, DPAs' lack of resources and delays in taking action affect the possibility of obtaining effective remedies, defeating the original purpose of DPAs as the preferred point of access for data protection violations.

The second issue pertains to the persistent opacity of automated systems and the reluctance of public authorities to share information. Even if CSOs are equipping themselves to obtain expert knowledge through coalition building, the lack of access to detailed technical information remains a core problem. When CSOs strategically mobilize FOI and GDPR tools, their transparency demands are blocked, adducing commercial and national security interests. Although transparency and protection of vulnerable individuals are core pillars of the GDPR architecture, in practice, we find that these principles are far from being implemented.

As a consequence, the pre-litigation phase becomes extremely burdensome for strategic litigants. By investing time and resources in seeking transparency or waiting for DPAs' actions, CSOs need to climb a wall before even reaching the litigation stage. We illustrate this metaphor in the visual below (Figure 1).

[94]Vovoula, *supra* note 80.

[95]Ctr. for Glob. Dev., *Governing Data for Development: Trends, Challenges, and Opportunities* Policy Paper 190, at 29 (Nov. 2020). *See also*, European Data Protection Board, First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities 7 (Feb. 26, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

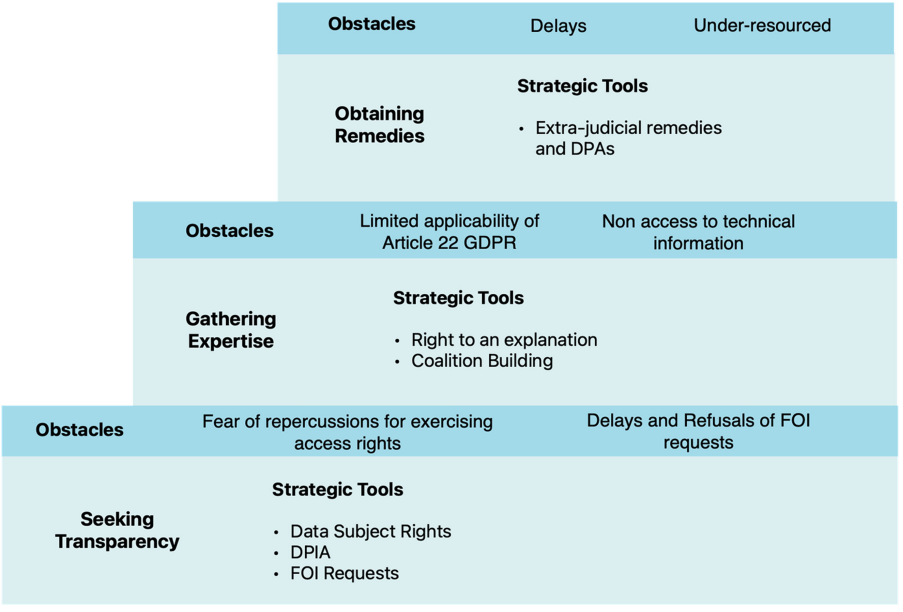

Figure 1. The Wall of Pre-Litigation.

Despite these challenges, CSOs actively work in this field, mobilizing access rights and available legal venues under EU data protection law. Transparency and fundamental rights protection in automated systems are key principles that CSOs are fighting for through strategic litigation and advocacy. Given the vital role of their work in promoting a digital society that adheres to fundamental rights and democratic principles, it is crucial to truly enable the GDPR's empowering potential and dismantle the wall of pre-litigation hurdles. To this end, we urge public authorities to make DPIAs publicly available, thus enabling CSOs and other stakeholders to collectively monitor data subjects' rights. We also suggest investing more resources in supervisory authorities and urging DPAs to prioritize monitoring, investigations, and complaint handling in the field of migration and asylum. The role of DPAs must be strengthened to protect this category of data subjects whose rights are severely affected by the increasing use of automated systems.

It is important to acknowledge the limitations of this study and consider potential future research directions in this area of study. Given the novelty of these technologies, our study only examines recent efforts by CSOs to challenge them, as most of the contested technologies have been recently introduced by government authorities. As more technologies become integrated into various aspects of migration and asylum governance, and as CSOs become more involved in this field, they may develop new strategies or gain a better understanding of how these technologies operate through increased collaboration among themselves and other partners, potentially leading to more legal actions. Our study's focus on recent challenges limits our contributions to the legal mobilization scholarship. Due to identified pre-litigation phase obstacles and the limited existing litigation in this field, we were unable to analyze changes in court case framing over time. We believe this will be a crucial area for future research. Moreover, although our Article focuses on the pre-litigation phase of mobilizing against automated systems, we recognize that this process is likely to evolve with the changes that the EU AI Act will bring, which will be another important area for future study.

Acknowledgements. We want to express our gratitude to our AFAR team members and the participants of the 'Strategic Litigation in European Union Law' workshop held at the University of Amsterdam in March 2024 and the 'STS MIGTEC' workshop held at the University of Utrecht in April 2024 for their valuable feedback on a previous version of this Article.

Competing Interests. The author declares none.

Funding Statement. This research is part of the Algorithmic Fairness for Asylum Seekers and Refugees (AFAR) Project, funded by the Volkswagen Foundation under its Challenges for Europe Programme.

Cite this article: Palmiotto F, Ozkul D (2024). Climbing a Wall: Strategic Litigation Against Automated Systems in Migration and Asylum. *German Law Journal* **25**, 935–955. https://doi.org/10.1017/glj.2024.52