

UNIVERSITY COLLEGE DUBLIN

European Master's Programme in Human Rights and Democratisation
A.Y. 2025/2026

Digital Authoritarianism in Democracies: The Digital Repression of Human Rights Defenders in US Immigration Enforcement

Author: Emma Galimberti
Supervisor: Melanie Hoewer

Word Count Declaration: 28250

Abstract

Governments have increasingly used digital technologies as tools of repression. Despite the democratic benefits of digital tools, especially for the work of Human Rights Defenders, the misuse of technology to oppress dissent is increasingly used by governments. Digital Authoritarianism refers to the use of technology in practices with authoritarian tendencies. Most of the literature is focused on Digital Authoritarianism in Authoritarian regimes, however, it is increasingly present in democratic governments. In fact, democracies can benefit from the covert nature of digital tools, whose use for repression is less evident than violent coercive strategies. With the increasing spread of anti-immigration sentiments, coupled with digitalisations of borders and of migration governance, digital tools are used by democratic governments to control immigration. However, the present thesis investigates how these Digital Authoritarian practices are actually targeting Human Rights Defenders as well, and how this can explain the increasing blurring of boundaries between democracies and authoritarian governments. Specifically, the present thesis focuses on the US as a case study, investigating immigration enforcement during the second Trump presidency (2025/2026). Given the contemporary relevance of the research, it was conducted through a qualitative thematic analysis of NGO and government data. Findings show that Digital Authoritarianism practices such as surveillance, data collection, and channelling are used within immigration enforcement to target Human Rights Defenders in ways that target their freedom of expression, right to privacy and freedom of association. The present thesis finds that the use of Digital Authoritarianism practices against Human Rights Defenders and the restriction on their rights can aid in explaining current threats faced by democracies and contributes to the literature on Digital Authoritarianism and its implementation by democratic governments.

Table of Contents

List of Abbreviations	3
I. Introduction	4
1. Research Question	6
2. Methodology	7
2.1. Qualitative Data Analysis	7
2.2. Case Study	9
II. Literature Review	11
1. What is Digital Authoritarianism?	11
2. Private Tech Companies	13
3. Digital Authoritarianism in Democracies	14
3.1 Conceptualising Practices	15
3.2 Blurring of Democracy	16
4. Repression	17
5. DA practices	19
5.1 Surveillance	19
5.2 Data Collection	20
5.3 Channelling	22
6. Human Rights Defenders	23
6.1 Criminalisation of Human Rights Defenders	24
6.2 Human Rights	25
7. Digitalisation of Immigration	26
8. Themes	28
III. Data Analysis	30
A. Surveillance	31
1. Background Information	31
2. Social Media Surveillance	33
2.1 Viewpoint-based immigration	35
2.2 Private Companies	37
3. Facial recognition	39
4. Spyware and Private Companies	41
5. Criminalisation	43
6. Chilling Effect	46
7. Debates on AI	47
B. Data Collection	49
1. Background Literature	49
2. A Centralised Database	50
2.1 Private Companies	50
3. Advertisement-based data collection	51
4. Automated License Plate Readers	52

4.1 Private Companies	53
C. Channelling	55
1. Background Literature	55
2. Social Media Covert Channelling	56
3. Criminalisation through Channelling Practices	59
D. Funding	60
E. Summary of Themes	62
IV. Discussion	63
I. The Blurring of Democracies	64
1. Freedom of Expression	64
1.1 Viewpoint-based immigration	65
1.2 Chilling Effects	66
1.3 Criminalisation	67
2. The Role of Private Companies	69
2.1 Accountability	69
2.2 Transparency	70
3. Digital Repression	71
4. National Security	72
V. Conclusion	74
1. Central Findings	74
2. Strengths and Limitations	75
3. Further Research	76
4. Recommendations	77
VI. Bibliography	79
1. Literature	79
2. Data Analysis Reports	86

List of Abbreviations

ALPR: Automated License Plate Reader

CBP: Customs and Border Protection

DA: Digital Authoritarianism

DOGE: Department of Government Efficiency

FOIA: Freedom of Information Act

HRD: Human Rights Defender

ICCPR: International Covenant on Civil and Political Rights

ICE: Immigration and Customs Enforcement

USCIS: United States Citizenship and Immigration Services

I. Introduction

“It’s vital to remember that we cannot defend democracy and freedom without combating digital repression and protecting those who defend human rights.”¹

In an age characterised by the rise of technology, digital tools become contested territory between mobilisation and oppression, depending on who uses them (Dragu and Lupu, 2021; Wilson, 2022; Hankey and Clunaigh, 2013). In fact, the same digital tools that are used by Human Rights Defenders (HRDs) to document violations, claim rights and determine accountability (Ristovska, 2016), can also aid the state in consolidating power (Dragu and Lupu, 2021). The term *Digital Authoritarianism* has emerged to describe the practice of governmental exploitation of technologies to pursue authoritarian objectives (Pearson, 2024, p. 72).

Digital Authoritarianism has initially been understood in terms of authoritarian states that use digital technologies to increase their repression towards governmental dissidents and manipulate information to benefit their political ideology (Dragu and Lupu, 2021; G’Sell, 2025). However, after key episodes such as the Snowden revelations in 2013, in which instances of mass surveillance by the US and UK governments were revealed to the public (Pearson, 2024), Digital Authoritarianism was identified as not confined to authoritarian regimes. The presence of Digital Authoritarianism in democracies has been further investigated and confirmed in academic literature (Pearson, 2024; Wijayanto et al, 2022; Earl et al 2022; Peron et al, 2025), which raises the query regarding how a democracy with its human rights standards and legal accountability processes can engage in practices of an authoritarian nature. This is developing within a context of global democratic retrenchment (Feldstein, 2021), particularly characterised by a fourth global wave of the far right (Peron et al 2025, Wilson 2022). This warrants more investigation into digital tools within democracies that could enable practices of an authoritarian nature (G’Sell, 2025), especially since protection frameworks are not keeping up with the increasingly fast development and implementation of digital tools in democracies (Feldstein, 2021). Digital strategies can offer advantages for democracies given they are less likely to create public and international reprisal compared to explicitly coercive strategies (Feldstein, 2021). Furthermore, this rise of

¹ (Barrueto and Al-Maskati 2025)

authoritarian tendencies can be facilitated by private technology companies that hold power to shape the digital tools and services, and shape how these services are provided to users (G'Sell 2025, p. 2). These factors all contribute to the incremental development of authoritarian practices even in states committed to democratic values (G'Sell, 2025).

A state is most likely to engage in digital forms of repression if they perceive a group as a threat to governmental order and stability (Earl et al, 2022 p4). This is why it is important to investigate Digital Authoritarianism in light of specific governance that is particularly directed against a group threat such as immigration. Immigration policies have not only become stricter in recent years, but borders and enforcement have become increasingly digitalised (Molnar 2021). Governments are now using digital tools to expedite the fight against immigration, making migrants easier to detect and surveil (Molnar 2019). Especially with the rise of AI in digital tools, the collection of data in the immigration field can risk bias and discrimination as well as raise concerns about privacy and non-consensual data sharing. There is, in fact, a part of the literature surrounding digital practices and their effects on immigrants (Yabanci, 2024; Molnar, 2019; Molnar, 2021; McGregor and Molnar, 2023); however, what is often overlooked is how these digital practices in countries' immigration governance can target human rights defenders. Digital technologies used for immigration control can result in the targeting of activists, journalists and dissidents, especially due to the limited regulations applied to them (Molnar, 2021 p72). When a democracy uses digital tools to target the rights of Human Rights Defenders, vital for democratic foundations (Koula, 2026), the boundary between democracy and authoritarianism can begin to blur.

This blurred boundary can be seen especially when the human rights of HRDs come into question due to their essential role in promoting rights and fundamental freedoms in democracies (Koula, 2026). Though HRDs are empowered by technology, which allows them to extend their work's reach and impact, the same digital tools they use often leave them vulnerable to the repression of governments through digital traces, access to their data, manipulation of information and surveillance (Hankey and Clunaigh, 2013). These techniques can put at risk the very rights they work to protect: freedom of expression, freedom of assembly and association and right to privacy.

Therefore, the present research aims to be a bridge between Digital Authoritarianism, immigration enforcement and Human Rights Defenders. The aim is to address the gap in

literature regarding DA in democracies, specifically focusing on HRDs in order to gain insights on the effects of DA practices on human rights and the implications this has for democracies.

1. Research Question

The present thesis aims to investigate in what ways democracies use Digital Authoritarianism practices to restrict the rights of HRDs and how this can explain the blurred boundary between democracies and authoritarian regimes. The following research question was developed to effectively investigate the topic:

How are Digital Authoritarianism practices in US immigration enforcement impeding the rights of Human Rights Defenders?

The research question will be answered by focusing on the following case study: the second Trump administration (2025-2026) in the United States. A thematic, qualitative data analysis will be conducted in order to shed light on the effects of Digital Authoritarianism on Human Rights Defenders, and on overall democratic governance. Existing research suffers from gaps when it comes to defining how rights are restricted and by whom (Glasius and Michaelsen, 2018 p3796). Therefore, the objective is that of identifying which DA practices implemented in immigration enforcement also target HRDs, and how they are implemented in ways that impede their rights.

The thesis is divided in 5 chapters: Introduction, which introduces the topic and motivations, and outlines the methodology of the research; the Literature Review, which gives an overview on the literature regarding Digital Authoritarianism, HRDs and Immigration, situating the present research within the debates; the Data Analysis which analyses and interprets the data; the Discussion which relays the meaning of the findings in the identified literature contexts; and the Conclusion where limitation as well as further research and recommendations will be given.

2. Methodology

2.1. Qualitative Data Analysis

While authoritarian control and its effect on fundamental freedoms is well researched in the literature, understanding its interaction with digital technologies requires an analytical framework that can fully grasp its impact and implications (G'Sell, 2025 p1). The methodology for this thesis incorporates a qualitative analytical approach to analyse the data collected regarding President Trump's second term in office (2025-2026). A qualitative approach was chosen because the purpose of the research is to understand how DA practices are occurring and to allow for interpretations of deeper understandings regarding the mechanisms behind and impacts of their implementation. The specific qualitative methodology used was a thematic analysis. As conceptualised by Braun and Clarke (2006), a thematic analysis identifies and analyses themes within data in order to interpret various aspects of the research topic. I chose a thematic analysis for two main reasons: firstly, given the still developing field of Digital Authoritarianism especially within democracies, an analysis that can identify themes and common practices can effectively contribute to the development of the field through the clarification of how it is observed in practice; secondly, given the short time frame in which my thesis is focused, an analysis of present patterns in observable data can aid in the formulation of interpretations and be used for further empirical research which is scarce at the moment. The themes in a thematic analysis refer to clusters of important information regarding the research question that represent some level of patterned meaning in the data (Braun and Clarke, 2006). The thematic analysis was approached through initially mapping out the relevant literature in the literature review and identifying practices of Digital Authoritarianism. These categories became the themes through which the data were analysed in order to answer the research question. This part of the analysis consisted of a deductive thematic analysis, meaning a top-down approach where themes were gathered from the literature and used to analyse the data set (Braun and Clarke, 2006). The analysis was based on the identification of which of these categories were present in the data, and in what particular patterns. A second part of the thematic analysis consisted of an inductive approach, meaning a bottom-up approach in which themes were identified from the data itself based on patterns of meanings that helped answer the research question (Braun and Clarke, 2006). A combination of both these approaches allowed the analysis to be driven by a

theoretical basis and contribute to a range of academic literature, while still linking the themes strongly to the data itself. The themes were analysed on a latent level, which refers to an analysis of underlying meanings, conceptualisation and interpretations of the themes rather than on a surface level analysis (Braun and Clarke, 2006). The themes were hand-coded in the data and identified not only through the specific word referring to the DA practice, such as “surveillance”, but also the definitions and actions that indicate that practice is occurring.

The data set consisted of publicly available and openly accessible data from NGOs, international organisations, and US governmental documents. Specifically, these included: NGO reports, field observations, NGO research, NGO reported court cases, UN Special Rapporteur documents, Official US governmental documents such as Executive Orders, Proposals, Communications and contracts, and Freedom of Information Act (FOIA) reports. These sources of data were chosen because international and national organisations that research and report on the topic collect direct information regarding the current situation, and given the limited two-year time frame of research, concrete field observations were necessary. The NGOs that were chosen are all included in at least one of the following criteria: national NGOs from the US, University Centers from the US, International NGOs that research the US as a location, Organizations specialised in technology and rights, organisations specialised in immigration, International Organisations with experts on the topic, National Governmental organisations that specialise in the topic. I excluded organisations that were not relevant within the field of technology, human rights defenders or immigration; that did not address the US as a location of research, or that conducted research before 2025. Interviews, while useful due to the recency of the topic, which is still evolving, were not conducted for ethical reasons for the safety of Human Rights Defenders. Finally, despite the scarce amount of academic research on HRDs in US immigration in the last two years, the data was triangulated with academic articles on the relevant topics.

It is important to recognise the difference in content and narrative within data from NGOs and data from the government. Hence, while all data was analysed for themes to answer the research question, NGO reports were investigated in light of what patterns of human rights harms emerged related to the themes, while government data was analysed in light of what explanations, narratives and motivations emerge in relation to the themes. The fact that the data came from very opposite voices helped discover a wider picture of exactly how DA practices harm HRDs and what this means for democracy.

Finally, I would like to mention that for this thesis, Generative Artificial Intelligence Claude was used, specifically for grammar checks, citation and bibliography support, and formatting.

2.2. Case Study

The United States has a historical relevance for human rights and democratic standards (G'Sell, 2025), the present research chose it as a case study to investigate if the standards they preach are implemented in practice. Given the findings that a rise in technology is linked to a rise in digital authoritarianism (Pearson et al, 2025), a focus on a particular field of governance in the US where the use of technology has risen (American Immigration Council 2025) is important for the identification of potential risks. Therefore, immigration governance during the second presidential administration in the US (2025-2026) is particularly relevant to researching how Digital Authoritarianism explains the blurring of democracies.

President Donald Trump's second term in office started in 2025, and one of the main targets of his administration was and continues to be immigration (Eshbaugh-Soha, 2026). His second term is characterised by an even more intense immigration stance, through deportations, violent enforcement, and violations of fundamental, constitutionally protected rights (Human Rights Watch 2026, American Immigration Council 2025). The height of ICE operations reached more than 100 arrests of immigrants per day, with a majority of these not having any criminal history (Human Rights Watch, 2026). This growing anti-immigration sentiment is driven by a perceived threat, which justifies greater approval of restrictions in the field (Hempel and Strapko, 2026). In the US, this perceived threat is linked to cultural and ethnic concerns and was found to be a strong predictor of anti-democratic attitudes (Bartels, 2020). Popular support for anti-immigration sentiment can prompt the government to engage in anti-democratic behaviour against the threats (Bartels, 2020 p22758).

The Trump administration has been found to exploit anti-immigrant sentiment in order to implement political objectives that are often found to be risky for democratic stability (Kapelner, 2024). During the first Trump administration, immigration already started being digitalised, especially at borders where algorithms were used by ICE to analyse and detain migrants (Molnar, 2019). Molnar (2021) argues that using technology in migration will exacerbate preventative attitudes in migration and negatively affect the rights of the immigrant population. What existing research has not adequately addressed is what other

groups of people are targeted by this aggressive and increasingly digital US immigration enforcement. I find Human Rights Defenders to be a distinct category of affected people that work closely within the immigration field and can be affected by the repressive practices employed by the US government.

The concept of Digital Authoritarianism, initially only applied to authoritarian regimes with states that had explicitly repressive governments, has been increasingly studied when it comes to its application in democracies (Roberts and Oosterom, 2024). With the increased digitalisation of the immigration field in the US and the increased hostility against immigration under Trump's new mandate (American Immigration Council 2025), it is important to research how Digital Authoritarianism manifests and how it can undermine democracy. Immigration enforcement, driven by fear of group threats and fueled by the development and increased use of technology, becomes a space where Human Rights Defenders risk being targeted and where democratic values are left behind.

II. Literature Review

1. What is Digital Authoritarianism?

With the technological advancement of the past years, the world is now facing an unprecedented amount of data availability. Every user can track real-time tweets, messages, videos and posts, and the dissemination of such data can affect public opinion (Feldstein, 2021 p3). Technology was initially seen as a liberating power used by activists to foster rapid change and document human rights violations (Feldstein, 2021; Hankey and Clunaigh, 2013). Governments have now caught up, and the same tools that can promote human rights are now used by states to oppress and hold on to power (Feldstein, 2021; Dragu and Lupu, 2021). The term Digital Authoritarianism describes this practice of technological exploitation for authoritarian means (Pearson 2024; Roberts and Oosterom, 2024; Wilson, 2022).

Despite significant advancements, the field remains marked by definitional instability. Pearson (2024) argues for a promotion-based definition of Digital Authoritarianism, to include any situation in which digital technologies systematically foster authoritarianism, regardless of the actor or the intention. This allows the concept to detach from its focus on intentionality, but shift towards analysing the direct effect of Digital Authoritarianism. Instead, Roberts and Oosterom (2024) identify the actor involved as a significant element for Digital Authoritarianism in order to better identify the mechanisms behind such practices, while still considering the effects on citizens and on governmental power relations. The present research positions itself somewhere in between when it comes to defining Digital Authoritarianism. In fact, while it acknowledges the importance of expanding the concept to any situation where Digital Authoritarian patterns are identifiable, regardless of the classification of the regime, it also takes into account the importance of recognising the actor. The focus will be on the state as an actor, in order to determine how such practices are implemented and, most importantly, how they blur the line between democracies and authoritarian regimes.

The term emerged in 2010 in a context of increasing use of technology as a method of state repression (Roberts and Oosterom, 2024). The field was popularised by the books Access

Denied and Access Controlled by Deibert et al. (2010), in which they identified three generations of control. The first was denial of internet access, the second was legal regulations of access as well as internet shutdowns, and the third focused on controlling the internet through a mixture of surveillance and monopolisation of the online narrative space. This schema is particularly useful because it helps focus research in specific time-relevant generations of control that help map out the development of Digital Authoritarianism. The first and second generations of internet control are relatively well-theorised and empirically documented, with denial of access, internet shutdowns and legal regulations seen as visible, measurable and mainly linked to authoritarian regimes (Deibert et al, 2010). The third generation, by contrast, operates through co-optation rather than exclusion: surveillance, narrative control, and information manipulation are harder to detect, harder to attribute, and produce ambiguous effects on rights. Furthermore, given its covert nature, this last generation is more characteristic of democratic countries that do not want to be associated with explicitly authoritarian practices (Feldstein, 2021).

As stated above, technology is readily being exploited for authoritarian use, in fact, higher levels of technological development actually lead to an increase in the government's use of such tools as forms of repression (Dragu and Lupu, 2021; Christensen and Groshek, 2019). This coincides with Feldstein's (2021) observation that the initial advantages enjoyed by civil society actors have largely dissipated as states developed and institutionalised counter-strategies. The relationship between technology and state authoritarianism is mutually reinforcing: they fund technological development and enable technology companies, while using such advancements to increase repression (G'Sell, 2025 p2). Roberts and Oosterom (2024) identify a category labelled as "First Effects on Citizens" as a relevant research perspective to assess the direct implications of Digital Authoritarian practices. This category refers to the analysis of how Digital Authoritarianism impacts citizens and what effects this may have (Roberts and Oosterom, 2024 p877). The present thesis agrees with the need to focus on the first-order effect, however, it applies an innovative take by focusing on the subcategory of Human Rights Defenders, whose definitions and implications will be discussed in more detail below. By investigating how these Digital Authoritarian practices are used and their effects on Human Rights Defenders' rights, the aforementioned relationship between technology and state authoritarianism will be further explored, but going one step further: focusing solely on democracies.

2. Private Tech Companies

The development and deployment of technology mainly occurs on behalf of private companies. Mutually beneficial relationships are established between private companies that seek profit, and regimes that require their service (Conduit, 2025 p764). Thus, identifying private companies is essential in the research of authoritarianism. However, Conduit (2025) only focused on authoritarian regimes and their interactions with companies. Instead, private companies and their role in authoritarian tendencies can be present in democracies as well. (G'Sell 2025, Peron et al 2025). Big Tech companies have significant access to user data, and as such, they have a lot of control over content and targeted advertising (G'Sell, 2025). G'Sell (2025) argues that the power held by private companies is often comparable to state authority, with the difference being that companies do not always have measures of human rights or democratic compliance. Furthermore, their commercial interests sometimes expand to be political or ideological, especially if in collaboration with the state. In that case, with growing funding for law enforcement and security, government surveillance becomes a market for private tech companies (Molnar, 2019 p67). This shows that private actors are involved in digital authoritarianism both as separate actors as well as in aiding the state. The latter often occurs through the provision of surveillance and data collection technologies to the state (Quadri et al., 2025; Koula, 2024).

The term “surveillance capitalism” has emerged to describe how reality has transformed into data that can be analysed and sold (Zuboff 2018 in Molnar 2021 p71; Yabanci 2024). Transforming sites of potential privacy and human rights breaches into profitable markets. Everyone's data is being used, but specific groups are being targeted, including people belonging to the migration space (Zuboff 2018 in Molnar 2021 p71). In fact, private companies have often, in research, been found to be used in migration governance (Molnar, 2021; McGregor and Molnar, 2023). Private actors emerge as potential facilitators when it comes to digital authoritarianism, in their ability to provide less-restrictive material for states to use. Firms now represent a way for states to bypass international or national oversight and still have access to enormous amounts of data (Yabanci, 2024). In addition, private actors are starting to display authoritarian tendencies of their own due to their increasing domination of the technological landscape, which grants them power to decide how the digital technologies are deployed, implemented or expanded (G'Sell, 2025). The private sector has its own obligation under national and international human rights law, but especially within the field

of migration, private contracts with the state are still in place despite rights violations, mostly through justifications of national security (Molnar, 2021 p71). This is particularly relevant for the present case study, a possible reliance on the private sector could further facilitate the covert implementation of digital authoritarian practices.

3. Digital Authoritarianism in Democracies

Technology in democracies has often been regarded due to its mobilisation effect, meaning its ability to mobilise democracy and human rights (Dragu and Lupu 2021). Digital Authoritarianism literature mostly focuses on authoritarian regimes, and the research on its role in democracies is underdeveloped (Pearson 2024). I argue that the view of technology as a double-edged sword only present in authoritarian regimes is simplistic, as it discards the role technology plays in suppressing rights even in democracies. There are two conceptualisations of Digital Authoritarianism: one in which the regime in question is authoritarian, and another in which the government is a democracy or a hybrid regime but similar practices are still carried out (Wijayanto et al 2022). I believe it is further important to investigate how digital authoritarianism manifests in democracies. However, I concur with Roberts and Oosterom (2024) in the fact that such analysis should have a rights-based focus due to the fact that most democracies are signatories to international human rights conventions and have translated these into national legislation as well. Furthermore, the relevance of rights stands in their representation as pillars of democracy (Rawaqa 2025) and thus Digital Authoritarianism analysed through a lens of which rights are impacted can shed light on the blurring between democracies and authoritarian regimes.

Democracies often present themselves as leaders in human rights, especially when it comes to technological development, including the US-led ‘Declaration for the Future of the Internet’ in April 2022, which gained support from sixty countries (G’Sell 2025), but this further highlights the importance of investigating digital authoritarianism in democratic governments to identify how these self-proclaimed standards are actually applied in practice. Feldstein (2021) finds that in practice, digital tools can be used for high-intensity coercion targeting large groups or known individuals, or low-intensity coercion, which involves systematic and covert actions that still can repress opposition. These concepts are important to understand what solutions should most appropriately be implemented, especially given the different motivations between democratic governments and authoritarian ones. In fact, authoritarian

practices in democracies are often implemented in response to national security, protection of sovereignty or countering disinformation (G'Sell 2025, Maerz 2025). Earl et al. (2022) argue that the use of digital tools to repress falls into the low-intensity category, hence being more likely to be used by democracies due to their non-physical and less detectable violent nature. In fact, democratic states are likely to use approaches that mirror authoritarian regimes, but usually implement them with less severity (G'Sell 2025).

3.1 Conceptualising Practices

Within the literature on digital authoritarianism, a lot of the focus is on the phenomenon in authoritarian governments (Maerz 2025). The present research argues that Digital Authoritarianism can be investigated as a practice-based phenomenon present within both democracies and authoritarian regimes, contributing to the emerging literature that focuses on democracies (Maerz 2025). Before delving into the conceptualisation of DA practices, it is important to define what is meant by authoritarianism. Altemeyer (1981) defined right-wing authoritarianism as an authority that demands to be trusted and respected, and that suppresses criticism, which is instead seen as divisive. I argue that, because of its authoritarian nature, Digital Authoritarianism can be used to explain the blurring of boundaries between democracies and authoritarian regimes. In order to do so effectively, the current thesis will focus on Digital Authoritarian practices. A practice can qualify as authoritarian, even if the state is not an authoritarian regime, if it suppresses freedom of speech, political pluralism, impacts accountability, or misinforms and threatens citizens (Pearson 2024). Focusing on practices also allows the research to unveil how violations occur and which mechanisms are involved, for example by taking into consideration the role of private companies and their interaction with states (Michaelsen and Glasius 2018). This thesis will consider practices as units of analysis used to analyse patterns of actions within a specific context that can reveal the nature and effects of state actions (Michaelsen and Glasius 2018).

A focus on authoritarian practices allows the research to analyse the impact of such practices regardless of the classification of the regime (Roberts and Oosterom 2024). It allows research to identify what states do with technologies and how their actions can be a threat to the rights of citizens. Within the literature on DA practices in democracies, Michaelsen and Glasius (2018) conceptualise two different types: illiberal practices and authoritarian practices. They distinguish them by stating that illiberal practices are mainly a human rights issue while

authoritarian practices are a threat to democratic processes. However, throughout their analysis, they indicate cases in which the two practices coincide, especially when it comes to the violation of freedom of expression. The present thesis will use the term DA practices to indicate a combination of both conceptualised practices, arguing that threats to human rights are often threats to democracy as well. Furthermore, given the focus on human rights defenders, and hence freedom of expression as an important focus, it is even more important to analyse DA practices by recognising the interconnectedness between Human Rights violations and threats to democracy.

3.2 Blurring of Democracy

I contend that Digital Authoritarianism can be used to better understand the blurred boundary between democracies and authoritarian governments. How digital practices contribute to the fading of democratic attributes is still a largely unexplored field (Maerz 2025), but I find that focusing on the effects of such practices on human rights can help contribute to expanding the understanding. Focusing on how digital authoritarianism impacts the protection of HRDs is especially relevant as it goes to target one of the main pillars of democracy: freedom of expression. Huq and Ginsburg (2018) identify the concept of *constitutional regression*, using the United States government as an example, which captures the incremental decay in three basic components of democracy: competitive elections, liberal rights to speech and association, and administrative rule of law. By analysing how digital authoritarianism affects HRDs, I can shed light on the component of liberal rights to speech and association. In fact, Huq and Ginsburg (2018) mention that this particular pillar focuses on the first-generation rights of speech, assembly and association, which are also the rights that are at stake for HRDs in their work. Constitutional retrogression theory provides a lens through which to analyse the impediments imposed on HRDs by DA practices, not only as isolated enforcement decisions but as contributions to a broader pattern of rights erosion and blurring of democracies.

However, Huq and Ginsburg (2018) don't want to anchor any analysis in a particular presidency, claiming that this could add an unnecessarily polarising element to the analysis. I find this perspective to be insufficient when adapting the framework to a study of Digital Authoritarianism. As the literature reviewed in this thesis demonstrates, DA practices are not structurally self-executing, and the actors behind them are particularly relevant when

analysing their implementation (Roberts and Oosterom 2024). Therefore, it is important to investigate how specific presidential governance can demonstrate tendencies of authoritarianism and to understand how they can link to wider constitutional regression. The contribution to the literature on democratic decline is twofold: Firstly, by applying a DA analytical lens to immigration enforcement, this thesis offers a mechanisms-level account of how one component of constitutional retrogression (the erosion of liberal rights to speech and association) is being impacted by digital means. Secondly, it challenges the tendency within literature to disregard HRDs, instead considering them as actors whose rights and ability to work can be an indication of the functioning of a democracy.

The role of Digital Authoritarianism in blurring the understanding of democracies is also linked to an erosion of accountability (Maerz 2025) and transparency (Stoycheff 2018). Stoycheff et al (2018) argue that a lack of transparency in the use of digital technologies can be damaging for democracies because it weakens the social collective action of a nation. This is particularly relevant for the work of Human Rights Defenders, who peacefully aim to protect human rights and hold governments accountable, so if their efforts are found to be controlled and suppressed, the relevance of human rights in democracy becomes at risk. Instead, Maerz (2025) finds that Digital Authoritarian practices are often employed by democracies to strengthen the government's grip on power and avoid democratic checks. Her findings report that the presence of DA practices that exert control in democracies can hinder civil liberties and the possibility for citizens to hold the government accountable for its actions. In fact, regarding accountability, Molnar (2019) argues that digital technologies are still not effectively regulated in ways that can protect vulnerable groups and hold states accountable. These factors are rendered even more dangerous in light of Artificial Intelligence and the integration of technology with automated systems, whose integration with repressive technologies is often done through a lack of transparency and accountability (Molnar 2019).

4. Repression

The study of repression has usually focused on state violence against mobilised dissent, but digital technologies have changed the dynamics of state repression (Earl et al. 2022). The instruments of repression available to state actors have been complemented by technology, and new forms of repression have also emerged. The concept of digital repression has

emerged to describe the use of new technologies to repress and maintain political control (Franz et al 2020, Roberts and Oosterom 2024, Feldstein 2021). Digital repression is not only characteristic of authoritarian governments, but its role and manifestation in democracies also challenges a blind spot in the literature on democratic governance.

For democracies, digital strategies can be advantageous due to their more subtle nature compared to violent repression. As conceptualised by Earl (2022), digital repression can either include traditional techniques against digital protesters, the use of digital tools for traditional repressive actions, or the development of information strategies to affect protesters. This last category, including information strategies, marks a shift from repression understood as a physical punishment or control, to a form of constructing and influencing reality. A state engages in digital repression especially out of fear and perceived group threat (Earl 2022, Pearson et al 2025). Digital authoritarianism strategies can offer more advantages for democracies to deal with threats than other coercive methods (Feldstein 2021).

Within this broader framework, the concept of preventative repression also emerges in connection to covert use of technologies. Preventative repression refers to the use of technology to reduce the threat of government opposition by nipping it in the bud (Dragu and Lupu 2021). In their study, Dragu and Lupu found that technological innovation increases the probability that the government attempts to stifle dissent before it manifests completely, though their research mainly focuses on authoritarian governments. However, given the nature of DA practices, I find that this type of repression can be characteristic in democracies as well, especially due to its covert nature. In fact, preventative repression can decrease the government's cost of repressive techniques and anticipate the dissenting group's use of technology for mobilisation, all this without explicit forms of violence (Dragu and Lupu 2021).

Despite the focus on protesters and political dissidents, I argue that the conceptualisations of the different forms of digital repression are applicable to human rights defenders too. This is due to their reliance on online platforms and technological tools for their work (Dragu and Lupu, 2021), as well as the more covert nature of some digital repression techniques that would allow democracies to act without as much international outrage. Physical and legal coercion are used to repress "digital protesters" just as any other type of activist. This is particularly important to note in the cases that defenders online and on the street can coincide.

For example, when it comes to HRDs taking video documentation of human rights violations, and being targeted for that. Furthermore, despite human rights scholarship often focusing on repression occurring after dissent has mobilised, DA practices offer new forms of preventative repression that can be just as harmful (Dragu and Lupu 2021). Therefore, it is important not only to investigate which DA practices affect HRDs in democracies, but also how they fit within the current conceptualisations of Digital Authoritarianism.

5. DA practices

Technology can be a useful way to analyse state practices and question a government's democratic functioning (Molnar 2019). Within the literature of Digital Authoritarianism, I find that there are three main categorisations of DA practices that are particularly relevant in the case of immigration in democracies: Surveillance, Data Collection and Channelling. As mentioned above, I believe these fit into the third generation of control in Digital Authoritarianism literature, which focuses less on the denial of internet access and more on the control of the online space through surveillance and information-spreading techniques (Deibert et al 2010). These three categories have been chosen to expand the literature of Digital Authoritarianism in democracy and to analyse how they are applied in practice. The following section delves into more detail for each practice.

5.1 Surveillance

Democracies are engaging in Digital Authoritarianism through the DA practice of surveillance, which appears in the literature as a practice of digital repression that can impinge on the rights of those targeted, including human rights defenders (Earl et al 2022, Maerz 2025, Feldstein 2021, Wilson 2022). While surveillance has usually been associated with specific targets, digital tools allow it to occur at a larger scale, which provides governments access to knowledge about any type of social movement or opposition (Earl et al 2022). Law enforcement surveillance technologies are based on the extraction and processing of data for the prevention of crime and protection of national security (Peron et al 2025, G'Sell 2025, Yabanci 2024). However, there has been a trend in democracies where surveillance has been used in intrusive manners, and hence classified as authoritarian

practices (Peron et al 2025, Maerz 2025). When surveillance starts impeding on the human rights of those affected, its lawfulness is criticised (Feldstein 2019). This occurs when citizens targeted by surveillance are regarded as internal enemies and so the expansion of these technologies becomes justified against them (Ugate 2012 in Peron et al 2025 p2).

Human Rights Defenders are increasingly targeted by surveillance software programs that are becoming available to the government (Wilson 2022). Without safeguards on surveillance in democracies, this can lead to rights abuses and thus a shift towards authoritarianism. When delving into the particular harms of surveillance, one of the main issues is its potential impact on civil liberties (Richards 2013, Roberts and Oosterom 2024). The reach that surveillance technologies can have on people's lives and behaviours is increasing, affecting privacy and freedom of expression as people start abstaining from expressing dissent (Richards 2013, McGregor and Molnar 2023). Another impact of surveillance is the fact that it creates a dynamic of unequal power relations when it comes to technology, rendering the surveilled group dependent on the actions and threats of the state (Richards 2013). Within this DA practice, the most relevant tools for democracies to engage in surveillance are: social media to access data and content (Maerz 2025, Wilson 2022, Roberts and Oosterom 2024, McGregor and Molnar 2023), facial recognition to detect and store biometric data (Molnar 2019, McGregor and Molnar 2023, Peron et al 2025, Yabanci 2024) and spyware to monitor individuals' activities (Quadri et al. 2025, Glasius and Michalsen 2018, Earl et al 2022). The implications of these tools are important to further research due to the fact that surveillance can have a chilling effect on democracy by causing human rights defenders to engage in self-censoring out of fear of punishment (Kitchin 2020), by perpetuating biases and discrimination (Molnar 2019). More information on the functioning of the specific tools will be discussed in the data analysis chapter.

5.2 Data Collection

As mentioned above, a main purpose of surveillance is that of controlling the behaviour of those targeted (Richards 2013). Instead, with the practice of data collection, the focus is on accessing information on individuals for preventative measures (Yabanci 2024), in order for the state to potentially map out dissidents or use the data when it is needed. Data collection comes at the expense of privacy, collected on a mass scale and without individual consent.

Digital technologies have allowed states to have unconsented access to large amounts of information, and digital profiles of users are built for insight into the ideologies of an individual (Christensen and Groshek 2019). This data can be used by governments to censor content, produce online informational campaigns, and identify opposition. States have an increasingly far-reaching reach into citizens' online and offline lives through this systematic collection of data (Yabanci 2024). Data collection is important to look into given the ability that states have to access information on vulnerable people without any particular safeguard in place (Molnar 2019). In his proposed framework of analysis for Digital Authoritarianism in migration governance in Türkiye, Yabanci (2024) identified *datafication* as a practice that impacts migrants and citizens. I argue that his conceptualisation of *datafication* is relevant for the present research on migration governance, when looking at the effects of this practice on human rights defenders. This is because the data collected on people can be used by the state for the formulation of policies, statements and decisions based on their information (Yabanci 2024).

Surveillance and data collection are often paired together in the analysis of DA practices, with data collection seen as a part of surveillance (Glasius and Michaelsen 2018, Hankey and Clunaigh 2013, Peron et al 2025). I have chosen to separate them for two main reasons: firstly, it allows the present research to distinguish between data collected by surveillance technologies to control and change the behaviour of specific groups of people, from data collection that occurs on a mass scale and is stored indefinitely in a preventative manner; secondly it allows the analysis to focus on different types of rights affected creating a more nuanced and layered understanding of the concept of surveillance.

When it comes to specific practices, data collection relies on methods that can trace and record movements of individuals (Yabanci 2024). States achieve this by increasingly storing and collecting personal data in large-scale databases that can share any type of information with every branch of law enforcement (McGregor and Molnar 2023, Peron et al 2025). The information is also gathered through systems such as Automated License Plate Readers (ALPRs) (Sania, Ziosi and Barez 2026), which contribute to the mass tracking of movements and activities (Yabanci 2024). Further details on the specific tools will be discussed in the data analysis chapter.

5.3 Channelling

The DA practice of *channelling* can aid in revealing when the work of HRDs is considered and treated as a domestic threat, and how, if that is the case, the pillars of human rights on which democracies are based start to erode. Channelling is a term deployed by Earl et al. (2022) to indicate a type of digital repression that revolves around information manipulation on behalf of the state to deliver preferred narratives and limit dissenting behaviour. While this practice includes elements of algorithm filtering and content censorship, the aspect that is most relevant for democracies is information channelling. Information channelling focuses on the strategy of redirecting and influencing attention towards domestic threats (Earl et al 2022). This is particularly useful for democracies as it allows the state to instigate attacks or endorse oppressive narratives, all while abstaining from direct and visible intervention (Feldstein 2021). It has, in fact, been found prevalent in democracies before. For example, in 2012, the South Korean National Intelligence Service posted thousands of Twitter messages from various accounts that were constructed to imitate ordinary citizens (Earl et al 2022). This was done to distract the online space from negative news, and to spread denigratory narratives on the opposition.

This DA practice consists of social manipulation and disinformation strategies that can come directly from national information agencies or the head of state themselves (Feldstein 2021, Roberts and Oosterom 2024). Disinformation becomes a DA practice when it is deliberately used to distribute misleading information, in efforts to manipulate public opinion or target specific segments of the public (Woolley & Howard, 2017). Furthermore, the use of technology for online disinformation has been found to reinforce the blurring of democratic institutions due to manipulation of content, which hinders reliability (Woolley & Howard, 2017). One of the main methods to do so is through social media, given the crucial importance of social media platforms for content dissemination.

Social media has become a vital tool for governments and political actors, which has made it possible for them to directly interact with the public (Brooks and Porter, 2019). While this open communication offered by social media has allowed democracy to flourish and given everyone a platform to voice their opinion, the present research argues that it can be classified as a harmful Digital Authoritarianism practice if used by the state to target specific dissenting

groups (Earl et al 2022, Feldstein 2021, Roberts and Oosterom 2024, Christensen and Groshek 2019, Yabanci 2024). In fact, this immediacy is particularly relevant when it comes to developing and spreading political narratives (Mirza et al. 2025). Governments are able to comment directly on events, and can be particularly influential now that social media has become one of the primary sources to obtain news (Brooks & Porter 2019). Furthermore, social media seems like a relevant tool for states given the ability for content to target existing bias in the population and to foment ideologies (Brooks & Porter 2019).

6. Human Rights Defenders

The present research focuses on Human Rights Defenders, due to their crucial role in promoting democratic principles (Rawaqa 2025). Human Rights Defenders (HRDs), as defined by the Declaration on Human Rights Defenders, are a vast range of individuals who strive to promote or protect human rights (UN General Assembly 1998). Article 1 of the declaration states that *“Everyone has the right, individually and in association with others, to promote and to strive for the protection and realisation of human rights and fundamental freedoms at the national and international levels.”* Based on this, Bennett (2015) characterises human rights defenders by their actions, rather than who they are. Other academics have also taken this *activity-based approach* to include anyone whose actions defend or promote human rights (Koula 2026). To further develop the concept, the Office of the UN High Commissioner, in a non-binding report, set out three requirements for HRDs: they must recognise the universality of human rights, the arguments do not necessarily need to be factually correct, and they need to engage in peaceful, non-violent actions (Koula 2024). The term is often interchanged with others such as “human rights activists” or “human rights workers”, and even protesters can at times be considered human rights defenders if their purpose is to promote and stand up for human rights.

When it comes to democracies, human rights defenders also face many risks despite the notion that democracies are supposed to protect fundamental rights (Krain et al. 2023). Krain et al. (2023) argue that human rights defenders in democracies are more likely to pursue “dangerous” information, due to the apparent protection of democratically adopted rights. However, by pursuing such information, they place themselves at a higher risk from actors with political motivation to avoid exposure or dissent. In their study, Krain et al (2023) found that the predicted number of killings increases as the regime becomes more democratic. The

risks within a democratic system must be further researched, especially within a context of democratic recession (Feldstein 2021).

6.1 Criminalisation of Human Rights Defenders

The present thesis argues that DA practices implemented by democratic states can also target the rights of human rights defenders through criminalisation tactics. In recent decades, criminalisation has become a tool to suppress civic space, and it is increasingly present in democracies (Quadri et al 2025, Wilson 2022, Koula 2026). It is usually understood as the use or misuse of law to silence or deter human rights defenders (Quadri et al 2025). There are various manifestations of criminalisation, Koula (2026) identifies three main types: the first involves creating primary and secondary legislation to target HRDs, the second consists of using existing laws to impact HRDs, and the third is the use of punitive means by the government to restrict HRDs. Legislation often targets essential freedoms such as freedom of expression, peaceful association and assembly. Falling under the last category of criminalisation, HRDs are increasingly facing risks of arbitrary arrests and undisclosed criminal charges (Koula 2026). Koula (2024) finds that state authorities are often responsible for targeting defenders as a way to stifle their actions that can challenge government policy. Criminalisation often rests on charges of “incitement”, “terrorism” or “foreign agent” which are used to impede HRDs' work (Quadri et al 2025). States create laws that can be interpreted vaguely and applied to various situations under the pretence of national security (Koula 2024). All of these represent violations of human rights enshrined not only within democratic systems but also international human rights treaties.

Risks are amplified when criminalisation is coupled with digital technologies (Quadri et al 2025). Research on the intersection between these fields is important to understand new risks faced by HRDs and to inform international human rights frameworks that rarely assess the role of technology in repression. In their study, Quadri et al. (2025) found hybrid criminalisation to be an emerging tool that uses both legal and digital repression on HRDs. They found that digital strategies are used to implement legal measures such as arbitrary detention, as well as to develop other strategies of online harassment and digital surveillance. This intersection of digital technologies and criminalisation can risk heightening the effectiveness of HRDs' criminalisation by impeding their individual rights but also hindering their collective advocacy network (Quadri et al. 2025).

One particular area of interest to research is when criminalisation labels are used by the state in an online space. This represents a risk to HRD rights because they can easily turn into online hate campaigns that, if started by the government, can have great influence on the opinions and actions of a country (Wilson 2022). This is a part of the channelling DA practice that aims to use authoritarian language to denigrate and criminalise HRDs. Wilson (2022), in a series of interviews with HRDs from Latin America, identified a series of categories related to anti-human rights speech, of which I find the most relevant for democratic states to be: accusations of corruption, accusations of subversion and terrorism, assertions of anti-patriotic behaviour, accusations of criminality, dehumanisation and stigmatisation. Furthermore, online harassment is often used in combination with legal accusations to create a multidimensional repressive ecosystem (Quadri et al 2025).

6.2 Human Rights

In a moment of increasing presence of digital technologies, it is important to continue researching how human rights are affected. Research has found digital technologies to influence freedom of expression and data privacy, bringing about new ways in which fundamental rights interact (Simoncini and Longo 2026). In the US, Human Rights Defenders are protected by national and international frameworks. In this research, I will focus specifically on freedom of expression, freedom of association and assembly, and the right to privacy due to their presence in the literature as being a possible consequence of Digital Authoritarianism (Glasius and Michaelsen 2018, Wilson 2022, Roberts and Oosterom 2024, Yabanci 2024). The international frameworks most applicable to protect the rights of HRDs are the International Covenant on Civil and Political Rights (ICCPR) and the UN Declaration on Human Rights Defenders (Rawaq 2025). Article 17 of the ICCPR, of which the US is a signatory, states that *“no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”*(UN General Assembly 1966).

Article 19 of the ICCPR states that *“Everyone shall have the right to hold opinions without interference”* including the right to *“impart information and ideas of all kinds”* through *“any media of his choice”*. Article 19 allows restrictions only on two conditions: for the respect of the rights or reputations of others; for the protection of national security or of public order, or

of public health or morals. Articles 21 and 22 describe *“the right of peaceful assembly”* and *“right to freedom of association”* to which *“no restrictions should be placed on the exercise of this right other than those imposed in conformity with the law”*.

The Declaration on Human Rights Defenders was adopted in 1998 by the UN General Assembly (UN General Assembly 1998), and it is not a legally binding instrument, but it contains standards for states to follow, and many of the human rights standards are based on other human rights instruments such as the ICCPR that are indeed legally binding (UN General Assembly 1966). Article 5 of the Declaration states that everyone has the right to *“meet or assemble peacefully”* when done for the *“purpose of promoting and protecting human rights and fundamental freedoms”*. Article 6 instead refers to the right to *“freely publish, impart or disseminate to others views, information and knowledge on all human rights and fundamental freedoms”* (UN General Assembly 1998).

Instead, turning to national frameworks, the US Constitution protects the aforementioned rights in the First and Second Amendments. The First Amendment states the protection of freedom of speech and the *“rights of the people peaceably to assemble”* (United States Constitution 1789). The Fourth Amendment mostly relates to privacy, stating *“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures”* (United States Constitution 1789).

These rights are particularly relevant as they allow HRDs to organise protests, challenge authoritarian narratives, communicate across networks and form coalitions (Rawaqa 2025). If states implement restrictions or use of force against these activities, they violate both the legal obligations outlined by the ICCPR and the moral obligations outlined by the Declaration. Instead, the right to privacy has become extremely important for Human Rights Defenders in the digital world due to their increased exposure to surveillance and data breaches (Rawaqa 2025). Therefore, I find the outlining of these rights fundamental for the understanding of what is expected from states when respecting universal human rights, especially for human rights defenders.

7. Digitalisation of Immigration

Democracies, especially in the West, have seen a rise in anti-immigrant rhetoric (Karahan 2025). Take Europe, the emergence of far-right politics, especially after 2015, has represented a challenge for democratic governments. The anti-immigrant discourse has been heavily intertwined with narratives and policies concerning security as a form of legitimisation. After the 2015 refugee crisis, immigrants started being considered potential threats to national identity and social cohesion. Many of the governments employing such rhetoric aim to find a group to target, creating a divisive effect which goes on to influence public perception and policymaking. This often comes hand in hand with the concept of securitisation, which argues that security depends on what political actors perceive as a threat to the state, and extraordinary measures are taken for protection. Kapelner (2024) argues that anti-immigrant backlash is threatening democracy because the state engages in anti-democratic politics with parts of the population due to a perception of excessive immigration in the state. I find that this occurs against HRDs that try to protect immigrant rights, and that this increase in anti-immigrant rhetoric is particularly relevant when coupled with an increase in digitalisation of the immigration system.

Digital Authoritarianism is present in migration governance, due to the increased digitalisation of border control and immigration enforcement (McGregor and Molnar 2023). There is no global regulatory framework to regulate the use of new technologies in migration governance (Molnar 2024, McGregor and Molnar 2023). Despite this, countries are relying on border surveillance technologies to deter people from reaching their land (Molnar 2024). Yabanci (2024) finds that in addition to surveillance, states are digitally collecting large amounts of biometric data to surveil and control immigrants. Yabanci (2024) conducted a study on Digital Authoritarianism in migration governance in Turkey, finding that it has different effects on citizens compared to non-citizens. In particular, he found that immigrants were mostly targeted with criminalisation threats and labelled as “criminals”, “illegals” or “unwanted”. Instead, citizens were targeted with public opinion manipulation through online platforms in favour of the government’s immigration policies. My research contributes to the study of Digital Authoritarianism in immigration by focusing on an additional group of the population that can be affected by technological misuse: Human Rights Defenders. Furthermore, it can contribute to understanding how the practices deployed by a democracy in migration governance can be authoritarian and negatively affect human rights, without the whole country necessarily being classified as an authoritarian regime.

The literature on digital authoritarianism in migration governance is still emerging, however, in studying the effects of DA practices, a difference has already been distinguished between the consequences that immigrants face compared to those that citizens face (Yabanci 2024). This is why it is so important to focus the research in this field on a particular group that is targeted, in this case, HRDs, to better understand what effects these digitalised immigration practices can have on democracy. As stated by Rawaqa (2025), how Human Rights Defenders are treated is a benchmark to understand the functioning of democratic governance. Therefore, the issue arises when technology facilitates the effect of anti-immigrant backlash on HRDs. In fact, due to the lack of safeguards on the emerging overuse of technology in immigration, Molnar (2021) finds that they often target activists, journalists, dissidents and any opposition.

8. Themes

With respect to the above literature review, which touched upon Digital Authoritarianism, Practices, Human Rights Defenders and Immigration, my main argument is that democracies are increasingly using Digital Authoritarian practices to impede the rights of Human Rights Defenders, and this sheds light on the blurring between democracies and authoritarian governments. Digital Authoritarianism can provide insights on threats to democracies due to its impact on accountability (Maerz 2025), transparency (Stoycheff 2018) and impacts on rights, especially freedom of expression (Huq and Ginsburg 2018). Given the global trend of digitalisation of immigration (Molnar 2019) and the new Trump administration's focus on upscaling immigration enforcement (American Immigration Council 2026), I find the US a relevant case study for analysis.

Table 1

The following table indicates the three main categories of DA practices identified in the literature of Digital Authoritarianism to be relevant within democracies, and for each category is the list of themes that the data will be analysed deductively for.

Category of DA Practice	Themes
Surveillance	Social media surveillance Facial recognition Spyware
Data Collection	Automated License Plate Readers Centralised Datasets
Channelling	Social Media Channelling

III. Data Analysis

To answer the research question: *How do Digital Authoritarian practices in US immigration enforcement impede the rights of Human Rights Defenders?* The present thesis analysed the data collected based on three main categories as identified in the literature review on Digital Authoritarian practices: Surveillance, Data Gathering and Channelling. Within these categories, an inductive thematic analysis was conducted to analyse and interpret the data based on the themes deducted from the literature review. Subsequently, in order to effectively answer the question, an inductive thematic analysis was conducted to analyse the data for new, emerging themes that related to DA practices. As explained in the methodology section, the themes were identified in the data through hand coding, with the purpose of interpreting and identifying patterns in the data to answer the research question. The inductive thematic analysis identified themes that I have classified as *mediating mechanisms*, meaning mechanisms through which DA practices are better understood to impede human rights and affect democracy.

The findings shed light on how the rights of Human Rights Defenders are being impeded by DA practices and how this places digital authoritarianism and its effect on HRDs as an appropriate perspective to demonstrate the increasing global blur between democracies and authoritarianism. Human Rights Defenders play a significant role in the protection of human rights worldwide (Koula, 2026). Through national and international frameworks, freedom of expression and association is protected, which includes the right to share information on human rights conditions. In the US, human rights defenders are often involved in activities such as monitoring and following ICE vehicles, filming ICE interactions, collecting evidence and documenting abusive practices (Human Rights Watch 2026). Agents have arrested and threatened human rights defenders engaged in these activities, and have even killed two individuals: Renee Good and Alex Pretti for their role in documenting and defending the rights of migrants (OHCHR 2026). This increased aggression toward HRDs is also seen through the use of technology that has become widespread in US immigration enforcement (Molnar 2019). Therefore, I argue that Digital Authoritarianism in US immigration enforcement shows how democracies are using DA practices to adversely impact the rights of Human Rights Defenders, and this can explain the increasing blur between democracies and authoritarian governments.

A. Surveillance

The data analysis on surveillance practices in US immigration enforcement reveals the targeting of human rights defenders on behalf of the state. Within surveillance, themes of social media surveillance, facial recognition and spyware were found to be relevant DA practices that impacted HRDs. These findings do not merely confirm that surveillance technologies are Digital Authoritarianism practices increasingly used in the context of immigration enforcement, but they reveal that Human Rights Defenders are an emergent and specifically targeted category, which is analytically underresearched in Digital Authoritarianism literature. In addition, the sub-themes of: private companies, criminalisation tactics, the chilling effect and AI have been identified as key mediating mechanisms that impact the right to privacy, freedom of expression and association, and protection from harm of Human Rights Defenders.

1. Background Information

Even when implemented in democracies, surveillance can be a Digital Authoritarian practice because it heightens people's susceptibility to authoritarian agents, laying a foundation where governments have complete knowledge and control on its citizens (Pearson 2024). Governments often engage in surveillance technologies to monitor and suppress dissent, but also to identify external influences that are perceived as a threat to the governmental order (Peron et al 2025). Mass or targeted surveillance has been widely considered a DA practice in the literature (Roberts and Oosterom 2024, Pearson 2024, Maerz 2025).

Legitimate and proportional surveillance is dependent on legal procedures that usually involve authorised warrants that specify the purpose and reasonable suspicion of the individual being targeted. With the accessibility that governments have to widespread mass surveillance, this safeguard is not always possible, thus increasing the likelihood of arbitrary surveillance (Glasius and Michaelsen 2020). Arbitrary surveillance infringes on the rights of a person through its invasion of privacy and suppression of freedom of expression (Michaelsen and Glasius 2018, Richards 2013). It is still widely adopted in democracies for reasons of national security and public order (Stoycheff et al. 2018). A recurring objective of governmental surveillance is that of controlling behaviour. It is used to influence or respond

to someone's behaviour, destabilising the power dynamic between the state that is surveilling and the targets of such surveillance (Richards 2013).

Furthermore, with the growing involvement of AI in surveillance technologies, concerns grow regarding the reliability and objectivity of the tool (G'Sell 2025, Feldstein 2019). AI is of major use in liberal democracies, and whether they are used for repressive purposes is an indicator of the quality of their governance (Feldstein 2019). Molnar (2021) finds AI to be increasingly integrated in technology used for migration governance, with one of the main concerns being the bias of these automated decision-making programmes. In his research on the expansion of AI surveillance, Feldstein (2019) found that liberal democracies engage in AI systems with policing and facial recognition systems, especially to control borders and to distinguish suspected terrorists from crowds. The complexity arises when the concept of "terrorist" is expanded to include government dissidents, allowing the use of AI to target even those protected by free speech.

Overall, within migration, surveillance has been linked to the use of tools such as satellites, drones, heat detection systems, which are usually deployed along the border zones (Yabanci 2024), facial recognition technologies and social media surveillance (McGregor and Molnar 2023). Other tools have also been characteristic of digitalised migration policies even outside the border, and they include: facial recognition, fingerprint scanning, spyware for data extraction and geolocators (Yabanci 2024, G'Sell 2025). These practices are argued to be authoritarian due to the extraction of data that occurs to monitor and control particular groups without their consent.

The surveillance tools for which US Immigration and Customs Enforcement is increasing funding are not only being used to target immigrants, but are now increasingly being used to target human rights defenders that oppose ICE (Front Line Defenders, 2025-2026). The acquired technology is mainly for purposes including: social media monitoring systems, cellphone location tracking, facial recognition, remote hacking tools and others (Patel and Rupert 2025, Human Rights Watch 2026). In the present data analysis, the theme of surveillance used against HRDs was not only identified in NGO reports, but also in government documents themselves. The difference lay in the justification of why such methods of surveillance were used to target HRDs. In fact, as will be analysed more in detail in each sub-section, there is a discrepancy between the themes that emerge in governmental

data compared to NGO data when it comes to the reasons and implementation of the practices.

2. Social Media Surveillance

In contrast to the heightened focus of Digital Authoritarianism literature on social media as a channelling forum for the state, in US immigration enforcement it is also largely used as a medium for effective surveillance (Human Rights Watch 2025). Social media surveillance orders are implemented with a lack of transparency on behalf of the state, which I argue contributes to inadequate protection for human rights defenders. The United States Citizenship and Immigration Services (USCIS) proposal, which refers to the proposed collection of information through social media identifiers on immigration forms, exemplifies this (The Department of Homeland Security, 2025). In fact, the proposal, which was later approved in February 2026 (The Department of Homeland Security, 2025), has no mention of what social media identifiers will be applied, indicating a lack of transparency when it comes to the development of the practices. The Center for Democracy and Technology published an official comment on the USCIS proposal, raising concerns about how this policy represents a violation of freedom of expression rights protected by the First Amendment of the American Constitution, arguing that consequences would be the potential punishment and deportation of individuals due to the targeting of citizens' lawful speech (Branum, 2025). CDT also identifies USCIS' proposal as an invasion of privacy, specifying that it would affect "immigrants and US citizens alike", which indicates the growing reach of immigration policies beyond only immigrants (Branum, 2025, p. 1).

In a published comment by the Brennan Center for Justice and the Knight First Amendment Institute at Columbia University, the organisations argue the proposal lacked practical justifications and did not address social costs such as the risks to First Amendment rights, including for US citizens (Brennan Center for Justice and Knight First Amendment Institute, 2025). Furthermore, the supposedly democratic processes in place for verification of the efficacy and constitutionality of the proposal were flagged in the report as ineffective and not applicable. To be more specific, this referred to a 2017 privacy compliance review that found the Department of Homeland Security could not demonstrate the value of social media information for the immigration process, and it produced recommendations to measure the viability of social media screening. The report finds that there is no evidence of such

recommendations having been applied in the current USCIS proposal. This suggests that the states are putting human rights defenders at risk with surveillance initiatives that are approved regardless of NGO comments on human rights violations, regardless of internal discrepancies, and regardless of the limited specifications on how the tools work.

The USCIS proposal also shows how the violation of privacy rights is not only a consequence of social media surveillance, but a method of effective implementation. I find this to be evident through the impact of social media surveillance on anonymous speech. As proposed, the USCIS social media screening process requires disclosure of anything the person in question has posted or said online (The Department of Homeland Security, 2025), countering the right to speak anonymously as protected by the First Amendment (United States Constitution 1789) and Article 19 of the ICCPR (UN General Assembly 1966), and making the obligation of content disclosure a method of effective monitoring. Further evidence for this is the targeting of social media through other directives: the Department of Homeland Security published a Privacy Impact Assessment in August 2025 regarding the *Analytic Tools in Support of the Protective Mission* program which was a project of information collection on social media in response to “an increased level of external threat activity directed towards the agency’s Senior Leaders and its personnel”(The Department of Homeland Security 2025 para.1). They mention that the project will consist of collecting publicly available information from social media to identify potential threats, without better defining in which situations it will be applied. Here, the dismantling of anonymity is justified due to an “external threat” faced by the agency (The Department of Homeland Security 2025 para.2). I find that once again this indicates a lack of transparency, as well as a justification for privacy breaches in the name of security.

This is particularly damaging to HRDs who increasingly depend on online tools (Branum 2025). The CDT, in a report to the OHCHR on Protection of Human Rights Defenders in the digital age (Seck et al 2026), recognises the reliance of HRDs on online media to conduct their work. However, they identify that digital surveillance in online media poses a risk to HRDs’ anonymity. Therefore, social media surveillance aims to dismantle protected online anonymity to potentially target human rights defenders. This is particularly evident in the case of immigrant human rights defenders as discussed in the following section.

2.1 Viewpoint-based immigration

Viewpoint-based social media surveillance indicates a shift of immigration enforcement from an identification system to one of ideological screening (Human Rights Watch 2025). Viewpoint-based immigration refers to the punishing and deportation of individuals based on their protected freedom of speech (Branum 2025), and it emerged as a relevant theme in the analysis when understanding how the DA practice of social media surveillance impacts immigrant HRDs. The Center for Democracy and Technology classification of the USCIS proposal as promoting viewpoint-based immigration enforcement (Branum 2025) is sustained by evidence of case studies regarding pro-Palestinian student speech. Badar Khan Suri, a Georgetown University Student who was detained due to his statements on X, the social media platform, where he opposed Israel's attack in Gaza, as well as the notorious case of Mahmoud Khalil, who was arrested and threatened with deportation due to his participation at the protests indicate cases of surveillance enabled by an expansion of anti-semitism discourse to include pro-Palestinian activism as a ground for denying immigration (Brennan Center for Justice and Knight First Amendment Institute 2025). These cases are cited in NGO reports that responded to the USCIS 2025 proposal as examples of potential consequences of social media screening (Brennan Center for Justice and Knight First Amendment Institute 2025, Braunum 2025). In fact, after the repression of pro-Palestinian student activists, other international students have reportedly stopped posting on social media about similar topics or removed previous posts that could attract government attention (Raphling 2025). A report by the Special Rapporteur on freedom of peaceful assembly and association relays that the use of immigration enforcement by the US to arrest and deport activists who defend Palestinian rights sets a dangerous precedent in which political expression becomes a security threat (UN General Assembly, Special Rapporteur Gina Romero 2025). Accordingly, Grey (2026) finds that the deportation of noncitizen students for pro-Palestinian views is a violation of their freedom of speech and constitutes viewpoint-based retaliation. She argues that immigration authority was weaponised to suppress dissent, and this threatens the role of American universities as places of democratic debate and human rights. Her findings are relevant especially in light of social media surveillance, which represents a medium through which the state can effectively weaponise immigration enforcement, having greater access to immigrant HRDs' published viewpoints.

These findings shed light on how the digitalisation of immigration enforcement and its methods of application by the government reveal a category of further vulnerability: human rights defenders who are also immigrants. National security reasons allow the government to limit protections of immigrant HRDs. This occurs especially when it comes to the application of the First Amendment, often declared to be limited for non-citizens (Branum, 2025 p3), which I would argue is used to justify the use of digital surveillance on immigrant human rights defenders. In fact, despite the government's limits on the First Amendment, immigrant HRDs are still protected by international human rights frameworks such as Article 19 of the ICCPR, which protects freedom of expression, and Article 21, which protects freedom of assembly (UN General Assembly 1966). In their annual report 2025/2026, Front Line Defenders (2026) signal the reduction of protection mechanisms for HRDs who are immigrants or asylum seekers in the US, claiming that many have been left facing deportation despite risks of returning to their home country. In fact, research finds that immigration officials are not constrained by First Amendment obligations when it comes to deporting illegal immigrants, resulting in immigrant HRDs not having ways to challenge deportation and arrest (Das 2020). Research on US immigration enforcement finds that the First Amendment is violated in instances of both inadmissibility and deportability of immigrants (Hudson and Gluzman 2025). Hudson and Gluzman (2025) found that immigration officials tend to target noncitizens for their criticisms of US immigration policy, and this can lead to starting removal or deportation proceedings. This is particularly relevant in moments of anti-ICE demonstrations and expressing dissent for the human rights violations committed by ICE (Human Rights Watch 2026), indicating this could be a motive for agents to target immigrant HRDs. Furthermore, Das (2020) finds that the US federal government retaliates against immigrant rights activists and argues that this is a serious threat to freedom of speech and to overall US democratic values. The ability to suppress dissent through deportation causes the stifling of freedom of expression and constrains advocacy. The same was found at the time for US citizens who advocated for immigrant rights and faced similar retaliation, though without the risk of deportation (Das 2020). Given the 2025 Trump administration's digital proliferation in immigration enforcement (Human Rights Watch 2026), I argue that these overall findings show a serious risk of viewpoint-based immigration enforcement through digital means that can affect the protected freedom of expression of HRDs.

2.2 Private Companies

I find that social media is particularly effective due to the involvement of private companies that allow the state to expand its reach while avoiding accountability (Molnar 2021). Firstly, I argue this is done by including Human Rights Defenders in national security narratives. Within social media surveillance, contracts with private companies include Signal Labs (USASpending.gov 2025) and Penlink (USASpending.gov), used to analyse posts and develop monitoring tools to gather information from multiple sources (Patel and Rupert 2025). These contracts specify that the platforms will be used to gather intelligence for “organised crime”, “trafficking” and “terrorism”, which the state has reportedly expanded to include “anti-Americanism”, “anti-Christianity” and “anti-capitalism”(Department of Homeland Security, Federal Register 2025). In addition, in an official governmental Memorandum, the President alludes to the need for “a new law enforcement strategy that investigates all participants in these criminal and terroristic conspiracies” (Department of Homeland Security, Federal Register 2025). However, in further developments of such statements, such as the recent June 3rd Executive Order (The White House 2026), themes of surveillance do not emerge directly, and mention of strengthening the enforcement of US customs law remains vague on that front. I argue that this vagueness allows the state to include human rights defenders in these narratives and to use private companies to effectively surveil them.

Evidence for this inclusion of Human Rights Defenders in the aforementioned narratives relating to national security is found in the method with which the state ensures private company collaboration, which seems to be either through legal contracts or through the use of legal means to force companies to share data (Electronic Frontier Foundation 2026). In a lawsuit by the Electronic Frontier Foundation against the Department of Homeland Security and ICE in April 2026, the FOIA lawsuit complaint shows that DHS has been issuing subpoenas to private technology companies in demand of data about protesters and people who have documented or reported ICE activities (EFF v DHS and ICE 2026). Access to such information would not only be a breach of privacy, but also impact the freedom of expression of defenders who are now facing consequences for having reported violations and expressed dissident opinions online. EFF claims the subpoenas are unlawful, and when pressed, DHS withdrew them rather than facing a court decision (Electronic Frontier Foundation 2026). The state seems to be implementing this DA practice of social media surveillance through the use

of legal tools whose process, however, lacks transparency. EFF sued the DHS and ICE exactly due to their refusal to share public-records documents about the processes behind the subpoenas (EFF v DHS and ICE 2026).

Relating to the use of private companies to avoid democratic accountability, I argue that US immigration enforcement and its agencies' access to private company surveillance technology allows them to violate the privacy rights of human rights defenders without facing evident repercussions. This can be seen through the Electronic Frontier Foundation's involvement with various cases of social media surveillance and private companies. Extremely relevant is the official letter sent by the NGO to the Office of the Attorney General in April 2026, requesting them to open an investigation into Google due to deceptive trade practices (Trujillo, EFF 2026). They claim Google has broken the promise stated in the Privacy & Terms page, of notifying users when their personal data will be disclosed to law enforcement. In particular, they refer to the case of Amandla Thomas Johnson, a student at Cornell University whose information was requested by ICE due to the student's participation in a pro-Palestine protest the year before. Not disclosing ICE's subpoena to Thomas Johnson prevented the student from challenging the request and protecting his data. In the letter, EFF claims that: "the ICE subpoena unconstitutionally targeted Thomas-Johnson for engaging in First Amendment activity by attending a protest". Challenging the subpoenas is a fundamental right of the user (Trujillo, EFF 2026). For example, in September 2025, DHS sent a subpoena to Meta in an attempt to unmask anonymous users behind the Instagram accounts that were tracking and reporting on ICE activity in California and Pennsylvania (Trujillo 2026). ACLU and state affiliates challenged the subpoena in court, and DHS withdrew it before a ruling. However, in the previous example of Thomas Johnson, no warning or possibility to contest was given by the company (Trujillo, EFF 2026). Furthermore, a subpoena was issued to Google after a citizen sent an email to an ICE attorney, and once they had obtained the data, agents appeared directly at the individual's home (EFF v DHS and ICE 2026). EFF submitted the action under the Freedom of Information Act (FOIA), claiming that since the beginning of 2025, DHS and ICE have issued administrative subpoenas to technology companies and internet platforms to access anonymous social media accounts of individuals reporting on immigration enforcement activities. I contend that this signifies a possible shift towards an overarching DA practice of surveillance, and its breaches of privacy rights are facilitated by the role of private companies. Private companies exacerbate the strain of social media surveillance on the

privacy rights of HRDs, and this is the case because of the lack of accountability on behalf of the state when accessing surveillance through third parties (Nambiar 2025). In fact, privacy is not considered a reasonable expectation when an individual entrusts data to third parties. Nambiar (2025) argues that the privacy settings of social media platforms, as developed by private companies, set expectations that data is private and not accessible to law enforcement; however, we have found that this is not the case. Immigration enforcement often requests access to such data, bypassing privacy standards by accessing it through private companies (Nambiar 2025, Molnar 2021).

The findings for this section reveal not only that the themes of digital authoritarian practices of social media surveillance are used and have the potential to be used against Human Rights Defenders, but that in their application they violate their freedom of expression and rights to privacy. Furthermore, other sub-themes emerged inductively from the data analysis, including: **viewpoint-based surveillance** which was closely linked to social media surveillance, and **private companies** as mediums through which the state effectively implements social media surveillance while bypassing privacy obligations.

3. Facial recognition

Facial recognition is a surveillance technology that uses cameras to identify an individual by matching them to stored images from a database, or by storing information on their identification (Feldstein 2019). Facial recognition technology in immigration enforcement is meant to identify illegal immigrants (Electronic Frontier Foundation 2023), but I argue that it often targets Human Rights Defenders in a way that puts their rights at risk. In fact, facial recognition technologies have been reported to be used against people engaging in protected speech (Electronic Frontier Foundation 2023)

I find that the state is able to effectively implement facial recognition technology by assigning different values to digital tools depending on the actor that uses them. In the analysis of an interview with Todd Lyons, the Acting Director of US Immigration and Customs Enforcement, he claims: “Protesters mask up without criticism, while ICE is vilified for protecting anonymity”, hence justifying the agency’s use of masks as the only remedy to “ICE officers and agents getting doxxed and threatened continually” (The Glenn Beck Programme 2025). Instead, protesters who conceal their identities are requested to be stripped

of their anonymity due to security reasons for ICE agents, which makes the use of facial recognition technologies against them more effective (The Glenn Beck Programme 2025). This introduces the dual mechanism behind technological tools: stripped of their liberating use when in the hands of human rights defenders (accused of doxxing enforcement agents and spreading information of their location online as warnings) and used as a digital authoritarian practice when in the hands of the state.

The field of facial recognition surveillance was expanded through the use of “Mobile Fortify”, an app that allows agents to conduct biometric screenings to prove immigration status (American Immigration Council 2026). When analysing an official Homeland Security Privacy Threshold Analysis on the application, the state document reveals that the app will be used during ICE operations once an individual is identified or “associates of that individual” (Department of Homeland Security 2025). The app allows officers to collect biometric data, geolocation information, photos and fingerprints, which can be stored on the CBP database. Furthermore, the PTA directly states that the app will be used regardless of the individual’s expressed consent. Every new piece of data will be held for 15 years with no way for the individual to remove or contest it (Human Rights Watch 2026). In the field, the Center for Democracy and Technology (2025) reports ICE agents using their phones aimed at protesters, suggesting the risk that they may be using Mobile Fortify for their surveillance. Concern emerges when ICE continues to use Mobile Fortify on anyone and doesn’t expand its current Privacy Threshold Analysis to these uses in the field.

With no regulations on facial recognition technology and due to its easy accessibility by agents (Center for Democracy and Technology 2025), rights can be violated when ICE films or records HRDs and possibly stores and shares their data. In an interview conducted by Human Rights Watch with Dalton, a human rights observer who was following an ICE vehicle to observe and report the enforcement operation, he states that agents approached him and took a photo of him and of his license plate after physically pushing him to the ground and arresting him (Human Rights Watch 2026). Reports on the Blaisdell Avenue confrontation in Minnesota on January 21st show similar findings of Border Patrol agents with professional filming equipment pointed at human rights observers (Human Rights Watch 2026). In these field interviews conducted by Human Rights Watch, journalists report having captured pictures of agents using the facial recognition app Mobile Fortify against protesters and individuals involved in observation activities, and it was recognised due to the presence

of a circle centred around the face of the subject they were pointing to, with messages on screen saying “searching face” or “processing”. Many other cases such as these were reported to Human Rights Watch (2026), suggesting the use of facial recognition surveillance is widespread and targeting human rights defenders. Once again, this provides evidence for the dual use of technology, which in the hands of immigration agents is used as a DA practice, while in the hands of human rights defenders it becomes an element to target in the name of government safety.

Compared to social media surveillance, facial recognition more clearly shows the nature of DA practices as authoritarian and damaging to democracies regardless of the intentionality behind the application of such practices (Pearson 2024). In fact, if facial recognition technologies are becoming widespread, so is the collection of data that is then subsequently stored without consent (Access Now 2021). In an open letter calling for the ban of facial recognition technologies, the NGO Access Now raises concerns over the creation of centralised biometric databases which can then be used by the government for any purpose they want (Access Now 2021). It doesn’t matter whether the data is then anonymised or processed only locally. It is in itself designed to violate people’s rights to privacy (Access Now 2021). The data is stored regardless of whether it was the state’s intention to apply the surveillance technique on the human rights defender. This also relates to the practice of data collection, which will be discussed in the following section, showing how surveillance systems seem to be connected and become a modality of facilitation that allows the state to collect enormous amounts of information on all individuals.

4. Spyware and Private Companies

The theme of spyware technologies emerged only in relation to the private companies that create them, contributing to the findings of social media surveillance in indicating a reliance of the state on the private sector. Despite the involvement of the private sector, justifications regarding the use of spyware on HRDs still revolve around national security narratives. In their annual report, Front Line Defenders reveal the US government infiltration of a private Signal group chat used by migrant rights defenders (Front Line Defenders 2026). This infiltration was done with the purpose of monitoring immigration cases, and confidential information was extracted and used in law enforcement reports. In these official law enforcement reports, the human rights defenders were labelled as “extremist actors”, which is

the common justification for the state to bypass security and privacy measures. Human Rights Watch's annual report on the US also flags the procurement of phone hacking and other commercial spyware technology acquired by ICE recently (Human Rights Watch 2025).

This previous evidence of states using spyware developed by private companies to target HRDs (Front Line Defender 2026) could lead to foreseeable harms to HRDs in the current administration. In October 2019, a lawsuit was filed against NSO Group, an Israeli-based company whose spyware software “Pegasus” in WhatsApp was found to target human rights activists, journalists, dissidents, lawyers and religious leaders (Access Now 2020). Citizen Lab investigated the incident and identified over 100 cases of targeted human rights defenders and journalists worldwide (Citizen Lab 2019). The NSO group claimed the use of Pegasus is to combat terrorism and criminal activity, but Access Now labelled their attack as a violation of privacy and an endangerment of the work of activists. The Biden administration placed restrictions on the NSO group due to its dangers of repression (Summer 2026). While this restriction has not, to date, been lifted, many are raising concerns about the possibility that the Trump administration could reinstall Pegasus for government enforcement purposes. This is especially due to the link between the President and the new American owner of NSO.

I argue that if the US reinstates a contract with NSO, the risk for HRDs in immigration enforcement will increase given the history of the company in targeting defenders (Citizen Lab 2019), but also given the trend that the government is moving towards contracting with other spyware firms. Evidence for this is seen through the spyware tool: Paragon. The US has recently reactivated their contract with Paragon Solutions, another Israeli company that develops spyware software that can infiltrate any information on the device on which it is applied. In a government letter to the US House of Representatives, in response to concerns arising over the Paragon Solutions contract, ICE authorises the use of these investigative techniques for “national security and public safety”, especially when it comes to drug cases (Lyons 2025). However, Paragon’s spyware, known as Graphite, has already been reportedly used by governments against human rights defenders (Access Now 2025), the most recent being the forensically proven involvement of Italian authorities in the targeting of individuals working for the rescue of refugees at sea (Marczac and Scott-Railton 2025, Access Now 2025). The fact that ICE has reportedly been using the software without appropriate transparency raises concerns about the targeting of human rights defenders, especially given the software’s history in the matter. Furthermore, it impedes HRDs’ use of digital tools,

which are considered essential to the exercise of freedom of expression (Anstis and Sprenger 2025), but if targeted with spyware, they no longer represent a tool through which HRDs can conduct their work.

Furthermore, the contracts with these spyware software companies show a lack of transparency on behalf of the government. In fact, the \$2 million contract signed with Paragon Solution doesn't name a specific product, though the company is most known for its spyware Graphite, which works in a very similar way to Pegasus (Campbell 2024). The US government has not publicly disclosed information on the use of Paragon's software, including information on what terms govern the services provided, how ICE will monitor potential abuse and how they will inform the public about possible impacts and grievances. This can be interpreted again as an intentional vagueness in their justifications, which only report reasons of national security, while avoiding transparency on important information for the safety of HRDs. The contract was put on hold by the Biden administration in 2024, and in August 2025, Trump reinstated the contract (Center for Constitutional Rights 2025). The Center for Constitutional Rights (2025) claims that the public has a right to know what spying tools are being used in immigration enforcement, reporting the necessity of this knowledge for both immigrants and human rights defenders. To achieve this, Just Futures Law and the Center for Constitutional Rights filed a Freedom of Information Act (FOIA) request to ICE and CBP requesting information about Paragon and another company: Cellebrite (Just Futures Law and CCR v. ICE and CBP, 2025).

These findings show how the purchase of spyware from private companies can be linked to a decline in rights for human rights defenders. Anstis and Sprenger (2025) find that spyware violates the right to privacy, the right to freedom of expression and the right to peaceful assembly of human rights defenders. Given the peaceful nature of the HRD work, violating their privacy by acquiring software that can access their data is rarely considered necessary under domestic and international human rights law (Anstis and Sprenger 2025).

5. Criminalisation

One of the main tactics used by the US government to infringe on the rights of HRDs in the immigration field is through criminalisation. As touched upon in the literature review, criminalisation refers to the use or misuse of law to silence or deter human rights defenders

(Quadri et al 2025). Regarding Human Rights Defenders, Koula (2026) identifies three main types of criminalisation: creating and enforcing legislation to target human rights defenders, using existing legislation to target human rights defenders, and using punitive measures to suppress human rights defenders. In their research on criminalisation and digital repression, Quadri et al (2025) identify, as part of criminalisation, charges of “incitement”, “terrorism”, “foreign agent” and “threat to national security”, used to delegitimise HRDs. Furthermore, attempts at keeping legislation vague allow states to interpret laws broadly in the name of national security (Koula 2024). I find that within the study of Digital Authoritarian practices, criminalisation emerges as a mediating mechanism that allows surveillance to impede the rights of HRDs.

Regarding the first type of criminalisation, which refers to creating new laws (Koula 2026), I argue that this is evident when it comes to the state’s regulation of technology use. In the section on facial recognition, I touched upon the criminalisation of masks in protests compared to the use of masks on behalf of immigration agents (Guariglia and Schwartz 2025). This came in response to increasing doxxing towards ICE agents, and the use of technology such as videos to document human rights violations (The Glenn Beck Programme 2025). Criminalising the use of technology when utilised by human rights defenders is against the internationally protected freedom of expression that includes activities of observing, recording and protesting law enforcement activities (Human Rights Watch 2026). In his research on doxxing, Chauvin (2026) finds that the proposed law that criminalises doxxing is actually in violation of the First Amendment. This is because one of the main purposes of the First Amendment is that of ensuring democratic accountability and protecting speech (United States Constitution 1789). Therefore, the “Protecting Law Enforcement from Doxxing Act” was argued to create a power imbalance between the government and its citizens, becoming a risk for transparency and accountability (Chauvin 2026). Furthermore, it is in violation of the First Amendment as it criminalises people based on the content of their speech and restricts lawfully obtained information of public interest (Chauvin 2026). This is an attempt on behalf of the state to limit the use of technology by criminalising HRDs, while at the same time using technological tools themselves to surveil citizens.

The state justifies the use of surveillance technologies by using specific narratives that criminalise immigrants and those that support them. Previous research has found that the discourse surrounding surveillance, used by DHS to legitimate intrusive technologies, was

based on explanations of efficiency and homeland security (Young 2024). This is in line with Quadri et al (2025) conceptualisation of criminalisation charges used against HRDs. I find that similar narratives are employed by this administration. In the aforementioned USCI social media proposal, the official proposal document described the need for social media identifiers as “informing identity verification”, for “national security” and for “public safety screening”. They mention Executive Order 14161: “Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats” and claim that the collection of necessary information falls within the grounds of this order (The White House 2025). Furthermore, there is a large inconsistency between the narrative used in NGO reports compared to that used in governmental documents. This further highlights the criminalisation tactic on behalf of the state. For example, a report by Patel and Rupert (2025) of the Brennan Center for Justice identifies the targeting of HRDs opposing ICE as a “serious threat to free speech and privacy rights”. The state instead justifies these practices through labels such as “domestic terrorists”, while NGO reports identify the use of surveillance technology as a form of “retaliation or intimidation” (The White House 2025).

Finally, regarding the second type of criminalisation for HRDs as identified by Koula (2026), the theme of surveillance emerges as being intersected with existing laws in two main ways. Firstly, surveillance is effectively implemented through the use of subpoenas that allow the state to access data gathered by private companies and then effectively surveil HRDs (EFF v DHS and ICE 2026). Secondly, surveillance interacts with existing legal measures when the state relies on surveillance-derived information to apply legal instruments of deportation (Branum 2025). This was explored in depth in the viewpoint-based immigration section, which shows that the social media surveillance of immigrant HRDs allows ICE to flag dissident opinions and threaten non-citizens with deportation. No novel legal instrument was used here, its reach was simply expanded to include dissident speech as relayed by social media surveillance (The Department of Homeland Security, 2025). In both cases, the harm to HRDs is achieved through the use of ordinary law procedures, whose focus seems to shift toward a suppression of freedom of expression rather than defending the state from criminal activity. In fact, this, as well as the previous two tactics of criminalisation, affect the freedom of expression of human rights defenders by allowing surveillance to be incredibly consequential for their work and targeting HRDs because of the content of their speech (Patel and Rupert 2025).

6. Chilling Effect

One of the main ways in which surveillance can impede the freedom of expression of HRDs is through the *chilling effect*. This theme was analysed in the data, emerging as an important factor that can help explain in what way surveillance seems to affect the freedom of expression of HRDs. The chilling effect refers to behavioural phenomena regarding how people behave when faced with laws or reactions that prohibit and endanger their activities (Penney 2025). Usually, the chilling effect refers to self-censorship and deterrence from speaking and exercising rights. Penny (2025) argues that the chilling effect emerges in light of legal restrictions, fear of punishment, or privacy threats. All three of these conditionalities appear in the above data on surveillance technologies in terms of criminalisation, violation of privacy rights and repressive repercussions. This is part of an identified worldwide trend of documented chilling effects, as reported by the UN Special Rapporteur on freedom of peaceful assembly and association, where people avoid exercising their rights to escape surveillance and repercussions (UN General Assembly, Special Rapporteur Gina Romero 2025).

In social media surveillance, the chilling effect arises from complete access to online ideological information, and the retaliation that occurs when an individual is flagged for what they post (Human Rights Watch 2025). In the Department of Homeland Security (2025) Privacy Impact Assessment on the *Analytic Tools in Support of the Protective Mission* program, the government addresses concerns about the collection of information through social media (DHS 2025 para 11). In explanation of what opportunities individuals have to decline providing information, the response indicates abstention from posting material online or limiting access to post viewership as solutions. These descriptions can be interpreted as an anticipation of a chilling effect, with abstention promoted by the state as an adequate solution to protect one's rights.

More explicit references were made in response to the subpoenas sent to private companies, including Meta and Google, when EFF Deputy Legal Director Aaron Mackey stated, “The public deserves to know what laws the agencies believe give them the power to issue these *speech-chilling* subpoenas” (Electronic Frontier Foundation 2026 para.5).

In terms of immigrant Human Rights Defenders, faced with the legal consequence of deportation due to viewpoint-based immigration, other students claimed to be refraining from posting on social media any indication that could cause repercussions (Raphling 2025). Therefore, they seem to be deprived of their freedom of expression due to the chilling effect. In fact, in Chapter 6 of his book *Repression, Conformity and Power in the Digital Age*, Penny (2025) draws a link between chilling effects and the reduction of rights. He argues that the chilling effects caused by surveillance threaten the truth-bringing role that speech has in society. Lastly, Penny (2025) finds that the chilling effect disproportionately affects minorities and disadvantaged groups, which causes the entrenchment of unequal rights in democracies. Within immigration enforcement, human rights defenders are an emerging group targeted disproportionately by DA practices and thus affected by the chilling effect.

When it comes to facial recognition technologies, I found the chilling effect to be closely linked to the criminalisation of masks (Guariglia and Schwartz 2025). In fact, the arbitrary use of human rights to justify the use of masks by law enforcement is a contradiction when the same rights are being violated through the surveillance of human rights defenders. In NGO reports, the state is being accused of criminalising masks at protests (Guariglia and Schwartz 2025). EFF defines this attempt as a violation of one's right to privacy and describes the use of masks as a “legitimate surveillance self-defence practice”(Guariglia and Schwartz 2025). However, I find that the privacy violation represented by facial recognition technology when masks are prohibited is often mediated by the chilling effect that such surveillance can cause. Chilling effects on speech can impact the freedom of expression of a human rights defender, especially when wearing masks as protection from surveillance has retaliatory effects (Guariglia and Schwartz 2025). Furthermore, the easy accessibility of facial recognition technology, as seen above through Mobile Fortify, allows people to be identified and tracked without their consent, this creates a chilling effect which will limit their ability to exercise their freedom of expression (Trujillo M 2026).

7. Debates on AI

The increasing integration of artificial intelligence in immigration surveillance systems doesn't introduce a new method of harm for human rights defenders; it exacerbates existing patterns of discrimination (Molnar 2019). AI can endanger HRDs through the reinforcement of discrimination, bias and stereotyping, which can lead to increased vulnerability for HRDs

belonging to marginalised communities (Rawaqa 2025). The Special Rapporteur on racism, racial discrimination, xenophobia and related forms of intolerance, and his 2024 visit to the US, reported on surveillance and racial profiling on behalf of agencies such as ICE and CBP toward Black, Arab, Islamic, Indigenous and Latino/Hispanic communities (UN General Assembly, 2024). His report shows how surveillance usually leads to the targeting of the targeted groups without reasonable suspicion or warrants, but mainly based on racial profiling. The special rapporteur expresses concern regarding the use of AI in surveillance due to racial profiling risks, and welcomes Executive Order 14110: Safe, Secure and Trustworthy Development and Use of Artificial Intelligence. This report was published in 2024; in 2025, President Trump revoked Executive Order 14110, stating it: “hinders AI innovation” and creates “unnecessarily burdensome requirements for companies developing and deploying AI that would stifle private sector innovation and threaten American technological leadership” (The White House 2026 para. 2). This dismissal of Executive Order 14110 as a safeguard against the risk of AI in amplifying discriminatory mechanisms reproduces a pattern observed also in the analysis of spyware surveillance, where constraints to protect from the misuse of technological tools are easily reversed. This shows a volatility in these orders that are intended to protect people from Digital Authoritarianism, but were easily reversed by the current administration, positioning themselves as guidelines more than institutionally embedded safeguards. The narrative used to justify the reversal of the AI Executive Order is once again interpreted in light of nationalistic tendencies as well as with a focus on capitalism and private sector engagement (The White House 2026). The revocation of such an order, and the aforementioned evidence on AI technology in surveillance practices, provides evidence for a lack of protection and a biased targeting of minority groups.

Given the aforementioned shift toward viewpoint-based immigration, I find these findings particularly impactful for HRDs when racial profiling could be integrated with ideological screening. Rawaqa (2025) finds that minority human rights defenders play an important role in the advancement of social justice in democracies, but they also face disproportionate discriminatory risks. In fact, when it comes to facial recognition technology, people in certain demographic groups, such as women, black people, or other ethnic minorities, are at risk of being misidentified given the technology’s biases and failures (Electronic Frontier Foundation 2023). Nowadays, private companies, including Clearview AI and MorphoTrust, sell face recognition products to law enforcement at a lower cost than internal development. Especially if automated and run by artificial intelligence, the systems are prone to errors.

Furthermore, the data collected by facial recognition technologies relies on the biometric classification of such data, which in turn relies on inferences and predictions of people's characteristics, which can be wrong and discriminatory (Trujillo 2026). Previous research on US surveillance technology has found facial recognition technology to be incorporated with AI systems, and findings related that the inaccuracy of the AI systems often led to gender and racial biases, especially against women and minorities (Feldstein 2019).

B. Data Collection

1. Background Literature

Data has now become something that law enforcement can purchase from privately-managed intelligence databases (Electronic Frontier Foundation 2023). Overall, the more data a government collects, the greater the risk of a data breach, including leaks and misuses. While the methods of data collection are often conceptualised as a part of surveillance techniques, the present thesis has decided to separate the two categories as was done by Yabanci (2024), due to the preventative nature and mass scale of data collection. In fact, the above section on surveillance mostly referred to instances in which specific groups or individual HRDs are directly targeted. Instead, technologies used for this section refer to mass data collection that targets large portions of the population and was found to also target HRDs.

Biometric data collection often involves private companies that sell collected data to governments, and this data is then used by the state to generate policies, decisions and narratives regarding groups that are considered to be threats (Yabanci 2024). Methods of data collection on behalf of these companies include Automated License Plate Readers, which are AI-powered technology that can capture information from a vehicle's license plate (Electronic Frontier Foundation 2023). The data accessible to law enforcement has increasingly become part of centralised, large databases that allow every part of the government to access any level of personal information, including patterns of movement and behaviour (McGregor and Molnar 2023). As part of the data analysis, other themes emerged when investigating data collection. In particular, private companies seem to have an important role as intermediaries when it comes to data access for governments (Cohn and Gedlu 2026). Furthermore, ad-based data collection was also identified as a relevant practice which further allows private companies and hence, governments, to access personal information from individuals

(Patel and Rupert, 2025; Christl al, 2026). These practices were found to violate especially the right to privacy of Human Rights Defenders who, affected by these systems of mass data collection, cannot retain anonymity online and offline.

2. A Centralised Database

The US is expanding its access to the data of all the people in its territory. In his second term, President Trump's administration has created the Department of Government Efficiency (DOGE), which aims to centralise the collection of personal data, accessing data from various governmental agencies (Human Rights Watch 2025, Guariglia and Trujillo 2025). This is in line with the governmental objective of having access to all types of data, with DHS currently seeking to access data from every category of government (Wang et al 2022). Fourth Amendment regulations and case law have failed to keep up with this extensive data proliferation (Ayoub and Goitein 2024). Human Rights Watch (2025) labels this as an "opportunity for mass privacy violations". In fact, a risk of centralising government information is that of overlooking the protections that were in place to maintain the privacy of individuals and ensure that the information is shared with agencies, such as ICE and CBP, that could potentially abuse it (Guariglia and Trujillo 2025). Abuse of data is linked to using data for purposes other than those for which it has been collected. I argue this is another instance of lack of government transparency, in which the state attempts to use data that has been collected without specifying its intention. However, when analysing the official governmental Executive Order No 14243 on the matter of database centralisation, the President explains that the objective of the administration is that of "removing unnecessary barriers" when accessing data and "promoting inter-agency data sharing" (The White House 2025). The conceptualisation of privacy limits as "unnecessary barriers" can be interpreted as a further reinforcement of the government's view of human rights as policies that come in the way of national security.

2.1 Private Companies

The creation of large databases is rendered even more risky for the rights of HRDs when coupled with access to private companies' databases. Accordingly, EFF reports that the Trump administration has attempted to reach its objective of centralised data collection also through the use of Palantir; ICE has been able to access data from various databases, allowing

it to centralise data (Cohn and Gedlu 2026). The risk is even greater when considering the role Palantir has in direct surveillance, such as by providing tools for facial recognition. EFF found Palantir to be used in connection with surveillance tools such as facial recognition toward people recording law enforcement, and then including the data in a larger database, which ICE has access to at any time (Cohn and Gedlu 2026). This reiterates the interconnectedness between surveillance and data collection, but it also shows the various facets of services a private company can offer to the state for it to engage in a combination of DA practices. Sharma and Adler (2026) argue that the April 2025 contract with Palantir allows ICE to create an automated immigration enforcement built between interconnected databases, eroding fundamental rights such as the Fourth Amendment protection.

3. Advertisement-based data collection

Ad-based surveillance technologies collect data on a person every time an app or website has ads, which are accessed by software to collect data such as a person's behaviour, characteristics and geolocation (Christl et al, 2026). The implications of this are important, especially given the systematic misuse of data that is purchased by governmental agencies and used for surveillance. Webloc, a geolocation system that monitors people based on the data purchased from apps and digital advertising, was found to supply ICE (Christl al, 2026, Patel and Rupert, 2025). Webloc is part of Penlink, a private social media software, and it collects data by purchasing it from apps and advertisements. While the Supreme Court has held that warrants are required to obtain cellphone location data that extends over a period of time, the position of the DHS and its agencies remains that this judgement does not apply if the data is obtained through private purchase (Patel and Rupert, 2025). This highlights the fundamental role that private companies have in the implementation of DA practices, allowing the state to bypass its own democratic laws.

Another preoccupying factor is the amount of data now available to these enforcement agencies (Christl et al 2026). Webloc can now find any information regarding an individual, including patterns around their lives and relationships. However, in the analysis of a document sent by Penlik in response to Citizen Lab's report on their software Webloc, the company states that the data was erroneous and that the geolocation does not include the gathering of personal information such as gender, interests, etc. Furthermore, they explain the need for the software as a commitment to aid law enforcement in searching and identifying

threats, in particular mentioning “terror threats”, “drug trafficking”, locating “kidnapped children” and “human trafficking” threats (Deibert 2026 at The Citizen Lab para 4). These themes are similar to the ones that emerge in official and non-official state communications when DA practices are justified. This adds a layer of interpretation to the role of private companies as more than just entities of collaboration with the government but actors that share in their same narrative tactics. Despite this, Webloc was reportedly used by law enforcement for the monitoring of people present at protests, and it has been used to do so before (Christl et al 2026). In 2020, it was found that these ad-based technologies were being used to collect information on activists, protesters and journalists from the Black Lives Matter movement, indicating similar practices are in place for HRDs in the immigration field.

4. Automated License Plate Readers

The DA practice of data collection is often enabled through the use of Automated License Plate Readers (Talla 2019). This theme emerges in relation to the tracking, storing and sharing of data within the immigration enforcement field. ALPRs are AI-powered cameras that analyse the images of vehicles and store information regarding location, date, time, and car details, and they act regardless of whether the target is suspected to have committed a crime (DeFlock 2026). Stanley (2025), through an ACLU report, identifies that the US Border Patrol, as part of the Customs and Border Protection (CBP), has installed a system of ALPR along borders which, he argues, carry out surveillance of all Americans’ movement. Little is known by NGOs about what is actually considered suspicious movement. The officers stop people under a supposed legal violation and subsequently question and search them.

ALPR cameras are installed in a location, often disguised as ordinary objects, and if many cameras are placed along specific routes, then enforcement agencies can have access to real-time tracking information of a vehicle (Electronic Frontier Foundation 2023). Their placement often coincides with sensitive locations such as immigration clinics or areas where protests take place. Furthermore, mobile ALPR cameras can be attached to law enforcement vehicles. The Data for Justice Project of ACLU Massachusetts, whose intention is to inform activists, advocates, journalists and others about governmental use of technology, reveals that nationwide departments can track drivers without a “warrant, probable cause or even reasonable suspicion of wrongdoing” (Epstein 2025). What this means for the rights of HRDs

is twofold: firstly, there is a strong argument for the violation of their privacy rights under the Fourth Amendment and under Article 17 of the ICCPR (UN General Assembly 1966) due to ALPRs' ability to reconstruct individuals' movements, access location information and overall give law enforcement access to information that would otherwise not be available. Furthermore, large collections of data are often linked to prolonged tracking, which can reveal information about a person's habits and behaviour. Stollmack (2025), in her research on ALPRs in the US, identifies that they impact Fourth Amendment rights of privacy given that license plate readers are often in contradiction to the reasonable and proportional aspect of searches and seizures. I believe this is the case, especially when ALPRs are used outside of their purpose of tracking criminals, but gather information about the life of anyone, including those who express dissent from the government. Furthermore, though not a central focus of her research, Stollmack (2025) argues the potential impact of ALPRs on First Amendment rights, including freedom of expression, due to the invasiveness of the technology and the potential chilling effects it can have on people.

ICE is increasingly gaining access to large databases in US cities. The NGO STOP reports that the NYPD's Domain Awareness system includes data on city-wide license plates that are captured all over by license plate readers (Surveillance Technology Oversight Project 2026). The fact that ICE has access to such a database raises concerns over the arbitrary use of such information. In a court document, *Schmidt and Arrington v Norfolk* (2026) on behalf of ACLU, the NGO argues that large access to license plate data poses an even greater danger for vulnerable groups such as "people attending protests". In fact, Keener, Finn and Baird (2025) conducted a descriptive statistical analysis on the locations of ALPRs in the US and found that they are mostly placed in Black and high-poverty neighbourhoods, arguing that how the data is stored and shared has implications for marginalised communities. This could include the previously identified category of immigrant HRDs, HRDs that are part of marginalised communities, or HRDs working with immigrants in these communities. Keener, Finn and Baird (2025) claim the state lacks transparency in disclosing information on the location of ALPRs, making the possible biased targeting of these technologies hidden from public scrutiny.

4.1 Private Companies

Once again, private companies are interlocked with governmental DA practices, allowing states to access larger and more detailed amounts of databases. The database where ALPR information is stored is mostly controlled by private companies. Companies mentioned in reports are: Flock, Vigilant Solutions (Motorola and Rekor. In particular, Vigilant Solutions was found to have a direct relationship with ICE, whose agents can access the nationwide database of the company (Stanley 2025). If the frameworks for protection in private companies are weak, allowing ICE to access databases despite potential restrictions (Finn and Baird 2025), the effects on rights can be negatively impactful.

Flock Safety is one of the most used companies for ALPRs (DeFlock 2026, Stanley 2025, ACLU 2025, Pinsoff 2026). The Data for Justice Project finds it has deployed almost 90000 cameras nationwide as of July 2025, which can automatically capture and record license plates, time stamps and location (Epstein 2025). The report identifies that one of the main issues of Flock is their data sharing process. The state departments that contract Flock can then share the collected data to the nationwide Flock network, an exchange of data that is directly facilitated by the company's system. Flock has asserted it no longer cooperates with CBP directly, but through the data sharing system, the report indicates how local police are aiding ICE agents with searches (Schmidt and Arrington v Norfolk 2026, Epstein 2025). Through a research of Flock audit logs, it can be seen that law enforcement targets human rights defenders as well (Maass and Alajaji 2025). This is done by targeting activist groups, which can create the risk that individuals curtail their freedom of expression, protest and association (Schmidt and Arrington v Norfolk 2026). In fact, the Electronic Frontier Foundation found that police departments use Flock Safety's ALPR system to investigate protests, mentioning people who participated in the February 2025 protest against deportation raids, and participants of protests at Tulsa City Hall in support of the activist Mahmoud Khali (Maass and Alajaji 2025). The NGO argues that a warrant should be required for access to such data, but the Flock system has simplified the immigration enforcement agents' access to any information.

This shows how the state's easy access to a private company, with such a developed and nationwide system used under the pretence of national security, inevitably targets human rights defenders in the immigration field by allowing the government to flag dissent, breach their privacy rights, suppress their freedom of expression and consequently create chilling effects (Maass and Alajaji 2025, Epstein 2025, Stanley 2025). To exemplify this, the EFF's

research of agencies that logged searches through Flock Safety found that the Lubbock Police Department in Texas ran searches for license plates on March 15th corresponding to a rally organised for raising awareness on the mental health impact of immigration policies (Maass and Alajaji 2025). Findings reported that “the searches hit 5,966 networks, with the logged reason 'protest veh [vehicle].’”. As mentioned above, police departments have been found to aid ICE in conducting Flock searches given the apparent discontinuity of the agency’s contract with the company; hence, it is possible to infer that searches regarding human rights defenders in the immigration field are often relayed back to immigration enforcement institutions. This is confirmed by EFF’s findings that the US Border Patrol has “made extensive use of Flock Safety's system for immigration enforcement, but also to target those who object to its tactics”.

C. Channelling

1. Background Literature

As discussed in the literature review, channelling refers to the practices of manipulating information in a way to exert control over narratives and influence public opinion (Earl et al. 2022, Feldstein 2021). Earl et al. (2022) identify two main types of channelling: overt and covert. Overt channelling refers to controlling a public forum of expression and complaints that the government uses to seemingly display openness while actually being able to: control how complaints and opinions evolve, shape the narratives around these complaints and use the same platforms to mobilise governmental support. While it seems counter-intuitive, allowing citizens to have an open space for governmental contestation was found to be productive because it facilitates public rather than private communication, which is easier to monitor for the state, and it allows the state to be aware of dissident opinions (Chen and Xu 2017).

The present findings of this thesis did not rely on sufficient data on overt channelling as a DA practice that targets HRDs. There were cases in which public governmental statements or proposals were open to discussion, for example, USCIS’s proposal on social media surveillance, which was uploaded on a forum open to suggestions and comments from civil society (The Department of Homeland Security, 2025). There were also instances in which the government openly responded to NGO reports on DA practices in order to counter their

accusations (House of Representatives, 2026). However, not only were these findings rare compared to covert channelling practices, but I argue they differ from the literature's conceptualisation of overt channelling. Firstly, they do not mention or involve human rights defenders individually in any openly public discourse space, which is consistent with the categorisation of HRDs as “terrorists” and “national security threats” that should not be given a platform to express their opinions. Secondly, the recent two years have been characterised by under-funding for NGOs (UN General Assembly 2025); there seems to be a shift of importance away from civil societies, hence already making their contributions less relevant when it comes to public discourse.

Instead, covert channelling involves less detectable methods of control in the online space and narrative (Earl 2022). These can include information channelling, which refers to directing and influencing attention through the control and spread of online information. Information channelling is less about controlling access and more about changing the beliefs and behaviours of the audience through disinformation (Earl et al 2022). The state is often involved with these covert techniques of social manipulation, as it can allow them to instigate and spread anti-opposition narratives while refraining from overt or physical suppression (Feldstein 2021). Woolley & Howard (2017) find democracies to be particularly engaged in social media as a form of information manipulation. Their study found fake and automated social media accounts to be characteristic of democracies, where political figures rent large network accounts for their campaigning. However, this rise of disinformation and hate speech is a threat to democratic processes due to its influence on rights, especially freedom of expression (G'Sell 2025, Maerz 2025).

The theme of social media channelling was found throughout the data to affect the freedom of expression of Human Rights Defenders. Furthermore, **criminalisation** was inductively identified as a theme, due to its relevance for the perpetuation of harmful narratives that justified violations of freedom of expression and assembly.

2. Social Media Covert Channelling

Violence has escalated in immigration enforcement operations, with some people being shot and five people having been killed during an immigration enforcement operation (American Immigration Council 2026). ICE agents have also been found to spray chemical

crowd-control substances at people observing or reporting immigration violations. These instances have been coupled with a lack of criminal justice and accountability, due to the changes that the administration has made in this second term by restricting the Office of Civil Rights and Civil Liberties in March 2025, which was mostly occupied with investigating the excessive use-of-force accusations (American Immigration Council 2026). I argue that this violence, in a context of increasing lack of accountability and legal system accessibility for people to turn to in the face of ICE violations against human rights defenders, has rendered it easier for the state to control the online narrative.

Disinformation spread on social media was a prevalent form of channelling in the data, and it constitutes a DA practice that impedes the rights of Human Rights Defenders (Earl et al 2022). This has emerged especially in response to unlawful use of force by ICE agents. The lawsuit *Chicago Headline Club et al. v Noem et al.* (2025) regards the case of a physically aggressive response at a non-violent protest where people were participating to raise awareness of the inhumane conditions at ICE detainment Centers in 2025 in Chicago. The intense use of force on these protesters was found to be a violation of their freedom of expression and assembly as protected by international frameworks as well as the US First Amendment to the Constitution. Methods of force included firing pepper balls, rubber bullets, tear gas and flashbang grenades into the crowd without warning, arresting protesters not engaged in any violent actions and using physical force to grab, push or kneel on people. In the official document of Judge Ellis' opinion and order, the actions of the protesters were found to be peaceful, nonviolent and protected under their First Amendment right (*Chicago Headline Club v. Noem* 2025). However, in the analysis of the order, themes were identified regarding the propagation of disinformation surrounding the events through social media. The order mentions interviews that were then shared to the public through YouTube and other online platforms, in which the narratives about these anti-ICE protesters were spread. In one CNN interview, ICE agent Bovino confirms the statement made by DHS that "cartels and the Latin Kings gang have placed bounties to incentivise violence against federal personnel" (*Chicago Headline Club v. Noem* 2025 pp 73). In another interview, President Trump describes protesters at the upcoming military parade on the 14th of June 2025 as people who hate America. Both of these are examples of narrative dissemination that ends up affecting human rights defenders who want to practice free speech and document human rights violations. I interpret the comparison of protesters to cartels as a further reiteration of the attempt to connect government dissident groups to groups already categorised as terrorists.

NGOs, such as the ACLU Illinois that reported on the case, claim these were “many lies they told in attempting to justify their violence” (ACLU 2026 para 7).

Judge Ellis also reports Trump's comment on Truth Social where he stated that “MASKS WILL NOT BE ALLOWED to be worn at protests. What do these people have to hide, and why???” This relates to the above section on surveillance and facial recognition technology, which is used against human rights defenders for their identification and subsequent data tracking (Chicago Headline Club v. Noem 2025 pp 37). This finding highlights how the dissemination of narratives by the state through social media reinforces the implementation of surveillance technologies, providing evidence for the state’s use of combined DA practices. Furthermore, from a position of authority, framing protesters and their right to anonymity as having something to hide reiterates an intention of expanding the categories of threat to include human rights defenders who go against immigration. I argue that these online narratives, as part of covert channelling strategies, are affecting the rights of human rights defenders through justification of physical violence against them, promotion of the suppression of their freedom of speech, and through the use of criminalisation tactics.

Furthermore, in a statement reported by the court order, Secretary Noem mentioned that violence against ICE officers by protesters is anything that can threaten their safety, going on to list examples such as videotaping, reporting on their locations, and other more physically violent actions (Chicago Headline Club v. Noem 202, p. 39). This can be interpreted as a restriction of what is considered allowed in the actions of human rights defenders, especially when it comes to limiting technological tools (messages, online warnings, videotaping violations) available to them. Thus, the tools through which they can do their work are being stigmatised, and they are at times faced with violent consequences (Human Rights Watch 2026). In fact, in an analysis by Human Rights Watch (2026), researchers report on the social media responses to the killing of Renee Good by an ICE officer; they find that the DHS posted on X how Good’s actions were a form of domestic terrorism, a statement which was found inconsistent with the video footage that reported the incident.

This particular DA practice is damaging to immigrant human rights defenders, who are further affected by these online narratives as they are associated with threats of deportation (Raphling 2025). An expert report on Mahmoud Khalil by Human Rights Watch indicates that the administration’s justifications for the arrest and possible deportation of Khalil, as well

as other students such as Yunseo Chung and Rümeyza Öztürk, were illegitimate and in violation of international human rights law (Raphling 2025). The report also transcribes comments made by President Trump on the White House X account, calling the protests: “pro-jihadist protests” (Raphling 2025 para 9), directly mentioning Mahmoud and announcing a campaign “against terrorist sympathisers” (Raphling 2025 para 9), threatening that this was the first arrest of many. Furthermore, the fact that a lot of the social media channelling comes directly from President Trump himself, or other leaders of the government, is important in understanding the influence of these discussions. In an analysis on social media content regarding Migration in the US, Francavilla et al (2025) find that it is often linked to political figures that more effectively influence public opinion due to their position. This further highlights how social media channelling as a DA practice effectively attempts to change and influence public opinion to maintain control (Earl et al 2022).

3. Criminalisation through Channelling Practices

Criminalisation and security narratives are main themes disseminated by the government, and such tactics are used by NGOs to explain the direct effect that these practices can have on HRD rights. However, this section will now delve deeper into the analysis of these criminalisation tactics as part of the wider online channelling technique of the government used to shape public opinion and disseminate information. I find that the aforementioned narratives of anti-Americanism (Raphling 2025) and direct correlations to terrorists or drug cartels (Deibert 2026, Chicago Headline Club v. Noem 2025) are a criminalisation tactic to discredit and accuse HRDs, as identified by Quadri et al (2025). This was observed in the social media examples above, but it can also be seen in official governmental statements. For example, in a Memorandum for the Secretary of State (September 2025), President Donald Trump disputes the increase of “attacks on US Immigration and Customs Enforcement” since January 2025, denouncing the use of social media for the doxing of ICE agents in Los Angeles (Secretary of Homeland Security 2025 para 4). Doxing refers to the disclosure of information such as addresses and location to the public, and he labels this as an attempt to “obstruct the operations of the Federal Government” (Secretary of Homeland Security 2025 para 4) and to “aid and abet criminal activity that the Federal Government is lawfully pursuing” (Secretary of Homeland Security 2025 para 4). Here the theme of criminalisation emerges in two distinct manners. Firstly, the discordance between the NGO interpretation of the facts and that of the government indicates a manipulation of narrative controlled by labels

of national security and anti-government or anti-American behaviour. Secondly, it also relates to the criminalisation of human rights activists as a consequence of the criminalisation of immigration. Koula (2024) identifies how criminalised conduct can lead to the criminalisation of defenders. They give the example of Poland's law on criminalising abortion, which then caused the potential criminalisation of those defenders who speak out against such law. These narratives are exacerbated and spread through the use of digital technologies. The United States also goes further by directly linking migrant rights defenders to the migrant crisis in the country; they reinforce this criminalisation tactic.

D. Funding

The present research finds that the situation HRDs find themselves in within the digitalisation of US immigration enforcement is exacerbated by the global trend of funding cuts for human rights (UN General Assembly 2026, Mary Lawlor). The Special Rapporteur on human rights defenders, Mary Lawlor, published a report in April 2026, indicating that the situation for human rights defenders has become precarious in the recent couple of years. She states that the international system, supposed to protect human rights, has been questioned by HRDs who are finding themselves facing double standards in states' approaches to human rights. She particularly mentioned a trend of funding cuts, most significantly led by the US, as obstacles that leave human rights defenders feeling less safe and less able to conduct their work. Consequences of funding cuts are many, but analysing the report in light of the present findings on HRDs in immigration enforcement, the most impactful consequences are: reduced capacity to provide legal aid and reduced capacity for monitoring and documentation (UN General Assembly 2026, Mary Lawlor p. 7).

A lack of funding also causes human rights defenders to face increasing digital attacks (Barrueto and Al-Maskati 2025). The under-funding on behalf of the Trump administration leaves HRDs with fewer resources and increasingly exposed to cybersecurity threats. In fact, in a report on HRDs, the NGO Access Now found that many of the cybersecurity organisations that helped defenders protect themselves and their work from digital threats were struggling due to USAID and other international funding cuts after the second term of the Trump administration (Barrueto and Al-Maskati 2025).

I find that funding cuts are also related to the increasing presence of private companies as actors that facilitate governmental implementation of DA practices. In the aforementioned document to OHCHR on Protection of Human Rights Defenders in the digital age, CDT also identifies the role of private social media companies in increasing the risks to HRDs (Seck et al. 2026, p.4). For example, Meta's decision to discontinue end-to-end encryption as of May 2026 for Instagram messages was identified as a breach of privacy rights. While not necessarily acting on behalf of the government, the harm to the rights of HRD rights was seen as a consequence of a "global shift away from funding civil society and toward targeting it" (Seck et al. 2026 p.4), which has "hampered its capacity to support and protect HRDs" (Seck et al. 2026 p.4) affecting the possibility of civil societies to work closely with private companies. In the 2025/2026 Global Report by Front Line Defenders (2026), the NGO recognised that direct dialogue between companies providing surveillance systems and human rights organisations is missing. This causes companies to have a limited understanding of their impact on communities of HRDs, and appropriate mitigation measures are not put into place. I argue that this can be related to the lack of funding on behalf of the state as well as the increased use of legal measures by the states to have private companies comply with them.

Furthermore, funding is important when the state invests in more technological devices that can ultimately be used in DA practices. When it comes to surveillance technologies, they are often funded by state grants such as the Homeland Security Grant Program, the Urban Areas Security Initiative and the Department of Justice program Byrne JAG (Lipton and Hamid 2026). These programs consist of reimbursements from the government for reasons cited as homeland security, to invest in equipment and software needed for surveillance (Lipton and Hamid 2026 para 12). Even private companies have adapted to such funding by selling their products as ideal for government-funded services. This is in contrast to the global trend, largely led by the US, of decreasing funding for human rights and civil society (UN General Assembly 2026 para.1), while enforcement institutions are being granted even more funds under the justification of national security (Swensen 2026). On June 10th 2026, US President Donald Trump approved the Secure America Act, which included \$70 billion for immigration enforcement (Swensen 2026). Therefore, while access to technological tools is increasing, so are the Digital Authoritarian practices implemented by the state.

Funding greatly impacts many of the themes analysed above, including the themes on AI development and criminalisation of HRDs (Gina Romero UN Assembly 2025). The Special Rapporteur on freedom of peaceful assembly and association reports on the effect that funding interruption can have on depowering activists and hence limiting their ability to counteract criminalisation narratives. Furthermore, it also limits their ability to participate in debates on new technologies, unable to limit the human rights impact of artificial intelligence and the chilling effects that technology can have on fundamental freedoms. The Special Rapporteur signals the speed with which funding cuts were implemented and finds that states lacked transparency and consultations (Gina Romero UN Assembly 2025 p.11).

E. Summary of Themes

Table 2

The following table indicates the main themes analysed in the data in this chapter, separated by differentiating between categories of HRDs targeted.

Type of HRD	Surveillance	Channelling	Biometric Data Collection	Mediating Mechanisms
Immigrant HRDs	Social Media Surveillance Facial Recognition technology and AI	Social Media Channelling	Centralised Database	Criminalisation: Deportation and Arrest Viewpoint-based immigration Chilling Effect Funding
HRDs engaging in digital tools	Social Media Surveillance Facial Recognition Technology Spyware	Social Media Channelling	Ad-based data collection	Private Companies Chilling effect Criminalisation: creating new laws Criminalisation: using existing laws (warrants, subpoenas) Criminalising charges (such as terrorism,

				national security) Chilling effect Funding
HRDs offline	Facial Recognition Technology	Social media Channelling	ALPRs	Chilling Effect Criminalising charges (such as terrorism, national security) Criminalisation: Arrests Private Companies Funding

IV. Discussion

The present thesis used a deductive-inductive thematic analysis to answer the research question: *How do Digital Authoritarian Practices in US Immigration Enforcement impede the rights of Human Rights Defenders?* My main argument was that Digital Authoritarianism in US immigration enforcement shows how democracies are using DA practices to adversely impact the rights of Human Rights Defenders, and that this can aid in explaining the increasing blur between democracies and authoritarian governments.

The research sought to investigate how DA practices that are used in immigration enforcement are targeting HRDs in ways that undermine their human rights. The focus on Human Rights Defenders as a category targeted by Digital Authoritarianism helps expand the understanding of the concept and investigate its effects in practice. Furthermore, the research aimed to investigate how Digital Authoritarianism explains the blurring between democracies and authoritarian governments. The focus on democracies instead of authoritarian regimes addresses the gap in the literature when it comes to focusing on Digital Authoritarianism mainly as a part of authoritarian governments (Maerz 2025), and helps contribute to the conceptualisation of how DA is expressed and implemented in democracies.

Overall, since 2025, the Trump administration has increased funding and resources dedicated to enhancing the state's immigration system and its access to digital technologies (American Immigration Council 2026). This has led to a prevalent use of technology for repressive means. I find that these techniques can be classified as Digital Authoritarianism practices, defined as such by the literature on the concept, due to the authoritarian nature of their functioning, the state as an actor in their implementation, and their corrosive effects on human rights (Pearson et al 2024). Focusing on human rights defenders allowed the research to analyse the impact of DA practices on groups of individuals that are vital to the functioning of a democracy. The findings in the previous chapter reported that Digital Authoritarian practices in US immigration enforcement are directly targeting Human Rights Defenders and violating their rights to freedom of expression, their rights to privacy, and rights to freedom of association or assembly.

I. The Blurring of Democracies

The US case illustrates not only that democracies can engage in DA practices, but also that a formal democratic categorisation is not a safeguard against authoritarian practices (Michaelsen and Glasius 2018). In fact, assessed against the nature of digital authoritarian practices as authoritarian regardless of the institutional classification of the government, immigration enforcement is increasingly engaging in practices that impact the rights of Human Rights Defenders and contribute to the blurring of democratic pillars. In democracies, Digital Authoritarianism can be identified through practices that deploy technology in ways that maintain governmental control (Pearson et al 2024). The present research does not attempt to talk about democratic decline, as that refers to a larger body of literature that uses various factors to evidence a clear decline in a country's democracy (Platner 2015). Instead, remaining within the literature on Digital Authoritarianism, it aims to show how the targeting of Human Rights Defenders through DA practices can create complications for democracies, and how Digital Authoritarianism can provide a perspective on the blurring between democracies and authoritarian governments through the misuse of technology.

1. Freedom of Expression

Immigration enforcement is being used in the US more than to control illegal immigration, but as a mechanism for attack on the democratic, constitutional government (American

Immigration Council, 2025 para.9). In the data analysis chapter, the present thesis found evidence for the use of DA practices on behalf of the state to infringe on rights such as the freedom of expression, freedom of association and right to privacy of Human Rights Defenders. As stated by Maerz (2025), this infringement on civil liberties is in itself a potential harm to a democracy. This is particularly evident through the use of Digital Authoritarian practices in impeding the freedom of expression of human rights defenders. As discussed in the literature review, Huq and Ginsburg (2018) developed a framework of analysis for constitutional regression in US democracy, with constitutional regression referring to an incremental decay in three components of democracy: competitive elections, liberal rights to speech and association, and administrative rule of law. With a focus on the pillar of liberal rights to speech and association, the effect of Digital Authoritarianism on the rights of HRDs can contribute to a wider analysis of constitutional regression of the United States. In fact, findings in the data analysis revealed that freedom of expression was one of the main rights impeded by the use of the DA practice: Surveillance (see pages 31- 49), Channelling (see pages 56-60) and data collection (see pages 49 - 55). Freedom of expression was restricted due to mediating factors such as viewpoint-based immigration (see pages 34-35), chilling effects (see pages 36-37) and criminalisation tactics (see pages 42-45 and 60). These factors are discussed below in light of their contribution to the understanding of democratic erosion.

1.1 Viewpoint-based immigration

Viewpoint-based immigration provides an insight into the blurring of the democratic and authoritarian boundary as it represents an aspect of immigration enforcement that impacts freedom of expression, while still being deployed within legal, official means. In fact, the erosion of democracy comes from the effect on First Amendment and International freedom of expression rights, rather than illegal measures of implementation, as seen by the USCIS proposal officially implemented in immigration despite concerns about impediments to freedom of speech (American Immigration Council 2025). The state is promoting the idea that social media screening executive orders are necessary for national security to protect the country and the agents of immigration enforcement from threats (The Department of Homeland Security, 2025). Particularly targeted by surveillance at immigration checkpoints are immigrant human rights defenders who are facing a system based on ideological screening, where their work can potentially harm their immigration status (Branum, 2025).

The fact that the freedom of expression of HRDs is affected by these actions can be interpreted as an expansion of the concept of “threat” to include even those who speak against human rights violations with views not accepted by the government. This is in support of the literature on digital repression in democracies, which states that perceived group threat is an important reason for a democratic state to engage in repression (Earl 2022, Pearson et al 2025). This is especially because digital authoritarianism offers advantages for democracies to deal with threats through mechanisms other than coercive methods (Feldstein 2021). The fact that the data analysis findings show HRDs being included in this perceived threat can represent a dangerous precedent in which freedom of expression passes to the background, and in practice the government is protected by their orders, proposals and justifications of national security. Furthermore, the findings on viewpoint-based immigration as targeting immigrant HRDs are in line with Rawaqa’s (2025) identification of minority HRDs as being at heightened risk of targeting by the government. This is damaging to the functioning of a democracy given that their work is essential for effective democratic governance due to their advancement of social justice.

1.2 Chilling Effects

I argue that the chilling effect is not only a consequence of DA practices anymore, but has become a direct mechanism for the state to impede the rights of HRDs, specifically freedom of expression. While direct censorship of online spaces would be an outright and public authoritarian move (G’Sell, 2025), in fact no evidence was found for it in the data analysis; the use of DA practices to endorse self-censorship (Department of Homeland Security, 2025 para.11) represents a more effective way for democracies to control dissent. For HRDs, the chilling effect is a functional impairment of their work given the fact that their capacity to document, report and organise depends on digital expression (Hankey and Clunaigh, 2013). Penny (2025) connects self-censorship to the erosion of participatory deliberation in democracies, stating that if people are chilled from freely expressing themselves, this goes on to impact the democratic nature of citizen participation. The present findings coincided with this, through the perspective of DA practices that seem to ensure the chilling effect occurs in order to stifle citizen participation.

Furthermore, the chilling effect explains how violations of privacy rights can actually lead to violations of freedom of expression and assembly. As stated by (Simoncini and Longo 2026),

technology is bringing about new ways for fundamental rights to interact. In fact, the *chilling effect* was often observed in correlation with breaches of privacy rights caused by facial recognition surveillance (Guariglia and Schwartz 2025), social media surveillance (Raphling 2025) and legal measures such as subpoenas used to access data (Electronic Frontier Foundation 2026). The breaches of privacy affect freedom of expression in their promotion of self-censoring techniques, with individuals afraid of being surveilled and of their privacy being breached, and thus engaging in self-censorship out of fear. This is in line with the findings by Kitchin (2020), who correlates surveillance and perceived surveillance as likely to cause chilling effects on speech and democracy, due to fear of being punished or targeted.

Overall, I find that chilling effects created by DA practices in US immigration enforcement are posing a risk to US democratic governance because human rights defenders are redefining their open speech, actions and beliefs to avoid surveillance and its consequences. In a digital world where a lot of advocacy is done online, citizens in high surveillance states have been less likely to use the internet to facilitate anti-governmental action (Stoycheff et al 2018). The findings of this thesis provide similar results, with human rights defenders avoiding the internet and social media for advocacy. However, there are still many instances of HRDs engaging in filming video footage of ICE raid violations, despite legal and physical consequences (Human Rights Watch 2026). In the long term, this could lead to a possibility that HRDs will avoid video documentation if the risks to their rights become too high, and the legal protective measures of democracy erode too much. This interpretation is in line with Penny's (2025) view that the more widespread the chilling effect is in a society, the more people become compliant, and the more those in power become harsh in their repression.

1.3 Criminalisation

Within the immigration field, Human Rights Defenders are included in the categorisation of perceived group threat, which has implications for the politicisation of their work. The work of human rights defenders is supposed to be vital for democracies due to their focus on upholding universal human rights (Rawaq 2025), however, the data analysis chapter shows that within the immigration field, HRDs are increasingly treated as political threats targeted with repercussions. I find that criminalisation of HRDs is a threat to democratic functioning due to its ability to restrict freedom of expression. Creating new laws such as the *Protecting Law Enforcement from Doxxing Act* (Chauvin 2026), or criminalising masks at ICE protests

(Guariglia and Schwartz, 2025), indicates a shift toward new laws that in itself threaten the freedom of expression of HRDs due to their targeting of people engaged in free speech as protected by the First Amendment (United States Constitution, 1789) and International Frameworks such as the ICCPR (UN General Assembly 1966) and the Declaration on Human Rights Defenders (UN General Assembly 1998).

In the literature on Digital Authoritarianism and Democracies, narratives of national security are often viewed as motivations for democracies to engage in practices with authoritarian tendencies (G'Sell 2025, Maerz 2025). I argue that the creation of an accusatory narrative surrounding immigrants and those who defend them is not merely a justification but an active tactic of criminalisation. Targeting freedom of expression due to national security and anti-terrorism reasons is not only a justification on behalf of the government for the implementation of surveillance and data collection technologies, but it becomes a mode through which the state wants to maintain control and influence public opinion (Quadri et al 2025). This is particularly visible through channelling, the DA practice of manipulating and controlling online information to limit dissenting behaviour (Earl et al 2022). As seen in the data analysis, the state used social media to spread information about immigrants and those who were engaged in protecting their rights (seepages 57-59). Maerz (2025) finds disinformation spread online to be closely linked to restriction of reliable information, which is a vital democratic component to create the environment for an engaged society. Furthermore, the data analysis found that the social media-channelling tactic reported a lot of references to national security and threat narratives, which, as Bartels (2020) finds, can be increasingly related to anti-democratic attitudes as well as public acceptance of government anti-democratic behaviour. Thus, this can be further interpreted as a criminalisation attempt by important government officials in order to gain more public approval.

This tactic of criminalisation aids in the argument that HRDs' work is being politicised, as it shows the gradual inclusion of human rights defenders in the category of perceived group threat, which is a main reason for governments to engage in digital repression (Pearson et al 2025, Hempel and Strapko 2026). However, it could be argued that the use of online tools to criminalise and spread damaging narratives regarding a group is in violation of Article 17 of the ICCPR, in which the HRDs are subjected to "unlawful attacks on honour and reputation" (UN General Assembly 1966).

2. The Role of Private Companies

2.1 Accountability

Digital Authoritarianism, and hence the use of digital tools, renders the blur between democracies and authoritarian governments subtle and more difficult to perceive than outright authoritarian repression (Feldstein 2021, Wilson 2022). However, the impact of DA practices on human rights is increasingly possible due to the mediation of private companies in representing a way for governments to escape accountability and transparency. Feldstein (2021) found that private companies were just as present in selling digitally repressive tools to democracies as they were to authoritarian governments, indicating a presence of private companies in the functioning of DA practices in democracies. In fact, a lot of the literature on Digital Authoritarianism and private companies is focused on surveillance capitalism (Zuboff 2018 in Molnar 2021 p71, Yabanci 2024, Conduit 2025). However, the present research brings original findings to the literature by showing that the role of private companies is not only limited to capitalising on digital repression, but also in their relevance for democratic governments to escape direct accountability. In fact, private companies themselves have human rights standards, but are not necessarily governed by international human rights accountability mechanisms (Lamensch 2024).

In her research on immigration, Molnar (2021) finds that the private sector is allowing the state to deflect from responsibility by engaging in actions that are harder to regulate. The present finding yielded similar conclusions. The use of private companies on behalf of the US government in ways that violate privacy rights and freedom of expression, as seen in the data analysis, shows that national and international accountability mechanisms that govern the state are bypassed through private companies. For privacy rights, this is particularly evident in social media surveillance, where private companies such as Penlink and Zignal Labs give data access to ICE through legal contracts or legal means such as subpoenas (EFF v DHS and ICE 2026). The use of legal mechanisms to access private company data gathered on HRDs further shows how private companies are not only intermediaries in the collection of data but represent a convenient point of access through existing legal measures, with which the state can obtain relevant information without necessarily having to surveil HRDs directly and account publicly for doing so. In fact, Nambiar (2025) finds that the US legal framework considers privacy rights to be less relevant when the individual deliberately gives their

personal data to a third party. However, I argue that immigration enforcement's access to such data is a risk to the privacy rights of HRDs, especially in light of the aforementioned viewpoint-based immigration system. By escaping accountability and not protecting the privacy of human rights defenders online, the findings suggest that the state can hinder the work of Human Rights Defenders. This comes at a time when human rights and other institutions are being deprived of funding (UN General Assembly 2025), while the Trump administration is increasing funding for immigration enforcement (American Immigration Council 2025). The lack of funding is exacerbating the inadequate protection for HRDs, as NGOs are not able to effectively face the growing power of private companies (Seck et al. 2020).

2.2 Transparency

The previous section touched upon the implications of DA practices and private companies on government accountability. However, I argue that the targeting of HRDs using technological tools is a threat to democracies also because of its underlying lack of transparency. When it comes to private companies, a lack of transparency is seen in the contracts drafted with the government, in which the specifications of what tools will be used and for what reason are left purposefully vague (see pages 54- 55). This was observed in various cases, including in the contract with Paragon Solutions, where the state lacked disclosure of information on how their spyware software was going to be applied, and the contract didn't clearly state which of their products the government was acquiring (Campbell 2024). Furthermore, in many of these contracts, justification for the use of DA practices often surrounds notions of "external threats" whose conceptual vagueness has been evidenced in the data analysis to increasingly include HRDs whose work is considered governmental dissidence (Department of Homeland Security, Federal Register 2025). Private companies don't concern themselves with disclosure of information, as was seen in the case of ALPRs where the state doesn't warn about the locations of this technology and the private company doesn't do so either (Keener, Finn and Baird 2025). Once again, the interaction between the government and private companies creates some legal holes that allow the state to overlook its democratic duties (Molnar 2021).

I find that aside from private contracts, US immigration policies and proposals are also often left vague in order to circumnavigate the disclosure of details and expand the effects of

immigration enforcement. This is seen through the use of social media as a surveillance practice, where official governmental data differs from that of NGOs, with the former explaining the use of social media identifiers in immigration as a necessity for national security but without going into detail on the particular information that is being surveilled (The Department of Homeland Security, 2025), while the latter reports violations of freedom of expression and privacy in the field, with HRDs targeted due to dissenting speech online (Branum 2025, Brennan Center for Justice and Knight First Amendment Institute 2025). This inconsistency between what is observed in practice and what is described by the government indicates that vagueness is a fundamental aspect of DA practice, because the less a state specifies in these orders, the more flexibility enforcement agents seem to have in their application. This can have important implications for the protection of HRDs given that the potential harms they can be exposed to are not made explicit or accounted for.

3. Digital Repression

Threats to democracy are visibly seen in the state's engagement in digital repression, with new insights from this research showing a tendency of democracies to use DA practices to shift towards more violent forms of repression, previously associated mainly with authoritarian governments (G'Sell 2025, Earl et al 2022).

Earl et al (2022) conceptualised digital repression as including: traditional repressive techniques against digital protesters, and digital repressive techniques used to reinforce traditional repressive measures. Regarding the former, this case study found violent, traditional repressive techniques to apply to HRDs even if they weren't engaging with digital tools. This was seen in the use of violent measures such as firing pepper balls, rubber bullets, tear gas and flashbang grenades to attack protesters, which were then justified through social media channelling practices by calling on national security and terrorism narratives (Chicago Headline Club v. Noem 2025). Many cases reported protesters being targeted after ICE agents had noticed they were filming or doxxing them (Guariglia and Schwartz 2025, Chicago Headline Club v. Noem 2025 pp 73), making it possible to interpret that when using digital tools, HRD rights are also at high risk of repression. Regarding the second categorisation, digital repressive techniques reinforced traditional measures through the use of surveillance to monitor individuals and then subsequently arrest or threaten them, as well as through the use of social media to spread narratives that could justify the violent attacks against peaceful

protesters (see pages 33-39). This connection between Digital Authoritarianism practices in democracies and physical repression was not a link accounted for in the current literature on DA in democracies, with the findings of this research showing a possible shift towards more violent expressions of Digital Authoritarianism in democracies.

The implications for more violent forms of repression are significant in democracies, especially in terms of the aforementioned concept of the *chilling effect*. As seen in the section above, the chilling effect occurs especially when people are afraid of freely expressing themselves due to possible repressive repercussions. If the repercussions are becoming more violent than expected from democracies, I argue this could potentially exacerbate the chilling effect, with HRDs being afraid of arrests and deportation (Branum 2025) and physical violence (American Immigration Council 2026).

Instead, the engagement in preventative repression confirms that an increase in availability of digital tools lowers the repressive costs of a democratic government by stifling dissident voices before they turn into social movements. The immigration enforcement system in the US also uses DA practices for the preventative repression of Human Rights Defenders. Dragu and Lupu (2021), in their framework on preventative repression, identified the following practices: voice recognition to scan mobile networks, tracking of citizens' movement using GPS, monitoring of emails and text messages, selective censoring of information, and use of malware or spyware to target personal digital items. The data analysis chapter confirmed such findings with an innovative perspective by specifically focusing on HRDs as the target group. In fact, the state was found to engage in location and movement tracking using ALPRs and ad-based surveillance systems such as Paragon solutions software were used as spyware on devices, and new executive orders set out social media identifiers as part of the immigration surveillance system. Instead, no evidence was found regarding censorship of information or voice recognition. This is in line with findings that censorship and internet control tend to be practices more characteristic of authoritarian regimes (Christensen and Groshek 2019, Maerz 2025).

4. National Security

Although this paper was not a legal analysis of human rights standards, it did investigate the effects of technological misuse on the human rights of HRDs. Therefore, I think it is

important to touch upon the clauses in international and national human rights frameworks that relate to national security. As seen in the data analysis and in the previous section discussing criminalisation, national security is used by the US government to explain the implementation of DA practices that can restrict the rights of HRDs. National security narratives are often integrated with other categorisations such as terrorism and drug affiliation to spread a narrative on HRDs and influence public opinion (see page 60, 72). In fact, in accordance with Quadri et al (2025), I find that national security was invoked to criminalise HRDs through digital tools, rather than as a legitimate reason for restricting rights.

Furthermore, this is supported by the practice-based perspective of the present research, as defined by Glasius and Michaelsen (2018), in which the effects of the DA practice are what constitute it as Digital Authoritarianism, rather than the legitimacy of the intention behind the practice.

A lot of the violations of freedom of expression promoted by executive orders and government proposals were often justified through narratives of national security. According to Article 19 of the ICCPR (UN General Assembly 1966), national security is mentioned as a possible reason to restrict the freedom of expression of individuals, but I argue that in this case it is not proportional and hence does not fall into this justification. This is in accordance with Rawaqa's (2025) findings that HRDs are labelled by governments as threats to sovereignty, but they are actually subjected to defamation and legal prosecution. In fact, as seen throughout the data analysis, restrictions on freedom of expression are coupled with repression on behalf of the government.

V. Conclusion

1. Central Findings

The present thesis aimed to contribute to the literature on Digital Authoritarianism in democracies by researching how DA practices impeded the rights of human rights defenders and what this meant for the blurring of democracies. The research question was: *How are Digital Authoritarianism practices in US immigration enforcement impeding the rights of Human Rights Defenders?* It was answered through a qualitative, inductive-deductive thematic analysis of NGO, governmental and International Organizations' data sources.

As explained in the methodology section, the focus on the US was important due to the increasing digitalisation of their immigration system (Molnar 2021), and because of the current Trump administration's restrictions on immigration (American Immigration Council 2025). This is extremely relevant when the US places itself as a leader in human rights and democratic standards but does not effectively implement such standards in practice. The research used DA practices as conceptualised by Glasius and Michaelsen (2018) because the focus was not on regime classification or on the intention behind governments' use of DA practices, but rather on the human rights effects of such practices on Human Rights Defenders, and the implications that these effects can have on core democratic pillars. The research contributed to the gaps regarding the effects of DA on Human Rights Defenders and contributed to the development of the concept as it is manifested within democracies.

This data analysis reported that surveillance, which had the most reporting on in the data, was found to be restricting freedom of expression and the right to privacy of human rights defenders, especially through techniques such as facial recognition technology, spyware and social media (see pages 33- 49). Instead, channelling was mostly present in a covert form and implemented through social media. The narratives spread through channelling constituted criminalisation tactics towards HRDs by associating and incriminating them with labels of national security, terrorism and drug trafficking(see pages 57-59). This technique of criminalisation was found throughout most practices to justify their implementation. The practice of Data Collection was found to be related to Surveillance, and mainly reported on the presence of mass databases collected through surveillance techniques, and with the help of private companies that provide ALPRs and Ad-based surveillance. The DA practices and

their impediment of rights and democracy seem to be mediated by mechanisms identified inductively, which include: private companies, criminalisation, funding and chilling effects.

These findings were used to support the argument that democracies are increasingly using DA practices to target Human Rights Defenders, and in doing so Digital Authoritarianism is contributing to the blurring of the boundary between democracies and Authoritarian governments. In particular, this occurs due to the presence of private companies as intermediaries for states to surveil and access data on Human Rights Defenders, while bypassing national and international standards of accountability, and impacting democratic accountability and transparency. A lack of funding exacerbates the unregulated interrelationship with private companies. In addition, criminalisation tactics and intentional chilling effects are mediating mechanisms that allow DA practices to be so harmful to the rights of HRDs.

2. Strengths and Limitations

The case study was very contemporary, focused on about a year and a half of the presidency. It would have been most effective to incorporate in the data direct experiences from Human Rights Defenders in the field, to better understand the impacts of Digital Authoritarianism on their work. Interviews were not conducted due to ethical reasons, but the present research recognises that they would have been very relevant and they would have provided an additional, hands-on perspective to the topic. The data that was analysed consisted of NGO reports and Governmental data, triangulated with relevant academic articles. Another limitation is the fact that each data set had a specific perspective and voice based on whether they came from the government compared to NGOs. While this was acknowledged in the data analysis and helped enrich the understanding of the research question by discussing narratives and interpretations, it must also be recognised that there is a level of bias embedded within how the information is presented.

The focus on the second Trump administration can be both a strength and limitation. On the one hand, the focus is very narrow, and there is no comparison to how the situation looked in previous presidencies. However, focusing on only one administration allowed the research to be specific and relevant to the current presidency, and the findings can be used to help HRDs understand what contemporary risks they face in the US at the moment. Furthermore, this

presidency was chosen due to drastic increases in immigration enforcement (Human Rights Watch 2025), so the present findings can also serve to better understand other countries that are currently also increasing efforts in immigration enforcement.

Another limitation concerns the generalisability of the results. While the US was chosen due to its democratisation and because it exemplified a situation where a specific part of governance is being fortified and digitalised, the fact that the focus was only on one country makes the research harder to generalise. The interpretations made from the data analysis and discussed in the Discussion chapter were specific for the US but related to claims on democracies in general. However, the present thesis acknowledges the difficulty of generalising the findings to other countries, especially if they differ significantly from the US. Despite this, the US represents a case of institutionalised democracy, and the large amount of data analysed shows important insights into the blurring between democracies and authoritarian governments.

Human Rights Defenders, in this research, were identified through an activity-based approach (Koula 2026), meaning that they could be anyone who worked to protect human rights. This could include: protesters, journalists, citizens and activists. Given the expansion of what constitutes a Human Rights Defender in recent years, it is important to keep in mind that HRDs and their work are grounded in human rights standards (Rawaq 2025). However, the present research recognises that, given the novelty of the case study topic, the data were not disaggregated, so a lot of the DA practices reported to be used by the government were also targeting individuals that would not fall into the categorisation of HRDs. To contrast this limitation, I only used data focusing on protesters that were not violent, on citizens that were engaged in activities that upheld human rights standards, and I differentiated between political activists, civil disobedients, and human rights defenders. These differentiations were done by focusing on the motivation and method of action to make sure they fell in line with those of HRDs as defined by the declaration on human rights defenders (UN General Assembly 1998). Despite this, I acknowledge the fact that many reports combined the various actors in their research, so differentiation was complex.

3. Further Research

Further research should focus on the role of private companies as direct actors in Digital Authoritarianism, apart from their correlation with the state. In fact, the present thesis found strong correlations between the state and private technology companies, in that the latter represented mediating mechanisms through which the state could bypass accountability. However, the literature also focuses on private companies as separate actors (G'Sell 2025), which would be important to investigate in the context of US immigration enforcement to better conceptualise the range of actors using DA practices to impact HRDs.

Furthermore, social media emerged in the data analysis as a relevant tool used by the state in various DA practices and for various functions. Further research would allow for a better understanding of other practices within social media, done on behalf of the state or of private companies, regarding algorithmic filtering and social media analytics (Mirza et al. 2025). These have been found before to impact democratic processes such as elections; therefore, it would be important to better understand their impact on Human Rights Defenders.

In addition, as was presented in the section on AI debates (see pages 47- 49), the increasing use of Artificial Intelligence within technology can negatively impact HRDs and those targeted by DA practices. While the theme of AI did emerge in the data, it was not overly present, and the main consequences identified by the present analysis were discrimination and potential biases. Given the presence of these discriminatory tendencies in automated technology, further research is needed to understand exactly how HRDs are targeted by AI. This should include focusing on minority groups and women as well, to better identify the different interferences on human rights.

4. Recommendations

The safeguards in place for technological tools are easily detracted from by the current administration, rendering the protection frameworks fragile and dependent on the government's needs for national security (The White House 2026 Executive Order 14110). This was seen in the retraction of Executive Order 14110, which was meant to protect the development of AI and avoid discrimination in its application. It was also seen in the reactivation of the contract with the spyware tool Paragon Solutions, with NGOs perceiving a threat of Trump lifting the ban on the company NSO and its spyware tool Pegasus (Access

Now 2025). The unreliability of these frameworks shows that new regulations need to be put in place to protect HRDs from digital technologies.

In the US, no national frameworks exist for the protection of human rights defenders (Rawaqa 2025). They are indirectly supported by foreign aid programmes that fund assistance for defenders. However, in light of the funding crisis discussed in the previous chapter, there is a heightened risk that funded programmes of protection be discontinued or weakened, as is occurring to many NGOs (UN General Assembly 2025). Thus, I would urge a separate framework of protection to be developed domestically in the US to safeguard the rights of HRDs and as a step to safeguard democracy. Furthermore, I concur with Rawaqa (2025) on her findings of disproportionate risks faced by minority HRDs, which my research has identified immigrant HRDs as being in this category. Thus, protection frameworks should accommodate the different risks faced by HRDs depending on immigration status, and the findings from this analysis can help inform which DA practices they are most likely targeted with. Furthermore, ICE is currently disregarding many of the regulations it had in place, such as those on refraining from detaining people in safe spaces such as schools, courthouses and places of service (Human Rights Watch 2025). Given the findings of human rights violations provided by the present thesis, I would argue it is vital to reinstate protective regulations, but also to expand them and include regulations on the use of technological tools.

VI. Bibliography

1. Literature

- American Immigration Council (2025) *Mass Deportation: Analysing the Trump Administration's Attacks on Immigrants, Democracy, and America*. Available at:
<https://www.americanimmigrationcouncil.org/report/mass-deportation-trump-democracy/>.
- Bartels, L.M. (2020) 'Ethnic antagonism erodes Republicans' commitment to democracy,' *Proceedings of the National Academy of Sciences*, 117(37), pp. 22752–22759. <https://doi.org/10.1073/pnas.2007747117>.
- Bennett, K. et al. (2015) 'Critical perspectives on the security and protection of human rights defenders,' *The International Journal of Human Rights*, 19(7), pp. 883–895. <http://dx.doi.org/10.1080/13642987.2015.1075301>.
- Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology,' *Qualitative Research in Psychology*, 3(2), pp. 77–101.
<https://doi.org/10.1191/1478088706qp063oa>.
- Brooks, H.Z. and Porter, M.A. (2020) 'A model for the influence of media on the ideology of content in online social networks,' *Physical Review Research*, 2(2). <https://doi.org/10.1103/physrevresearch.2.023041>.
- Chauvin, N. (2026) 'The unconstitutional attempt to criminalise naming ICE agents,' *UCLA Law Review Discourse*, 73, p. 144. Available at:
<https://ssrn.com/abstract=5315719>.
- Chen, J. and Xu, Y. (2017) 'Why do authoritarian regimes allow citizens to voice opinions publicly?' *The Journal of Politics*, 79(3), pp. 792–803.
<https://doi.org/10.1086/690303>.
- Christensen, B. and Groshek, J. (2019) 'Emerging media, political protests, and government repression in autocracies and democracies from 1995 to 2012,' *International Communication Gazette*, 82(8), pp. 685–704.
<https://doi.org/10.1177/1748048518825323>.

- Conduit, D. (2025) 'Digital Authoritarianism and the Global Technology Industry: Evidence from Iran,' *Government and Opposition*, 60(3), pp. 751–772.
<https://doi.org/10.1017/gov.2024.31>.
- Das, A. (2020) 'Deportation and dissent: protecting the voices of the immigrant rights movement,' *New York Law School Law Review*, 65, p. 225. Available at:
https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1758&context=nyls_law_review.
- Dragu, T. and Lupu, Y. (2021) 'Digital authoritarianism and the future of human rights,' *International Organisation*, 75(4), pp. 991–1017.
<https://doi.org/10.1017/s0020818320000624>.
- Earl, J., Maher, T.V. and Pan, J. (2022) 'The digital repression of social movements, protest, and activism: A synthetic review,' *Science Advances*, 8(10), p. eabl8198. <https://doi.org/10.1126/sciadv.abl8198>.
- Eshbaugh-Eshbaugh-Soha, M. (2026) 'The President's immigration executive actions,' *American Politics Research*, 54(3), pp. 352–365.
<https://doi.org/10.1177/1532673x261420768>.
- Feldstein, S. (2019) 'The Global Expansion of AI Surveillance.' Washington, DC: Carnegie Endowment for International Peace. Available at:
https://assets.production.carnegie.fusionary.io/static/files/files__WP-Feldstein-AISurveillance_final1.pdf.
- Feldstein, S. (2021) 'Introduction,' in *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Online edn. Oxford: Oxford Academic, pp. 1–21.
<https://doi.org/10.1093/oso/9780190057497.003.0001>.
- Francavilla, G.M., Sansonetti, G., Gasparetti, F. and Micarelli, A. (2025) 'A comparative analysis of social media content on migration in Italy and the United States,' *CEUR Workshop Proceedings*, Vol-3957. Available at:
<https://ceur-ws.org/Vol-3957/SOCIALIZE-paper06.pdf>.
- G'Sell, F. (2025) 'Digital authoritarianism: from state control to algorithmic despotism,' in De Gregorio, G., Pollicino, O. and Valcke, P. (eds) *The Oxford*

Handbook of Digital Constitutionalism. Online edn. Oxford: Oxford Academic. <https://doi.org/10.1093/oxfordhb/9780198877820.013.20>.

Glasius, M. and Michaelsen, M. (2018) 'Illiberal and authoritarian practices in the digital sphere: prologue,' *International Journal of Communication*, 12, pp. 3795–3813. Available at: <https://ijoc.org/index.php/ijoc/article/view/8899>.

Hankey, S. and Ó Clunaigh, D. (2013) 'Rethinking risk and security of human rights defenders in the digital age,' *Journal of Human Rights Practice*, 5(3), pp. 535–547. <https://doi.org/10.1093/jhuman/hut023>.

Hempel, L. and Strapko, N. (2025) "'Taking What's Ours': Restrictionist attitudes toward immigration and threat to sense of group position in the United States,' *Sociological Inquiry*, 96(2), pp. 264–284. <https://doi.org/10.1111/soin.70017>.

Hudson, D. and Gluzman, M. (2025) 'Interesting intersections of immigration and First Amendment law,' *FIU Law Review*, 19(1), pp. 215–228. Available at: <https://dx.doi.org/10.25148/lawrev.19.1.7>.

Human Rights Watch (2025) *"We Need U": How the U Visa Builds Trust, Counters Fear, and Promotes Community Safety*. Available at: <https://www.hrw.org/report/2025/12/02/we-need-u/how-the-u-visa-builds-trust-counters-fear-and-promotes-community-safety>.

Huq and Ginsburg, T. (2018) 'How to lose a constitutional democracy,' *UCLA Law Review*, 65(1), pp. 78–169.

Kapelner, Z. (2024) 'Anti-immigrant backlash: the Democratic Dilemma for immigration policy,' *Comparative Migration Studies*, 12(1). <https://doi.org/10.1186/s40878-024-00370-7>.

Karahan, A. et al. (2025) *International Immigration and Security Policies*. Özgür Yayınları eBooks. <https://doi.org/10.58830/ozgur.pub766>.

Keener, S., Finn J and Baird, A. (2026) *Surveillance Inequality: Race, Poverty, and the Geography of Automated License Plate Reader Deployment*. SSRN Available at: <http://dx.doi.org/10.2139/ssrn.6064548>

- Kitchin, R. (2020) 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19,' *Space and Polity*, 24(3), pp. 362–381. <https://doi.org/10.1080/13562576.2020.1770587>.
- Koula, A.-C. (2024) 'Human rights violations committed against human rights defenders through the use of the legal system: a trend in Europe and beyond,' *Human Rights Review*, 25(1), pp. 99–122. <https://doi.org/10.1007/s12142-024-00717-8>.
- Koula, A.-C. (2025) 'Strengthening the rule of law: the necessity of protecting human rights defenders from criminalisation,' *Human Rights Law Review*, 26(1). <https://doi.org/10.1093/hrlr/ngaf039>.
- Lamensch, M. (2024) *Digital Authoritarianism: The Role of Legislation and Regulation*. CIGI Policy Brief No. 182. Center for International Governance Innovation. Available at: <https://www.jstor.org/stable/resrep56962>.
- Martínez-Fernández, A. and Beaver, W. (2025) 'Thoughtlessness in the age of homeland security: race, surveillance, and bureaucratic violence in immigration enforcement,' *Polity*, 57(1), pp. 29–55. <https://doi.org/10.1086/733431>.
- McGregor, L. and Molnar, P. (2023) *Digital Border Governance: A Human Rights Based Approach*. Colchester and Geneva: University of Essex and Office of the United Nations High Commissioner for Human Rights. Available at: <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>.
- Michaelsen, M. and Glasius, M. (2018) 'Authoritarian Practices in the Digital Age—Introduction,' *International Journal of Communication*. Available at: <https://ijoc.org/index.php/ijoc/article/view/8536>.
- Mirza, S.J. et al. (2025) 'The role of social media analytics in crafting international political narrative,' *The Critical Review of Social Sciences Studies*, 3(2), pp. 2456–2468.

- Molnar, P. (2019) 'New technologies in migration: human rights impacts,' *Forced Migration Review*, 61, pp. 7–9. Available at:
<https://www.fmreview.org/ethics/molnar>.
- Molnar, P. (2021) 'Surveillance sovereignty: migration management technologies and the politics of privatisation,' in *Migration, Security, and Resistance*. Abingdon: Routledge, pp. 66–82. <https://doi.org/10.4324/9781003058526-3>.
- Molnar, P. (2024) 'The Politics of Exclusion and Fear,' in *The Walls Have Eyes: Surviving Migration in the Age of Artificial Intelligence*. New York: The New Press. Available at:
<https://research.ebsco.com/plink/793acb39-3ec1-3d1b-ad44-7b17560854a8>.
- Nambiar, V. (2025) 'Watching and waiting: modern social media surveillance of immigrants and Fourth Amendment implications,' *Federal Communications Law Journal*, 77(2), pp. 199–224. Available at:
http://www.fclj.org/wp-content/uploads/2025/02/77.2.4_Watching-and-Waiting.pdf.
- Pearson, J.S. (2024) 'Defining digital authoritarianism,' *Philosophy & Technology*, 37(2). <https://doi.org/10.1007/s13347-024-00754-8>.
- Penney, J.W. (2025) 'Conventional chilling effects theories and their limits,' in *Chilling Effects: Repression, Conformity, and Power in the Digital Age*. Cambridge: Cambridge University Press, pp. 17–38.
<https://doi.org/10.1017/9781108641784.003>.
- Peron, A.E.D.R., De Magalhães, D.A.M. and Caetano, G.F. (2025) 'Beyond digital repression: techno-authoritarianism in radical right governments,' *Cogent Social Sciences*, 11(1). <https://doi.org/10.1080/23311886.2025.2528457>.
- Plattner, M.F. (2015) 'Is democracy in decline?' *Journal of Democracy*, 26(1), pp. 5–10. <https://dx.doi.org/10.1353/jod.2015.0014>.
- Quadri, S.S.A. et al. (2025) 'The Criminalization of Human Rights Defenders: trends, tactics, and international responses,' *Social Sciences Spectrum*, 4(2), pp. 756–773. <https://doi.org/10.71085/sss.04.02.333>.

- Rawaqa, S. (2025) 'Identifying and regulating human rights defenders (HRDs),' *The International Journal of Human Rights*, 29(10), pp. 1735–1765.
<https://doi.org/10.1080/13642987.2025.2517571>.
- Richards, N.M. (2013) 'The dangers of surveillance,' *Harvard Law Review*, 126(7), pp. 1934–1965. Available at: <https://www.jstor.org/stable/23415062>.
- Ristovska, S. (2016) 'Strategic witnessing in an age of video activism,' *Media Culture & Society*, 38(7), pp. 1034–1047. <https://doi.org/10.1177/0163443716635866>.
- Roberts, T. and Oosterom, M. (2024) 'Digital authoritarianism: a systematic literature review,' *Information Technology for Development*, 31(4), pp. 860–884.
<https://doi.org/10.1080/02681102.2024.2425352>.
- Sania, J., Ziosi, M. and Barez, F. (2026) 'From democracies to autocracies: how AI systems enable authoritarianism by design,' *arXiv preprint arXiv:2606.17286*, pp. 1–14. <https://doi.org/10.48550/arXiv.2606.17286>.
- Sharma, C. and Adler, S. (2026) 'Immigration enforcement intermediaries,' *BYU Law Review*, 52 (forthcoming). Available at: <https://ssrn.com/abstract=6345099>.
- Simoncini, A. and Longo, E. (2026) 'Digital constitutionalism and fundamental rights: reconfiguring liberty and power,' in De Gregorio, G., Pollicino, O. and Valcke, P. (eds) *The Oxford Handbook of Digital Constitutionalism*. Oxford: Oxford University Press, pp. 1–21.
- Stolmack, A.A. (2025) 'Eyes on the road: strengthening Fourth Amendment protections against law enforcement's accelerating use of automated license plate readers,' *UCLA Criminal Justice Law Review*, 9(1). Available at: <https://escholarship.org/content/qt93j6c64n/qt93j6c64n.pdf>.
- Stoycheff, E., Burgess, G.S. and Martucci, M.C. (2018) 'Online censorship and digital surveillance: the relationship between suppression technologies and democratisation across countries,' *Information Communication & Society*, 23(4), pp. 474–490. <https://doi.org/10.1080/1369118x.2018.1518472>.
- United Nations General Assembly (1966) *International Covenant on Civil and Political Rights*. Geneva: United Nations, Available at:

<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

United Nations General Assembly (1998) *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms*, Geneva: United Nations, Available at:

<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

United States Constitution (1789) *The Constitution of the United States of America: Analysis and Interpretation*. Available at:

<https://constitution.congress.gov/constitution/amendment-1/>.

Wijayanto, W. et al. (2022) 'Digital authoritarianism in Southeast Asia: a systematic literature review,' in *Proceedings of the 6th International Conference on Social and Political Enquiries*. EAI.

<https://doi.org/10.4108/eai.14-9-2021.2321400>.

Wilson, R.A. (2022) 'Digital authoritarianism and the global assault on human rights,' *Human Rights Quarterly*, 44(4), pp. 704–739.

<https://doi.org/10.1353/hrq.2022.0043>.

Woolley, S. and Guilbeault, D. (2017) 'Computational Propaganda in the United States of America: Manufacturing Consensus Online.' *Project on Computational Propaganda Working Paper No. 2017.5*. Oxford: Oxford University, pp. 1–29. Available at:

<https://ora.ox.ac.uk/objects/uuid:620ce18f-69ed-4294-aa85-184af2b5052e/files/m386d8772770fb4c448390aa70a2ef1b4a>.

Woolley, S. and Howard, P. (2017) 'Computational Propaganda Worldwide: Executive Summary.' *Project on Computational Propaganda*. Oxford: Oxford University, pp. 1–13. Available at:

<https://ora.ox.ac.uk/objects/uuid:d6157461-ae6d-48ff-a9a9-2d93222a9bfd/files/m8be3ef66dde61927afdc7ad7d166b0f4>.

Yabanci, B. (2024) ‘Surveil, datafy, publicize: digital authoritarianism and migration governance in Turkey,’ *Democratisation*, 32(4), pp. 1016–1041.
<https://doi.org/10.1080/13510347.2024.2433091>.

2. Data Analysis Reports

Access Now (2020) Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts. Available at:
<https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/> (Accessed 5 June 2026).

Access Now (2021) Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance. Available at:
<https://www.accessnow.org/wp-content/uploads/2022/08/BanBS-Statement-English.pdf> (Accessed 5 June 2026).

Access Now (2025) Paragon must answer for spyware use against civil society and journalists. Available at:
<https://www.accessnow.org/press-release/paragon-must-answer-for-spyware-use-against-civil-society/> (Accessed 5 June 2026).

ACLU of Illinois (2026) Chicago Headline Club v. Noem. Available at:
<https://www.aclu-il.org/cases/chicago-headline-club-v-noem/> (Accessed 10 June 2026).

American Civil Liberties Union of Colorado (2025) Coalition of Civil Rights and Advocacy Organizations Deeply Opposed to Use of Flock Cameras for ICE Surveillance. Available at:
<https://www.aclu-co.org/press-releases/coalition-of-civil-rights-and-advocacy-organizations-deeply-concerned-about-use-of-flock-cameras-for-ice-surveillance/> (Accessed 16 June 2026).

American Immigration Council (2026) How ICE Went Rogue: A Brief Analysis of the Legal Authorities Governing ICE and CBP Operations — and How They’re Being Undermined and Violated by Policy and Practice. Available at:
<https://www.americanimmigrationcouncil.org/fact-sheet/ice-cbp-legal-analysis/> (Accessed 18 May 2026).

Ayoub, E. and Goitein, E. (2024) Closing the Data Broker Loophole, Brennan Center for Justice. Available at:
<https://www.brennanCenter.org/our-work/research-reports/closing-data-broker-loophole> (Accessed 14 June 2026).

Barrueto, L. and Al-Maskati, M. (2025) How U.S. Funding Cuts Expose Civil Society to Digital Attacks, Access Now. Available at:
<https://www.accessnow.org/u-s-funding-cuts/> (Accessed 14 June 2026).

Branum, B. (2025) CDT Opposes Trump Administration Initiative to Routinely Collect Social Media Identifiers from Applicants for Immigration Benefits, Center for Democracy and Technology. Available at:
<https://cdt.org/insights/cdt-opposes-trump-administration-initiative-to-routinely-collect-social-media-identifiers-from-applicants-for-immigration-benefits/> (Accessed 8 May 2026).

Brennan Center for Justice and Knight First Amendment Institute (2025) Brennan Center and Knight Institute Submit Comments Opposing DHS Proposal to Collect Social Media Identifiers. Available at:
<https://www.brennanCenter.org/our-work/research-reports/brennan-Center-and-knight-institute-submit-comments-opposing-dhs-proposal> (Accessed 6 June 2026).

Brennan Center for Justice and Knight First Amendment Institute (2025) Letter to “Agency Information Collection Activities; New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms.” Available at:
<https://www.brennanCenter.org/media/13951/download/05.05.25-bcj-uscis-sm-m-comments.pdf?inline=1> (Accessed 6 June 2026).

Campbell, Z. (2024) US Immigration Agency Contract with Spyware Company Poses Risk to Rights Systems Needed to Hold Industry, Governments to International Standards, Human Rights Watch. Available at:
<https://www.hrw.org/news/2024/10/17/us-immigration-agency-contract-spyware-company-poses-risk-rights> (Accessed 27 May 2026).

Center for Constitutional Rights (2025) Legal Groups Sue Trump Administration to Uncover Use of Israeli Spyware Tools on U.S. Communities. Available at:
<https://ccrjustice.org/home/press-Center/press-releases/legal-groups-sue-trump-administration-uncover-use-israeli-spyware> (Accessed 10 June 2025).

Center for Democracy and Technology (2025) Letter to Chief Privacy Officer Jankowski. Available at:
<https://cdt.org/wp-content/uploads/2025/11/Coalition-Letter-on-ICE-Mobile-Fortify-FRT-Nov2025.pdf> (Accessed 8 May 2026).

Chicago Headline Club v. Noem (2025) Judge Sara L. Ellis: Opinion and Order, Case No. 25-cv-12173, United States District Court for the Northern District of Illinois Eastern Division. Available at:
<https://cases.justia.com/federal/district-courts/illinois/ilndce/1:2025cv12173/487571/281/0.pdf?ts=1763733493> (Accessed 10 June 2026).

Chicago Headline Club v. Noem (2025) Plaintiff Complaint for Injunctive and Declaratory Relief, Case No. 25-cv-12173, United States District Court for the Northern District of Illinois Eastern Division. Available at:
<https://www.aclu-il.org/cases/chicago-headline-club-v-noem/?document=Chicago-Headline-Club-v-Noem-Complaint#documents> (Accessed 10 June 2026).

Christl, W. et al. (2026) Uncovering Webloc: An Analysis of Penlink’s Ad-based Geolocation Surveillance Tech, Citizen Lab Report No. 191, University of

Toronto. Available at:

https://citizenlab.ca/wp-content/uploads/2026/05/191_Uncovering_Webloc.pdf (Accessed 5 June 2026).

Citizen Lab (2019) NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases. Available at:

<https://citizenlab.ca/research/nso-q-cyber-technologies-100-new-abuse-cases/> (Accessed 5 June 2026).

Cohn, C. and Gedlu, B. (2026) Palantir Has a Human Rights Policy. Its ICE Work Tells a Different Story, Electronic Frontier Foundation. Available at:

<https://www.eff.org/deeplinks/2026/04/palantir-has-human-rights-policy-its-ice-work-tells-different-story> (Accessed 5 June 2026).

Deibert, R. (2026) Letter to Citizen Lab research report, The Citizen Lab. Available at:

https://citizenlab.ca/wp-content/uploads/2026/04/Citizen-Lab-Mail-Fwd_-Citizen-Lab-research-report_Redacted.pdf (Accessed 7 June 2026).

DeFlock (2026) What are ALPRs? Available at: <https://deflock.org/what-is-an-alpr> (Accessed 14 June 2026).

Department of Homeland Security (2025) Analytic Tools in Support of the Protective Mission, United States of America. Available at:

https://www.dhs.gov/sites/default/files/2025-09/25_0820_priv_pia-ice-066-protectivemission.pdf?inline=1 (Accessed 8 June 2026).

Department of Homeland Security (2025) Privacy Threshold Analysis (PTA), United States of America: Privacy Office. Available at:

<https://www.documentcloud.org/documents/26209262-mobile-fortify-pta/?ref=404media.co> (Accessed 17 June 2026).

Department of Homeland Security (2025) U.S. Citizenship and Immigration Services, United States of America. Available at:

<https://public-inspection.federalregister.gov/2025-03492.pdf> (Accessed 18 May 2026).

Department of Homeland Security (2026) Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, United States of America. Available at:

https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202511-1615-008
(Accessed 5 June 2026).

Electronic Frontier Foundation (2023) Street Level Surveillance: Automated License Plate Readers. Available at:

<https://sls.eff.org/technologies/automated-license-plate-readers-alprs>
(Accessed 5 June 2026).

Electronic Frontier Foundation (2023) Street Level Surveillance: Facial Recognition Technology. Available at: <https://sls.eff.org/technologies/face-recognition>
(Accessed 30 May 2026).

Electronic Frontier Foundation (2023) Street Level Surveillance: Police Database.

Available at: <https://sls.eff.org/technologies/police-databases> (Accessed 5 June 2026).

Electronic Frontier Foundation (2026) EFF Sues DHS and ICE For Records on Subpoenas Seeking to Unmask Online Critics. Available at:

<https://www.eff.org/press/releases/eff-sues-dhs-and-ice-records-subpoenas-seeking-unmask-online-critics-0> (Accessed 27 May 2026).

Electronic Frontier Foundation v. U.S. Department of Homeland Security and Immigration and Customs Enforcement (2026) Complaint for Injunctive Relief, Civil Action No. 1:26-cv-01368, United States District Court for the District of Columbia. Available at:

<https://www.eff.org/document/eff-v-dhs-ice-administrative-subpoenas-complaint> (Accessed 27 May 2026).

Epstein, G. (2025) Flock Gives Law Enforcement All Over the Country Access to Your Location, The Data for Justice Project, ACLU of Massachusetts. Available at:

<https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/> (Accessed 16 June 2026).

- Front Line Defenders (2026) Global Analysis 2025-26. Available at:
https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf
 (Accessed 5 June 2026).
- Guariglia, M. and Schwartz, A. (2025) Criminalising Masks at Protests is Wrong, Electronic Frontier Foundation. Available at:
<https://www.eff.org/deeplinks/2025/06/criminalizing-masks-protests-wrong>
 (Accessed 30 May 2026).
- Guariglia, M. and Trujillo, M. (2025) The Dangers of Consolidating All Government Information, Electronic Frontier Foundation. Available at:
<https://www.eff.org/deeplinks/2025/06/dangers-consolidating-all-government-information>
 (Accessed 7 June 2026).
- Human Rights Watch (2025) United States: Events of 2025, Country Report. Available at:
<https://www.hrw.org/world-report/2026/country-chapters/united-states#c2ec02>
 (Accessed 27 May 2026).
- Human Rights Watch (2026) “A Manufactured Crisis”: Minnesota Communities Terrorized by the Federal Government. Available at:
<https://www.hrw.org/report/2026/06/18/a-manufactured-crisis/minnesota-communities-terrorized-by-the-federal-government>
 (Accessed 27 May 2026).
- Just Futures Law and Center for Constitutional Rights v. United States Immigration and Customs Enforcement and United States Customs and Border Protection (2025) Complaint for Declaratory and Injunctive Relief, Civil Action No. 25-cv-8995, U.S. District Court for the Southern District of New York. Available at:
<https://ccrjustice.org/sites/default/files/attach/2025/10/10-30-25%20JFL%20CCR%20FOIA%20Complaint%20ECF%20Version.pdf>
 (Accessed 15 June 2026).
- Lipton, B. and Hamid, S. (2026) “Free” Surveillance Tech Still Comes at a High and Dangerous Cost, Electronic Frontier Foundation. Available at:
<https://www.eff.org/deeplinks/2026/02/free-surveillance-tech-still-comes-high-and-dangerous-cost>
 (Accessed 28 May 2026).

- Lyons, T. (2026) Letter to Representative Lee, House of Representatives, United States of America: Immigration and Customs Enforcement. Available at: <https://www.documentcloud.org/documents/27988741-ice-letter-response-to-congress/> (Accessed 15 June 2026).
- Maass, D. and Alajaji, R. (2025) How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists, Electronic Frontier Foundation. Available at: <https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safety-s-alpr-network-surveil-protesters-and-activists> (Accessed 28 May 2026).
- Marczac, B. and Scott-Railton, J. (2025) Graphite Caught First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted, Citizen Lab. Available at: <https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spywarefinds-journalists-targeted/> (Accessed 5 June 2026).
- Patel, F. and Rupert, M. (2025) ICE Wants to Go After Dissenters as well as Immigrants, Brennan Center for Justice. Available at: <https://www.brennanCenter.org/our-work/research-reports/ice-wants-go-after-dissenters-well-immigrants> (Accessed 5 June 2026).
- Pinsof, J. (2026) San Jose Can Protect Immigrants by Ending Flock Surveillance System, Electronic Frontier Foundation. Available at: <https://www.eff.org/deeplinks/2026/02/op-ed-san-jose-can-protect-immigrants-ending-flock-surveillance-system> (Accessed 5 June 2026).
- Raphling, J. (2025) Expert Report for Mahmoud Khalil Impacts on the Right to Free Expression, Human Rights Watch. Available at: <https://www.hrw.org/news/2025/06/05/expert-report-mahmoud-khalil> (Accessed 27 May 2026).
- Schmidt, L. and Arrington, C. v. City of Norfolk (2026) Brief of Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Virginia in Support of Plaintiffs-Appellants and Reversal, Case No. 2:24-cv-00621-MSD-RJK, United States District Court for the Eastern District of Virginia. Available at:

<https://www.aclu.org/cases/schmidt-v-norfolk?document=Brief-of-Amici-Curiae-Electronic-Frontier-Foundation-American-Civil-Liberties-Union-and-American-Civil-Liberties-Union-of-Virginia-in-Support-of-Plaintiffs-Appellants-and-Reversal> (Accessed 5 June 2026).

Seck, M. et al. (2026) Response to the OHCHR's Call for Inputs on Protection of Human Rights Defenders in the Digital Age, The Center for Democracy and Technology. Available at:
<https://cdt.org/insights/response-to-the-ohchrs-call-for-inputs-on-protection-of-human-rights-defenders-in-the-digital-age/> (Accessed 8 May 2026).

Secretary of Homeland Security (2025) Countering Domestic Terrorism and Organised Political Violence, United States of America: Federal Register. Available at:
<https://www.whitehouse.gov/presidential-actions/2025/09/countering-domestic-terrorism-and-organized-political-violence/> (Accessed 20 June 2026).

Stanley, J. (2025) New Report Highlights How CBP and Border Patrol are Becoming a Repressive Internal Intelligence Agency, American Civil Liberties Union. Available at:
<https://www.aclu.org/news/privacy-technology/border-patrol-alpr-dragnet> (Accessed 14 June 2026).

Summer, L. (2026) Letter to Secretary Lutnick, U.S. Department of Commerce, United States of America: Committee on Oversight and Government Reform. Available at:
<https://summerlee.house.gov/sites/evo-subsites/summerlee.house.gov/files/evo-media-document/2026-05-06.lee-letter-to-commerce-re-nso-group.pdf> (Accessed 15 June 2026).

Surveillance Technology Oversight Project (2026) Dear Mamdani: Dismantle NYC's Surveillance State. Available at:
https://static1.squarespace.com/static/6786da0226ec38320c099635/t/69a74f26da718d22c0b57a82/1772572454655/2026.2.26_STOP%2BReport_Dear%2BMamdani_FINAL.pdf (Accessed 14 June 2026).

- Swenson, C. (2026) US Congress Approves Immigration Funding Despite Abuses: Lawmakers Should Still Press for Transparency and Accountability, Human Rights Watch. Available at:
<https://www.hrw.org/news/2026/06/16/us-congress-approves-immigration-funding-despite-abuses> (Accessed 14 June 2026).
- Talla, V. (2019) Documents Reveal ICE Using Driver Location Data From Local Police for Deportations, American Civil Liberties Union. Available at:
<https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data> (Accessed 14 June 2026).
- The Glenn Beck Programme (2025) Glenn's Tough Message to the ICE Shooter's Mom | Guests: Todd Lyons & Dr. Jay Bhattacharya. Available at:
<https://pod.wave.co/podcast/the-glenn-beck-program/glenns-tough-message-to-the-ice-shooters-mom-guests-todd-lyons-dr-jay-bhattacharya-92525>
 (Accessed 20 June 2026).
- The White House (2025) Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats, Executive Order No. 14161, United States of America: Presidential Actions. Available at:
<https://www.whitehouse.gov/presidential-actions/2025/01/protecting-the-united-states-from-foreign-terrorists-and-other-national-security-and-public-safety-threats/> (Accessed 15 June 2026).
- The White House (2025) Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, Executive Order No. 14243, United States of America: Presidential Actions. Available at:
<https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/> (Accessed 12 June 2026).
- The White House (2026) Fact Sheet: President Donald J. Trump Takes Action to Enhance America's AI Leadership. Available at:
<https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/> (Accessed 20 June 2026).

The White House (2026) Fact Sheet: President Donald J. Trump Strengthens Customs Enforcement. Available at:

<https://www.whitehouse.gov/fact-sheets/2026/06/fact-sheet-president-donald-j-trump-strengthens-customs-enforcement/> (Accessed 20 June 2026).

Trujillo, M. (2025) Letter to Office of the Attorney General Request to Investigate Google's Promise to Notify Users Before Turning Over Data, Electronic Frontier Foundation. Available at:

<https://www.eff.org/document/eff-letter-re-google-notice-california> (Accessed 27 May 2026).

Trujillo, M. (2026) Open Letter to Tech Companies: Protect Your Users From Lawless DHS Subpoenas, Electronic Frontier Foundation. Available at:

<https://www.eff.org/deeplinks/2026/02/open-letter-tech-companies-protect-your-users-lawless-dhs-subpoenas> (Accessed 27 May 2026).

United Nations General Assembly (2024) Visit to the United States of America:

Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Human Rights Council. Available at: <https://docs.un.org/en/A/HRC/56/68/Add.1> (Accessed 5 June 2026).

United Nations General Assembly (2025) Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Gina Romero.

Available at: <https://docs.un.org/en/A/80/219> (Accessed 5 June 2026).

United Nations General Assembly (2026) Defending dignity and claiming rights:

human rights defenders hold firm to universal values as others desert them, Human Rights Council. Available at: <https://docs.un.org/en/A/HRC/61/40> (Accessed 5 June 2026).

United Nations Human Rights Office of the High Commissioner (2026) USA: UN experts welcome Minnesota truth-seeking entity and urge nationwide investigations. Available at:

<https://www.ohchr.org/en/press-releases/2026/03/usa-un-experts-welcome-minnesota-truth-seeking-entity-and-urge-nation-wide> (Accessed 4 June 2026).

USASpending.gov (2025) Contract Summary: Delivery Order (DO). Available at:
https://www.usaspending.gov/award/CONT_AWD_70CMSD25FR0000089_7012_47QSWA18D008F_4732 (Accessed 15 June 2026).

USASpending.gov (2025) Contract Summary: Purchase Order (PO). Available at:
https://www.usaspending.gov/award/CONT_AWD_70CMSD25P00000138_7012_-NONE_-NONE- (Accessed 15 June 2026).

Wang, N. et al. (2022) American Dragnet: Data-Driven Deportation in the 21st Century. Center on Privacy & Technology at Georgetown Law. Available at:
<https://www.law.georgetown.edu/privacy-technology-Center/research/american-dragnet-data-driven-deportation-in-the-21st-century/> (Accessed 14 June 2026).